Breakthrough

BUILDING AN EQUAL WORLD FOR WOMEN AND GIRLS

Equality Now

A just world for all women and girls

Credit: Aakansha Saxena

Experiencing technology-facilitated gender-based violence in India:

Survivor narratives and legal responses

November 2025

Contents

About the project

Following the publication of our Ending Online Sexual Exploitation and Abuse of Women and Girls: A Call for International Standards Report, Equality Now has been advocating for legal and policy changes to address technology-facilitated gender-based violence (TFGBV), with a focus on sexual exploitation and abuse. Equality Now identified three countries - India, Kenya and the US - to undertake campaigns with local women's rights organisations that would gather evidence of survivors' lived experiences and help increase the understanding of national and international policymakers on the changes required at both international and national levels to end TFGBV, with a focus on sexual exploitation and abuse. In India, Equality Now engaged several stakeholders to better understand the gaps, challenges, opportunities and priorities in addressing TFGBV. This research study was commissioned by Equality Now to Breakthrough, to gather evidence of survivors' lived experiences in India.

Acknowledgments

This report is a joint publication by Equality Now and Breakthrough. The report was made possible by the collective effort of a team of many individuals around the world. In particular, we acknowledge the contribution of Breakthrough's Project team: Manjusha Madhu (Lead, Co-author and Co-researcher), Richa Singh (Co-author and Co-researcher), Amala Dasarathi (Legal Consultant), and Barsha Chakraborty (Advisor - Gender, Tech and Policy) and from Equality Now: Amanda Manyame (Digital Law and Rights Advisor), Bryna Subherwal (Global Head of Advocacy Communications), Fareeha Ali Yahya (Global Content Officer), Julie Thekkudan (South Asia Consultant), and Tsitsi Matekaire (Global Lead - End Sexual Exploitation).

In addition, we would like to extend our gratitude to Nancy's Very Own Foundation, for providing funding to support the creation of this invaluable report.

Finally, the study team is deeply grateful to all the study participants for agreeing to participate in the study and giving us their time. We would especially like to thank all the survivors, acknowledging how difficult it is to revisit experiences of violence.

About Breakthrough

Breakthrough works on culture change by shifting social norms that limit women and girls from reaching their full potential. We work with adolescents and young people aged 11-25 years aiming for an entire generation to shift and push for change. Over time, we have worked with more than 2.3 million adolescents and young people, aged 11 to 25, to encourage aspiration, agency, leadership and negotiation through our work in schools and communities. We also support them with media tools that shape public narratives.

This has resulted in a generation of young people shifting to think and act in confident, intentional ways. Girls are negotiating to stay in school, delaying marriage, exercising choices around life goals, stepping into non traditional career paths. Boys are stepping up to contribute, support and uphold equal rights for all.

This gives hope that a more equal world is possible for future generations.

About Equality Now

Equality Now is a worldwide human rights organisation dedicated to securing the legal and systemic change needed to end discrimination against all women and girls, everywhere in the world. Since its inception in 1992, it has played a role in reforming 120 discriminatory laws globally, positively impacting the lives of hundreds of millions of women and girls, their communities and nations, both now and for generations to come.

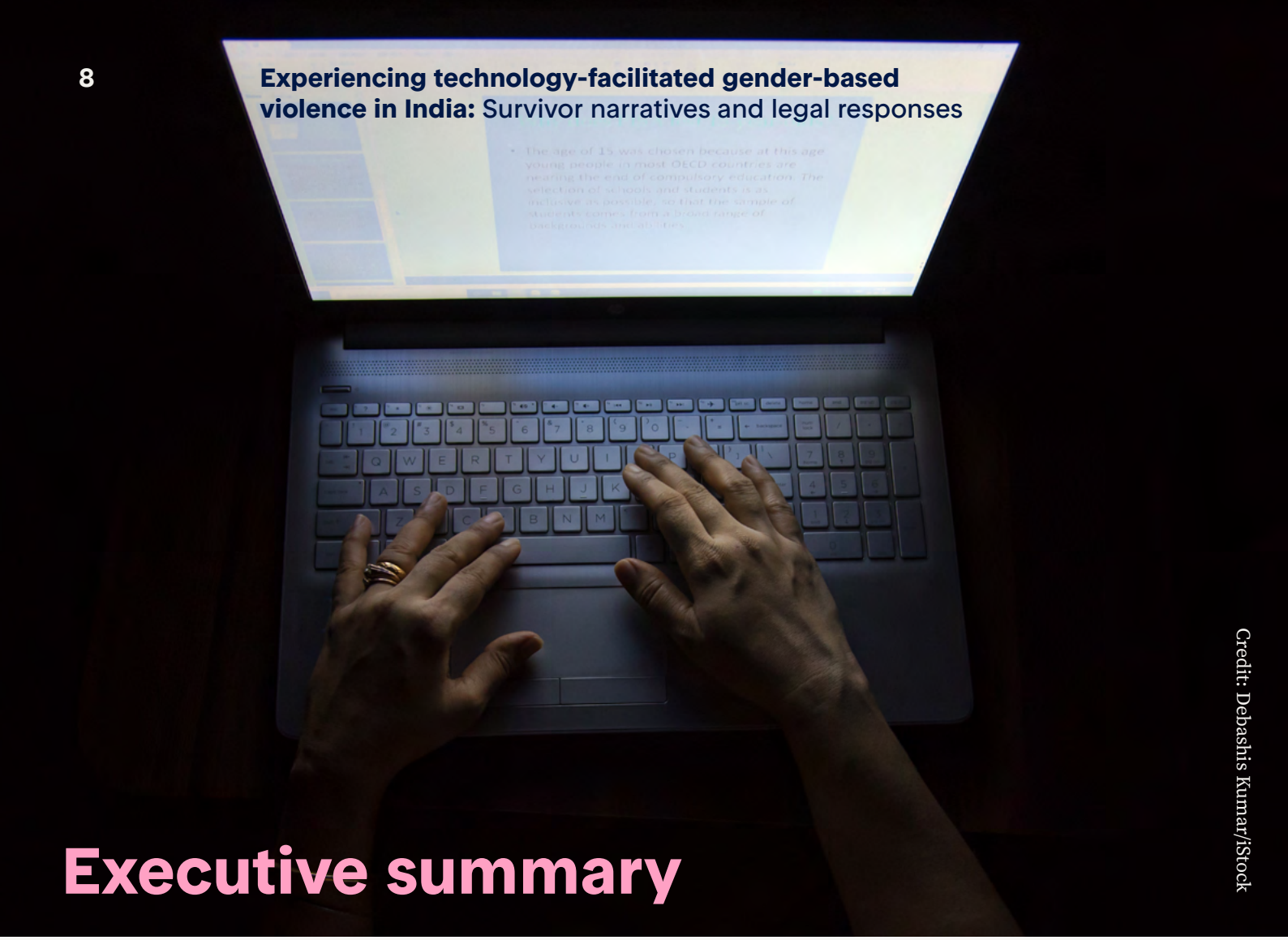
Working with partners at national, regional and global levels, Equality Now draws on deep legal expertise and a diverse range of social, political and cultural perspectives to continue to lead the way in steering, shaping and driving the change needed to achieve enduring gender equality, to the benefit of all.

Abbreviations and acronyms

AC TIGE:	Action Coalition on Technology and Innovation for Gender Equality
AI:	Artificial Intelligence
BNS:	Bhartiya Nyaya Sanhita (Erstwhile Indian Penal Code)
BNSS:	Bhartiya Nagrik Suraksha Sanhita (Erstwhile Code of Criminal Procedure, India)
CEDAW:	United Nations Convention on the Elimination of All Forms of Discrimination against Women
CIGI:	Centre for International Governance Innovation
CSAM:	Child Sexual Abuse Material
CSO:	Civil Society Organisation
DCP:	Deputy Commissioner of Police (in the Indian context)
FIR:	First Information Report (in the Indian context)
GBV:	Gender Based Violence
GEF:	Generation Equality Forum
IDIs:	In-depth Interviews
IO:	Investigating Officer (in the Indian context)
IPC:	Indian Penal Code
IP Address:	Internet Protocol Address
ISP:	Internet Service Providers
IT:	Information Technology
KIIs:	Key Informant Interviews
MRAs:	Men's Rights Activists
NCDII:	Non-Consensual Distribution of Intimate Images
NFHS:	National Family Health Survey (India)
NGO:	Non-Governmental Organisation
OBC:	Other backward Castes (in the Indian context)
OCSEA:	Online Child Sexual Exploitation and Abuse
OGBV:	Online Gender Based Violence
OSEA:	Online Sexual Exploitation and Abuse
POCSO Act:	Protection of Children from Sexual Offences Act
SC:	Scheduled Castes (in the Indian context)
SP:	Superintendent of Police (in the Indian context)
SRHR:	Sexual and Reproductive Health and Rights
ST:	Scheduled Tribes (in the Indian context)
SVRI:	Sexual Violence Research Initiative
TFGBV:	Technology-Facilitated Gender-Based Violence
TFVAW:	Technology-Facilitated Violence Against Women
UN:	United Nations
UNESCO:	United Nations Educations, Scientific and Cultural Organisation
UNFPA:	United Nations Population Fund
US:	United States
VAW:	Violence Against Women
WIPPL:	Women in Politics and Public Life

Glossary

- **Doxing:** Online sharing of private information to publicly expose and shame the person targeted (Equality Now, 2024)
- **Cyberbullying:** Constant and intentional online bullying to undermine the victim's self-esteem (UNFPA, 2022).
- **Cyberstalking:** Persistent, unwanted and/or threatening surveillance, contact and/or pursuit by technological means (UNFPA, 2022)
- **Image-based abuse:** The creation, use and distribution of imagery, including shallow fakes and deepfakes, often sexual in nature without consent. Other alternative terms used include non-consensual sharing of intimate images/non consensual distribution of intimate images (NCDII) (Equality Now & Thomson Reuters Foundation, 2021).
- **Online harassment:** Repeated conduct that threatens, pesters, scares or abuses someone by sending degrading, offensive or insulting comments or images. Online sexual harassment mainly affects women, girls and LGBTQI+ individuals (UNFPA, 2022).
- **Sexual coercion and extortion:** Often referred to as "sextortion" involves online blackmail, where money, sex/sex acts, or additional explicit images are demanded in order to prevent the publication of intimate images or private information (UNFPA, 2022).
- **Trolling:** When someone posts or comments online to deliberately upset others (Australian Government, 2024).
- **Mobbing:** Mobbing or networked harassment includes coordinated and organised attacks against particular individuals or issues, such as by groups that target feminists or people who post about racial equality issues online (Dunn, 2020).
- **Online grooming:** Grooming involves establishing a relationship with someone to manipulate, exploit, or abuse them. Typically, the process includes selecting a victim, gaining access to them, and isolating them through online means and digital technology (Equality Now & Thomson Reuters Foundation, 2021).
- **Child Sexual Abuse Material (CSAM):** Refers to visual material that depicts acts of sexual abuse and exploitation of children (Equality Now & Thomson Reuters Foundation, 2021).
- **Scheduled Castes (SC) and Scheduled Tribes (ST):** The Constitution of India recognises certain castes, races, and tribal groups as Scheduled Castes and Scheduled Tribes under Article 341 and 342. These groups have been historically disadvantaged or marginalised (National Human Rights Commission, India, 2021).
- **Other Backward Class (OBC):** In the Indian context, Backward (i.e. educationally or socially disadvantaged) refers to classes of citizens other than the Scheduled Castes and the Scheduled Tribes as may be specified by the Central Government of India in its lists (Ministry of Social Justice and Empowerment, Government of India, 2025; Singh, 2023).
- **Right to be Forgotten or Right to be Erased:** A right for individuals to request the removal of their personal data circulating on the Internet (Mali, 2022).
- **Strategic Litigation:** Processes presented to judicial and quasi-judicial bodies intended to create a lasting systemic effect beyond merely remedying the victims' suffering (Office of the United Nations High Commissioner for Human Rights et al, 2021).



Credit: Debashis Kumar/iStock

Executive summary

Access to technology, its usage, and the need to be technologically literate is indispensable to modern life. With technology and the internet becoming an integral part of our lives, the numerous digital mediums and platforms available have become spaces where gender-based violence (GBV) is actively perpetuated and amplified. Digital devices and services are increasingly being insidiously used for GBV, especially for those from vulnerable groups. While technology-facilitated gender based violence (TFGBV) is part of the continuum of GBV, aspects such as the anonymity of the perpetrator, scale of the potential audience and content consumers, the perennial nature of violations in the digital realm, and easily available access make this form of GBV distinct. A consistent pattern with TFGBV is the disproportionate targeting of women and LGBTQI+ individuals, with social locations and intersecting forms of marginalisation playing a critical role. Further, several studies have highlighted existing gaps within legal structures across many countries, which act as a significant deterrent for the system to respond promptly and effectively to support TFGBV survivors.

This study uses nine In-Depth Interviews (IDIs) with survivors and 11 Key Informant Interviews (KIIs) with experts such as lawyers, cyber police officials[1], civil society organisations (CSOs) and academics, to understand the nature and impact of TFGBV in the Indian context, and the legal framework that exists to respond to these forms of violence. Some of the lawyers interviewed had experienced TFGBV themselves, thus providing insights as both survivors and legal professionals. The research participants were based across locations such as Delhi, Patna, Hyderabad, Kochi, and Trivandrum. Locating survivors was difficult due to the ethical and legal complexities associated with reaching out to them through helplines, case workers, organisations working with survivors and lawyers. Further, the cyclical nature of this type of violence, given the permanence and reach of the internet, emerged as another key barrier in reaching out to survivors.

In this study, TFGBV is characterised as an act of violence carried out by one or more individuals and either facilitated, intensified, or exacerbated, partially or entirely, through information and communication technologies or digital media, targeting a person based on their gender and/or sexual identity or by imposing harmful gender norms. (UNFPA, 2021; NORC at the University of Chicago & International Centre for Research on Women, 2022)

Key findings

Building on this understanding, the following key findings emerged from the study:

- **Heterogeneous nature of TFGBV:** The forms of TFGBV that were most reported included doxing, online stalking and harassment, non-consensual distribution of intimate images (NCDII) and morphing of images. These manifestations of TFGBV were geography agnostic, that is, the geographical location of the violence did not necessarily affect the nature of the incident, duration, impact, or the life cycle of the case. Findings from the study also highlight how women are systematically targeted owing to vulnerabilities such as financial distress and a lack of or limited family and social support.

- **Social norms and impact including curtailment of rights:** The ability to speak up, name and address digital violations was deeply entrenched in social norms around gender and sexuality, especially for young women and LGBTQI+ individuals. Young women feared victim blaming and curtailment of their freedoms induced by societal constraints, especially from parents and the police. For LGBTQI+ people, there was an additional and constant fear of having their identity involuntarily exposed. Nearly all survivors reported self-imposed withdrawal from the digital space due to the violence they experienced.

  Saliently, and similar to GBV cases in the physical world, orchestrated attacks on a woman's character are often central to TFGBV cases. Sharing photos on pornographic sites and other chat platforms, and circulating images with the "promise of sex" or "availability of sex" emerged as distinct patterns under the larger umbrella of image-based sexual abuse.

- **Systemic social exclusions and TFGBV:** While the form of TFGBV did not seem to be determined by the survivor's identity, in cases where survivors belonged to marginalised communities such as Scheduled Castes (SC) or Scheduled Tribes (ST), the violence they faced was rooted at the intersection of their gender identity with their caste or tribal identity. The findings also highlight the role of the survivor's social, financial and cultural privilege in responding to TFGBV, whether in terms of survivors' capacity to explore alternative redressal mechanisms outside of the legal system or whether to engage with the Indian legal system.

- **Legal frameworks:** Findings from lawyers emphasised the need to use clauses from the Information Technology (IT) Act in conjunction with laws such as the Scheduled Caste/Scheduled Tribes (SC/ST) Atrocities Act and relevant sections from the Bharatiya Nyaya Sanhita (BNS) to strengthen cases. Further, the quashing of Section 66A of the IT Act has left a critical gap in the legal landscape. While the rationale for striking down this section on grounds of upholding free speech is well established, there is a need to work towards filling this gap to address the certain specific ways TFGBV is perpetrated.

- **Intermediary accountability:** Obtaining information from technology platforms and companies regarding TFGBV cases emerged as a challenge cited by cyber police, caseworkers, and activists.

- **Federal variations in legal response:** The interviewed lawyers revealed that those practicing in Kerala often represent their clients in court and at police stations more frequently than lawyers in other states. While it is possible that the study's participants happened to be those who had more substantial engagement with the system, there is a need to examine these regional variations and the factors influencing these disparities.

- **Ideas of justice among survivors:** For most survivors, ideas of justice revolved around punitive and speedy action to stop the violations. Recognising the nature of the internet, it is crucial that the removal of the offending material is prioritised and achieved while investigating the criminal offences. Many survivors shared other avenues for requesting removal of content such as mass reporting on the concerned platform, using helplines run by technology companies or requesting CSOs to remove violent content from the internet and platforms.

  Another strongly emerging concern was the legal system's failure to adopt survivor-centred response. Systemic redressals remain narrowly focused on the 'crime' and its punishment and paid little attention to supporting survivors to deal with their trauma and long-term recovery.

- **Barriers to justice:** Hesitation in filing and pursuing formal police complaints was a common thread across interviews with survivors and experts. The substantial time taken by the legal system, systemic apathy, ignorance, and lack of resources emerged as key factors hindering survivors from approaching the Indian legal system.
- **Social norms and systemic apathy:** Social norms are also deeply entrenched within the legal system, particularly within law enforcement authorities in India. The study findings highlight that this manifests in how they define violence, their limited understanding of how abuse impacts the survivor, and a culture of victim blaming.
- **Nonsystemic engagement:** While survivors reported approaching lawyers for legal advice, very few cases translated into further legal action. Lawyers interviewed in Delhi spoke about using creative, informal pressure-building strategies that do not have legal standing, such as sending "legal notices" or getting a police officer to call the perpetrator, to pressure them to stop the violence.

Recommendations

Based on these findings, the study recommends the following under larger overlapping categories of legislation and policy changes, building awareness and support, and strengthening research and the evidence base:

- The Indian legal system must go beyond a punitive framework and **centre restorative forms of justice and healing**. **Strengthening provisions such as the right to be forgotten/right to erasure** can go a long way in facilitating a survivor's healing process and pursuit of justice.
- A carefully **developed ethical code for online media should** help prevent online violations while recognising the importance of free expression in a democracy.
- There is a need to work towards **increasing intermediary and tech accountability and responsiveness** to address TFGBV effectively.
- **Breaking and disrupting the gradation of cybercrimes, which prioritises financial forms of cybercrimes over TFGBV,** ingrained in the legal system is critical.
- There is a **need to increase stakeholders' awareness about provisions like the national cybercrime reporting portal and the cybercrime helpline** and how cases can be reported and tracked through these platforms.
- Considering the dynamic nature of technology, lawyers, judges, and cyber police, **regular capacity building is needed to respond** effectively to TFGBV cases. **Repeated training on what comprises electronic evidence** is also critical. Along with this, **budgetary provisions and infrastructure for cyber stations need to be increased**. The **study also revealed the need for more digital forensic labs**.
- At the implementation level, **strategic litigation can be used as a feminist tool to generate pathways to justice** in India. Across several countries, strategic litigation has helped in bringing a gender lens to aspects of the litigation process, which has resulted in better judgments.
- Research needs to be strengthened to **document the prevalence of TFGBV, recognising that technology has made inroads into all forms of GBV**. A **repository of TFGBV cases where local and cultural contexts have been critical, especially around language**, can enable the system to handle TFGBV cases better.

Credit: lakshmiprasad S/iStock

Introduction: context and rationale

Purpose and scope of the report

The discourse around GBV increasingly recognises the significant role technology and online spaces are playing in amplifying and perpetuating such abuse. The University of Melbourne & UNFPA (2023, p.4)[2] noted that TFGBV could be "experienced in a range of contexts, including dating and intimate partner relationships," with many young women disproportionately affected. According to Amnesty International (2018), social locations and intersectional marginalities are critical in how and why people are targeted online. The anonymity of offenders, coupled with the prevalence and ongoing nature of this violence and harm, complicates efforts to trace and prove the violations in court.

The increasing prevalence of TFGBV has motivated governments the world over, CSOs, feminists and activists, advocacy groups, and UN agencies to identify effective mechanisms to address these violations, to ensure people's rights not just in the offline space but also in the online universe. While evidence is mounting both in India and globally on online and digital violence, there is still significant work that needs to be done.

Global and scant literature in South Asia highlights that a significant number of girls, women, and marginalised communities experience TFGBV, especially doxing, cyberbullying, cyberstalking, non-consensual intimate image sharing and distribution, amongst other forms, even if they are not active online or have limited access to the digital space. Media reports and grey literature allude to how those belonging to systemically marginalised communities or those from certain professional backgrounds especially those in the public space, such as journalism, public representation, and activism, tend to experience TFGBV in acute ways. Several studies highlight that women in politics and public life (WIPPL) are especially targeted by TFGBV because of their high visibility and public-facing role (Transform, 2023[3]; UNFPA, 2021[4]). According to UNESCO (2020)[5], globally, 73% of women journalists reported experiencing online violence in the course of their work. Further, 20% of women journalists said they had been attacked or abused offline in connection with the online violence they experienced.

A study by the Inter-Parliamentary Union (2016) based on data from 55 women parliamentarians across 39 countries from different regions of the world, reported that 41.8% of them had seen images or comments with sexual, defamatory, or humiliating connotations of themselves being circulated through social media. A Plan International (2023)[6] report based on research with over 14,000 girls and young women across 31 countries also found that young women and girls who speak out online about political causes, feminism, racism, or sexual and reproductive health and rights (SRHR) face backlash.

The digital universe in India is fast expanding, with all pivotal policies, from education to governance models, aggressively pushing for increased internet uptake. In today's society, digital literacy, accessibility and usage are indispensable, and there is a need to foreground greater uptake while ensuring digital spaces remain safe, especially for women, girls, and those from marginalised communities.

In India, like other parts of the Global South, the digital gender divide has been a major hindrance to the digital rights of women and individuals from communities who have been historically and socially marginalised. As Iyer, Nyamwire, and Nabulega (2020, p.3) argued, there is a critical need for "a radical shift in developing alternate digital networks grounded in feminist theory." Lack of or limited access to technology and the internet hinders people from accessing their rights and entitlements. Yet, India's National Family Health Survey 5 2019 - 2021 (NFHS-5), reports that only one in three women (33%) have ever used the internet, compared to more than half (57%) of men. Rural India presents a more adverse scenario, with men twice as likely as women to have used the internet - 49% versus 25% (Ministry of Health and Family Welfare, Government of India, 2019-2021). However, numerous studies indicate the likelihood of a massive boom in the telecommunications market, with an overwhelming number of women driving the internet surge (Nielsen, 2022).

Literature alludes to how the digital realm reflects the divides and inequalities in the physical world and often replicates and exacerbates them. The online universe is deepening pre-existing structural social divides and inequity, particularly along the lines of gender, class, caste, location, religion, and disability, further entrenching discrimination and marginalisation. A smattering of empirical studies document the manifestations and nature of TFGBV in India. Udwaida and Grewal (2019) highlight that women in West Bengal reported harassment by "wrong numbers," where they receive relentless phone calls from unknown men. Similarly, an IT for Change study exploring TFGBV experiences in the southern part of India notes that nearly 82% of women surveyed in colleges (total sample size of 881) had faced online sexual harassment, including image-based sexual abuse. The study also reiterated how intersectionalities and other identity factors affected how women were being targeted. For example, nearly 22% of women who had faced sexual harassment also saw perpetrators comment on their skin colour (Gurumurthy, Vasudevan & Chami, 2019). There is a vital need for greater empirical work to map patterns of interlinkages between offline and online violence more robustly, to establish methodical correlations.

In a vital exercise aimed to map research priority areas for TFGBV, Sexual Violence Research Initiative (SVRI) in collaboration with the Association for Progressive Communications, UN Women, and the Global Partnership to end Online Abuse and Harassment have identified "a set of research priority recommendations for addressing the global problem of TFGBV through a transparent, methodologically sound, comprehensive, and inclusive process." The project considered the five domains which are - 1. Nature, Prevalence, and Impact; 2. Responses, 3. TFGBV Prevention, 4. Populations and 5. Measures and Methodologies. It focused on the first two, i.e. Nature, Prevalence and Impact and Responses whilst touching on the remaining three. The shared research agenda, as the creators explain, "serves as a guide for stakeholders in the field to advocate for more and better resources to address knowledge gaps and build better programmes to respond to and prevent TFGBV (SVRI, 2024, p. 1)."

The present study aspires to add to the scant critical research examining the experiences of TFGBV amongst women and LGBTQI+ people in India. It includes a focus on understanding how the legal landscape underpins the TFGBV discourse in India today and the factors, particularly social norms, impeding survivors from accessing legal remedies. The study also examines the judicial system's response to specific cases of TFGBV, including the success of legal proceedings, the complainants' perceived sense of justice, the structure and procedures of the court process, and the various challenges encountered. These include evidentiary difficulties, procedural delays, lack of victim support, and the inadequacy of legal provisions.

Conceptual framework

1. Types and forms of gender based violence

Over the last decade, several terms such as online gender-based violence (OGBV), technology-facilitated violence against women (TFVAW), TFGBV, online sexual exploitation and abuse (OSEA), digital violence, and cybercrime have been used to describe a fast-growing and increasingly mutating problem.

In 2017, the United Nations Committee on the Elimination of Discrimination against Women (CEDAW)[7] recommended state parties to address "contemporary forms of violence occurring online and in other digital environments" in its General Recommendation No. 35.[8] In 2022, UN Women along with the World Health Organization convened an expert group in New York, US as a part of their joint programme on violence against women (VAW) data. One of the main agendas of this meeting was to develop a comprehensive definition of TFGBV/TFVAW. The group recognised that the existing conceptual definitions of TFGBV/TFVAW include key elements such as violence against women or GBV, the gendered motivations and dimensions, the naming of technologies generally or specifically through which the violence was perpetrated, the medium or space where it happens, the forms and harms of TFGBV, and the continuum of GBV (UN Women & World Health Organization, 2023).

The report of this meeting states that, "Variations in the proposed focus and scope of these different elements that constitute the proposed definitions, are reflected in the naming of the act that deeply differs from one definition to another, such as online or digital VAW, online GBV, cyber violence against women and girls, technology-facilitated GBV, digital dimension of VAW, among others (UN Women & World Health Organization, 2023, p. 4)."

A study by NORC at the University of Chicago and the International Center for Research on Women (2022, p.1) which assesses TFGBV in India states that, "...technology-facilitated GBV is gaining increased attention within research and advocacy spaces. Academics, practitioners, and researchers in the country mostly refer to this form of GBV as online gender-based violence, cyber violence, online harassment, or cybercrime."

The COVID-19 pandemic also played a role in drawing increased focus on TFGBV. The Generation Equality Forum (GEF), convened by UN Women, kickstarted a Global Acceleration Plan to speed up progress towards achieving gender equality by bringing together multiple stakeholders who will drive shifts through Action Coalitions. The Action Coalition on Technology and Innovation for Gender Equality (AC TIGE) identified TFGBV as one of its four priority action areas (UN Women & World Health Organization, 2023).

Further, studies such as The Left Out Project Report centre transgender, non-binary and gender-diverse people's experiences of OGBV to challenge and conceptualise current framings of this type of abuse. They highlight the need to move beyond the oversimplification of OGBV as meaning violence against women (specifically cisgender women) and to instead define OGBV as violence that is experienced as a direct result of one's gender identity and gender expression (Nyx McLean & Thurlo Cicero, 2023).

For the purpose of this study, we understand TFGBV as an act of violence perpetrated by one or more individuals that is committed, assisted, aggravated and amplified in part or fully by the use of information and communication technologies or digital media, against a person based on their gender and/or sexual identity or by enforcing harmful gender norms. This definition is a mix of TFGBV definitions developed by UNFPA, and NORC at the University of Chicago, and the International Center for Research on Women (UNFPA, 2021; NORC at the University of Chicago & International Center for Research on Women, 2022).

The inaugural paper from the Centre for International Governance Innovation (CIGI) on a safer internet, elaborates on the specificity of TFGBV. "As a novel manifestation of gender based violence, there are some factors that make TFGBV particularly unique, including the possibility for cross-jurisdictional abuse, the ability for abusers to remain anonymous, the constant access to the survivor through connected devices, the perpetual nature of digital content, the ease with which content can be copied, the breadth of audiences witnessing the abuse and the opportunities for abusers to join forces on digital platforms to organise attacks (Dunn, 2020, p. 4)."

The 2022 study by NORC at the University of Chicago and the International Center for Research on Women outlines the prevalence of TFGBV in India. It identifies harassing phone calls from unknown numbers, non-consensual sharing of intimate images, online sexual harassment, and abusive comments and threats from 'troll armies' or 'cyber troops' as the most prevalent forms of TFGBV in the country. This perspective aligns with insights gathered from discussions with a civil society organisation that offers workshops and operates a helpline addressing TFGBV in India, along with an academic specialising in men's rights activists (MRAs).

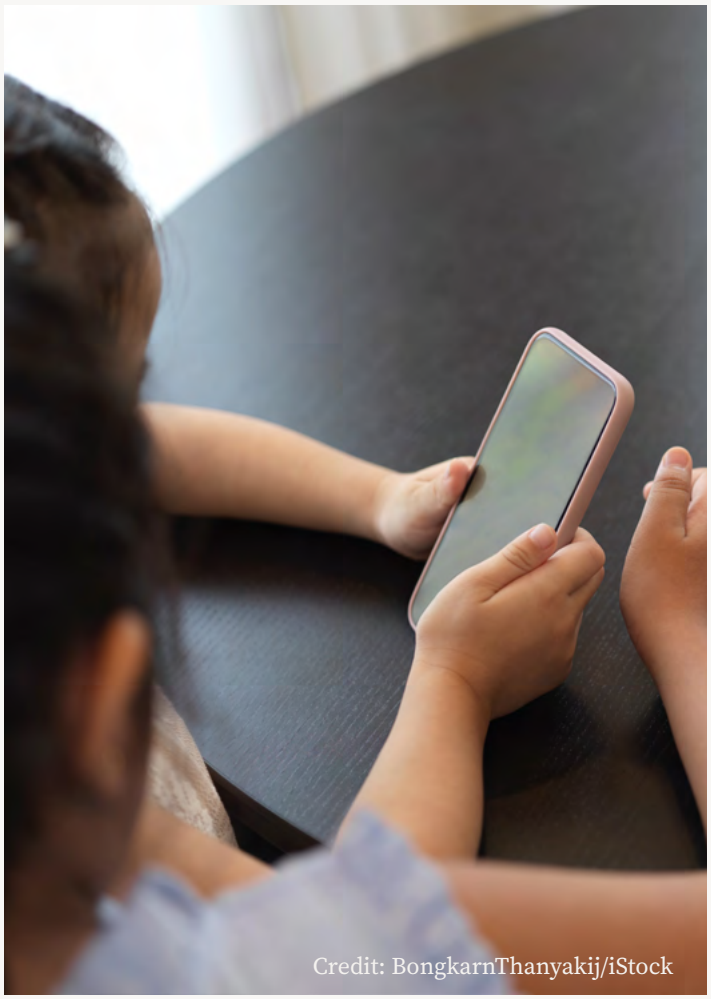
"... in 2015 or earlier years, ... we were seeing a lot more harassing phone calls and SMS and WhatsApp messages... abusive WhatsApp messages and things like that. I think it has evolved now. One of the most common violations [that people call about is impersonation, combined with morphing of images and] intimate image sharing. It's not even about their own image anymore, it's about morphed images."
~ Representative from a civil society organisation that conducts workshops and runs a helpline to address TFGBV in India.

"There was this incident and there have been a couple of more incidents, even recently, where women complained about harassment that happened to them. There have been a lot of people actually coming and talking on social media supporting these men. Most of them align somewhat to the right wing probably. The silencing that happens to women who speak up against abuses seems to have increased recently."
~ Academic who has worked extensively on MRAs in India

The UN Report of the Special Rapporteur on Violence Against Women, its causes and consequences on online violence against women and girls from a human rights perspective (2018) lists the various forms of TFGBV. These include threats, inciting GBV, harassing digital communication, dissemination of harmful lies, impersonation, trafficking of women, disclosing private information (or threatening to do so), doxing, sextortion, trolling, unauthorised access to information or devices, manipulated images, mobbing (or networked harassment) and stalking. The CIGI safer internet paper on TFGBV points out that each of these forms of TFGBV has its own unique markers, but many of these overlap with each other (Dunn, 2020). For example, "harassment encompassed a variety of unwanted digital communication (Duggan, 2017; Digital Rights Foundation, 2018). It can involve a brief incident, such as a single targeted racist or sexist comment (Lenhart et. al., 2016) or a long term organised attack, such as the Gamergate campaign[9]."

This study was carried out as a part of a larger study by Equality Now which focuses on online sexual exploitation and abuse, as a particular type of TFGBV. Online sexual exploitation and abuse (OSEA) encompasses a number of sexually exploitative and harmful behaviours that occur or are facilitated online and through the use of digital technologies. OSEA includes online grooming, live-streaming of sexual abuse, child sexual abuse material (CSAM), online sexual coercion and extortion, technology-enabled sex trafficking, and image-based sexual abuse[10]. (Equality Now & Thomson Reuters Foundation, 2021).

Considering the connections between these categories (TFGBV, TFVAW, OGBV, OSEA etc.) and the anticipated challenges in identifying survivors (explained in detail in the methodology section), this study uses the term TFGBV to maintain a broader scope. However, we were intentional about identifying cases of OSEA (image-based sexual abuse, live streaming of sexual exploitation and abuse, and sexual coercion and extortion) to align with the larger study. The study maintains flexibility with regard to the terminology used to refer to the violence, abuse, and exploitation while also mapping the various terms used by stakeholders.


Credit: BongkarnThanyakij/iStock

2. Demographics most affected by TFGBV and the perpetrators

Several studies have shown that women and LGBTQI+ people face higher levels of online harassment and abuse (NORC at the University of Chicago & International Center for Research on Women, 2022; Dunn, 2020). This is further exacerbated due to their other intersecting identities, such as caste, class, religion, and disability, indicating the offline-online continuum as discussed earlier. The online harassment and abuse of women who speak up on various issues, such as journalists, human rights defenders, and politicians, is also well-documented. A report by the International Center for Journalists highlights the abuse that an Indian journalist, Rana Ayyub, has received online, noting that it is representative of the broader abuse against female journalists in the country (Fathima, 2023). Studies state that women who are in abusive relationships also face TFGBV from their intimate partners (Dunn, 2020).

Another group that is disproportionately affected by TFGBV is children and young people. A study by Q3 Strategy (2024) emphasises that children and young people are disproportionately at risk from online child sexual exploitation and abuse (OCSEA) and cyberbullying due to an expanding, yet inadequately regulated and safeguarded, digital presence. The report by Plan International (2023) found that across all 22 survey countries, 64 % of girls and young women can be classified as having a high level of social media usage, 23 % having a medium level and 13% a low level. Further, across all the survey countries, 58 % of girls reported that they have personally experienced some form of online harassment on social media platforms.

Evidence suggests that perpetrators can be individuals as well as groups. They can be anonymous, spread across geographies, operating with fake identities, or strangers as well as people known by their victims.

3. Access to technology and the internet: the rural-urban divide

According to the Internet in India report by Kantar and Internet and Mobile Association of India, 45% of the Indian population does not access the internet. However, out of those that do, rural India has more internet users than urban India. Further, 82% of people are accessing the internet using someone else's mobile phone. Of this 82%, 63% of people are from rural locations, 77% are female and 43% are over the age of 35 years. Also, there is considerable state-wise disparity in terms of reach and access (Kantar & IAMAI, 2023). More than 85% of women in Goa, Sikkim, and Kerala have mobile access compared to less than 50% of women in Jharkhand, Andhra Pradesh, Gujarat, Uttar Pradesh, Chhattisgarh, and Madhya Pradesh (Ministry of Health and Family Welfare, Government of India, 2019-2021).

These statistics point towards a rapidly changing and layered landscape in terms of access to technology and the internet. The role of access, ownership, and the rural-urban divide are all aspects that need to be examined further as we study the issue of TFGBV.

Credit: Aakansha Saxena

4. Current legal landscape and support mechanisms

According to the Annual Web Index published by World Wide Web Foundation in 2014-15, out of 86 countries surveyed, 74% of legal systems were not responding appropriately to TFGBV (Dunn, 2020). Further, a study conducted by Women's Rights Online in 2016, of which India was a part, also highlighted the gaps in police and judicial systems in responding effectively to TFGBV (Dunn, 2020). Accounts by people who have experienced TFGBV in India across spaces have also highlighted victim blaming, online violence not being taken seriously by authorities, and overall apathy from the legal system. Further, aspects like cross-jurisdictional abuse, the complexities associated with evidence in such cases, and questions of accountability (especially with regard to digital platforms and service providers[11]) make legal remedies for TFGBV a challenging terrain (Dunn, 2020).

In India, the Indian Penal Code (now changed to Bharatiya Nyaya Sanhita), the Information Technology (IT) Act, and the Protection of Children from Sexual Offences (POCSO) Act have penal provisions that can be applied to TFGBV. However, there are gaps such as certain forms of violence being addressed for children but not adults and several forms of TFGBV (especially with its ever-evolving nature) not being addressed by these laws (Equality Now & Thomson Reuters Foundation, 2021).

A 2023 study by IT for Change on the judiciary's response to OGBV in India, reiterates these challenges through an analysis of cases in Indian courts. The study highlights that forms of violence like gendered hate speech, gender trolling, and doxing are not recognised under Indian law. This results in these cases being filed as defamation (civil and criminal) or criminal intimidation which do not adequately address the injustice survivors/victims have faced (Rajkumar, 2023).

Another glaring example of the lack of understanding of TFGBV by the legal and judicial system that this study highlights is concerning bail conditions. The findings were that there was a lack of consideration in bail conditions for the risks that the technological nature of the abuse and violence posed. While there are some conditions to deal with 'offline' actions, the lens to address online actions was lacking. The study argues that some general bail conditions such as "avoiding all contact with an alleged victim/survivor of the crime", could be interpreted to include contact online. However, bail conditions directly related to the use of online tools, with specific emphasis on online activities, must be incorporated (Rajkumar, 2023).

Interestingly, the present research noted how a miniscule number of cases actually made it to the police or the courts, owing to diverse reasons which are elaborated later in the report. As Rachna*, one of the Delhi based criminal lawyers we spoke with for the study, observed, laws addressing technology-facilitated and online violence have not been tested enough due to cases not reaching courts. This makes it difficult to assess and understand the extent to which the laws effectively apply in different cases, thereby rendering the laws a complicated and challenge area for discussion and intepretation. The factors that prevent cases from reaching courts need to be studied more. The researchers were informed that survivors may be reluctant to talk about their experiences of TFGBV.

Methodology

The study employed qualitative methods through In-Depth Interviews (IDIs) and Key Informant Interviews (KIIs) to explore the nature, manifestations, and impact of TFGBV, with a focus on OSEA. It also explored the legal remedies that survivors accessed and the impediments that they faced in doing so. Acknowledging that the manifestations of TFGBV are constantly evolving and emerging, a qualitative study enabled the documentation and study these forms of violence more descriptively, centring survivor experiences and their understanding of TFGBV (UN Women and World Health Organization, 2023).

Eight IDIs with survivors based in locations such as Delhi, Patna, Hyderabad, Kochi and Trivandrum, were conducted. Further, 11 KIIs were also conducted. Out of these, seven KIIs were with lawyers primarily working in Delhi and Kerala. For more information on the interview format and questions, please see Annexure 4.

One of them had experience of working across several states in India. The researchers spoke to a group of three cyber police officers[12] in Kerala (counting this as one KII). Lastly, the researchers spoke to a representative from a CSO (working to address TFGBV), a professor (working on men's rights activism particularly in the digital realm) and a person working at the intersection of gender, policy and technology. Apart from these, an adolescent survivor who has experienced TFGBV was also interviewed. The case had already been reported to the police. While this interaction was an exception to the research participant criteria, the interview was ursued it with the required consent in order to better understand adolescents' experiences of these forms of violence and how they accessed legal recourse.

Apart from that interaction, all survivors were adult (18+) survivors. This was because speaking to participants under 18 about violence in India is a complex terrain that raises ethical and legal issues such as mandatory reporting under the Protection of Children from Sexual Offences Act (POCSO). Speaking to children would have required significant preparation, which would have been challenging considering the short duration of the study.

At the conceptualisation stage, for the purpose of the study and to inculcate a pan-India lens, the research employed internet penetration data to assess the high ranking and lowest-ranking states in India. Based on government data from the Telecom Regulatory Authority of India, the National Family Health Surveys, and material from credible private entities, four states were selected for this study; Delhi and Kerala as they consistently rank amongst the top Indian states in terms of internet penetration and women users, along with Uttar Pradesh and Odisha which rank amongst the lowest. However, the researchers were not able to strictly adhere to this plan due to several challenges during the course of the study:

- **Difficulty in reaching survivors:** Multiple channels for reaching survivors of TFGBV were assessed. These include social media calls, conversations with organisations and lawyers working with survivors, and through Breakthrough's programme teams present across select North Indian states. However, this was a challenging process. Organisations and lawyers cited ethical challenges in reaching survivors including those from marginalised backgrounds. The researchers were informed that survivors may be reluctant to talk about their experiences of TFGBV.

Credit: Aakansha Saxena

- **The nature of TFGBV:** The fear that TFGBV does not completely end, due to being online, was palpable amongst the survivors and experts interviewed. Survivors fear (and rightly so) that even if digital material was deleted, there is always a possibility that they might re-emerge somewhere else in the future. For example, a conversation with a Delhi lawyer detailed an instance where a client's photo which had been previously deleted on a platform following complaints, recently reappeared on another platform. A survivor in Kerala explained that videos of her being "slut-shamed" and "violently trolled", often with sexually explicit language, are repeatedly reposted despite ongoing legal proceedings.

- As a mitigation strategy, the researchers expanded the stakeholder conversations to include more lawyers and cyber cell experts[13] to accommodate as many voices as possible. For more information on the cyber cell framework in India, please see Annexure 2. The study's regional focus to pursue leads as and where they materialised was also expanded.

- The initial plan was to undertake data collection in Delhi, Uttar Pradesh, Jharkhand and Kerala. However, owing to the dearth of promising leads for survivors or domain experts in Jharkhand, the study moved its efforts to West Bengal. The state has a similar reach in terms of internet penetration. However, due to external factors such as massive protests in the state of West Bengal around a sexual violence case, the data collection had to be postponed and eventually cancelled due to timeline restrictions.

Importantly, over the course of the study, our understanding of the relationship between geography and forms of TFGBV evolved. Insights from the participant interviews revealed that the nature and forms of TFGBV tend to be geographically agnostic. The physical location of the survivor often does not necessarily influence the trajectory of the violence or its manifestation. However, with regard to the interface of TFGBV and the legal system, we observed pronounced regional variations. Conversations and interviews in Kerala were particularly productive because more cases seem to be making it to the police and courts.

Ethical considerations

Protecting the rights, integrity, and wellbeing of all the research participants was a primary focus in designing, developing, implementing and reporting this study.

- The research tools were designed to ensure protection for participants from any physical and mental harm, including embarrassment, humiliation, and damage to self-esteem.

- A two-member research team interviewed survivors in-person. All conversations were in-person unless the participant was more comfortable with a virtual medium.

- The two research team members could understand and speak English, Hindi and Malayalam, which was sufficient for the geographies covered in the study.

- Voluntary participation was emphasised and adhered to for all the study respondents, including the right to withdraw at any stage.

- The participants gave informed consent, including permission to record and publish results. As part of the consent process, all information regarding the duration, procedures, confidentiality issues, potential risks, and benefits of the study to the individual/society/community was shared.

- Confidentiality of identities was maintained, including anonymity in publication, to prevent the tracing of participants.

- Post-study obligations were followed through clear processes to end the research relationship with participants. The research study findings were shared back in a way that participants could easily understand.

- The research team was equipped with support information (helplines, list of relief organisations etc.) that could be shared with participants in case support was needed as Breakthrough was not equipped to directly help.

- Interview transcripts are stored on a secure, password-protected platform accessible only to the research team. We will store the data for two years[14], after which it will be safely deleted.

Key findings

Credit: show999/iStock

This section highlights the significant findings from the study. These subheadings do not denote water tight categories but serve as a road map to highlight principal takeaways.

To ensure the research findings resonated with a larger audience, both in the global south and north, the findings are organised under two main domains to facilitate cross-learnings and collaborations. These are among the 5 domains from the global TFGBV shared research agenda (SVRI, 2024):

- **Domain 1: Nature, Prevalence, and Impact**
- **Domain 2: Responses**

Domain 1: nature, prevalence and impact

1.1 Heterogeneous nature of TFGBV

The survivors interviewed for this study span a wide demographic from adolescent Dalit girls in Delhi to middle-aged professionals in Kerala, tribal young mothers, LGBTQI+ students, and high-profile journalists. This diversity underscores that TFGBV affects individuals across age, gender, caste, class, and sexuality. The age range of survivors included adolescents (as young as 13–17) and women in their 30s and 40s.

Forms of violence experienced by the participants interviewed include online stalking, doxing, morphing, impersonation via fake accounts, non-consensual sharing of intimate images, cyberbullying, organised online attacks, and even financial fraud. For some, this violence originated from strangers online, while others faced harm from known individuals such as friends, colleagues, family members, political actors, or members of their immediate communities. The platforms used to perpetrate these acts were equally varied: social media (e.g., Facebook, Instagram), gaming platforms like PUBG, and messaging apps.

The legal outcomes reveal a fragmented and often inadequate response. While a few survivors, particularly those with legal, media, or activist support, were able to file formal complaints (with some cases still pending), others opted not to pursue legal redress due to the emotional toll, financial cost, and inefficacy of the justice system. One survivor, belonging to a scheduled tribe and LGBTQI+ community, who is a student in Kerala, chose not to pursue justice due to fear of stigmatisation, time constraints, and lack of resources. Another, a well-known journalist, managed to seek legal support only through the backing of her employer, a luxury not available to most of the survivors engaged in this study.

Importantly, the psychosocial impact is profound. Survivors speak of mental fatigue, public shaming, career disruption, and the sense that justice systems are not designed to protect them. Many disengaged from online spaces entirely, citing safety concerns. Others, particularly women from marginalised communities, noted the near impossibility of navigating the digital world without facing systemic abuse.

A complex, intersectional picture of TFGBV emerges, where experiences do not neatly fit into legal definitions or institutional categories. The experiences shared by the study's participants make clear that addressing TFGBV requires a nuanced, survivor-centered approach that recognises overlapping identities, varied digital contexts, and the structural inequalities that shape both harm and access to justice.

> *"It's difficult to talk about these cases in one breath or in one way because each is very different. In some we file a police complaint, some we've just written to Twitter, Facebook, and YouTube asking them to take [the content] down. Some you have to go to court to get an injunction, and then nothing else happens. And you don't want anything else to happen. Or in others you file a criminal complaint and you pursue that. Also there are other kinds of cases where people, where women are just facing it, it may not be necessarily sexual but certain kinds of language, certain kind of attention online. Even if you put a face of a woman saying she's a communist, there's nothing wrong with that, but that brings her into a certain limelight online. It's very contextual where it incites hatred against her, or it makes her subject to other kinds of violence online."*
>
> **~ Rachna*, Delhi based lawyer (works on human rights and gender with a focus on criminal law)**

Summary table of documented survivor experiences

Type of Interview	Personal Profile	Mode of Interview	Nature of Violence	Nature of Perpetrator	Legal Action/Recourse
IDI 1	34-year-old engineer, young mother, based in Patna, middle class	Online Interview Survivor did not want to meet in person	Online Impersonation/ fake account, "slut shaming", Receiving Vulgar Messages	Seems to be from known circle	Yes, via an activist friend who works on TFGBV issues who had contacts with the cyber police
IDI 2	38 year old female doctor	In person, Delhi	Virtual Stalking, Harassment	Two people in her community of friends and contacts	Yes, through a colleague who had personal connect with senior police officials
IDI 3	Female, adolescent, scheduled caste	In person, Delhi	Doxing, Morphing, Virtual Stalking, Offences against a Child	Family and friends	Case filed and ongoing
IDI 4	Female in her 20s, Hyderabad based	Online	Receiving Vulgar and Abusive Messages on Gaming Platform (PUBG)	Unknown	Reported on the gaming site Ban of PUBG made formal complaints with the police etc, complicated
IDI 5	Male, Studying for master's degree, Kerala based, belonging to a Scheduled Tribe and LGBTQI+ community	Online	Organised cyberbullying, Anonymous Calls/ Threats,Morphing, Doxing Possibly targeted owing to participation in Kerala's Pride March	Unknown, got calls from numbers based in foreign countries	*"I could not pursue or follow through with a legal case. I was in my third year of graduation. I didn't have the time or money...I didn't want to waste my time for people who were out to waste my time"*
IDI 6	Female, prominent journalist, married, Kerala based	In person	Organised cyberattacks on Facebook multiple times, Doxing, Morphing	Unknown, political party members, some based abroad	Yes, cases pending *"I have a support system. My legal battles are being handled by the company. That is a big thing otherwise this would not have been possible for me. Ordinary people won't be able to do it, the number of times you need to go to a police station. A lot of my friends and colleagues would follow up for me and that's how I have been able to sustain this. For lone people, particularly for women, this would have been nearly impossible. You become mentally tired, frustrated."*

Type of Interview	Personal Profile	Mode of Interview	Nature of Violence	Nature of Perpetrator	Legal Action/Recourse
IDI 7	Female, 30 yrs, Kerala based, actor, OBC	In -person	Organised cyberattack on Facebook multiple times, Doxing, Morphing	Known and unknown, school friend, All Kerala Men's Association	Yes, cases pending *"No action is being taken. All you can do is block...When people ask 'Why didn't you make a complaint? What is the point?' Imagine what it must be like for people who don't know anything about all this, what is the protection for people who don't know what cyber attack is? I don't use Facebook anymore. I have experienced every kind of abuse. I got no justice"*
IDI 8	Young mother, belonging to a Scheduled Tribe, Kerala based	In-person	Organised Cyber attack, Doxing, Morphing	Known and unknown, Youtube personalities	Yes, ongoing
IDI 9	Middle aged woman, college counsellor, Kochi based	Telephonic (Did not want to meet in-person)	Morphing, False Accounts/ Impersonation	Unknown	Meetings with cyber police, no formal complaint, Important verdict around Facebook sharing information with Kerala police
KII 1	Delhi based young lawyer, Female	In-person	Online stalking, Image-Abuse Sexual Abuse	N/A	
KII 2	Delhi, Male, young lawyer	In-person	Online stalking, impersonation	N/A	Talked about how he resorts to calling the police or sending the perpetrator notices so as to instill fear in them. He did not think pursuing the formal legal route was effective
KII 3	Young Female lawyer, Delhi based, TFGBV survivor	In-person	Experienced online stalking, impersonation/ fake account, received dick pic on Instagram. Dealt with other kinds of cases as a lawyer: -University Student "accidentally"uploads pornographic clip onto common drive where they were supposed to upload assignments -DV cases where tech has been used to perpetrate violence	Unknown	Filed case with cyber police, Felt it was ineffective "*After my experience, I don't bother telling people to follow up as there is nothing there.*"

Type of Interview	Personal Profile	Mode of Interview	Nature of Violence	Nature of Perpetrator	Legal Action/Recourse
KII 4	Young Delhi based lawyer, female	Online	Non-consensual sharing of intimate images, The bois locker room case	N/A	Sending legal notice to perpetrators as an effective strategy to intimidate perpetrators. Pointed out that cyber cases are difficult to investigate.
KII 5	Young lawyer /activist, female (experience across geographies) TFGBV survivor	Online	Personally experienced cyberbullying, morphing Worked on TFGBV cases wherein specific communities/ activists have been targeted such as women hailing from Scheduled Tribes and Muslim communities Worked with survivors of the Bulli bai case		*"Privacy of the victim does not hold in TFGBV. Technology is beyond the victim. The violation is public before the survivor makes it public which makes it distinct."* *"Survivors who are subjected to this form of violence become activists owing to lack of support structures"*
KII 6	Senior Lawyer, Kerala based, Female	In-person	Financial frauds targeting vulnerable women Activists/Vocal women who are subjected to targeted TFGBV Discussed one of Kerala's earliest prominent TFGBV cases around an organised online racket on Facebook in 2015	N/A	Actively pursues a lot of cases in court

Type of Interview	Personal Profile	Mode of Interview	Nature of Violence	Nature of Perpetrator	Legal Action/Recourse
KII 7	Kerala based POCSO (Protection of Children from Sexual Offences Act, 2012) lawyer, female	In-person	Online grooming, Sexual coercion and extortion, Blackmailing, Non consensual distribution of intimate images Character assassination of survivors in courts by lawyers is widely prevalent Organised vicious attack of well known/ celebrity/activists women is widely prevalent	N/A	"*Digital space is completely anti-women, science and technology. More women are using these technologies, and we think that this will improve women's status. Still, in actuality, this space is used for harassing women to make comments about women's bodies, etc*" Pointed out the dearth of cyber forensic labs in Kerala and India leading to significant pending cases
KII 8	CSO activist, female. Works at a Hindi digital information helpline intended for women and LGBTQI+ people.	Online	Evolution of TFGBV from harassment via blank calls In 2015 to impersonation combined with morphing of images, intimate image sharing, and distribution During COVID, sexual exploitation shifted online. Video calls are recorded and then distributed, reducing livelihood opportunities	N/A	The helpline of this particular CSO, which is one of the most effective and widely used ones, ironically gets calls from people trying to perpetrate TFGBV- How to track their partner's phones etc. Both genders call in with men more in number (not statistically verified, anecdotal)
KII 9	Puducherry based academic studying Men's Rights Activist spaces and the manosphere culture in India	Online	Indian manosphere culture takes inspiration from the American right wing, Andrew Tate is widely popular References to the red pill and blue pill with the consumption of the red pill meaning ability to know the "real" truth	N/A	Along with feminism, LGBTQI+ activism is vehemently opposed owing to its position that gender operates in a spectrum

Type of Interview	Personal Profile	Mode of Interview	Nature of Violence	Nature of Perpetrator	Legal Action/Recourse
KII 10	Researcher mapping tech and policy	Online	N/A	N/A	*"Harms of GBV are beyond what is understood as illegal. It is something that adds up incrementally."* *"Not just what is understood as illegal but what leads to fatigue, perspective of what comprises GBV needs to come from those whose lived reality it is."*
KII 11/ FGD	Three police officers with a cyber police station in Kerala	In-person at the cyber station	Receive a lot of financial fraud cases, alarming rise of digital arrest cases Weak passwords of social media accounts, people use their mobile number etc as a password which is easy to hack Case of two YouTubers abusing each other online in sexually explicit language	N/A	Difficulty of accessing information from diverse platforms, for example, WhatsApp does not give information The police cited the arrest of the Telegram head over similar charges Awareness/Prevention is important Virtual stalking, intimate videos/ photos being leaked online The 2020 rule mandating intermediaries for social media giants such as META was critical

1.1 (a) 'Public' vs 'private'

Jalaja*, a lawyer with extensive experience in working on TFGBV cases across the country, pointed out the lack of 'privacy' for survivors.

> *"The privacy of the victim is not understood in tech-based violence because technology is beyond the victim. If my body has been physically violated and I choose not to tell people, I can get away with not being seen as a victim. Here [online] the proof is before you, so you know somebody else has spoken, you are targeted, [and] a hundred things float about you."*
> **~ Jalaja* while talking about TFGBV in the workplace**

Unlike GBV cases that occur in the physical realm, where the violence may not become public, in TFGBV cases, the evidence and material are in the public domain, freely available on the internet and social media. This erodes a survivor's ability to control the narrative to shield themselves from further harm, as the violence is both persistent and visible to a wide audience. The blurring of public and private boundaries in digital spaces not only heightens the trauma but also makes it more difficult for survivors to disengage from or escape the violence.

1.1 (b) Geographies and technology-facilitated gender-based violence

This research began with the aim of focusing on specific geographies within the country to identify overall patterns of TFGBV. Based on internet penetration data, the study had proposed looking at two states on the higher ranking spectrum and two at the lower end to understand how digital cultures might be manifesting differently, potentially resulting in diverse forms of TFGBV. The hypothesis was that variations in digital gender violence, and the diverse ways technology facilitates GBV, might vary depending on the extent of internet penetration in a region.

While challenges arose in terms of how data collection could be conducted in these states, as delineated above, a major finding of the study was around how manifestations of TFGBV were geographically agnostic. That is to say, the manifestations and types of TFGBV across regions were similar largely comprising doxing, online stalking and harassment, non-consensual distribution of intimate images, and morphing of images. Also, owing to the nature of the internet, location did not necessarily impact the nature of the incident, its duration, ramifications, or life cycle of the legal case, if it got to that stage. For example, one of the survivors interviewed was a resident of Bihar (a state in North India) and on holiday in Delhi (the capital of India), when the violence happened. The case was reported in Delhi, with a closure notice coming from the police in Mumbai (a city on the West coast of the Indian peninsula). It remains unclear to the survivor and her lawyer why they got the final notification from Mumbai police, stating that the case had been officially closed.

Sharing photos on pornography sites and other online chat platforms, circulating images with the "promise of sex" or "availability for sex" emerged as patterns under the larger umbrella of image-based sexual abuse.

> *"Yes, porn sites and all. They pasted my phone number on those sites along with a caption saying, 'You can call this number; this individual is available for sex, or he is interested in having sex with strangers.' They also shared my images from social media platforms on those sites."*
> **~ Anil*, Survivor from Kerala while sharing the violence he faced which was primarily connected to his identity as a LGBTQI+ person and his role in organising Kerala's Pride March**

> *"They wrote it in all the public toilets here. Wherever they can they wrote it down. 'Available' 9XXXXXXXX. I received two thousand to three thousand calls per day. Day and night. Continuously."*
> **~ Supriya*, Survivor from Kerala while talking about the online abuse she faced due to her job as a journalist**

1.2 Social norms and impact

The study unearthed the many ways the "digital speaks to the non-digital," as one of the lawyer put it. The ability to speak up, name, and address digital violations was deeply entrenched in social norms around gender and sexuality. Survivors experienced significant stigma and shame, and feared being outed and ostracised by society, including their parents and the police. This stood out specifically in testimonies of young women who did not want their parents to know about the violence that they had experienced, anticipating they would be blamed, their characters judged, and their freedoms restricted.

"You remember the bois locker room[15] incident. We advised the girls and obviously they did not even want their parents to know these things. So then we just had to figure out, we had to speak to these tech people and figure out the way of writing to Instagram, [and] getting it stopped."
~ Rachna*[16], Delhi based lawyer (works on human rights and gender with a focus on criminal law) while sharing her observations about women and girls filing police complaints

In almost all the cases, morphing and sharing images of the survivor was accompanied by sexual innuendos and deeply misogynistic and hateful texts. The societal norm of who is a 'good woman' often lay at the heart of the issue, making attacks on a woman's 'character' central to these forms of violence.

"The picture of my head was morphed into some semi-nude woman's picture, and they used to paste them in public comments. That's how I saw them."
~ Rama*, Survivor from Kerala while sharing about the violence she faced online

"That person took all the single photos, in which only I was there. That person took those photos and mentioned weird, lewd comments in the caption and a lot of very very bad and vulgar [words], in those hashtags. Then everyday he was posting a new picture on that profile. Then he started mentioning me in the stories also from that profile and started tagging me and taking out my karwa chauth[17] pictures and putting captions, like "slutty whore".
~ Prajakta*, Survivor currently residing in Patna while describing the TFGBV she faced

1.3 Curtailment of rights

An immediate ramification of TFGBV is survivors' withdrawal from the digital space and a rapid curtailment of their digital and other rights in general. Most survivors reported that this withdrawal was self imposed. In other cases, it was actively suggested by the police. For example, Rama, a survivor, reported how when she approached the cyber police about the slow progress of her case, she was asked to stop using Facebook - "*The cops used to say, why can't you withdraw from Facebook?*".

"I have put on the privacy [settings] so that nobody can message me or tag me in stories. I did not have that before on my Instagram profile....and obviously I have stopped posting a lot like I did before. So yes."
~ Prajakta*, Survivor describing the impact of the violence she faced on her social media usage

"Already, I barely trust people online and after this incident I was like, it is better not to engage with anybody online until you actually know them because it doesn't make sense, and it was an ugly feeling. ... I was scared to open my mic later... that again, I would have to go through the same thing. It's always like they can do anything to you..... But in terms of how it felt - it was very ugly. I just didn't feel like engaging with random people anymore even though I really enjoyed playing the game. It did scare me."
~ Diana*, Survivor from Hyderabad who spoke about facing online harassment during online gaming

"I was fed up with all these things. For some time I withdrew from my screen appearance but after that I restarted my programmes and other things. But I... stopped this discussion because one or other word will be misinterpreted and I have to go through the trauma again all over, no?"
~Supriya, a survivor from Kerala while talking about the impact of the online abuse she faced due to her work as a journalist

The impact of TFGBV is not just limited to survivors withdrawing from digital spaces but also restricting freedoms such as speaking up, organising, and protesting.

> *" After the last Pride March, I thought I would become active in this year's Pride March, but those experiences and memories are still stopping me from being active in the LGBTQ+ community's activism...I am doing post graduation [studies], so if I have to go through those experiences once again I will lose my education and life. So, instead of fighting for the marginalised people and talk[ing] for my community, I am forced to stay behind."*
> **~ Anil***

1.4 Social location, intersectionality and technology-facilitated gender-based violence

The forms of TFGBV did not seem to depend on the survivor's individual profile. However, in cases where survivors belonged to marginalised communities such as Scheduled Castes (SC) or Scheduled Tribes (ST), they faced additional targeting due to their gender and caste and/or tribe identity.

> *"He said that when an Adivasi[18] woman is walking on the road, even if she strips a man walking by her, the law here won't charge any case against her. He has said that in that news, in that video. He has made it a point to refer to my caste to insult me. I am a ****** Christian. He has particularly mentioned that too."*
> **~ Divya*, Survivor from Kerala while describing the various instances of TFGBV she has faced.**
>
> *"Oh, that was very prevalent in cyber trolling. 'You don't look good, why do you look like this?' [Those are the] kind of statements I have received. 'How did he feel like raping this one? Just look at her.' They were commenting with such statements."*
> **~ Rama*, Survivor from Kerala while talking about how her OBC identity has been targeted in the cyber trolling she has faced.**

In cases involving LGBTQI+ people, one common tactic was using the co-called 'evidence' of their identity to blackmail the survivor by threatening to expose them to their family and social circle. While the study was able to include only one person who identified as LGBTQI+, he shared that his peers and friends had experienced similar forms of abuse.

> *"More than that, they started messaging my family members. For example, they began sending messages to my brother-in-law, my sister's husband. The messages were saying I was LGBTQI+ and several other slur words which described me as homosexual. I haven't done my coming out properly. Only my brother and sister know about my sexual identity. Other family members were unaware of this, so informing them [in this way] disturbed my life."*
> **~ Anil***

On the other hand, the power of privilege in effectively addressing TFGBV was highlighted in the interviews with lawyers. Rachna*, a lawyer in Delhi, narrated a case where both the perpetrator and survivor attended a prestigious university in Delhi and were from affluent families. During the course of their romantic relationship, the woman had shared naked photos of herself with the perpetrator. At some point, while the relationship was still ongoing, she received a message from an unknown man on social media asking if she was the same person whose photographs he had seen on a chatting website. The person identified her through her public social media profile. The boyfriend (perpetrator) had been posting her photos on random websites and chatting with people, pretending to be her. The survivor found out about two to three months after the perpetrator had started doing this.

Rachna* mentioned that both parties were around 20 to 21 years old at the time and the survivor did not want to file a police complaint or involve her family. While she was clear that she felt no shame for having shared the pictures, she wanted the violation to stop so she could stop engaging with the perpetrator altogether.

"I won't be able to deal with it, it's too much, and I won't get what I want. I just want them (the photos) to be removed, and I want nothing [else]. I don't want this boy to contact me and I want this to stop. That was her focus, and it was really not [about] having somewhere where you get into criminal[ising] this thing, where the onus falls on you, and you have to withstand that and the entire investigation and trial process. She was in shock, and she was on the verge of thinking that something was wrong with him. I just want it to stop and he needs to go for therapy or something.."
~ Rachna*, Delhi based lawyer describing a TFGBV case she handled

She contacted Rachna who sent a legal notice[19] to the perpetrator. The perpetrator's father eventually got involved because of the legal notice and faced the possibility of his son going to jail. The perpetrator apologised and signed a settlement agreement[20] wherein he promised to undergo counselling for two months. He also undertook to provide all relevant links of where he had posted the survivor's intimate images. Rachna explained that, although the agreement had no legal validity, they had drawn it up to ensure the matter was taken seriously. In what is an important and unique aspect, the perpetrator's father hired a tech company to delete all relevant material from the internet.[21] His laptop was examined to identify all links and websites he had accessed. Since he had been doing this for only about two to three months, all the links he had accessed during the time were identified.

Similarly, Neelam*, a lawyer based in Kochi, Kerala talked about a case involving a survivor from the Indian Foreign Service. She stressed how the survivor was adamant to see the matter in court, indicating her social, financial and cultural capital to withstand the pitfalls of a long-drawn-out legal battle. Further, as the survivor had been on maternity leave at that time, it was her brother who was engaging with Neelam and following up on the matter. This connects back to Rachna* another lawyer who pointed out that one of the factors that decides what course a case takes is 'how much the woman can withstand'.

Sitara*[22], a senior lawyer based in Trivandrum, Kerala with extensive experience of handling TFGBV cases pointed out larger patterns relating to cases involving financial fraud especially along the faultlines of gender and class. She elaborated on how women were increasingly targeted in online financial fraud, often due to the perpetrator's confidence that the women would not be able to speak up - at least not as much as their male counterparts.

In one case, a woman with disability was targeted in an intricate financial scam by an anonymous perpetrator who promised marriage in return for services such as setting up bank accounts. It was only when the woman received a legal notice and call from the Mumbai cyber police that she became aware of the scam. The police accused her of being a conspirator in a financial scam where almost ten million was transferred through four bank accounts that were in her name.

In addition to having a disability and severe health complications, she was from a poor background and had negligible family support, making her particularly vulnerable to such elaborate online scams[23]. She contacted a Sitara, a local lawyer who was known to her and had previously supported her financially. The matter was resolved when Sitara stepped in and provided evidence to the police regarding the survivor's circumstances, including financial hardship and her physical and mental condition. Her familiarity with the survivor enabled Sitara to explain to the police how she had been specifically targeted owing to her vulnerabilities.

Domain 2: responses

2.1 Legal frameworks: limitations and possibilities

The Information Technology Act, 2000 (IT Act) is India's primary legal framework pertaining to cybercrimes and is gender-neutral. Further, relevant sections of the new Bharatiya Nyaya Sanhita 2023 (BNS), which replaced the erstwhile Indian Penal Code, 1860 and the Bharatiya Nagarik Suraksha Sanhita (BNSS) which replaced Criminal Procedural Code, 1973 are also applied in some cases. Sections 75 (Sexual Harassment), 77 (Voyeurism and the capture and distribution of sexually explicit intimate images without consent), 78 (Stalking), 351 (Online harassment/trolling, Criminal Intimidation), 356 (Defamation) of the BNS and Sections 67, 67(A), 66(E), 72 (Breach of privacy/Doxing) of the IT Act - all constitute the relevant laws for TFGBV cases.

A Summary of the Laws in India to address TFGBV

Bharatiya Nyaya Sanhita, 2023 (BNS)	**Provisions**
Section 77, (Voyeurism)	A person of any gender can be accused of committing the crime of voyeurism, though a victim can only be a cis woman. The provision is flexible to cover various forms of TFGBV, including the capture and distribution of intimate images without consent. Image-based sexual abuse is typically dealt with under this provision.
Section 78, (Stalking)	This provision explicitly recognises the monitoring of a woman online as constituting stalking.
Section 79, (usage of words or gestures to insult the modesty of women)	This provision provides for acts intended to insult the modesty of a woman. Specifically, it covers uttering words, making sounds or gestures, exhibiting objects, or intruding on a woman's privacy with the intention to insult her modesty. The punishment for this offense is simple imprisonment for up to three years, a fine, or both.
Section 75, (Sexual harassment)	Sending obscene material (photos, pictures, films, messages) to a woman on social media is an act of sexual harassment. Showing or sending a woman pornographic or sexually explicit material without her consent is also a form of sexual harassment.
Section 356, (Defamation)	Many types of TFGBV also qualify as defamation; a provision which can be used by persons of any gender as complainants.
Section 351, (Criminal intimidation by anonymous communication)	This can also be used to deal with online harassment and trolling by anonymous users/accounts online.
Section 351, (Criminal intimidation)	This provision can be used to deal with harassment and threats in the context of TFGBV.

A Summary of the Laws in India to address TFGBV	
Information Technology Act, 2000 (IT Act)	**Provisions**
Section 66A	This provision is often touted as a provision enacted to address TFGBV. It criminalised a broader category of offensive speech. It was struck down by the Supreme Court as unconstitutional for being overbroad and susceptible to misuse, in particular that it would result in violations of freedom of speech in a landmark judgment.
Section 66E	Under this provision, voyeurism is a crime, irrespective of gender of the victim. Section 66E classifies knowingly or unknowingly, without consent, taking a photograph of the intimate/private areas of a person, sending such a photograph to someone else or publishing such a photograph, under circumstances which violate the person's privacy, as a crime.
Section 67	This provision criminalises the publication of any "obscene" material online, irrespective of the consent of the people in the material. Section 67 is similar to Section 296, BNS, though the punishment for circulating obscene material is higher under the IT Act.
Section 67A	This provision criminalises the publication of any sexually explicit material online, irrespective of the consent of the people in the material.
Section 72 ('penalty for breach of confidentiality or privacy')	The IT Act does not have any provisions that deal with online stalking. In cases of online stalking, often Section 72 is applied. This provision covers any situation where a person discloses private information about another person online without their consent. It is used as an umbrella provision to cover various types of TFGBV.
Section 69A	Orders to block content can be issued under Section 69A by the Central Government, including its ministries, under various circumstances, including for disrupting "public order." These orders are not required to be made publicly available or published anywhere and can directly be sent to intermediaries for compliance.
Section 79	The provision holds intermediaries liable for third-party content in two situations: (i) when intermediaries assist in the publication of illegal third-party content and (ii) when intermediaries fail to comply with a government order requiring the removal of specific third-party content. In *Shreya Singhal v. Union of India*[24], the Supreme Court reinterpreted Section 79 to the extent that now intermediaries can only be held accountable for failing to comply with court orders or government notifications requiring them to delete specific content, and not for the publication of any content on their platform. This is, basically, India's safe harbour regime. Intermediaries are not entitled to safe harbour if they fail to comply with a government or court order to remove content.

Many lawyers highlighted the need to use clauses from the IT Act in conjunction with laws such as the SC/ST Atrocities Act and the relevant sections from the BNS to strengthen their arguments. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, also provide ethical guidelines for intermediaries and technology companies. This study exposed the need to understand and address the gaps in laws in order to deal with TFGBV cases effectively. The study also analysed relevant case law, with a summary included in Annexure 3.

While online gender rights, within the context of human rights and resistance movements, have found articulation, the challenge is is often understood as a contest of rights, i.e. how to exercise the rights to safety and protection from violence online while at the same time upholding other fundamental rights such as the right to privacy and the right to freedom of expression. In India, gendered abusive online speech is not recognised as a criminal offence; the difficulty is when this aspect clashes with notions of free speech and expression. Even though the rationale for striking down Section 66(A) of the IT Act has been widely recognised and respected by feminists and digital rights activists, there is still the need to address the specific ways people of diverse genders are targeted online. "The quashing of 66(A) has left a void. There is an urgent need to address it," says Sitara, a lawyer from Kerala.

2.1 (a) Balancing freedoms and protection: The case of Section 66A, IT Act

Section 66A of the IT Act was added as an amendment in 2009 to address cybercrimes, specifically crimes against women/TFGBV (Chibber & Chowdhury, 2015).

It criminalised sending certain categories and types of information through communication devices, with imprisonment of up to three years and a fine.

The provision criminalised a range of content content, namely content that was:

1. "Grossly offensive"
2. "False and meant for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will"
3. "Meant to deceive or mislead the recipient about the origin of such messages"

Section 66A was frequently invoked to prosecute social media users for political commentary and satire, prompting widespread concern over its misuse to curtail constitutionally protected free speech[25].

The provision's constitutionality was challenged by multiple petitioners, including Shreya Singhal, a New Delhi-based lawyer working on digital rights, various NGOs, and companies in the *Shreya Singhal* v. *Union of India* case before the Supreme Court of India. The petitioners argued that the provision impinged upon freedom of speech and expression guaranteed by Article 19 of the Constitution of India.

The Supreme Court struck down the provision because it violated various aspects of free speech under Article 19 of the Constitution.

The Court held that:

- The provision was overbroad and vague, which violated Article 19(1)(a), as it did not make explicit the particular types of speech it aimed to restrict.
- The provision "arbitrarily, excessively and disproportionately invades the right of free speech," which the Court described as a "chilling effect" on free speech.
- The provision did not fall within the reasonable exceptions to freedom of speech. It declared the provision 'void ab initio'- meaning it should be treated as though it never existed.
- The Court held that all pending cases under the provision would be dismissed, and no new cases could be registered.

The judgment was lauded for its salient role in upholding freedom of expression, specifically online speech, and its jurisprudence on Article 19 of the Constitution. While the spirit and rationale of repealing Section 66(A) were necessary to maintain free speech, it left a critical gap within the legal framework for addressing TFGBV. Many forms of TFGBV, such as online harassment, threats, and abuse, could have fallen under the broad content previously covered by the provision. Recognising this gap, the Kerala Police Act[26] was amended in 2020. However, the amendment was withdrawn the same year due to issues similar to those raised on Section 66(A).

There have also been situations in other countries where the tensions between the right to free expression and free speech and securing the digital rights of women and marginalised communities have come to the forefront. For example, in Kenya, Section 29 of the Information and Communication Act, 1998, which had similar provisions and implications as Section 66A of the IT Act, was struck down by the High Court of Kenya's Constitutional and Human Rights Division in 2016 for being repressive and vague, and open to abuse by the state to target online speech.[27] In the US, the Communications Decency Act penalises anyone who '*utilises a telecommunications device, whether or not conversation or communication ensues, without disclosing his identity and with the intent to annoy, abuse, threaten or harass any person at the called number or who receives communications' with fines or imprisonment*.'[28] It has also received criticisms similar to Section 66A, although US courts have found that it does not meet the threshold to be declared unconstitutional.

Moreover, various UN Special Procedures reports and statements also address TFGBV while still upholding freedom of expression. For instance, the Special Rapporteur on the right to freedom of opinion and expression for 2021 focused on gender justice and freedom of expression in her report to the UN General Assembly, emphasising that free speech on the internet should be ensured while accounting for and redressing TFGBV.[29] The UN Human Rights Council has also referenced TFGBV in its consensus resolution 38/5, calling on all states to ensure that women and girls can access their right to free speech and expression on the internet without facing discrimination or backlash for it.[30]

Globally, conversations have been taking place on whether TFGBV can constitute hate speech or meet the threshold to qualify as criminally punishable speech, not just offensive speech that is not criminal. Broadly, speech qualifies as hate speech when it poses a real and immediate risk of violence against the targeted individual or group, and reflects a clear intent to cause harm by the speaker.

2.1 (b) Intermediary accountability

Internet service providers (ISPs) are often considered "mere conduits" under legal frameworks such as the EU's E-Commerce Directive, meaning they are not typically held liable for third-party content transmitted through their networks. In the US, Section 230 of the Communications Decency Act provides broad immunity to intermediaries, including platforms and ISPs, for user-generated content. ISPs usually take action only when legally required—such as through court orders—since they usually lack the infrastructure and mandate to proactively monitor or moderate content, unlike social media platforms.[31]

Some social media platforms have introduced content moderation measures, online safety training, and policies aimed at improving user safety. However, many users remain dissatisfied with how these platforms handle reports of violence, including TFGBV. A key concern is that enforcement of platform rules is often automated or lacks sensitivity to the socio-political context in which the content originated. Furthermore, many technology companies lack adequate linguistic and cultural expertise to address reports of violence in non-English languages.[32] This serves as a significant barrier for many Indians who experience abuse in regional languages or culturally specific contexts.

The liability of social media platforms and websites in cases of TFGBV has been central to ongoing policy and legal discussions in India. Search engines like Google and Bing have attempted to distinguish themselves from other intermediaries, claiming they are merely aggregators of links and should bear minimal liability.[33] Indian courts have accepted this argument only to a limited extent: search engines are still required to take down or disable access to illegal or offending content when notified, and cannot claim complete neutrality or ignorance of the content they index.[34]

Broad liability regimes that impose liability on intermediaries for the actions of users of platforms are considered prone to censorship and pre-emptive blocking of content, leading to unjustified curbs on freedom of speech. Safe harbour regimes, where intermediaries are given immunity for the actions of their users (user-generated content) except in certain circumstances, seem to have a better approach to balancing free speech with protection from violence.

Intermediary accountability in India

In India, intermediaries must take down objectionable content only if ordered by a court of law or competent executive authority such as the Ministry of Electronics and Information Technology, for example. Under Section 69A of the IT Act, the central government, including its ministries, can issue orders to block content under various circumstances, such as threats to 'public order.' These orders are not required to be made public and can be sent directly to intermediaries for compliance.

The laws and rules described below provide a framework for intermediary accountability in India.

Law	Provision	Implications
Information Technology (IT) Act	Section 79 of the Act holds intermediaries liable for user-generated content in two situations: (i) when intermediaries assist in the publication of illegal user-generated content and (ii) when intermediaries fail to comply with a government order requiring the removal of specific content	In *Shreya Singhal v. Union of India,*[35] the Supreme Court of India read down Section 79 to the extent that now intermediaries can only be held accountable for failing to comply with court orders or government notifications requiring them to delete specific content, and not for the publication of any content on their platform.
The Information Technology (Intermediary Guideline) Rules, 2021 and the Code of Ethics and Procedure and Safeguards in Relation to Digital/ Online Media (IT Rules)	Rule 3(2)(b) deals with the publication and proliferation of non-consensual intimate imagery, with the intention to intimidate, harass, or abuse the individual(s) in the imagery. In such cases, intermediaries are required to take down the content within 24 hours of receiving a complaint through their Grievance Officer. Each intermediary is required to have a Grievance Officer and easily accessible information on how to contact them, according to Rules 4(6) and 4(8).	The IT Rules were notified by the Central Government under Section 87 of the IT Act. They replaced the Information Technology (Intermediaries Guidelines) Rules, 2011. The IT Rules define social media intermediaries as: "an intermediary which primarily or solely enables online interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services."
	Rule 4(4) requires significant social media intermediaries to "*endeavour to deploy*" technology-based measures to proactively identify and remove content that "*depicts any act or stimulation in any form depicting rape, child sexual abuse or conduct whether explicit or implicit*," and its identical republication.	

Law	Provision	Implications
	Rule 3(1)(d), a social media intermediary is required to take down any content that violates the interest of the sovereignty and integrity of India, the security of the state, friendly relations with foreign states, public order, decency or morality, contempt of court, defamation, incitement to an offence or information which violates any law which is in force, after receiving "actual knowledge" of such content on its platform.	"Actual knowledge" refers to a takedown notice from a government authority or a court order directing the takedown of content. The content is required to be taken down within 36 hours of the intermediary receiving "actual knowledge." This has been criticised for limiting both the intermediary and content creator's right to challenge such takedown before the action is taken, thus impacting freedom of speech.
	Rule 4(2) requires significant social media intermediaries providing messaging services (such as WhatsApp) to identify the "first originator" (the first person who sent a message) of information when required to do so by a court order or a government order under Section 69 of the IT Act.	This requirement has been criticised as government orders under Section 69 are not publicly available and are also not provided in responses to RTI enquiries,[36] citing state security reasons. Further, this weakens the end-to-end encryption promised by platforms to its users and can prove legally flawed when the first originator is outside Indian territory, as then the first originator is considered the first originator of the message in India.
	Under Rule 4(a), significant social media intermediaries[37] are required to have a Chief Compliance Officer, who is responsible for ensuring the intermediary's due diligence and compliance with the IT Act and IT Rules.	The Chief Compliance Officer, who must be a senior level/managerial employee of the intermediary residing in India, is personally liable before the law in case of non-compliance by the intermediary.
	Rule 4(b) requires intermediaries to appoint a nodal contact person	That person is responsible for 24/7 coordination with law enforcement authorities, to facilitate the intermediary's compliance with the law.
	Rule 4 (c) requires intermediaries to appoint a Resident Grievance Officer	That person is responsible for ensuring that the intermediary follows the law concerning its grievance redressal mechanisms.
	Rule 4(d) mandates the publication of monthly compliance reports	The report should provide details of complaints received by them and action taken, in addition to a list of links removed through their own monitoring through automated tools.

"People see me as an empowered woman, very strong woman, and I am not supposed to be in trauma. I am not supposed to say that I am sad or I am worried or that these things worry me. That is an additional burden on me, people like me."
~ Supriya*, Survivor from Kerala

In summary, while social media platforms have implemented various measures to monitor and control harmful content, significant challenges remain in addressing region-specific nuances and language barriers that hinder effective moderation. The legal framework in India, particularly through the IT Act and related guidelines, seeks to balance the protection of individual rights and public order with the preservation of the right to freedom of speech. However, the reliance on government orders for content takedowns, coupled with the inherent limitations in technological and linguistic capabilities, often results in a mechanical approach to moderation that may inadvertently stifle legitimate expression. Ultimately, the evolving dialogue around intermediary liability underscores the need for more contextually sensitive and transparent regulatory practices that can more effectively reconcile the dual imperatives of safeguarding citizens and upholding democratic freedoms.

Experiences of survivors and practitioners

Activists, caseworkers, and cyber cell police noted the challenges law enforcement bodies faced in obtaining relevant information regarding TFGBV cases from the platforms and technology companies. Conversations with cyber police officers shed light on the extensive legal and protocol labyrinth they have to navigate while handling TFGBV cases involving giant tech conglomerates such as Meta which operates social media platforms including Facebook and Whatsapp. Accessing information from these platforms takes time and is human resource intensive. In most cases the cyber police are refused relevant information pushing them to resort to legal measures to acquire them. Even then it is far from effective owing to multi country jurisdictional limitations. In some cases, despite legal mandates, platforms fail to take prompt and necessary action in the pursuit of criminal cases.

For example, a survivor in Kerala, a middle-aged single mother who worked as a psychiatrist whose photos were morphed and shared on Facebook, told us that her case was the first in which Kerala police filed a criminal complaint against Facebook for not removing the intimate photos, despite a written order.[38] The police had issued a notice under Section 79 of the IT Act requesting Facebook to remove the images - an action which the platform is legally required to comply with within 36 hours of a request. However, when no action was taken even after a week and in the absence of any formal communication from Facebook on the matter, the Kerala police filed a criminal case against the social media platform.

Even as challenges in accessing information emerged as a critical issue for law enforcement, it is worth pausing to reflect on whether all cases receive the same intense level of follow-up. Many survivors pointed out the apathy they encountered when engaging with the police. In the counsellor case, mentioned as IDI 9 in the summary table of documented survivor experiences, her familiarity with the cyber police, owing to her work as a college counsellor, seems to have ensured that they were cooperative and she was treated with respect and not ignored when she filed a formal complaint. She filed the complaint within an hour of finding out about the pictures. However, she pointed out that, *"familiarity is not the same as having a hold in the system. I did not carry that kind of weight, hence the case was closed without finding out who was behind it."*

> "You asked me about justice. If there is a concept called 'justice' anywhere at all, [one] must receive it when they are suffering. When we are living after forgetting all this, after a long time...if a court order comes then, are we receiving justice? No. This is a personal opinion. If there is any justice...or there is no justice for you. There should be [some clarity]."
> **~ Supriya*, Survivor from Kerala**

2.2 Federal variations

While the overall patterns of TFGBV remain consistent across regions, it was crucial to investigate how these cases were dealt with in the locations they happened or where complaints were filed. The study found indications of substantially greater engagement (engagement moving beyond police complaints and legal advice, cases going to courts) by the survivors and lawyers with the law in Kerala - a state where internet penetration is among the highest in the country. An important verdict with the potential of significantly altering the way TFGBV cases are handled in India has come out of Kerala. The Kerala High Court's judgement in Sooraj V. Sukumar v. State of Kerala recognised social media as a 'public space' thereby enabling the law to operate beyond the confines of a 'defamation' case and opening up the possibility of pursuing matters under criminal law. It is important to note that this recognition was made in an order denying anticipatory bail to an accused person in a case under the Scheduled Castes and Scheduled Tribes (Prevention of Atrocities) Act, 1989[39], but it has been cited by the Kerala High Court in other orders in TFGBV cases.

> *"Yes, the order said social media is a public space. You can complain. Until then, if somebody humiliates someone in court, the case could be treated as defamation. And if the case is defamation, they have to pay money. Everyone can't do that because the police won't take the case. So once Bechu Kurian made that judgement, the people who were humiliated on YouTube started making police complaints. And the police began taking action."*
> **~ Divya*, Survivor from Kerala**

Lawyers across Kerala consistently highlighted the quashing of Section 66(A) of the IT Act as a significant obstacle in effectively dealing with TFGBV cases. While many of the lawyers and activists in Kerala who participated in the research recognised the possibility of misuse of Section 66(A), particularly with regard to free speech in a democracy, they pointed out that the quashing had left a critical gap in the legal landscape. The gap, they argued, has allowed perpetrators to operate with impunity as legal action in TFGBV cases often resulted in minor fines as punishment. This insight was identified by lawyers who are frequently representing survivors in courts and at police stations, unlike their counterparts in other states. Drawing on their experience, they were acutely aware of the gaps in other laws and offered insights on the various legal clauses, in the IT Act and others, that could apply to TFGBV cases.

Further, in 2020 the Kerala government attempted to introduce an amendment to the Kerala Police Act to prevent the misuse of social media against women and children in order to address the gap referred to above. The proposed amendment was as follows:

> *"118 A. Punishment for making, expressing, publishing or disseminating any matter which is threatening, abusive, humiliating or defamatory.*
>
> *Whoever makes, expresses, publishes or disseminates through any kind of mode of communication, any matter or subject for threatening, abusing, humiliating or defaming a person or class of persons, knowing it to be false and that causes injury to the mind, reputation or property of such person or class of persons or any other person in whom they have interest shall on conviction, be punished with imprisonment for a term which may extend to three years or with fine which may extend to ten thousand rupees or with both."*
> **(Kerala Police Amendment Ordinance, 2020).**

The amendment received a lot of criticism over concerns that it could be used to curtail free speech, and was eventually put on hold the same year (Thomas, 2020).

The varying levels of engagement with the laws and legal processes across geographies stood in stark contrast to awareness of and engagement with TFGBV cases, even in places like Delhi, the country's capital. A possible explanation is that the people we engaged with in Kerala were those with substantial engagement with the system. Activists and lawyers from Kerala had a stronger engagement with the legal frameworks currently in place to address TFGBV cases. Further to this study, an investigation into regional variations in response systems in greater detail is required.

2.3 Ideas of justice

For most survivors, their expectations from the system, if they chose to engage with it at all, were intimately linked to their personal understanding of justice. For many, it was punitive, such as seeing the perpetrator behind bars. But as outlined above, justice also entailed speedy action by the legal system and an immediate halt to the violations they were being repeatedly subjected to. While sentencing and punishment were important, most survivors lacked access to the basic means to deal with the trauma. Justice was also about protection, recognition, and dignity.

From the survivors interviewed survivors, it was clear that survivors need systems that not only punish perpetrators, but also actively prevent ongoing harm and ensure their safety. Yet, despite these urgent needs, survivors reported that they lack access to support mechanisms like mental health care, psychosocial support, and financial assistance to begin addressing the long-term emotional and psychological impacts of the abuse. The absence of these critical services often left them to navigate their trauma in isolation, reinforcing a sense of abandonment and deepening the injustice they suffered.

"You asked me about justice. If there is a concept called 'justice' anywhere at all, [one] must receive it when they are suffering. When we are living after forgetting all this, after a long time...if a court order comes then, are we receiving justice? No. This is a personal opinion. If there is any justice...or there is no justice for you. There should be [some clarity]."
~ Supriya*, Survivor from Kerala

"If at least I was informed or I got to know about some action that has been taken against this guy or both the guys in that case, I think that was the bare minimum that should have happened. That is [my view] from a systemic perspective.
And then from a societal perspective, the whole thing about being apologetic for a friend's behaviour is something [It's] definitely not the first time I have faced, It shows [how] deeply entrenched it is, and how helpless it makes you feel. That was the closest that I got. Everybody was trying to make an excuse for these guys' behaviour, not really holding them accountable.
And then I was like, at least I need to hold them accountable, at least I need to give that message to the extent I can. That no, those two cannot just get off, get away by doing these things."
~ Shalini*, Survivor currently residing in Delhi

"If I knew that person I would have confronted that person or I would have liked to. That person, he or she, whoever that person was, I wanted that person to know what he has done and he should face those consequences. I wanted that but that did not happen. So, that is traumatising, more traumatising than what has happened to me. To know that that person is free and has not faced the consequences of what they have done, that is discomforting actually."
~ Prajakta*, Survivor currently residing in Bihar

The right to be forgotten

Linked to survivors' conceptualisation and expectation of justice is the right to be forgotten. The right to be forgotten is an extension of the right to privacy and regarded as important in TFGBV cases. Known in the EU General Data Protection Regulation[40] as the "right to erasure", in the context of TFGBV it pertains to the deletion of all vestiges of objectionable material online including personal information of a survivor.

Divya, a survivor, recounted how she regularly searched herself to check if any images or videos of her had surfaced again on the internet. Similarly, Rachna, one of the lawyers interviewed, shared an incident involving a friend whose objectionable images that had previously been removed from the internet following a legal case resurfaced years later, threatening her current employment. These examples highlight the precarious nature of digital privacy and underscore the limitations of current protections.

There is no specific law in India that provides for the critical right to be forgotten. It is not statutory in the Indian context. At present, the "right to be forgotten" often depends on the discretion and empathy of individual judges. For instance, in 2020, the Orissa High Court[41] denied bail to an accused who had raped a college classmate and uploaded a video of the rape to Facebook, citing the severity of the crime and its digital amplification. While rejecting bail, given the heinousness of the crime, the Court observed that the right to be forgotten is an integral component of the right to privacy and must be available to victims and survivors in such contexts by way of mechanisms to delete offending content from intermediary platforms.

However, even though the right to be forgotten has come up in numerous contexts in Indian jurisprudence, there is no settled legal position on it. In the Orissa case, the Court held that in situations where a survivor's privacy has been seriously violated, the survivor or the prosecution can request courts to have the offending content removed from public platforms, regardless of ongoing criminal proceedings. The Court commented that "information in the public domain is like toothpaste, once it is out of the tube one can't get it back in and once the information is in the public domain it will never go away."[42] Interestingly, it noted that the criminal justice system and Indian law are focused on sentencing and punishment, not redressing the harm and trauma caused to victims/survivors of sexual violence. It also observed that it is unreasonable to expect victims/survivors to approach courts to get all offending content taken down as the legal system can often be "confusing," "complex," and "intimidating." However, such verdicts are few and far between.

Moreover, while the Court did focus on the issue of consent in data processing and collection when examining the facts of the current case, it stated that consent is not a factor in this case because "no person, especially a woman, would willingly reveal and portray the ambiguous aspects of their character."

Strengthening the right to be forgotten could go a long way in facilitating survivors' recovery, healing and access to justice.

2.3 (a) Barriers to justice

Similar to GBV cases occurring in the physical realm, survivors of TFGBV were most inhibited by prolonged legal processes, systemic apathy, lack of awareness and a lack of resources to effectively respond to their cases.

The most important need that all survivors reiterated was for the violation to stop. The fact that violations tend to be repeated and continuous owing to the nature of the internet, stopping the violation rendered it the single most important deciding factor for survivors. Many chose to mass report on the platform concerned or use tech platform helplines or those run by NGOs to request swift removal of the objectionable material. Interestingly, none of the survivors who took part in the study were aware of the national cybercrimes reporting number.

> *"We tried to move things legally with the help of this organisation called S*. With those efforts, we could block two or three accounts that were campaigning against the Pride March. The problem with the legal action is that most social media handles that conduct these sorts of campaigns use anonymous IDs. So, we do mass reporting against these accounts and force the social media platforms to act against the accounts."*
> **~ Anil*, Survivor from Kerala**

A caseworker noted that the police would often resort to the same actions of raising complaints on the concerned social media platform and getting them to take the material down, as a tech savvy survivor might.

For more details on reporting protocols and procedures, please see Annexure 1.

Time

The study explored the many critical ways time was instrumental in the access of and engagement with the legal system, from the police to the judicial system. Speed is of the essence in cases of TFGBV, which the present system is not equipped to handle, stemming from myriad factors such as systemic apathy and lack of awareness.

Moreover, survivors often lack monetary and other resources to pursue their cases. *"What is the point, if justice comes many years after what happened? It's already behind us, no one wants to relive it,"* said a survivor.

In addition to the limitations in existing laws, the broader legal system did not seem to invoke confidence in the study participants. All the survivors and experts involved in the study expressed hesitation in filing and pursuing formal police complaints. For most lawyers, this hesitancy stemmed from their observation that pursuing a long-drawn case was futile, given that the police and judicial systems were largely unaware of the modalities and complexities of TFGBV.

Since time is of the essence in TFGBV cases, the issue becomes even more pressing, and the current system simply cannot deal with the speed at which the forms manifest and spread. In fact, survivors often turned to helplines set up by agencies and NGOs for quicker resolutions.

> *" Unfortunately, even the police could not do anything for me, and my case was closed recently. I got an email that it has been closed. There were no comments there. Nobody has called me since February. I did not even get a call from them or an email, I got one email from them, grievance report, and then I got an email saying that the case has been closed. So, there is a big loophole in the system."*
> **~ Prajakta*, Survivor residing in Bihar currently**

> *"The IO (Investigating Officer) told me to come back when something happens."*
> **~ Sonal* (reporting a fake account that had been created with her images, her photo and phone numbers being circulated)**

> *"Other than that, I don't expect any immediate justice in this case. Besides, the longer it takes, the more years it takes, our children would suffer more. As they grow older, they would be subjected to another version of the torture that they suffered now."*
> **~ Divya*, Survivor from Kerala**

Social norms and systemic apathy

Participants in the study attested to how deeply entrenched social norms were within the legal system, particularly within law enforcement. The concepts of what is considered offensive or derogatory are heavily influenced by social and cultural conditioning, making them deeply subjective and challenging to navigate. Most survivors who reported their cases to the cyber police reported that their cases were not taken seriously.

"It was upsetting for me to not have been taken seriously the first time. I went to the police after suffering that amount of torture and harassment. If I don't get a salary for a month, what will be the situation of my kids?," **points out Divya. This is reiterated by many of the study participants.**

TFGBV cases are usually not taken as seriously as other cybercrimes, such as those relating to fraud.

"There is a level of trivialisation. In the sense that other people have been investigating frauds of much magnitude, like crores and crores being taken away. And then a lady goes there and says that I was abused. They don't give any importance to this. The immediate response is 'Why don't you block [them]?'..."
~ Sitara*, Lawyer from Kerala while sharing her observations about police investigations carried out for cybercrimes.

A corollary to this and thus another serious limitation of the present legal system is its inability to offer support and sensitivity to survivors. There is a lack of any support whatsoever. As one of the lawyers we spoke pointed out, "*the present system is all about crime and punishment, nothing in it helps the survivors deal with their trauma.*"

"When I met Saroj, a cyber cell officer, he said, 'See, this is cyberspace. If you need a healthier environment, if you need safety, then it is your responsibility.' It was my responsibility, he said, so it was not even a step from your side. He was like, it is your responsibility if you want safety, block them and if it's still not working, delete your account and leave.*

"Because 90% of the officers I went to didn't know what abuse is. When I tried to make them understand about emotional abuse, they are like, 'So that person doesn't touch you?' They always want to know whether there was physical or sexual touch, otherwise it is not abuse. To register it as emotional abuse, they ask, 'What is that? Is there abuse like that?' So basically, they are unaware. They just write a test and reach a position. What's the test to become a police officer? Is there a psychological test? Do they have awareness? They don't know how to behave with survivors, especially when asking and framing certain questions. Everything should be sensitive; that is not there. It is the problem."
~ Rama*, Survivor from Kerala

"People see me as an empowered woman, very strong woman, and I am not supposed to be in trauma. I am not supposed to say that I am sad or I am worried or that these things worry me. That is an additional burden on me, people like me."
~ Supriya*, Survivor from Kerala

"The officer receiving the complaint won't be sensitive about gender. Most officers are like that, so their response will be very weird. They will say you went for all this, you are outspoken. That is why you have to go through all these women who are not going for all these and do not have to experience all these, and slowly, they will transfer the blame onto her. The officers' first response will be negative. That is the problem with the system."
~ Soumya*, Lawyer from Kerala

Survivor experience: Divya

Divya's experience sheds light on the deeply misogynistic and unethical practices prevalent within the informal online journalism ecosystem in Kochi, Kerala. Her account illustrates the systematic dismantling of the personal and professional life of a working-class woman from a Scheduled Tribe.

Divya*, 30, had moved from Idukki, a hilly district with minimal employment options, to Kochi in pursuit of better income opportunities. She was from a tribal community, generally residing in parts of Kerala such as Idukki, and officially recognised as a Scheduled Tribe[43]. She lost her father, who had promised to "make her a doctor", at an early age and was forced to marry, "the day I turned 18."[44]

She had three children early in her marriage, and her husband turned out to be a violent alcoholic. One episode of abuse led to a miscarriage, causing her to lose an almost eight-month-old pregnancy.[45] Divya talked about the mental and physical torture she endured, including at the hands of her father-in-law, who would refuse to eat the food she cooked and insisted she use separate dishes while cooking.

With minimal formal training and barely completing her education, she took up various jobs to make a living in Kochi. Eventually, during COVID-19, she ended up working with a man who ran an online "crime" channel and who used to run a magazine in the 90s, which regularly targeted famous personalities in sleazy, sexist, and sensationalist ways. Divya worked as a 'newsreader,' making her the face of this channel with over 10 million subscribers. Each employee was given a target of producing 25 videos every day, for them to keep their jobs and earn incentives.

Matters came to a tipping point when Divya was asked to pose as a famous woman politician in sexually suggestive ways so that the man (her employer) could 'leak' the videos, claiming them to be a scoop. By then, Divya and her employer had already been arguing over the use of sexual innuendos as thumbnails for her news segments.

When she refused to do the video, her employer mentally tortured her by constantly badgering her about not meeting her targets and not getting enough views, prompting her to leave her job.

She was hired by another online news channel, which fired her in days at the behest of her previous employer, who reached out to everyone in the close-knit online journalism community operating out of Kochi asking them not to hire her. After this, her former employer went on an offensive, making videos featuring Divya, telling viewers how he got her fired from her new job.

In addition, together with a female employee, he called everyone on her contact list, including from her children's school, telling them that she was a "prostitute" who had been caught in multiple raids on individuals involved in the sex trade, and that she was of 'immoral' nature and a drug addict.

"My kids were publicly humiliated in school, including by their teachers. They refused to go back, and it took substantial counselling to get them to do so. With the threats and harassment getting out of hand, in 2021, I went and filed a complaint at the [police] commissioner's office. Just a formal complaint written on a white paper. I had also told the circumstances of the complaint - that I had been asked to pose as a famous woman politician.

Initially, the cops didn't take it seriously...In about three weeks, the perpetrator released a video claiming that he had the female politician's nude video and would release it. This sent the police into a frenzy. They immediately recorded my statement and raided the man's office on the same night, seizing everything they could find there, including CCTV footage. He was arrested the next day, and I was taken for evidence gathering."
After these developments, Divya* reached out to Neelam*, through a friend, for legal support. *"I told her, 'I don't have a single rupee to pay you. I have no support, but I have suffered so much. Please try to do something about this case. I had met her at a time when I was in a terrible situation. I could not even find a job, and had no money. The whole world thought of me as a cheat and prostitute, as someone caught in raids. I could not walk around without people recognising me and calling me names."*

Subsequently, Divya* was systematically targeted by other male YouTubers who, declaring solidarity with the jailed perpetrator, made more videos about her. These included some featuring her estranged husband making derogatory comments about her interspersed with selective video footage from an earlier altercation with him. *"They all made videos maligning and publicly challenging me. One of the female employees who had worked with him called and threatened me further. I filed a police complaint against her and other YouTubers as well."*

Divya's cases against her former employee and other YouTubers who perpetrated online violence against her - some of which are still ongoing - have been instrumental in reshaping the legal landscape pertaining to TFGBV. One of her cases involving a male YouTuber led to the important 2021 Bechu Kurian judgement by the Kerala High Court, which legally recognised social media space as a public space.

The court ordered the accused to delete all "offensive" videos of hers from the internet. Nevertheless, due to the subjective nature of what constitutes "offensive" content, certain videos have remained accessible despite Divya's concerns.

2.4 Creative and informal approaches to TFGBV

Most survivors approached lawyers for legal and other counsel but only a minuscule number of their complaints translated into actual cases or criminal complaints. Many lawyers, particularly those based in Delhi , stressed on how they get clients reaching out for one-off consultations. Many lawyers have also resorted to innovative ways to deal with TFGBV cases, primarily focused on getting the violations to stop. Most often this entailed two mechanisms. One was getting a police officer to call the perpetrator, getting them to take the matter seriously and more often than not, the perpetrators stopped almost immediately. The other was sending legal notices, which also got the perpetrators to stop. In India, a legal notice is a formal written communication sent by one party to another, warning them of a legal action that may be initiated if a specific demand or issue is not addressed. In both scenarios the aim was to lend gravity to the matter without having to formally pursue it, thereby avoiding the need for formal reporting.

A Delhi-based lawyer explained how, in such cases, he usually sends legal notices or works with the police who in turn speak to the perpetrator with "vazan in his awaaz." This roughly translates to the police making a stern call to the perpetrator with the aim of getting the perpetrator to stop their actions.

The gap in empathetic responses from the state often pushes survivors to become support systems for others. As Jalaja*, a lawyer supporting survivors put it, *"A lot of people become activists after the violence happens to them. Where systems fail, then they become support systems for others."*

Credit: Aakansha Saxena

Expert experience: Soumya

Soumya*, a special public prosecutor handling POCSO cases in Kerala shed light on how TFGBV affects survivors under the age of 18 and how the legal system responds. Drawing from her experience, she referred to several cases involving online grooming and sexual coercion and extortion.

"It's common for them [perpetrators] to know how to groom these children, and they will create a spider like web and trap them. This child will meet them in some isolated space like a shed or hut. They have a network and people to arrange everything. And this child will go there, and she will face sexual harassment, penetrative sex, and molestation.

The harasser will record this also. So if initially the perpetrator only had a picture or a video of a hug or kiss, now, he has more videos. Then he will blackmail using these videos, saying that they will be shared. He will continuously repeat the threats and blackmail."

Soumya also talked about cases where child victims committed suicide following their experiences of online grooming and sexual coercion and extortion. While in such cases this causality is not an established fact, medical and other investigations post the suicide have often hinted at the possibility.

"Now when conducting the postmortem of this child, when examining the vaginal area, the doctor will find out that the child was a victim of sexual atrocity. When police go and investigate this suicide, the girl's mother will say: she had several friends, or she had one or two friends," but this case will not be followed as a rape case or a sexual atrocity case. So, the case will be closed based on the mother's statement that she committed suicide because she was scolded. Then, it closed as unnatural death and suicide because of the mother's scolding."

On being asked about how many such cases see comes across in a year, Soumya* said, "*I am not sure about it, but most such cases start through mobile phones and relations made through social media platforms,"* highlighting this as an area that needs attention.

Further, Soumya's interview reiterates the study's finding about social norms being deeply ingrained in the legal system even in the context of cases involving children. She highlights how lawyers often try to defend a case of sexual exploitation by trying to raise questions on the girl's 'character'.

"*The victim is a child aged 14 or 15 years old. First, they will try to form a black mark in the character of the girl. If that girl had a romantic relationship, they will try to expose it most at the time of the cross-examination they will continuously ask about her romantic relation, that person's name, the love story and all that. However, none of this is relevant because all of this is one's privacy.*

A person can have a relationship or a love affair; you can't tell them that groping or sexually harassing that person is ok, or you can't deny their right to file a case against sexual harassment because of having a relationship with someone... Then, when they ask these kinds of questions to children, they will lose their confidence, and kids will get scared very easily."

Concluding remarks

Credit: powerofforever/iStock

While the discourse around TFGBV is rapidly evolving, most of it is still around questions of surveillance, big tech, and data, with a lot of resources available in the English language. Conceptually, there is engagement with monolithic categories and broad-stroked analysis. While the manifestations of TFGBV might not be singular to regions, the study foregrounds the need to understand digital cultures and responses to TFGBV cases in the granular, in the local context, and from the perspective of the survivor. The difference in how the state of Kerala engaged with legal frameworks around TFGBV is a case in point. In the Indian context, further research into why regional variations in responses to TFGBV exist in the first place is needed.

There is a crucial need to ensure the safety of women and LGBTQI+ individuals who are disproportionately targeted in the online world, while also upholding the right to free speech and privacy, amongst other rights. Many more TFGBV cases likely exist than are officially reported or publicly known. This highlights the urgent need to increase awareness and understanding of TFGBV, particularly in rural and underserved areas.

> *"The way we communicate is also crucial. Specifically, what language do we use to explain what happened to a victim? Since much of this information is available in English, it raises the question: how do you talk about your experience of violation to seek support? Who do you turn to for help?"*
> **asks Jalaja*.**

Identifying and mounting multi-stakeholder engagements for effective and sustainable change is equally important. Five key stakeholders identified in interviews[46] as the biggest influencers in cyber laws, who can be targeted include:

- Law enforcement agencies that can ethically hack and solve cybercrime-related cases.
- Intermediaries, i.e., various online service providers as defined in Section 2(w) of the Information Technology Act.
- Technical experts who have thorough knowledge of the ins and outs of a system.
- Banking sector companies, online wallet companies, etc. that provide online money transaction platforms.
- NGOs working in this field (though the number is meagre), public prosecutors, lawyers, and judges.

Credit: PeopleImages/iStock

Recommendations

"We know technology runs much faster than appropriate legislation to come and that is why there is a clear constraint between law and technology, and hence the present subject requires a thorough techno-legal-experimental attitude and flair to solve various legal issues or problems."
Bivas Chatterjee, a Special Public Prosecutor and cyber law expert (Editor, 2018)

The study has produced a range of systemic-level recommendations to strengthen the legal and other redress mechanisms available to survivors of TFGBV. These recommendations can be broadly grouped into three key areas, namely:
(1) legislative and policy reform,
(2) building awareness and support systems, and
(3) strengthening research.

While this categorisation is intended to streamline the presentation of findings, it is important to note that many recommendations intersect across these domains.

3.1 Legislation and policy changes

1. Need to foreground the right to be forgotten

In the digital age, where intimate and identifying content can be rapidly and endlessly shared, survivors of TFGBV face immense challenges in reclaiming their privacy and dignity. The ability to have harmful content removed and prevent its further circulation is a critical form of redress. However, there is no specific law in the country that deals with the right to be forgotten. It is not statutory in the Indian context. The government of India should explicitly recognise and legislate the right to be forgotten as a statutory right, with particular emphasis on its relevance in cases of TFGBV. As an essential extension of the fundamental right to privacy, this right should enable survivors of TFGBV to request the removal of personal and objectionable content such as intimate images or identifying details from online platforms and search engines, regardless of the status of ongoing criminal proceedings.

In crafting the law, the government of India should consider and ensure the following:

- Survivor-centred approaches that allow for swift and confidential takedown procedures through both judicial and quasi-judicial bodies.
- Clear accountability obligations for ISPs and digital platforms to act on validated right to be forgotten requests in a timely manner.
- Non-discrimination in access to the right to be forgotten, especially for women, LGBTQI+ persons, and other marginalised survivors of TFGBV.
- Integration of the right to be forgotten into provisions of existing data protection and cybercrime frameworks, to ensure cohesive enforcement.
- Attention should be paid to the complexity and sensitivity of the issue owing to the potential challenges of balancing the right to be forgotten with other fundamental rights such as freedom of expression and the right to information.

A model for such legislation exists in the European Union's General Data Protection Regulation (GDPR), which formally enshrines the right to erasure under Article 17. This provision allows individuals to request the deletion of personal data where it is no longer necessary for the purpose it was collected, or where the data subject withdraws consent. It has been successfully used in cases involving non-consensual sharing of intimate images, giving survivors a concrete legal path to reclaim control over their digital identities.

As illustrated by the testimonies of Divya and Rachna, the strengthening of this provision could go a long way in facilitating survivors' healing and pursuit of justice.

2. Generation of an online media ethical code

There is an urgent need to develop and implement a robust ethical code for online media that protects individuals against harm while safeguarding freedom of speech and expression as a cornerstone of democracy. This requires meticulous and methodical work and political will.

As Divya, based on her experience, pointed out,
"They claim this is an online news channel. There are about 120 entertainment channels in Cochin alone. News channels comprise almost double the number of entertainment channels. None of them (who have set up such channels) have done a journalism course or know anything about journalism. If you have an email ID, you can set up a channel from your house. No capital is needed to set up something like that, and if you have viewership for your channel then you make money. Satellite channels, for example, have a lot of restrictions. Online media has no such thing. Moreover, some act as one caucus and systematically target people."

The problem is not limited to Kerala, where Divya resides, but exists across India. A review of the content of self-styled YouTubers moonlighting as online journalists shows that almost all their content is mostly homophobic, misogynistic, and deeply regressive. Women and LGBTQI+ people, in particular, become soft and easy targets for them. The vast popularity of these personalities speaks to how deeply entrenched social norms around gender and sexuality are in society.

Accordingly, there is a need to develop and enforce a comprehensive ethical code for online media platforms. This code should include safeguards against harmful, discriminatory and unethical content, particularly that which targets women and girls in all their diversity, whilst upholding the principles of freedom of expression and access to information, including freedom of the press. Implementing clear standards, registration mechanisms and oversight structures, alongside public education on theical journalism, would curb TFGBV and other online harms while protecting democratic functions of the media.

3. Need for restorative forms of justice

Integrating restorative justice mechanisms into India's criminal justice system, especially for TFGBV cases, is necessary.

The Indian criminal justice system is increasingly veering towards punitive measures as opposed to restorative forms of justice and healing, as evident in the recent RG Kar case[47] that shook the country. None of the survivors or lawyers interviewed for this report could point out a single experience wherein they had received mental or physical support from the system, while pursuing their cases.

Several key stakeholders across different levels of government, the judiciary, and civil society must take action to integrate the restorative justice system. Drawing from international good practices, such as those used in the Netherlands[48], India should invest in survivor-centred approaches that prioritise harm repair, remedies and reparations, survivor agency, systems support, and legal accountability. This includes counseling services and survivor-led justice pathways.

4. Increasing intermediaries' accountability and responsiveness

There is a need to strengthen and enforce intermediary accountability under the Information Technology Act. This Act already mandates that intermediaries must take down unlawful content within 36 hours upon receipt of actual knowledge or a legal order from law enforcement. However, in practice, compliance is often delayed, inconsistent, or opaque, particularly in cases involving TFGBV.

To address this, there is need for the government of India to undertake the following:

- Create an independent grievance redress mechanism to hold intermediaries accountable for failure to act within the prescribed timelines.
- Mandate greater transparency from intermediaries through regular reporting on content moderation actions, particularly those involving gender-based harms.
- Support capacity-building for law enforcement and judicial officers on effectively using existing legal provisions, such as section 79 of the Information Technology Act, to compel intermediary action in TFGBV cases.
- CSOs can also provide digital literacy training on digital rights and advocate for platform accountability by documenting intermediaries' non-compliance when they help survivors file timely complaints, build coalitions, and engage in strategic litigation.

5. Addressing the hierarchy of cybercrimes

The goverment, in collaboration with state-level law enforcement agencies and judicial training institutions should prioritise sustained capacity building and sensitisation efforts for police, prosecutirs and judicial officers on the nature and impact of TFGBV. Strengthening insitutional understanding of TFBGV as a serious and evolving form of harm is essential to ensuring timely, survivor-centred and rights-based responses across the justice system.

Currently, cybercrimes involving financial loss often receive greater instutional attention and resources, while TFGBV cases are frequently deprioritised or mishandled. This reflects broader soci-culture norms that equate harm with economic loss and overlook the severity of gendered online abuse.

It is therefore critical for the government of India to consider undertaking the following:

- Integrate into exisiting capacity-building initiatives to challenge harmful stereotypes, promote trauma-informed approaches, and equip officials to respond effectively to the range of harms associated with TFGBV, including digital exclusion, reputational damage, re-traumatisation and the loss of education or livelihood opportunities.

- Conduct public awareness campaigns similar to those focused on financial cybercrimes should be developed to increase understanding of TFGBV among officials and the general public with the goal of promoting accountability, support for survivors, and access to justice.

3.2 Building awareness and support

6. Strengthening existing structures

Throughout the course of the study, a serious lack of information and awareness cutting across all actors including survivors, police personnel (especially cyber police), lawyers, and judges was noted. None of the participants in this study reported that they used the national cybercrime reporting portal or the toll free number to report TFGBV. On the portal, crimes can be reported either anonymously or with personal details. According to the majority of lawyers who participated in the study, the online complaint tracking option is non-functional.

Based on this, the government of India should consider the following recommendations:

- Invest in targeted awareness campaigns, especially in regional languages, to inform the public about the national cybercrime reporting portal and toll-free line, particularly women, girls, and LGBTQI+ individuals.
- Improve the functionality of the portal and toll-free line, ensuring that any complaint tracking system is user-friendly and reliable.
- Mandate regular, survivor-centred, and gender-sensitive training for actors such as cybercrime police and the judiciary on handling TFGBV cases.
- Ensure access to legal aid, counselling, and digital safety resources into the reporting process to support survivors.
- Develop and use a feedback mechanism to gather user insights and continuously improve.

7. Capacity building of lawyers, judiciary and cyber cell staff

Law enforcement agencies should prioritese capacity-building of personnel, including police officers, cyber cell officers and judicial actors, on TFGBV. This should include both technical traning on digital platforms, technological tools and legal frameworks relevant to TFGBV and sensitivity training to ensure survivor-centred and trauma informed engagement.

Efforts should also be made to actively recruit and induct younger, tech-savvy professional into cyber cells, as their familiarity with digital platforms and online harms can significantly enhance institutional responsiveness and effectiveness.

8. Developing understanding of electronic evidence

Law enforcement agencies, in collaboration with police training academies should prioritse ongoing training and capacity-building on the collection, preservation and admissibility of electronic evidence, particularly in cases involving TFGBV.

Although electronic evidence, including messages, emails, screenshots and metadata, is increasingly recognised by Indian courts as valid and critical, many officers lack the technical knowledge to identify and secure such evidence appropriately. Survivors are often left to bear the burden of collecting and preserving this evidence on their own without institutional guidance or support, which can compromise access to justice.

The following recommendations should be considered:

- Strengthening institutional responses and upholding survivor's legal rights through repeated and structured training across police forces on the legal standards, protocols and practical tools required for handling digital evidence.
- Ensuring that law enforcement is equipped to manage electronic evidence in a timely and professional manner is essential to improving case outcomes and building survivor trust in the justice system.

9. Enhancing budget and infrastructure resources

Along with capacity building, increasing budgetary provisions and infrastructure for cyber stations as well as opening up more digital forensic labs are critical. Current infrastructure remains insufficient in many states, as documented in a 2023 report by the Bureau of Police Research and Development.

To ensure a timely, effective and survivor-centred response to TFGBV, there is an urgent need to:

- Expand digital forensic capacity, equip cyber cells with high-end technology and conduct state-level assessments to determine the infrastructure needed to meet local case volumes and realities.
- Strengthen cyber infrastructure to improve access to justice and ensuring the legal system kepps pace with the evolving nature of digital harms.

10. The use of strategic litigation

Civil society is encouraged to undertake strategic litigation cases, working collaobratively with survivor-led and support organisations. Strategic litigation should be strengthened and supported as a tool to advance gender justice in cases of TFGBV. By identifying patterns across cases, engaging legal practioners and framing issues within a broader systemif context, strategic ligitation can help shift judicial attitudes, improve evidentiary standards and influence court practices. While policy reform is essential, strategic litigation offers a complementary pathway to address implementation gaps and promote survivor-centred jurisprudence.

3.3 Strengthen research

11. Relevant government ministries and research bodies should prioritise the development of a robust gender-sensitive research agenda on TFGBV, with a strong emphasis on local context, language inclusion and disaggregated data. Current national level data fails to capture the full scope and nuance of TFGBV, particularly as experienced by marginalised communities.

12. Relevant government ministries are encouraged to:

- Ensure that research move beyond national averages and include state-specific, language accessible studies that reflect regional realities, lived experiences and social norms influencing reporting. This will support and inform more effective policy and institutional responses
- Collect disaggregated data by gender, caste, class, age, ability, and location is essential for designing targeted interventions and monitoring impact.
- Invest in survivor-led and community-based research models, as these offer deeper insights into the social and structural drivers of TFGBV and the barriers to accessing justice.

Bibliography

African Development Bank Group. (2016). *Minding The Gaps: Identifying Strategies to Address Gender-Based Cyberviolence in Kenya.*

Alliance for Universal Digital Rights. (2023). *The Feminist Principles for Including Gender in the Global Digital Compact.*

Amnesty International. (2018, March 21). *Research: Toxic Twitter – A Toxic Place for Women.* Retrieved from Amnesty International: https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1-1/

Australian Government. (2024, June 13). *Trolling*. Retrieved from eSafetyComissioner: https://www.esafety.gov.au/young-people/trolling#

Bureau of Police Research and Development, Ministry of Home Affairs, Govt. of India. (2023). *Data on Police Organisations.*

Chibber, M. &. (2015, March 25). *A little reminder: No one in House debated Section 66A, Congress brought it and BJP backed it*. Retrieved from Indian Express: https://indianexpress.com/article/india/india-others/a-little-reminder-no-one-in-house-debated-section-66a-congress-brought-it-and-bjp-backed-it/

Digital Rights Foundation. (2018). *Cyber Harassment One Year Report, December 2017- November 2018.* Lahore, Pakistan: Digital Rights Foundation.

Duggan, M. (2014, October 30). *5 Facts about Online Harassment*. Retrieved from Pew Research Center: https://www.pewresearch.org/short-reads/2014/10/30/5-facts-about-online-harassment/

Dunn, S. (2020, December 7). *Technology-Facilitated Gender-Based Violence: An Overview.* Retrieved from Centre for International Governance Innovation: https://www.cigionline.org/publications/technology-facilitated-gender-based-violence-overview/

Editor. (2018, November 13). *Bivas Chatterjee, Special Public Prosecutor, Govt of WB, on Challenges in Cyber Law and Skills to Become a Good Cyber Lawyer*. Retrieved from SuperLawyer: https://superlawyer.in/bivas-chatterjee-special-public-prosecutor-govt-of-wb-on-challenges-in-cyber-law-skills-become-good-cyber-lawyer/

Equality Now & Thomson Reuters Foundation. (2021). *Ending Online Sexual Exploitation and Abuse of Women and Girls: A Call for International Standards.* Retrieved from Equality Now: https://equalitynow.org/resource/ending-online-sexual-exploitation-and-abuse-of-women-and-girls-a-call-for-international-standards

Express News Service . (2015, March 24). *Section 66A: Seven Instances of Alleged Abuse on Social Media*. Retrieved from Indian Express: https://indianexpress.com/article/india/india-others/section-66-a-instances-of-alleged-abuse-on-social-media-2324927/

Fathima, A. (2023, February 16). *Rana Ayyub is targeted online every 14 seconds, says an ICFJ study*. Retrieved from The News Minute: https://www.thenewsminute.com/news/rana-ayyub-targeted-online-every-14-seconds-says-icfj-study-173333

Gurumurthy, Vasudevan & Chami. (2019). *Born digital, Born free? A socio-legal study on young women's experiences of online violence in South India.*

Inter-Parliamentary Union. (2016). *Sexism, Harassment and Violence Against Women Parliamentarians.*

Iyer, Nyamwire and Nabulega. (2020). *Alternate Realities, Alternate Internets.*

Kantar & IAMAI. (2023). *Internet in India 2023.*

Lenhart, A. M.-F. (2016). *Online Harassment, Digital Abuse, and Cyberstalking in America.* New York: Data & Society Research Institute.

Mali, P. (2022). Privacy Law: Right To Be Forgotten in India. *NLIU Law Review*, 1-2.

Ministry of Health and Family Welfare, Government of India. (2019-2021). *NFHS 5, 2019-21*. Retrieved from Ministry of Health and Family Welfare, Government of India: https://mohfw.gov.in/sites/default/files/NFHS-5_Phase-II_0.pdf

Ministry of Social Justice and Empowerment, Government of India. (2025, March 10). Retrieved from Ministry of Social Justice and Empowerment, Government of India: https://socialjustice.gov.in/common/31548

National Human Rights Commission, India. (2021). *Constitutional and Civil Rights to Protect Scheduled Castes and Scheduled Tribes from Atrocities and The Law Against Witch Hunting.* Retrieved from National Human Rights Commission, India: https://nhrc.nic.in/sites/default/files/Civil%20Rights.pdf

Neilsen. (2022, May). Retrieved from Neilsen: https://www.nielsen.com/news-center/2022/nielsens-bharat-2-0-study-reveals-a-45-growth-in-active-internet-users-in-rural-india-since-2019/

NORC at the University of Chicago & International Centre for Research on Women. (2022). *Case Study: Technology-facilitated Gender Based Violence in India.*

Nyx McLean & Thurlo Cicero. (2023). *The Left Out Project Report: The Case for an Online Gender-Based Violence Framework Inclusive of Transgender, Non-Binary and Gender-Diverse Experiences.* Association for Progressive Communications .

Office of the United Nations High Commissioner for Human Rights et al. (2021). *Strategic Litigation for Gender Based Violence: Experiences in Latin America.*

Plan International. (2023). *Free to be Online?*

Q3 Strategy. (2024). *Decoding Technology-Facilitated Gender-Based Violence.*

Rajkumar, M. &. (2023). *The Judiciary's Tryst with Online Gender-Based Violence.*

Singh, R. (2023, October 20). *India News*. Retrieved from Business Standard: https://www.business-standard.com/india-news/obcs-decoded-how-backward-classes-in-india-were-categorised-and-recognised-123102000571_1.html

Special Rapporteur on violence against women and girls, its causes and consequences. (2018). *Report of the Special Rapporteur on Violence Against Women, its Causes and Consequences on Online Violence against Women and Girls from a Human Rights Perspective.*

SVRI. (2024, September 19). Retrieved from SVRI - Sexual Violence Research Initiative: https://www.svri.org/topic-specific-research-agendas/technology-facilitated-gender-based-violence-global-shared-research-priorities/

Thomas, L. S. (2020, November 23). *[BREAKING] Section 118A: Amid backlash, Kerala Government backtracks on controversial amendment to Kerala Police Act*. Retrieved from Bar and Bench: https://www.barandbench.com/news/s118-a-kerala-police-act-implemented-kerala-govt-pinarayi-vijayan

Transform. (2023). *Technology-Facilitated Gender-Based Violence as an Attack on Women's Public Participation: Review of Global Evidence and Implications.*

Udwadia and Grewal. (2019). *Free to be Mobile.*

UN Women & World Health Organization. (2023). *Technology-facilitated Violence against Women: Towards a common definition, Report of the meeting of the Expert Group 15-16 November 2022, New York, USA.* Retrieved from UN Women: https://www.unwomen.org/sites/default/files/2023-03/Expert-Group-Meeting-report-Technology-facilitated-violence-against-women-en.pdf

UN Women and World Health Organization. (2023, March). *The State of Evidence and Data Collection on Technology-facilitated Violence against Women.* Retrieved from UN Women: https://www.unwomen.org/sites/default/files/2023-04/Brief-The-state-of-evidence-and-data-collection-on-technology-facilitated-violence-against-women-en.pdf

UNESCO. (2020). *Online violence Against Women Journalists: A Global Snapshot of Incidence and Impacts.*

UNFPA. (2021). *Making All Spaces Safe: Technology-Facilitated Gender-Based Violence .*

UNFPA. (2022). *16 Days of Activism Against Gender Based Violence*. Retrieved from United Nations Population Fund: https://www.unfpa.org/thevirtualisreal-background#glossary

University of Melbourne & United Nations Population Fund. (2023). *Measuring Technology-Facilitated Gender-Based Violence. A Discussion Paper. .*

Annexure 1

Reporting GBV, including threat-based GBV, to the authorities.

- A crime can be reported to any police station and by calling the Police Control Room number (100). The police cannot refuse to register a First Information Report (FIR) on the grounds of jurisdiction, and the police are duty-bound to register the complaint in the form of a Zero FIR.[49]

- There is no separate treatment of TFGBV and other types of GBV in law, at this stage or any stage of a criminal case.

- The Bharatiya Nagarik Suraksha Sanhita (BNSS), which has replaced the Code of Criminal Procedure, 1973 (CrPC) sets out procedures that the police and courts must follow in proceedings of a criminal case. It makes minor changes to the criminal procedure here, by providing that a complainant may not have to go to the police station to report an offence. It also mandates that a female police officer record complaints under Section 75, BNS (Sexual Harassment). These changes minimally impact the process of initiating a criminal complaint.

- Any person can report a crime regarded as a cognisable criminal offence (serious criminal offence) to the police - not only the person to whom it happened or a witness to the crime but anyone who has knowledge that it took place. Sexual offences are all cognisable offences, and the police are duty-bound to register any complaint about a sexual offence as an FIR, irrespective of the person making the complaint. They also have the authority to immediately start investigations and make arrests (without needing permission from a judge/a warrant), in the case of all cognisable offences.

- A person can approach the police by going physically to their nearest police station or the closest "beat chowki." The "beat chowki" in charge should forward the complaint to the local police station while informing the person reporting the crime.

- There are also Mahila (women) police stations across India that are staffed largely with women police officers and specifically meant to cater to crimes against women, in addition to women's helplines in several states/districts.

- Police cannot refuse to register an FIR after receiving a criminal complaint that alleges that any cognisable offence has taken place; they are duty-bound to register an FIR right away.[50] The Supreme Court has unequivocally held that the police cannot question whether the information is genuine if it describes a cognisable offence. The police must write down what the person giving the information is telling them and register an FIR based on it. They are not permitted to do any preliminary enquiry before registering an FIR in the case of any cognisable offence.[51]

- The BNSS provides remedies at two levels to enable complainants to get their FIRs registered, if the police illegally refuse to do so. A written complaint can be made to the district Superintendent of Police ("SP," hereafter) (the police chief of the district). The SP can order the Officer-in-Charge of the concerned police station to register an FIR. In urban areas, a complaint can also be made to the Deputy Commissioner of Police ("DCP" hereafter) (head of police districts in urban areas).[52] Secondly, an application can be made by the complainant in the court of the area Judicial Magistrate asking the court to order the police to register the complaint as an FIR and start their investigation.[53] A criminal complaint can also be filed against offending police officers who refuse to register FIRs.[54]

- Following the registration of an FIR, the police are duty bound to provide the complainant with a copy of the FIR and begin their investigation.[55] Investigation entails finding and recording statements of witnesses, search for/of any relevant property (including electronic devices), seizure of any relevant property (including electronic devices), arrest of any accused/suspected person(s) for the police to speak to them and investigate if they committed the offence(s) (this can include their continued stay in judicial custody (jail/prison) beyond the police's need to speak to them in the case of cognisable offences for the safety of the complainant/witnesses etc.). Arrest and the remaining of any accused in custody is also dependent on the police's timeline, and efficiency, of investigation as, if they fail to file a chargesheet within a fixed period (differs depending on the offence), any accused in the case can be released on bail, as is part of their right against long/endless pre-trial detention when they have not been charged with any offence(s).

- Broadly, the investigation of a criminal offence entails the following:

  - Police visit any place of offence (in the case of TFGBV, they would "visit" the offending website/look at the content etc) to ascertain the facts and circumstances of the case

  - They collect evidence, find out who was witness to the crime, and arrest any suspected offender(s). Collection of evidence relating to the commission of the offence may consist of:

    - Examination of various persons including the accused, reduction of their statements into writing if the police officer thinks fit for court record

    - The search of places or seizure of things considered necessary for the investigation or trial

  - Assessment of whether there is sufficient evidence for trial, and if so, taking the necessary steps for the same by filing a charge sheet (this is when the investigation ends)

- The primary objective of a charge is to give accused persons full information about the entire details of what crime they have been accused/charged of committing to enable them to prepare their best defence against it, as is crucial to the right against wrongful incarceration.

- Between the registration of an FIR and the trial of the case (the court hearing the matter), there are numerous places where a case may be closed, either because the police are not able to find enough evidence to charge any accused person(s) with committing the crime or the complainant turns "hostile" (decides they do not wish to pursue the case anymore and either stop responding to the police and cooperating or may inform the police informally that they do not wish to pursue the case). While there are timelines for cases to be investigated and concluded given in the BNSS, these are not mandatory and are rarely, if ever enforced, often making it hard to ensure that the complainant(s) and witnesses in criminal cases even remain physically available to continue pursuing the case. Procedural inadequacies in the investigation and collection of evidence by the police may also result in the lack of a charge being able to be formed against an accused, or in an acquittal.

- While the burden for conviction of an accused is high (against all reasonable doubt), their acquittal can take place for a variety of reasons, including procedural reasons.

- Post acquittal/conviction, appeal procedures open up for both the prosecution and defence, and involve appealing before higher criminal courts, which can eventually result in a case reaching the Supreme Court (at the highest level).

Annexure 2

Information on cyber cells and cybercrime infrastructure in India

- The Government of India runs a National Cybercrime Reporting Portal under the Ministry of Home Affairs. "Cybercrimes," at large, can be reported on this portal, with a separate user interface/space for reporting crimes against women and children. The Portal also runs a national cybercrime helpline, as part of its initiatives. This press release from the Ministry of Women and Child Development from 2014 is interesting to read.

- Complaints can be made on the portal either anonymously or with the complainant's identifying details, in cases of crimes against women and children. Complaints filed can also be tracked online. However, many lawyers report that the tracking system is non-functional. Four categories of complaints can be made on the portal for crimes against women and children:

  - Complaint regarding CSAM (child sexual abuse material)
  - Complaint regarding sexually abusive content/ content featuring rape
  - Complaint regarding "Sexually explicit act"
  - Complaint regarding "Sexually obscene material"

- The Ministry of Home Affairs has also established the Indian cybercrime Coordination Centre (I4C)[56] as a part of this ecosystem "*to act as a nodal point at National level in the fight against cybercrime*." Further, "*It aims to provide a platform to deal with cybercrimes in a coordinated and comprehensive manner. One of the important objectives of I4C is to create an ecosystem that brings together academia, industry, public and government in prevention, detection, investigation and prosecution of cybercrimes.*" This includes a "volunteer programme" where "*Good Samaritans are welcome to register as cybercrime Volunteers in the role of Unlawful Content Flaggers for facilitating law enforcement agencies in identifying, reporting and removal of illegal / unlawful online content*."

- In 2016, the Ministry of Home Affairs in partnership with the Ministry of Women and

- Child Development developed the Scheme for cybercrimes Prevention against Women and Children. This initiative includes an online reporting programme for addressing and resolving cybercrimes, sanctions for a forensic unit, a capacity-building unit to assist and improve law enforcement responses, a research and development unit to improve technology, and an awareness creation unit to disseminate education and awareness campaigns.[57]

- Courts have also been established in various districts to specifically deal with cybercrimes of all kinds, including online fraud, intellectual property-related crimes etc., and not necessarily TFGBV.[58]

- Some states have also been using funds under the Nirbhaya Fund for Safe Cities to address TFGBV.[59]

Annexure 3

Indian case law relevant to TFGBV

1. In *Justice K S Puttaswamy (Retd.), and Anr v. Union of India and Ors., WP(C) 494 of 2012*, a landmark judgment on the right to privacy and its contours under Article 21 of the Constitution of India, the Supreme Court recognised that the right to bodily integrity and informational privacy are integral parts of the right to privacy. (Feminist critiques of the right to privacy are well-documented[60] – the framework of privacy is often used to shield abusers and control women's sexuality, in addition to making it harder for marginalised groups to navigate bodily autonomy and expression alongside the need to receive protection from harm.)

2. In *In Re: Prajwala Letter Dated 18.2.2015 Videos Of Sexual Violence And Recommendations, SMW (Crim) 3 of 2015,* the Supreme Court of India directed Google, Facebook, and WhatsApp to remove access to rape and child sexual abuse material from their platforms. The court also directed these intermediaries to utilise AI systems to screen and delete content at the point of uploading, if it contained rape or child sexual abuse material . Moves such as these have been criticised for bearing the possibility of over-censorship and therefore, violation of freedom of speech.[61]

3. In *State of West Bengal v. Animesh Boxi @ Ani Boxi, Case No. GR: 1587/17, order dated 07.03.2018 (Court of Judicial Magistrate, First Class, 3rd Court Tamluk, Purba Medinipur, West Bengal),* the complainant had sent "personal private photos" (court's language) to the accused. When he asked her to meet him, and she refused, he threatened to post her pictures on social media. The accused also hacked her phone and uploaded more intimate photos and videos from her phone on Pornhub, with clear identifying details of the complainant – her name, her father's name, and her nickname. The victim came to know about this as her brother found her videos on Pornhub. This case is significant as the first judgement on "revenge porn" resulting in a conviction.

   In March 2018, the accused was convicted of offences under Sections 354A (sexual harassment), 354C (voyeurism), 345D (stalking) and 509 (insulting the modesty of a woman) of the IPC and Sections 66E (violation of privacy), 66C (identity theft), 67 (electronically publishing obscene material) and 67A (electronically publishing material containing sexually explicit act) of the IT Act. He was sentenced to five years imprisonment along with a fine of Rs. 9,000. The Court held that the absence of bodily harm to the victim was immaterial as injury to reputation was deemed 'injury' under Section 44, IPC. The prosecution relied on both electronic evidence and witness testimony. The electronic evidence included the accused's mobile number, which was listed as the registration number of the PornHub account through which the video was uploaded; the IP address, which indicated that the SIM card used to upload the video was registered in the accused's name; and the email and porn website user accounts in the accused's name through which the video was uploaded.

   In its judgment, the court referred to this as a person undergoing "virtual rape" every time a person views such imagery of theirs online, saying, "*Even forsake the contents are removed from the virtual world but what will happen if anybody had already downloaded those and again it will spread in the virtual world and it will never end and virtual rape will be committed against the victim till the last day of her life*." (for clarity, "virtual rape" is not a legal term or an offence in Indian law) The court also defined the term "revenge porn"[62] in its judgment. Despite the terminology used by the Court being less than satisfactory and not legally accurate, the judgement is a rare example of progress within the Indian justice system, where the law is applied to the facts of the case, without questioning morals or victim blaming. . The Court also correctly identified that the harm experienced by the victim is continuous and repeated, which the victim also expressed before the Court in her testimony.

4. In *Mrs. X. v. Union of India, W.P.(CRL)1505/2021,*[63] the Delhi High Court held that intermediaries are required to remove all offending information from their platforms, including re-uploads of the same content/the same content in the case of non-consensual intimate imagery, not just the links of offending content provided by a complainant. In this case, photos of the complainant, Mrs. X, had been uploaded by a third party she had met online and then once in person. The accused threatened to leak Mrs. X's photos, that he had access from her phone during their meeting, and kill her son, if she did not pay him money. After Mrs. X had given him jewellery and emptied her bank account, he still uploaded her images online.

Starting in August 2021, Mrs. X made numerous attempts to have the images removed. She filed a police complaint against the accused on the grounds that he had made a YouTube channel in her name and posted daily explicit videos and photographs of her. In addition, she approached Google, Microsoft, Bing, YouTube and Vimeo seeking the removal of the posts, and filed complaints with www.cybercrime.gov.in. All these attempts were unsuccessful. As a result, Mrs. X approached the Delhi High Court seeking a court order directing that the links with her images be blocked by the concerned intermediaries. Mrs. X flagged that despite consistent efforts to remove the images, they kept being re-uploaded.

The court recognised how victims/survivors needing to keep searching the internet for new uploads of non-consensual intimate imagery involving them could cause trauma and appointed Sr. Adv. Saurabh Kirpal as amicus curiae (a legal expert to assist the court) to draft guidelines/directions for intermediaries to follow to ensure that non-consensual intimate images are not re-uploaded. In March 2022, the Delhi High Court found that the accused had been arrested in another case, and his laptop had been seized by the police with 83,000 non-consensual intimate images of women, including Mrs. X, and hence the offender could no longer re-upload Mrs. X's images. However, the court decided to keep the case alive "*to ensure that the victims like [Mrs X] are not forced to approach the authorities/ intermediaries including the search engine repeatedly for removal of any offending content.*"

In its directions, the Court held that under Indian law intermediaries are required to undertake "reasonable effort" to ensure that their users do not post "obscene" content. The Court also held that intermediaries must undertake "reasonable effort" to ensure that reposted offending images are removed without being approached by survivors/victims afresh each time. Without reasonable effort by intermediaries concerning such content, they would not be entitled to safe harbour protection under the law.

The Court also defined "non-consensual intimate imagery," noting that "revenge porn" is a colloquial term but does not cover many kinds of non-consensual intimate imagery that may be uploaded online. It also recognised the broader "life disruptions" that the dissemination of such content can have on a person's life, including job loss and rejection by their family/ society. The Court described the uploading of non-consensual intimate imagery in the present case as a "clear violation of the provisions of the IT Act and IT Rules ... [and] a violation of the right to privacy," specifically informational and communicational privacy, referring extensively to the right to privacy as enshrined by the Supreme Court in *Puttaswamy v. Union of India*. The Court concluded by giving broad recommendations, which are not binding, for the police and intermediaries to follow to specifically deal with the distribution of non-consensual intimate imagery, including more robust complaint mechanisms and more proactive monitoring and action by the police and intermediaries in such cases.

5. In *Rout v. Union of India, BLAPL No. 4592 / 2020,*[64] the High Court of Odisha rejected a bail application of an accused who had raped a woman, his classmate from college, and then uploaded a video of the incident on Facebook. After the police intervened, the accused deleted the video, which he had uploaded through a fake profile bearing the victim/survivor's name. The accused was charged with various offences under the IPC including rape (section 376), distribution of obscene content (section 292), forgery (section 465), forgery to harm reputation (section 489) and outraging a woman's modesty (section 509). He was also charged under the IT Act with computer-related offences (section 66), identity theft (section 66C), publishing obscenity (section 67), and publishing sexually explicit content (section 67A).

While rejecting bail, given the heinousness of the crime, the Court observed that the right to be forgotten is an integral component of the right to privacy and must be available to victims/survivors in such contexts by way of mechanisms to delete offending content from intermediary platforms. The right to be forgotten has come up in numerous contexts within the Indian justice system,, and there is no settled legal position on it.[65] The Court held that in situations where a victim/ survivor's privacy has been seriously violated, the victim/survivor or the prosecution can request courts to have the offending content removed from public platforms, regardless of ongoing criminal proceedings. The Court commented that "information in the public domain is like toothpaste, once it is out of the tube one can't get it back in and once the information is in the public domain it will never go away." (paragraph 5) Interestingly, it noted that the criminal justice system and Indian law are focused on sentencing and punishment, not redressing the harm and trauma caused to victims/survivors of sexual violence. It also observed that it is unreasonable to expect victims/ survivors to approach courts to get all offending content taken down as the legal system can often be "confusing," "complex," and "intimidating."

While the Court did focus on the issue of consent in data processing and collection when examining the facts of the current case, it stated that consent is not a factor in this case because "no person, especially a woman, would willingly reveal and portray the ambiguous aspects of their character."

6. In *X v. YouTube, CS(OS) 392/2021,*[66] the Delhi High Court upheld an actor's right to privacy, directing various internet intermediaries and websites to takedown explicit videos of the actor available on multiple video-sharing platforms without her consent. The actor said that the videos had been recorded as part of her audition for a role in a web series. As the producer of the videos took down the videos on the actor's objection, the Court found that the actor's consent to have these videos online had been explicitly withdrawn. Despite the removal of the content by the producer, 36 websites/platforms (arrayed as defendants in this case by the actor concerned) continued to have the videos up. Some of the videos were also edited to add obscene, objectionable and pornographic commentary. As a result of these videos circulating on the internet, the actor faced constant harassment by anonymous callers and sought protection from having this content on the internet from the Delhi High Court.

   Although the Court acknowledged the absence of a statutory right to be forgotten, it ultimately concluded that the actor's right to privacy should be safeguarded, given the evident and immediate impact on her personal and professional life, as well as the irreparable harm caused by the non-consensual circulation of videos depicting her in a sexual manner. An interim order was passed by the Delhi High Court against the defendants, directing them to take down all the offending videos, within 36 hours of the order being passed.

7. In *X v. Union of India, W.P.(CRL) 1082/2020,*[67] the Delhi High Court was concerned with a case of a woman whose photographs had been taken from her social media accounts and published on a pornographic website. The photos were not "intimate" or "sexual" in nature but were taken from the woman's private social media accounts without her consent and uploaded on this website. Following the failure of the police to act within a week, the woman approached the High Court for relief. By this time, the photos had been viewed over 15,000 times. The Court highlighted that the photographs were not obscene or offensive in themselves, but as they had been taken from her social media accounts without her consent, to be uploaded on a pornographic website alongside "derogatory captions", publication of the photographs constituted an offence under section 67, IT Act as the "only purpose of posting the petitioner's photograph on a pornographic website could be to use it to appeal to the prurient interests of those who are likely to see it." (paragraph 85) It added that the publication of these images would likely result in "ostracisation and stigmatisation" of the woman, which required an "immediate and efficacious remedy."

   During interim proceedings, the Cyber Prevention Awareness and Detection Unit submitted before the court that because of technological constraints, it couldn't guarantee to the court that it could eliminate the photos from the internet. The court issued an interim order for the removal of the photos, but the woman informed the court that the photos had been reposted on other websites, rendering the interim order ineffective. The police also stated that while law enforcement requests intermediaries for information or the removal of content, intermediaries do not always cooperate. Following this, the Court redirected platforms to remove the photos and issued various directions to the police and intermediaries to follow in the case at hand to assist the woman in ensuring her photos remain off the internet.

Annexure 4

Guiding questions for in-depth interviews with survivors:

Note: The points mentioned in brackets are points for the interviewer to probe on.

1. Personal details:
   - Age
   - Gender
   - Place of residence (family, migration due to job/ education?)
   - What do you do? (education, career)
   - Caste
   - Religion
2. What are the technological mediums you use for communication? (sole/shared ownership)
3. Do you use the internet? If yes, since when?
4. What do you use the internet for? What platforms do you use?
5. Can you tell us about the violence you faced online/on a technological medium?
   - What happened?
   - Where did it happen?
   - Who was the perpetrator? (multiple, anonymous, not based in India—follow up tailored basis this)
   - How did it impact you/your life?
   - How has it impacted your experience of using the internet/these technological mediums?
   - When/how did you realise that what was happening to you was violent/abusive/exploitative? How did you make sense of it/understand it?
   - What have been the sources for you to get information about such violence?
6. Did you share about it with someone?
7. Did you want to seek support?
8. What kind of support did you want?
9. Did you seek support?
10. Did you want to report the violence? (what encouraged you, what stopped you)
11. Were you aware about the various reporting options available to you? (information sources)
12. Who did you report to?

(Note: If the participant does not mention legal recourse, specifically probe about that— awareness, access, what prevented them etc. And if a participant mentions legal recourse probe about various aspects such as filing an FIR/ experience with police/at police stations, expectations from the legal system, evidence, accessing lawyers, experience in the courts etc.)

13. How was the experience of reporting the violence?
14. Was the perpetrator punished?/ Did you feel you got justice? Did it help you?
15. Are there laws for such forms of violence? If yes, can you tell us about the ones you're aware of?
16. Do you know other people who have faced such violence? (If yes, probe on what, where, by whom, did they report—as many details as they know and are comfortable sharing)
17. Do you think your socio-economic identities (gender, caste, where you are located etc.) played a role in the violence you faced and your access to legal remedies?
18. What are your thoughts on our legal system? Is the experience of accessing the legal system in our country the same for everyone?
19. As you reflect back on your experience, what are some things that you think can help people who face such violence?

Guiding questions for key informant interviews:

Police officers/Cyber cell officers:

1. cybercrime has become an important issue in the last few years. Why do you think that is the case?
2. What kind of acts get covered under cybercrimes in India?
3. Can you give us a broad sense of the kinds of cybercrimes that get reported?
4. What are the kinds of cases that women or people from the LGBTQI+ community report? (their understanding/ perception of these cases)
5. Who is/are the perpetrators in such cases?
6. Could you give us a rough estimate of the number of cybercrime cases that get reported in your station in a year? Specifically cases that are gender based?
7. Has the reporting of such cases increased over the years? If yes/no, what do you think is the reason?
8. Are all police officers trained to deal with such cases? Or only some?
9. Is the procedure for dealing with these reports different? Or the same as other crimes?
10. Are cyber cells present across all police stations?
11. What is your understanding/assessment of cybercrimes in India?
12. When women/people from LGBTQI+ community come in to report such crimes, what do you think they expect from the police?
13. Are there challenges that the police face in dealing with such cases? (evidence - jurisdiction, identifying relevant sections of the law, evidence etc)
14. The people who report such cases, what socio-economic groups do they generally belong to? Have you had any observations on this?
15. Do you think these cases happen in specific parts of India?
16. How do these cases impact the women/people from LGBTQI+ community who face them? (online offline continuum of violence)
17. According to you, what can help police officers be more equipped to deal with such cases?
18. What are the terms that people use while reporting these cases? What is the terminology that the police use for these cases?

Lawyers:

1. What type of cases related to technology facilitated/online gender-based violence have you seen being reported to the police, taken to court?

2. What are the types of such cases that you have handled?

3. Is the law comprehensive enough to address the various types of such cases that get reported? Is the law and our justice system equipped to deal with such cases considering their ever-evolving nature?

4. What sections of the law related to such crimes are used the most and least?

5. Has the reporting of such cases increased over the years? If yes/no, why?

6. How many such cases do you deal with in a year?

7. How long do these cases go on for?

8. What is the general trajectory of these cases?

9. What is the person who reports such violence generally expecting?—Based on the cases that you have handled.

10. How do these cases play out in court?

11. Is it challenging to deal with such cases? If yes, why and what makes them challenging? (jurisdiction, evidence etc.)

12. Who is/are the perpetrators in such cases?

13. What socio-economic groups do people who report such cases generally belong to? Where are they located?

14. How do these cases impact the women/people from LGBTQI+ community who face them?

15. What prevents people from seeking legal remedies for such cases? What helps people in seeking legal remedies for such cases? (access, awareness, the process, cost, time)

16. What do you think needs to be done to better support people who face such violence?

17. Have there been any critical judgements that act as legal precedents in courts with regard to such cases?

18. What is the terminology being used in the legal space while discussing such cases?

Civil Society Organisations working on the issue:

1. Can you give us an overview of the work you do on the issue of technology-facilitated/online gender-based violence?
2. What is the terminology you use while working on these issues?
3. How has the discourse around these forms of violence evolved over the last few years?
4. What are the forms of TFGBV/OGBV you have come across in your work?
5. How do these forms of violence impact women in all their diversity?
6. How have you seen a person's other socio-economic identities like caste, location etc. play into them facing this violence or reporting such violence?
7. Do you think the laws in India that deal with such forms of violence are adequate and effective?
8. What is the kind of support that people who have faced such violence are looking for? (in case they have directly worked with survivors)
9. What are the various reporting mechanisms available to people for such violence? How effective are they? (platforms, police, workplace)
10. Who is/are the perpetrators in such cases?
11. Do you know people who have sought legal remedies for such cases? What has their experience been?
12. What prevents people from seeking legal remedies for such cases? What helps people in seeking legal remedies for such cases? (access, awareness, the process, cost, time)
13. What do you think needs to be done to better support people who face such violence?

Endnotes

1 In India, cyber police officers are tasked with handling cybercrimes and work within various law enforcement agencies at the state and national levels. https://cyberpolice.nic.in/

2 University of Melbourne – United Nations Population Fund (2023). Measuring technology-facilitated gender-based violence. A discussion paper https://findanexpert.unimelb.edu.au/scholarlywork/1737738-measuring-technology-facilitated-gender-based-violence--a-discussion-paper

3 Transform. (2023). Technology-Facilitated Gender-Based Violence as an Attack on Women's Public Participation: Review of Global Evidence and Implications.

4 UNFPA. (2021). Making All Spaces Safe: Technology-Facilitated Gender-Based Violence. Mentioned in the bibliography

5 UNESCO (2020). Online violence Against Women Journalists: A Global Snapshot of Incidence and Impacts https://unesdoc.unesco.org/ark:/48223/pf0000375136

6 https://plan-international.org/uploads/2023/06/SOTWGR2020-CommsReport-edition2023-EN.pdf

7 The United Nations Committee on the Elimination of Discrimination against Women, 1979. https://www.un.org/womenwatch/daw/cedaw/cedaw.htm

8 General recommendation No. 35 (2017) on gender-based violence against women, updating general recommendation No. 19 (1992). https://digitallibrary.un.org/record/1305057?ln=en&v=pdf

9 P.5, CIGI paper. In 2014, thousands of people in the games community began to systematically harass, heckle, threaten, and dox several outspoken feminist women in their midst, few of whom were journalists. The harassment occurred under the social media hashtag "Gamergate".The misogyny rampant in the gaming world is a growing area of research and activism. One of the survivors we spoke with for this study gave us a sense of how this problem is manifesting in India.

10 The term "revenge porn" is commonly used while referring to image based sexual abuse. This study will refrain from using this term as the use of the term pornography instead of sexual abuse suggests a degree of consent from victim(s). Further, the research shows that such abuse is not just a spiteful action of an ex lover but motivations may vary including coercion in domestic violence situations, malice, bullying and harassment. (Equality Now)

11 A company or individual that offers technology-related products and services to businesses and consumers

12 In India, cyber police officers are tasked with handling cybercrimes and work within various law enforcement agencies at the state and national levels. https://cyberpolice.nic.in/

13 Cyber cell expert refers to individuals with specialised technical skills in cybersecurity, who may or may not be directly employed by the police

14 Currently as per sector standards and practices, data is typically stored for 3 years. India's data protection law, The Digital Personal Data Protection Act (DPDP), which provides certain guidelines and timeframes around this (basis nature and purpose of data collected) is yet to be enforced despite having been passed by the government in August 2023

15 Bois Locker Room was an Instagram group of which members were sharing images of their classmates and other underage girls without their knowledge or consent along with crude comments ranging from body shaming to jokes on sexual assault and rape. https://www.bbc.com/news/world-asia-india-52541298

16 All names used in the report are pseudonyms to protect the interests of the study participants

17 A festival in some parts of North India where married women fast for the safety and longevity of their husbands.

18 Adivasi communities of India are the Indigenous or tribal peoples who are considered the original inhabitants of the Indian subcontinent. They belong to the Scheduled Tribes community.

19 The efficacy of legal notices to thwart further damage and quickly address TFGBV is another finding of the study. This will be discussed later in the report.

20 Though technically the agreement had no validity in law but they had drawn it up so that it was taken seriously.

21 The perpetrator had also sent it to people, so the team had to go through all chats and delete them but as the lawyer points out, "there's always a chance that it will turn up somewhere."

22 All names used in the report are pseudonyms to protect the interests of the study participants

23 We consciously decided not to contact this person in the interest of larger ethical considerations. The woman had recently managed to move on after the Mumbai police closed all legal matters concerning her. We didn't want to possibly risk a trigger wherein she would be left more vulnerable.

24 *Shreya Singhal v. Union of India* AIR 2015 SC 1523

25 Express News Service, 2015

26 *118 A. Punishment for making, expressing, publishing or disseminating any matter which is threatening, abusive, humiliating or defamatory. Whoever makes, expresses, publishes or disseminates through any kind of mode of communication, any matter or subject for threatening, abusing, humiliating or defaming a person or class of persons, knowing it to be false and that causes injury to the mind, reputation or property of such person or class of persons or any other person in whom they have interest shall on conviction, be punished with imprisonment for a term which may extend to three years or with fine which may extend to ten thousand rupees or with both."* (Kerala Police Amendment Ordinance, 2020)

27 Geoffrey Andare v Attorney General & 2 others [2016] KEHC 7592 (KLR) (Kenya)

28 47 U.S.C. § 223(a)(1)(C) of the Communications Act of 1934, as amended by the Communications Decency Act of 1996.

29 https://docs.un.org/en/A/78/288

30 https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/38/5

31 https://cdn.internetdemocracy.in/idp/assets/downloads/reports/un-srvaw-report/Internet-Democracy-Project-Submission-Online-VAW-2-November-2017-4.pdf

32 https://www.npr.org/2021/10/23/1048746697/facebook-misinformation-india; https://www.nytimes.com/2021/10/23/technology/facebook-india-misinformation.html; https://edition.cnn.com/2021/10/26/tech/facebook-papers-language-hate-speech-international/index.html; https://www.reuters.com/article/world/facebooks-flood-of-languages-leaves-it-struggling-to-monitor-content-idUSKCN1RZ0DL/; https://restofworld.org/2021/newsletter-south-asia-facebooks-language-problem/

33 For instance, Google argued this in *Subodh Gupta v. Herdsceneand*, CS (OS) 483/2019 (Delhi High Court) and *Mrs. X. v. Union of India*, W.P.(CRL)1505/2021 (Delhi High Court)

34 L.M. Hinman, "Searching Ethics: The Role of Search Engines in the Construction and Distribution of Knowledge" argues that Google, for instance, is not just a conduit for access to knowledge but plays an active role in knowledge creation, today.

35 *Shreya Singhal v. Union of India* AIR 2015 SC 1523

36 This is from my experience of filing RTIs seeking copies of orders under Section 69 during my time at the Internet Freedom Foundation

37 The IT Rules create an additional category of "significant" social media intermediaries, which are social media intermediaries that have a certain minimum number of subscribers, as notified by the Central Government. (All prominent social media platforms like Facebook, Instagram, WhatsApp, X fall within this category)

38 https://www.onmanorama.com/content/mm/en/kerala/top-news/2023/08/21/in-a-first-kerala-police-files-criminal-case-against-facebook.html

39 https://www.indiacode.nic.in/bitstream/123456789/15338/1/scheduled_castes_and_the_scheduled_tribes.pdf

40 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, pp. 1–88)

41 *Rout v. State of Odisha* BLAPL No.4592 OF 2020

42 See paragraph 5 of the judgement

43 The Indian state recognised the Indian caste system and introduced reservations to mitigate and challenge these deep seated discriminatory practices emanating from caste and tribal status. Scheduled Castes and Scheduled Tribes are social categories acknowledged by the state and many dalit and tribal communities comprise the list.

44 Her mother rears some livestock while her only brother suffers from drug addiction and has been in a mental health facility for nearly 14 years. There is barely any larger family support as her parents had an inter caste marriage- her father was tribal Malayan while her mother is an upper caste Roman Catholic. Her case is being dealt on a pro bono basis by the Kochi lawyer.

45 The husband in turn came from a violent family where his mother had committed suicide unable to withstand her husband's physical torture

46 For example, these groups were identified in an interview with an online portal, Bivas Chatterjee, Special Prosecutor, cybercrimes with the West Bengal government

47 https://www.ndtv.com/india-news/aparajita-bill-rg-kar-medical-college-rape-murder-explained-mamata-banerjees-new-law-for-death-penalty-in-rape-cases-6481371

48 For instance, a 2017 legislative initiative proposed embedding restorative justice as a formal element within the Dutch Code of Criminal Procedure (Article 51h), mandating mediation pathways and enabling victims to provide statements and seek reparations. See: https://www.maastrichtuniversity.nl/news/restorative-justice-should-be-further-integrated-criminal-law

49 Under erstwhile S. 170, Code of Criminal Procedure, 1973 (*State of Karnataka by Nonavinakere Police v. Shivanna @ Tarkari Shivanna*, 2014 (8) SCC 913 and affirmed in numerous other judgments by High Courts.)

50 Section 154, CrPC/Section 173, BNSS

51 *Lalita Kumari v. Government of Uttar Pradesh &Ors.,* AIR 2014 SC 187

52 Section 154, CrPC/Section 173, BNSS

53 Section 156, CrPC/Section 175, BNSS

54 Section 166A, IPC/Section 199, BNS

55 Section 154, CrPC/Section 173, BNSS

56 https://cybercrime.gov.in/Webform/cyber_volunteers_concept.aspx

57 https://www.mha.gov.in/en/division_of_mha/cyber-and-information-security-cis-division/Details-about-CCPWC-CybercrimePrevention-against-Women-and-Children-Scheme (Details on disbursal of funds have not been updated since 2018)

58 https://www.dnaindia.com/business/report-first-cyber-court-set-up-in-delhi-1277777

59 https://www.thehindu.com/opinion/op-ed/the-long-wait-for-safety/article61557981.ece

60 Anita L. Allen and Erin Mack, How Privacy Got Its Gender, University of Pennsylvania Law School Faculty Scholarship Paper 1309 (1991), https://scholarship.law.upenn.edu/faculty_scholarship/1309; PJ Patella-Ray, Beyond Privacy: Bodily Integrity as an Alternative Framework for Understanding Non-Consensual Pornography, 21(5) Info., Communication and Society 786 (2018).

61 https://cdn.internetdemocracy.in/idp/assets/downloads/reports/un-srvaw-report/Internet-Democracy-Project-Submission-Online-VAW-2-November-2017-4.pdf

62 The Court defined "revenge porn" as follows: "Sexually explicit images of a person posted online without that person's consent especially as a form of revenge or harassment. Revenge porn or revenge pornography is the sexually explicit portrayal of one or more people that is distributed without their consent via any medium. The sexually explicit images or video may be made by a partner of an intimate relationship with the knowledge and consent of the subject, or it may be made without his or her knowledge. The possession of the material may be used by the perpetrators to blackmail the subjects into performing other sex acts, to coerce them into continuing the relationship, or to punish them for ending the relationship."

63 Judgment available at: https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2023/06/smp26042023crlw15052021171217-470026.pdf

64 Judgment available at: https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2021/01/Official-Judgment.pdf

65 For instance, *Vasunathan v. The Registrar General, High Court of Karnataka* 2017 SCC OnLine Kar 424; *Khan v. Quintillion Business Media Pvt. Ltd* 2019 (175) DRJ 660; *Dave v. State of Gujurat* [MANU/GJ/0029/2017]

66 Order available here: https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2021/11/Order-23082021.pdf

67 Order available here: https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2021/04/X-v-Union-of-India.pdf

Equality Now

A just world for all women and girls

equalitynow.org

supporters@equalitynow.org

@equality-now

Breakthrough

BUILDING AN EQUAL WORLD FOR WOMEN AND GIRLS

inbreakthrough.org

contact@inbreakthrough.org

@breakthrough-india