

ANNUAL REPORT 3

AUGUST 2024 – JULY 2025

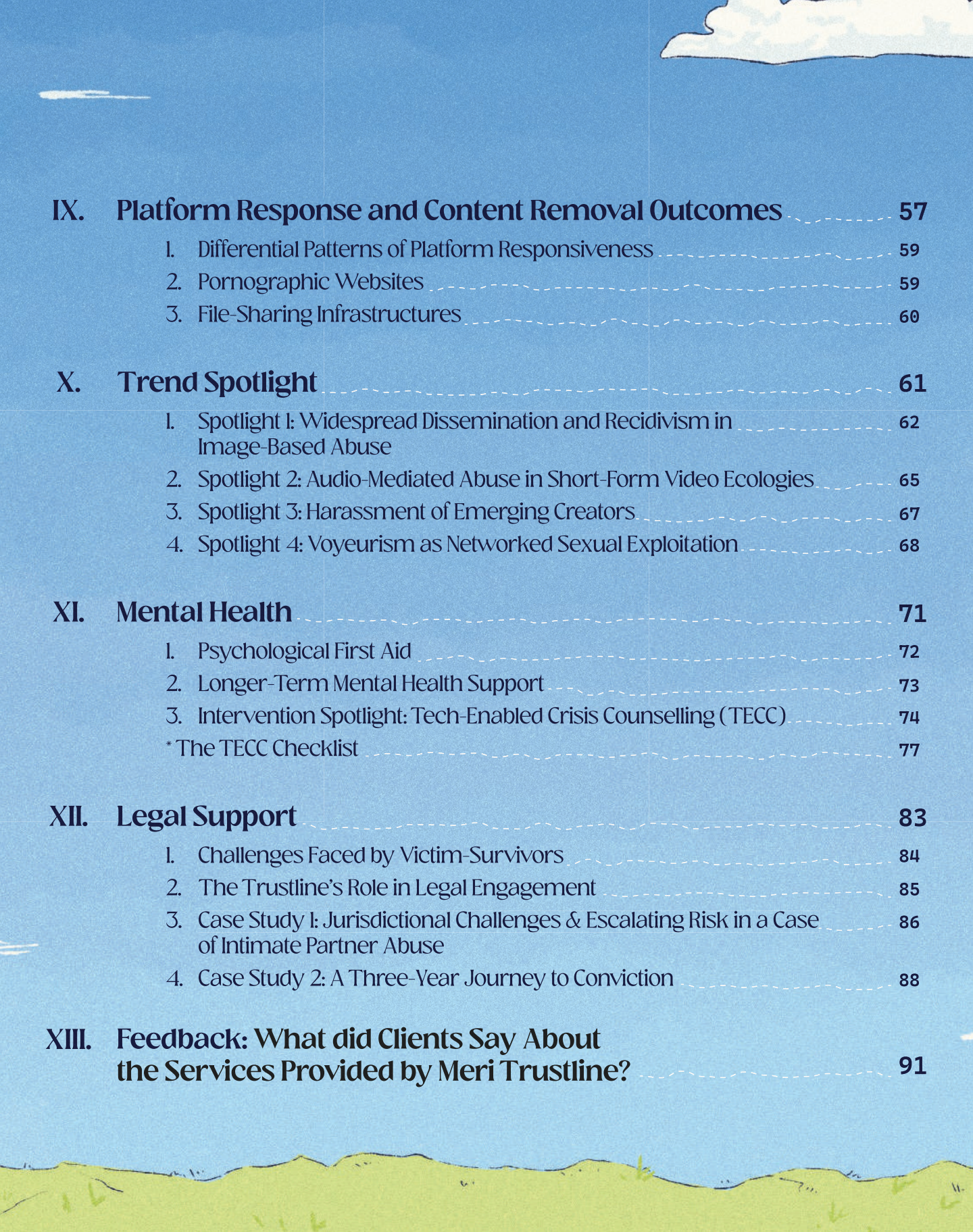
MERI TRUSTLINE

63631 76363



INDEX

I.	Glossary & Key Terms	1
II.	Meri Trustline Who We Are and What We Do	3
III.	Situating the Data	7
IV.	15 Technology Facilitated Gender Based Violence (TFGBV) Signals from Year 3 at Meri Trustline	13
V.	Methodological Note	17
VI.	Limitations	18
VII.	The Experience of Harm	19
	1. Gender	21
	2. Age	22
	3. Location	23
	4. Relationship Between Victim-Survivor and Perpetrator	25
	5. Types of Danger: Frequency and Pattern	26
VIII.	Mechanics of Harm in TFGBV	29
	1. Harm Through Sexualised Imagery	31
	2. Harm Through Child Sexual Abuse and Exploitation Material (CSAEM)	36
	3. Harm Through Digitally Manipulated Content/Deepfakes	40
	4. Harm Through Denigration and Reputational Targeting	44
	5. Harm Through Coercive Intimidation	48
	6. Harm Through Identity Exposure and Manipulation	52



IX. Platform Response and Content Removal Outcomes	57
1. Differential Patterns of Platform Responsiveness	59
2. Pornographic Websites	59
3. File-Sharing Infrastructures	60
X. Trend Spotlight	61
1. Spotlight 1: Widespread Dissemination and Recidivism in Image-Based Abuse	62
2. Spotlight 2: Audio-Mediated Abuse in Short-Form Video Ecologies	65
3. Spotlight 3: Harassment of Emerging Creators	67
4. Spotlight 4: Voyeurism as Networked Sexual Exploitation	68
XI. Mental Health	71
1. Psychological First Aid	72
2. Longer-Term Mental Health Support	73
3. Intervention Spotlight: Tech-Enabled Crisis Counselling (TECC)	74
* The TECC Checklist	77
XII. Legal Support	83
1. Challenges Faced by Victim-Survivors	84
2. The Trustline's Role in Legal Engagement	85
3. Case Study 1: Jurisdictional Challenges & Escalating Risk in a Case of Intimate Partner Abuse	86
4. Case Study 2: A Three-Year Journey to Conviction	88
XIII. Feedback: What did Clients Say About the Services Provided by Meri Trustline?	91

I. Glossary & Key Terms

- × **AI**
Artificial Intelligence: Computational systems capable of performing tasks that typically require human intelligence such as generating, modifying or analysing text, images, audio, and video.
- × **CCTV**
Closed-Circuit Television
- × **Childline**
Government-linked child helpline for children in distress in India, accessible at 1098.
- × **CSAEM**
Child Sexual Abuse and Exploitation Material
- × **Cybercrime Portal**
The National Cybercrime Reporting Portal in India (cybercrime.gov.in): Through which individuals can file complaints related to online offences.
- × **Deepfake**
AI-generated photo, video or audio that creates a realistic but false depiction of a real person.
- × **DMCA**
Digital Millennium Copyright Act: A US law commonly used to submit takedown requests to platforms for removal of harmful content.
- × **eSafety Commissioner**
Australia's independent online safety regulator.
- × **FIR**
First Information Report: The formal document that is filed to report a cognisable offence and initiate a criminal investigation by the police in India.
- × **Grievance Officer**
A designated officer mandated under the Information Technology Rules, 2021, for every significant social media platform to receive and resolve user complaints related to content and platform conduct.
- × **Hash-matching**
A technology used by platforms to detect and prevent re-upload of previously identified harmful content via a unique digital fingerprint.
- × **IT Act**
Information Technology Act, 2000: India's primary legislation governing digital offences and intermediary liability.
- × **IT Rules**
Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules governing platform obligations.

- × **IWF**
Internet Watch Foundation: A UK-based organisation working with platforms on detection and removal of child sexual abuse material.
- × **Manodhairya Scheme**
Maharashtra government's victim compensation scheme for survivors of sexual assault and acid attacks.
- × **NCRB**
National Crime Records Bureau: A Government of India Body that compiles and publishes national crime statistics, including cybercrime data.
- × **NCII**
Non-Consensual Intimate Imagery: Intimate or sexual content that is created, shared or circulated without the consent of the person depicted.
- × **POCSO**
Protection of Children from Sexual Offences Act, 2012: India's primary legislation for the protection of children from sexual abuse and exploitation.
- × **PFA**
Psychological First Aid: An evidence-informed approach to supporting individuals in acute distress—focused on grounding, reassurance and immediate stabilisation.
- × **Recidivism**
For the purpose of this report, the reappearance of removed harmful content through new accounts, altered formats or migration to different platforms.
- × **TECC**
Tech-Enabled Crisis Counselling: Meri Trustline's integrated response model combining digital incident response, crisis stabilisation, and psychosocial accompaniment.
- × **TFGBV**
Tech-Facilitated Gender-Based Violence: Gender-based harm carried out, amplified or extended through digital technologies.
- × **URL**
Uniform Resource Locator: A web address used to locate specific content online.
- × **UT**
Union Territory: An administrative division in India governed directly by the Central Government.
- × **Zero FIR**
An FIR filed at any police station in India regardless of jurisdiction, then transferred to the appropriate station.
- × **1930**
India's national cybercrime helpline number.

II. Meri Trustline: Who We Are and What We Do



About Meri Trustline:

Meri Trustline **6363176363** is a national online safety helpline in India, operated by RATI Foundation that supports children, women, and other marginalised genders facing technology-facilitated abuse. The helpline works to ensure timely response and pathways to redressal through an integrated model that combines technical intervention, psychosocial care, and legal guidance.

Core Areas of Support:

1. **Content Takedown:** Escalation and removal of harmful or abusive online content.
2. **Mental Health Counselling:** Psychological first aid, emotional stabilisation, and resilience-building.
3. **Social Support:** On-ground assistance and institutional coordination in complex cases.
4. **Legal Guidance:** Information on legal options and, where feasible, facilitation of representation.
5. **Technical/Informational Assistance:** Evidence preservation guidance, safety planning, and verified referrals.

Operating Hours:

The helpline operates on weekdays from 9:00 AM to 5:00 PM.

Contact Channels:

Individuals can reach Meri Trustline by phone or WhatsApp at **6363176363**, by email at **meritrustline@ratifoundation.org**, or through the online reporting form at **meritrustline.org**.

Handling Calls and Messages:

All calls and messages are managed by trained counsellors who are fluent in Marathi, Hindi, and English, and follow RATI Foundation's Standard Operating Procedures. Counsellors assess the nature of risk, guide callers on how to preserve evidence, and provide immediate psychological first aid.

Content Takedown Support:

Meri Trustline assists callers by escalating requests to platforms to remove or block harmful content. Through established escalation channels, the helpline seeks to reduce further circulation and mitigate ongoing exposure.

Collaboration with Technology Platforms:

The helpline engages with major platforms such as Meta (Facebook, Instagram, and Threads), YouTube, and Aylo, functioning as a trusted escalation partner with services.

Engagement with Law Enforcement:

Where cases involve immediate risk or serious criminal harm, the helpline supports victim-survivors in contacting relevant authorities and coordinating with law enforcement agencies to enable a timely protective response.

Ground Support and Institutional Coordination:

For vulnerable callers, Meri Trustline collaborates with Child Welfare Committees, District Child Protection Units, Childline services, Child Care Institutions, and civil society organisations to enable comprehensive support beyond digital intervention.

Mental Health Support:

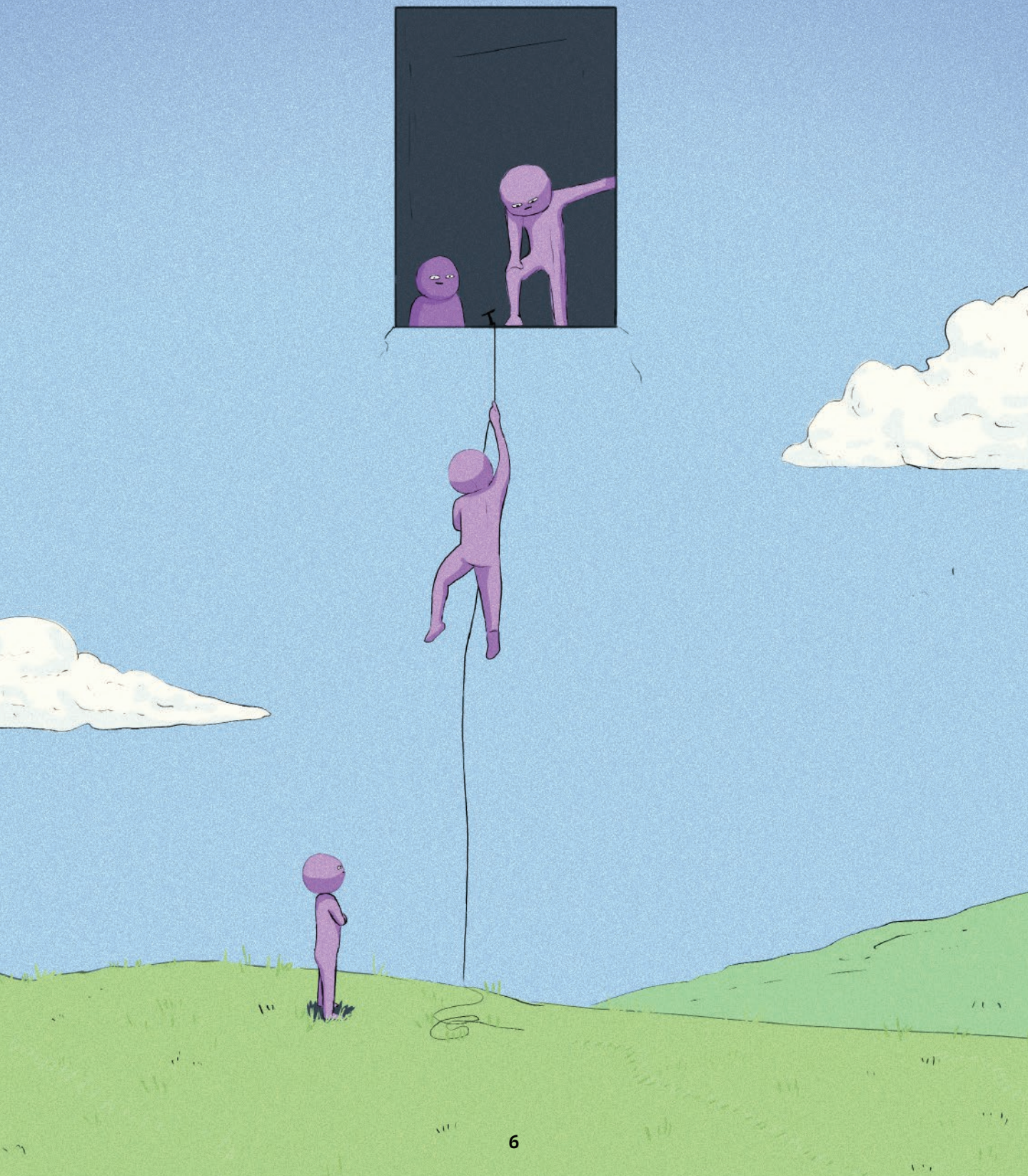
Psychological first aid is provided to help callers manage acute distress, particularly if incidents have occurred recently or have produced a prolonged emotional impact.

Legal Guidance and Support:

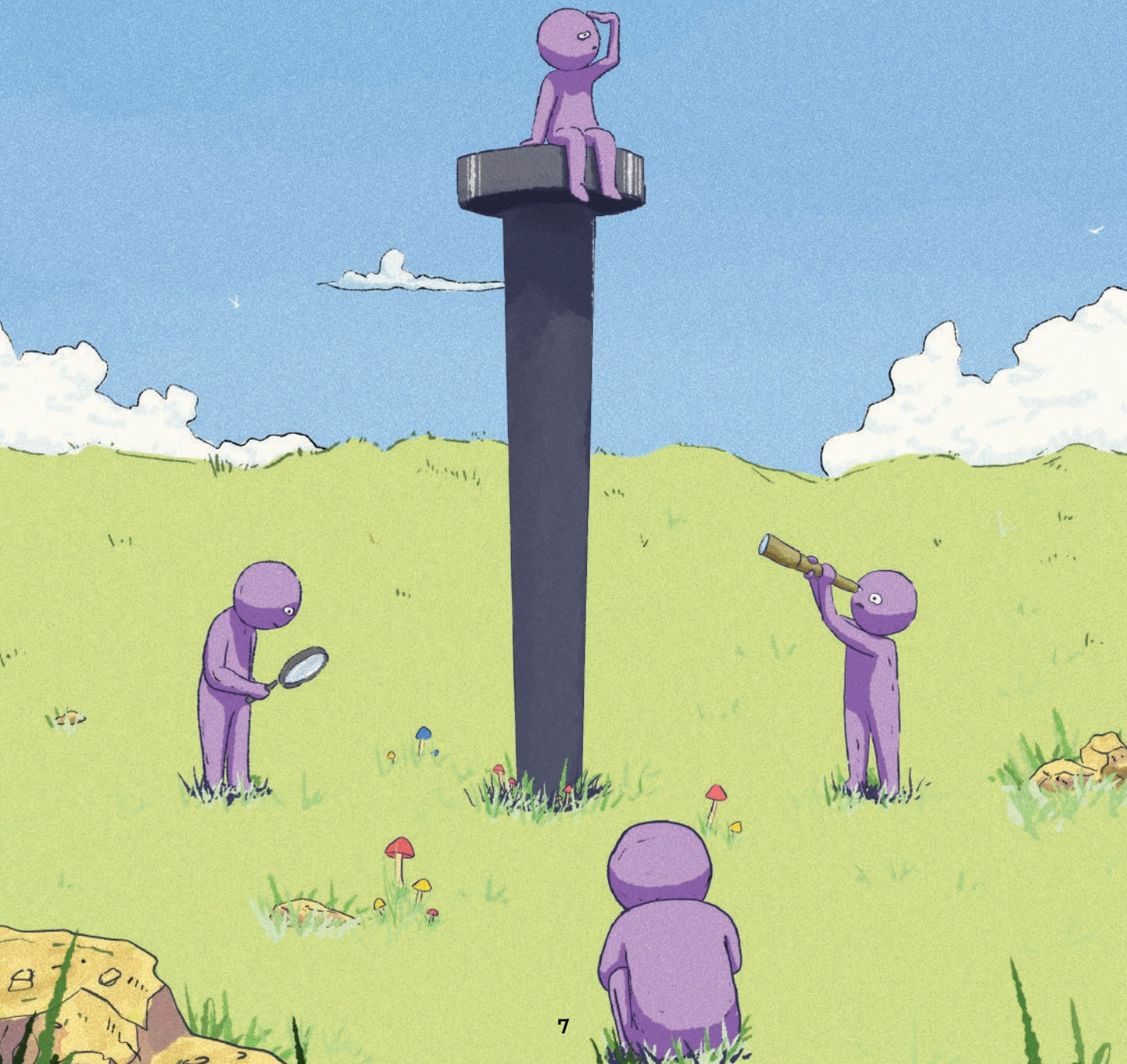
The helpline consults RATI Foundation's legal team on cases involving protective laws such as the POCSO Act and provisions addressing online abuse. It facilitates tele-consultations for legal advice and, in some cases, connects callers with legal representation.

Privacy and Confidentiality:

Meri Trustline follows strict confidentiality protocols. Counsellors collect only the information necessary to understand the risk and provide assistance, ensuring that callers are not required to disclose personal details beyond what is relevant for their safety and response.



III. Situating the Data



Online harm is fluid at the edges. It shapeshifts in response to the pressures placed upon it. New laws, platform rules, reporting mechanisms and technological safeguards constantly try to limit certain forms of abuse. But harm adapts by changing its form, location and method.

In Year 3, Meri Trustline received **626 calls** of which **130 victim-survivors** required and received active intervention. Across these cases, the Trustline documented **253 categorised instances of danger** and reported **1137 harmful links and accounts** to platforms, resulting in **981 takedowns**. These figures point to an important shift in the nature of the helpline's work.

Content that was removed or restricted in one space resurfaced in another, typically on platforms that were less regulated or harder to monitor. Removed content was remixed, repurposed, recontextualised and reuploaded. This made the abuse more coded and veiled. Material that appeared less explicit to an outside observer could still carry deeply harmful meanings for those targeted.

The data highlights the layered and multi-platform nature of technology-facilitated abuse. **A single case involves multiple online threats against an individual.** For example, impersonation along with the circulation of sexualised content across several accounts and services. Responding to even one strand of harm often requires intervention across multiple platforms and technical intermediaries.

New vectors of harassment gained prominence. **Abusive or manipulated audio allowed harm to circulate in ways that were difficult to detect, classify and remove.**

At the same time, the tools available to perpetrators became easier to access and use. **Techniques that once required specialised skills, such as image manipulation, synthetic media generation or coordinated cross-platform targeting, can now be executed through widely available apps & platforms.** This contributed to a diversification and intensification of attack patterns.

Technology and algorithms were not the only dominant themes of Year 3. Patterns of online abuse reflected broader social inequalities. **Gender, religion and other forms of marginalisation also influence who becomes vulnerable to online harm.** In contexts already shaped by misogyny, communal hostility and polarisation, online harm tends to take on more organised and persistent forms.

During the period under review, **a growing number of individuals sought mental health support alongside technical assistance.** This shift was significant. It reflects both the intensity of the abuse experienced and an increasing recognition that psychological recovery is central to meaningful redressal. Requests for legal guidance were also frequent, although **sustained engagement with formal justice mechanisms remained difficult.** Concerns about stigma, procedural delays, jurisdictional uncertainty and prolonged public scrutiny continue to shape these decisions.

This timeframe also coincided with reduced investment by several major social media platforms in moderation and trust-and-safety functions globally. Frontline operational effects seemed evident in **slower content removals, less predictable reporting pathways and an increased volume of harmful material requiring intervention.**¹

Meri Trustline's work sits at the intersection of psychosocial support, technical response and legal guidance. Unlike institutional datasets, its case records offer a grounded view of online harm as an ongoing process rather than a series of discrete incidents.

Data from the latest available National Crime Records Bureau Crime in India 2024 report also indicates a continued rise in cybercrime. **NCRB recorded 1,01,928 cybercrime cases in 2024, reflecting a 17.9% increase** from 86,420 cases in 2023.¹ The cybercrime rate also rose from 6.2 to 7.3 per lakh population. During 2024, 72.6% of registered cybercrime cases were recorded under the motive of fraud. This was followed by sexual exploitation at 3.1% and extortion at 2.5%.

However, **NCRB records only 3,288 Cyber Crimes cases against Women nationally in 2024.** Women-centric cybercrime cases form only about 3.2% of all registered cybercrime cases nationally. Of these, 2,511 cases involved publishing or transmitting sexually explicit material while 777 cases were recorded under other women-centric cybercrimes.

Similarly, **NCRB records only 1,238 Cyber Crimes cases against children nationally in 2024.** Of these, 1,099 cases involved publishing or transmitting material depicting children in sexually explicit acts while 139 cases were recorded as other cybercrimes against children. These cases form only about 1.2% of all registered cybercrime cases nationally.

The state-wise distribution of these narrower categories reveals uneven recording of technology-facilitated gender based violence. Under women-centric cybercrime categories, the highest recorded figures came from Odisha with 719 cases, followed by Uttar Pradesh with 572, Chhattisgarh with 292 and Telangana with 251. By comparison, Maharashtra recorded 89 such cases and Delhi recorded 78.

Under child cybercrime categories, Chhattisgarh recorded 268 cases, followed by Rajasthan with 174, Delhi with 151, Uttar Pradesh with 137, Kerala with 92 and Karnataka with 77. Maharashtra recorded 48 such cases.

The metropolitan data shows a similar pattern. Across the 19 metropolitan cities, NCRB records 390 women-centric Cyber Crimes cases in 2024. These were concentrated in a few cities: Hyderabad recorded 185, Delhi City 78, Bengaluru 44, Ahmedabad 23 and Mumbai 21. For child Cyber Crime categories, the city-level total was 189 cases, with Delhi City alone recording 151, followed by Bengaluru with 23. **Several major cities, including Mumbai and Pune, recorded zero cases in cyber crime against children category.** These figures suggest not the absence of harm but the challenges of reporting and recording of cases with formal systems.

Even as recorded numbers are few, technology-facilitated gender-based violence has increasingly become a recognisable part of the news cycle. While the majority volume of harm remains unreported and under-recorded, certain cases occupied public attention and discourse.

¹Crime in India 2024, NCRB



**Selected Incidents of TFGBV
Highlighted in the Media:
August 2024 - July 2025**



21 August 2024 - RG Kar victim identity circulation

Following the rape and murder of a doctor at RG Kar Medical College, the victim's name, photographs and video clips circulated widely online. The Ministry of Electronics and Information Technology directed platforms to remove the content after intervention by the Supreme Court.²

19 November 2024 - Harassment targeting Rana Ayyub

Journalist Rana Ayyub reported doxxing, over 200 abusive calls and messages, circulation of personal details and the spread of an AI-generated sexualised video using her likeness across social media platforms.³

23 May 2025 - Bengaluru Metro Voyeurism

An Instagram account posting secretly filmed images and videos of women commuters on the Bengaluru Metro led to police action and an arrest after the content had been circulated to thousands of followers.⁴

20 June 2025 - Deepfake impersonation of Anjana Om Kashyap

The Delhi High Court directed the takedown of a YouTube channel that was using journalist Anjana Om Kashyap's image, news clips and deepfake content to impersonate her.⁵

14 July 2025 - Assam AI-morphing and fake Instagram case

Police arrested a former college acquaintance for allegedly using AI-morphed images and videos of a woman, creating a fake Instagram page in her name and causing the content to go viral.⁶

These incidents reveal patterns of harmful circulation and the breakdown of control over personal content & identity. While they are often framed as products of emerging technologies, they also reflect a more foundational rupture- the violation of consent that lies at the core of gender-based violence. In this sense, what appears new is also continuous with older forms of harm.

²Mahapatra, D. (2024), Remove victim's name, videos from electronic, social media: Supreme Court. The Times of India, 21 August.

³Reporters Without Borders. (2024), Rana Ayyub, the face of India's women journalists plagued by cyber-harassment, 27 November.

⁴Jena, S. (2025), Voyeurism on Bengaluru Namma Metro: Women secretly filmed, videos uploaded online. The News Minute, 22 May.

⁵Thapliyal, N. (2025), Delhi High Court orders take down of YouTube channel using deepfake impersonations of Aaj Tak's Anjana Om Kashyap. LiveLaw, 25 June.

⁶Baruah, S. (2025), 'Adult content' made her an overnight sensation. Now, a police arrest reveals how Assam woman was victim of AI used by ex-collegemate. The Indian Express, 14 July.

An illustration of a green field with several brown cardboard boxes scattered around. Three purple, featureless humanoid figures are present. One figure is kneeling and opening a box, while another stands nearby with arms crossed. A third figure is walking away in the background. A large speech bubble originates from the kneeling figure, containing the title text. The boxes are of various sizes and some have small labels.

IV. 15 TFGBV Signals from Year 3 at Meri Trustline

The casework documented in Year 3 points to a set of clear shifts in how tech-facilitated gender-based violence is occurring, circulating, and being addressed.

1. Cases are becoming more complex and persistent.

A key shift in Year 3 is the increasing density of harm within individual cases. Many involved multiple links, accounts or uploads, with content resurfacing through reposts, altered versions, and new accounts even after initial reporting.

2. Pornographic and unregulated websites are playing a bigger role in harm.

A growing share of casework involved content moving beyond mainstream platforms into adult content sites, file-hosting services and other weakly governed online environments, where reporting pathways are harder to navigate and removal is more difficult to sustain. Regulatory attention in India remains largely focused on significant social media intermediaries, thus leaving this expanding segment of the harm ecosystem comparatively under-addressed.

3. More harmful content is being edited, repackaged, or synthetically created.

Harmful material is becoming more adaptive in form, allowing it to reappear in altered versions that are harder to classify and contain. Editing, remixing, manipulated audio, and deepfake content featured more prominently in Year 3.

4. Anonymous and secondary perpetrators are becoming more common.

Year 3 suggests a shift away from abuse being contained within known relationships alone. It was observed that harm was often initiated or amplified by unknown actors operating through pseudonymous or rapidly created accounts. In several cases, the source of abuse was followed by others who reposted, edited, archived, or amplified the material. These actors often had no direct relationship to the victim-survivor but played a major role in extending harm.

5. Moderation systems are failing to detect less explicit but still harmful content.

Material did not need to be overtly explicit to cause serious harm. Less explicit but still sexualised or reputationally damaging content often proved harder to remove, exposing a gap between platform thresholds and survivor experience.

6. Voyeuristic and non-consensual recording continue to feed digital harm.

Year 3 showed how acts of recording, watching, or capturing people without their consent could become the starting point for wider digital circulation once content was uploaded, reframed, or redistributed online.

7. Visibility is increasingly linked to harm, particularly for emerging influencers.

Casework suggests that people who are locally recognisable, socially visible, or building an online presence may face disproportionate reputational risk once harmful content begins to circulate. Visibility does not necessarily bring protection; in many cases, it increases exposure.

8. Reputational harm is a major part of the caseload.

The harms documented in Year 3 were not limited to sexual exposure. Humiliation, denigration, and social discredit emerged as central ways in which abuse was produced and experienced.

9. The harms reported are not only sexual, but also communal, identity-based, and socially targeted.

Some cases involved caste, religion, gender, or community-based targeting, including slurs and inflammatory circulation. This widens the frame from sexual abuse alone to digitally amplified social hostility.

10. CSAEM cases show harm by known perpetrators and wider digital circulation.

CSAEM casework in Year 3 highlights two linked patterns: such abuse often emerged from proximate social environments; and once circulated, it moved into spaces where removal became slower and more fragmented.

11. More victim-survivors are open to mental health support.

A notable shift in Year 3 was the increasing willingness of victim-survivors to seek mental-health support alongside technical assistance. This signals a growing need to set up mental health support infrastructure.

12. Survivors want legal redress but legal processes remain difficult to stay with.

Requests for legal guidance remained frequent, but sustained engagement with formal systems was often hard to maintain. Delays, uncertainty, scrutiny, and procedural burden continued to shape what survivors were willing or able to pursue.

13. Platform responses remain uneven.

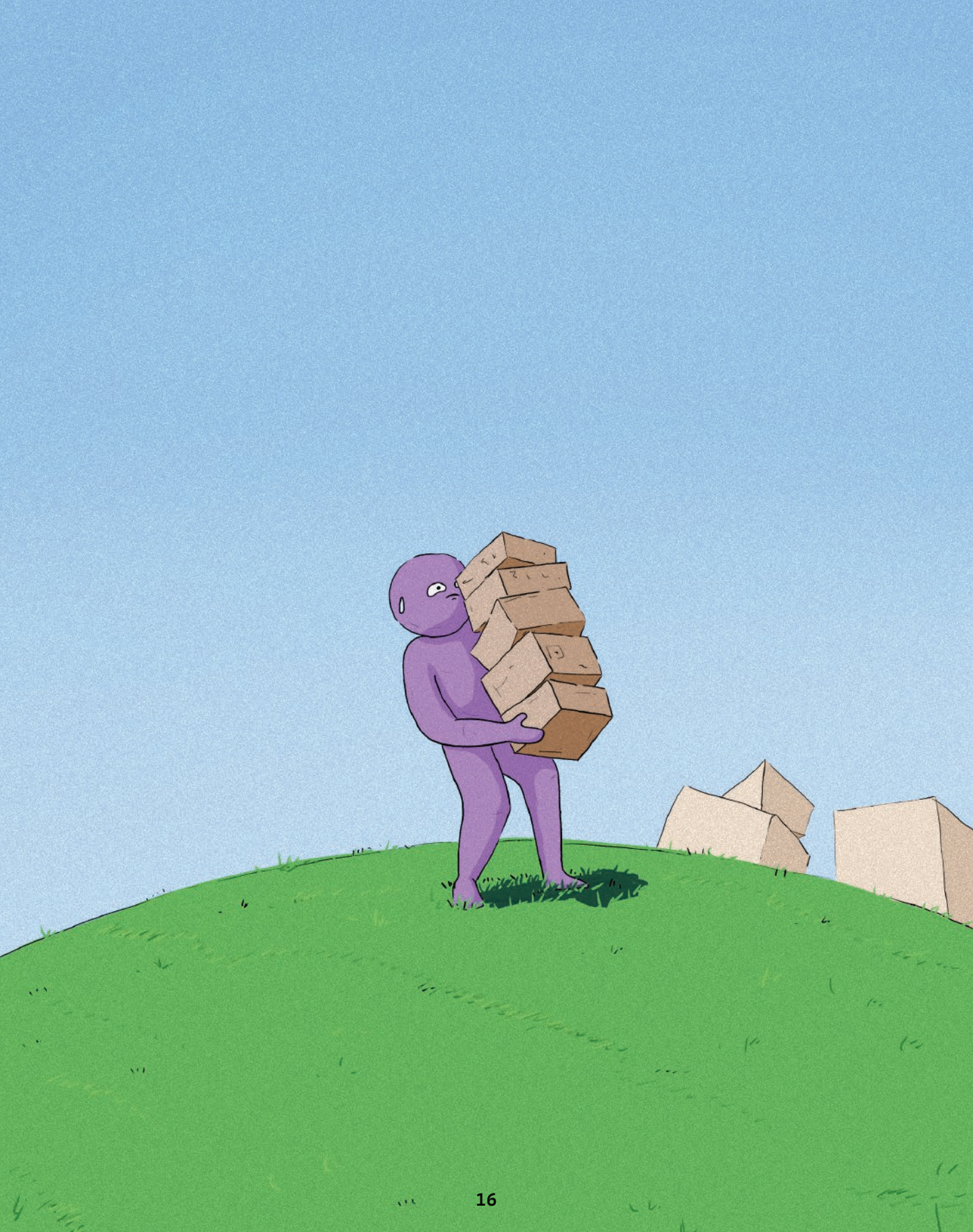
Even where removals were achieved, relief remained highly dependent on where the harm appeared and how platforms responded. In practice, victim-survivors encountered a patchwork of more and less responsive environments rather than a consistent system of redress.

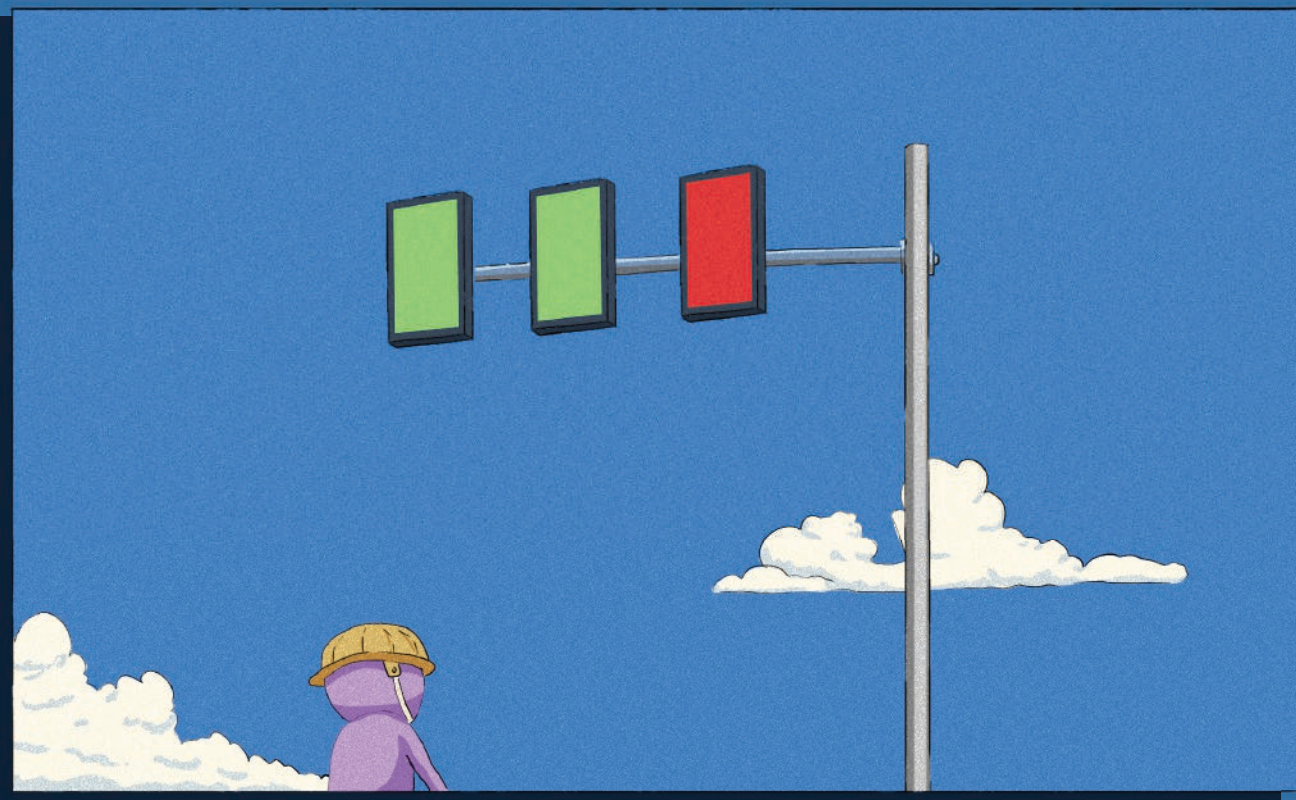
14. Reports are coming from a wider geographic spread.

Year 3 reflects a broader spatial spread of cases, including smaller towns and non-metropolitan districts, suggesting that technology-facilitated harm is surfacing now from a wider range of social and geographic contexts.

15. An integrated, multidisciplinary response is increasingly necessary.

Year 3 reinforces that online harm cannot be addressed through content removal alone. The casework points to the need for combined technical intervention, psychosocial care, legal guidance, and, in some cases, on-ground institutional coordination.





V. Methodological Note

This report analyses Meri Trustline case records from August 2024 to July 2025.

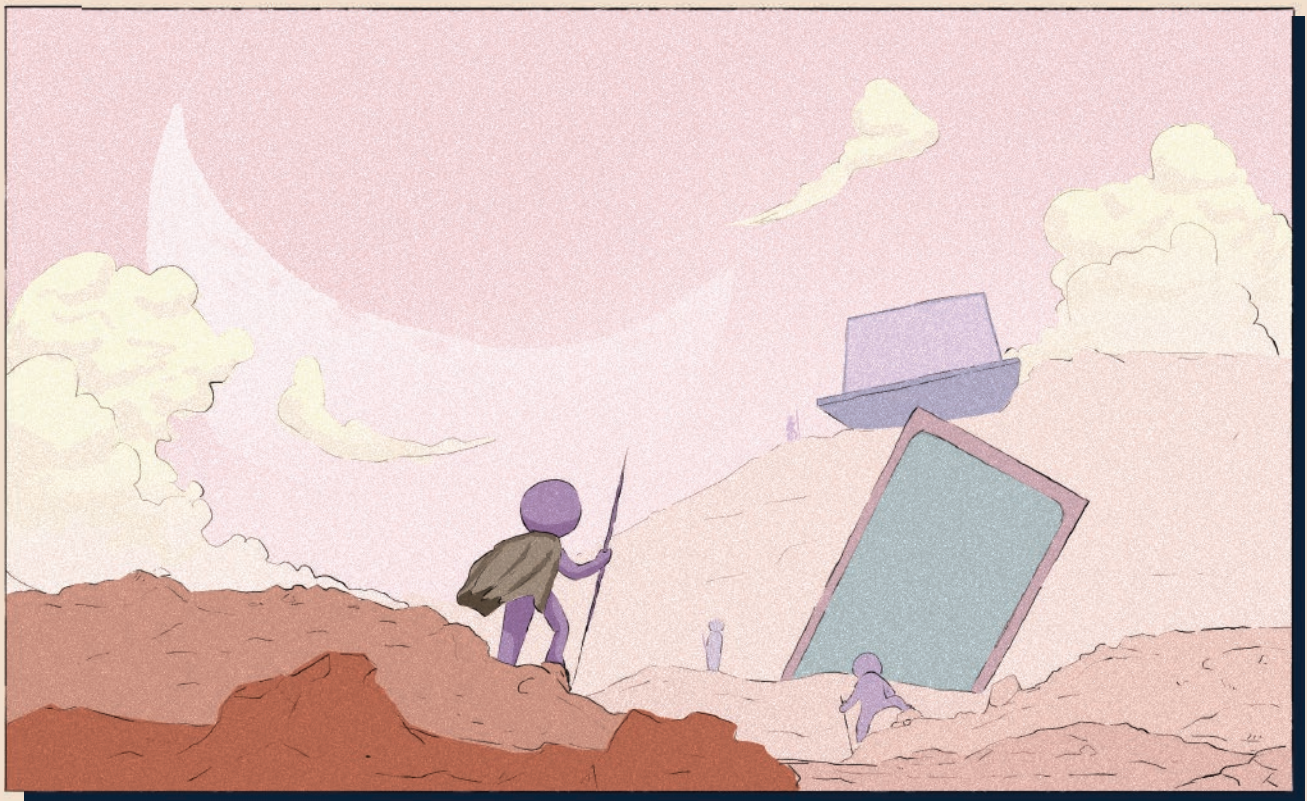
Three analytical units are used throughout the report. This allows the report to capture both the experience of harm and the scale of technical response required to address it.

Victim-survivors⁷ refer to individuals who contacted the Trustline and required active intervention. In Year 3, 130 individuals required such intervention. This unit is used to understand who seeks support and to examine demographic trends.

Instances of danger refer to specific harmful events reported within a case, such as impersonation, threats, or the circulation of sexualised content. In Year 3, 253 categorized instances of danger were recorded across these 130 cases. The number of instances exceeds the number of victim-survivors because a single individual reported experiencing multiple harms simultaneously or sequentially.

Content actioned refers to individual profiles, links, or pieces of content reported to platforms by the Trustline for removal or redress. In Year 3, 1,137 such harmful links and accounts were reported, of which 981 were successfully taken down.

⁷Lakshané, R., & Kumar, S. (2024), The Crying Shame of Image-Based Abuse Apps.



VI. Limitations

The data presented in this report reflects the information available within Meri Trustline's case records and should be read with the following constraints in mind.

1. The Trustline's caseload represents a help-seeking population, i.e., individuals who were aware of the service, able to access it, and willing to seek support. It is not a measure of prevalence.
2. In line with good practice, victim-survivors are met with the presumption of belief and good faith. Post the initial assessment made by trained counsellors, information is collected only to the extent necessary to provide appropriate support. Therefore, our case records largely reflect reported experience and are not formal, investigative records.
3. In Year 3, some victim-survivors who had reported in previous years returned with cases of recurring harm. However, these instances are not recorded as new cases and therefore remain undercounted in the data.

The illustration depicts a person with dark hair and a small hoop earring lying on their side on a light-colored, sandy or rocky surface. Their eyes are closed, and they have a somber expression. A small, stylized purple figure stands near the person's hand. In the background, a large screen or window shows a bright green field under a blue sky with white clouds, with a purple figure standing in the distance. The overall mood is one of isolation and contemplation.

VII. The Experience of Harm

Technology-facilitated abuse in Year 3 was characterised by the extended circulation of offending content across digital platforms.

Table 1 - Trustline Response Outputs Across Three Years

Service Output	Year 1 (2022–23)	Year 2 (2023–24)	Year 3 (2024–25)
Calls Received	823	697	626
Cases Handled	222	141	130
Harmful links reported to platform	Not available*	537	1,137
Harmful links taken down	259	409	981
Accounts recovered	18	11	2
Cybercrime complaints filed	118	156	95
Counselling support provided	186	110	105
Legal advice / representation	3	15	10

*Note: This data was not comprehensively recorded in Year 1 of the Trustline

In Year 3, Meri Trustline received 626 calls, of which 130 victim-survivors required and received active intervention. This represents a marginal decline from 141 in the previous year. But during this period, the Trustline reported 1,137 pieces of content (accounts and links) for removal, a substantial increase of approximately 112% compared to Year 2, when 537 pieces of content were reported.

While the number of individuals seeking structured support saw a marginal reduction, many survivors reported multiple, overlapping instances of danger. Harmful content frequently continued to circulate, resurface, or migrate across platforms after initial removal efforts. This resulted in a higher operational load per case and points to the persistence of abuse beyond a single reporting cycle.

Survivors in cases involving recurring content often described sustained uncertainty linked to the continuing possibility of exposure—a dynamic that trauma scholarship has long recognised, noting that distress intensifies when threat remains unresolved and embedded within everyday life.⁸

⁸Herman, J. L. (1992), *Trauma and Recovery*. Basic Books.

Adolescents and young adults continued to approach the Trustline in substantial numbers, particularly in cases involving peer-network harassment, coercive sharing of images, impersonation, and relationship-based abuse. But a larger share of cases involved older individuals, whose experiences of online abuse intersected with livelihood concerns, family expectations, and community standing. In such contexts, the circulation of sexualised content or threats of exposure was perceived as risks with immediate and longstanding social and material consequences.

Taken together, these patterns suggest that technology-facilitated abuse in Year 3 was experienced less as a discrete digital episode and more as a socially embedded condition of vulnerability. Its impact is directly shaped by the social and material pressures associated with the particular stage of life in which the survivor encountered the harm.

Gender

Table 2: Gender Distribution of Victim-Survivors (Year 3)

Gender	Number (n)	Share (%)
Female	89	68%
Male	34	26%
Gender not disclosed	7	6%
Total	130	100%

In Year 3, the victim-survivors that Meri Trustline supported largely comprised women and girls. Of the total, 68% (n = 89) of victim-survivors identified as female; 26% (n = 34) as male, while 6% (n = 7) did not disclose their gender. This distribution remains broadly consistent with patterns observed in previous reporting cycles.

Literature on digital gender inequality in India notes that women often face heightened reputational risk and social surveillance in online environments, which can increase both their susceptibility to technology-facilitated abuse and their reliance on confidential or intermediary forms of assistance.⁹ With its primary focus on children, women, and marginalised genders, Meri Trustline's outreach and service are designed to reflect this reality.

⁹IT for Change, *Access to Justice Issues in Cases of Online Gender-Based Violence*, in *Online Gender-Based Violence Judicial Resource Guide*

But boys and men nonetheless also continued to approach the Trustline with cases requiring intervention, and their presence within the caseload has remained relatively stable across reporting cycles. This pattern is consistent with comparable helplines internationally. Data from both the UK Revenge Porn Helpline¹⁰ and the Digital Rights Foundation Digital Security Helpline¹¹ similarly indicate that women constitute the majority of help-seekers, while male survivors are more frequently represented in financially motivated sextortion and blackmail-related harms.

Age

The youngest victim-survivor in the reporting period was below the age of 5 years and was featured in a reel soundtracked with an abusive audio clip. Another 10-year-old was a minor influencer who was also featured in a reel with sexually suggestive music and context. The oldest victim-survivor was 58 years old, who reported a case of hacking.

The age profile of victim-survivors in Year 3 reflects both continuity in younger cohorts and a gradual increase in help-seeking among older individuals.

Table 3: Age Profile of Victim-Survivors (Year 3)

Age Group	Number (n)	Share (%)
Pre-adolescents (below 13)	2	2%
Adolescents (13–17)	24	18%
Young adults (18–22)	34	26%
Emerging adults (23–27)	18	14%
Adults (28+)	33	25%
Age not disclosed	19	15%
Total	130	100%

¹⁰SWGfL, Revenge Porn Helpline Annual Report 2024
¹¹Digital Rights Foundation (DRF), Digital Security Helpline Annual Report 2024

Pre-adolescents (below 13)

Two cases of pre-adolescent children were reported to Meri Trustline in Year 3. In both cases, they were featured in content reported to us by third-party adults who had stumbled upon the content online.

Adolescents (13 to 17 years)

Adolescents constituted 18% (n=24) of victim-survivors in Year 3. The proportional share of adolescents in the caseload has declined over the three-year period. However, this may reflect changing help-seeking patterns or the Trustline's growing reach among adult populations, rather than a reduction in adolescent exposure to harm.

Young adults (18 to 22 years)

Individuals aged 18 to 22 represented 26% (n=34) of victim-survivors in Year 3. This cohort remained one of the largest groups seeking support.

Emerging adults (23 to 27 years)

Victim-survivors aged 23–27 accounted for 14% (n=18) in Year 3. This cohort's consistent presence across all three years suggests a sustained and stable pattern of help-seeking among individuals.

Adults (28 years and above)

Victim-survivors aged 28 and above constituted 25% (n=33) of the caseload in Year 3.

Age undisclosed

15% (n=19) of victim-survivors did not disclose their age in Year 3. This was due to any one of the following three reasons: a reluctance to share details; the case did not require personal details; or the case reached the Trustline through third-party reporters.

Location

Of all the victim-survivors who approached the Trustline in Year 3, 86% (n = 112) were located within India: with cases having been reported from 20 states and two Union territories. A small proportion of victim-survivors – 5% (n = 6) contacted the Trustline from outside India (USA, Algeria, Sweden). In 9% of cases (n = 12), the location was not disclosed.

As in previous reporting cycles, the largest share of cases originated from Maharashtra (24.6%, n = 32), followed by West Bengal (12.3%, n = 16) and Delhi (9.2%, n = 12). Together, these locations accounted for nearly half of the Trustline's active caseload during the reporting period.

At the same time, cases were also reported from a wider group of states, including Karnataka, Kerala, Assam, Tripura, Uttar Pradesh, Tamil Nadu, and Gujarat, among others. Although the number of cases from each of these locations was smaller, their presence reflects the geographically dispersed character of technology-facilitated abuse.

Comparison with earlier reporting cycles indicates a gradual diffusion in the spatial profile of reported cases. In Year 1, reports were more tightly clustered within a limited number of states. Year 2 recorded a modest widening in geographic spread. By Year 3, cases were received from a broader range of states, including smaller towns and non-metropolitan districts.

The geographic profile of Trustline casework does not map neatly onto NCRB cybercrime reporting patterns, indicating that awareness of services, language accessibility, connectivity gaps, and local referral ecosystems continue to shape help-seeking behaviour across states.

Table 4: Geographic Distribution of Victim-Survivors (Year 3)

State / Territory	Number (n)	Share (%)
Maharashtra	32	24.6%
West Bengal	16	12.3%
Delhi (UT)	12	9.2%
Uttar Pradesh	7	5.4%
Kerala	6	4.6%
Madhya Pradesh	6	4.6%
Gujarat	4	3.1%
Haryana	4	3.1%
Karnataka	4	3.1%
Assam	3	2.3%
Rajasthan	3	2.3%
Telangana	3	2.3%
Bihar	2	1.5%
Punjab	2	1.5%
Sikkim	2	1.5%
Chandigarh (UT)	2	1.5%
Himachal Pradesh	1	0.8%
Jharkhand	1	0.8%
Meghalaya	1	0.8%
Odisha	1	0.8%
Outside India	6	4.6%
Location not disclosed	12	9.2%
Total	130	100%

Relationship Between Victim-Survivor and Perpetrator _____

Technology-facilitated abuse operates across two overlapping relational contexts. Anonymous interactions can enable rapid escalation and wide dissemination of harm, while abuse by socially proximate perpetrators is more likely to intersect with ongoing relationships and offline social pressures.

Table 5: Relationship of Victim-Survivors with Perpetrators (Year 3)

Relationship with perpetrator	Number (n)	Share (%)
Unknown perpetrators	91	70%
Known perpetrator	39	30%
Total victim-survivors requiring intervention	130	100%

In Year 3, perpetrators were more often anonymous or unknown to victim-survivors. Of these, 70% (n = 91) reported that they did not know the individual responsible for the abuse, while 30% (n = 39) identified the perpetrator as someone known to them. In the cases where perpetrators were known, they were overwhelmingly reported to be male, accounting for 92% (n = 36) of cases.

Abuse involving known perpetrators frequently occurred within the context of existing social relationships and was observed in cases involving non-consensual intimate imagery and forms of reputational denigration. In these situations, prior access to personal communication, images, or shared social networks shaped how harm unfolded. The circulation of content often intersected with offline relational environments, including family settings, peer groups, or intimate partnerships, and often intensified the social consequences of abuse.

In contrast, incidents involving unknown perpetrators were more commonly associated with harms such as sextortion and blackmail, impersonation, online threats, and networked harassment. In many such cases, imagery or personal information appeared to be sourced from accessible online profiles and repurposed to facilitate abuse. Anonymity, the use of multiple or rapidly created digital accounts, and cross-platform circulation enabled perpetrators to initiate and escalate harm without prior social proximity.

The relational profile of harm has shifted across reporting cycles. Year 1 casework was dominated by abuse within pre-existing relationships. By Year 2, anonymous harms had grown significantly. In Year 3, incidents involving unknown perpetrators constituted a clear numerical majority.

Types of Danger: Frequency and Pattern

In Year 3, the 130 victim-survivors whose cases required intervention reported 253 categorised instances of danger. (As individual cases frequently involve overlapping forms of online abuse, the total number of recorded harm instances is higher than the number of victim-survivors.)

The largest single category was denigration or damaging reputation (16.6%, n=42), indicating the centrality of humiliation, defamation, and networked social exposure as forms of harm.

Table 6: Distribution of Categorised Online Harms (Year 3)

Harm Type	Instances (n)	Frequency (%)
Denigration / Damaging reputation	42	16.6%
Erotic posing	23	9.1%
Threats of online consequences / Violence	21	8.3%
Sextortion / Blackmail	17	6.7%
Impersonation	15	5.9%
Doxxing / Outing	14	5.5%
Harassment through sexually explicit content	13	5.1%
Content featuring penetrative sexual activity	12	4.7%
Harassment through non-sexual content	11	4.3%
Intimate content without nudity	11	4.3%
Threats of on-ground consequences / Violence	10	4.0%
Sexually explicit remarks	10	4.0%
Solo sexual activity	10	4.0%
Digitally manipulated imagery / deepfake	10	4.0%
Content featuring non-penetrative sexual activity	8	3.2%
Account hacked	6	2.4%
Partial nudity	5	2.0%
Financial fraud	4	1.6%
Unspecified / other	5	2.0%
Adult pornographic content	3	1.2%
Repeated harassment / cyberstalking	3	1.2%
Total	253	100.0%

Harms involving the creation, capture, or circulation of intimate and sexualised visual content without consent constituted a substantial portion of the combined share of reported instances. These included erotic posing (9.1%, n=23); penetrative sexual content (4.7%, n=12); solo sexual activity imagery (4%, n=10), non-penetrative sexual content (3.2%, n=8); partial nudity (2%, n=5); harassment through sexually explicit content (5.1%, n=13); digitally manipulated imagery including deepfakes (4%, n=10); and adult pornographic content used in harassment contexts (1.2%, n=3).

This was followed by threat-based harms where coercion and intimidation were key mechanisms, including threats of online consequences (8.3%, n=21); threats of on-ground violence (4%, n=10); and sextortion or blackmail (6.7%, n=17).

Harms involving identity manipulation and exposure, including impersonation (5.9%, n=15) and doxxing or outing (5.5%, n=14), further contributed to the spread and persistence of abuse, often facilitating reputational damage and wider dissemination of harmful material.

Account hacking (2.4%, n=6) and financial fraud (1.6%, n=4) were also reported. The small number of formally registered cases in these categories reflects the largely informational nature of the support provided.

Child Sexual Abuse and Exploitation Material (CSAEM) was reported in 10% of cases (n = 13 of 130 victim-survivors). Given the distinct legal framework governing this category under the Protection of Children from Sexual Offences Act, 2012, CSAEM cases are analysed separately in a dedicated section of this report.



VIII. Mechanics of Harm in TFGBV



Research on technology-facilitated violence shows that harm is not caused only by the content itself but by how it is used, shared, and made visible on social networks. Reputational harm is amplified through visibility and circulation¹². Intimate imagery is used to exert control¹³. Sustained threats can shape behaviour by creating a constant fear of escalation¹⁴. Such harms tend to overlap in practice, producing layered experiences rather than clearly bounded episodes¹⁵.

In line with this understanding, harms documented in Year 3 are examined through **six primary mechanisms of harm**, which focus on how abuse operates; how it is produced; how it spreads; and how it affects victim-survivors.

The six mechanisms identified are:

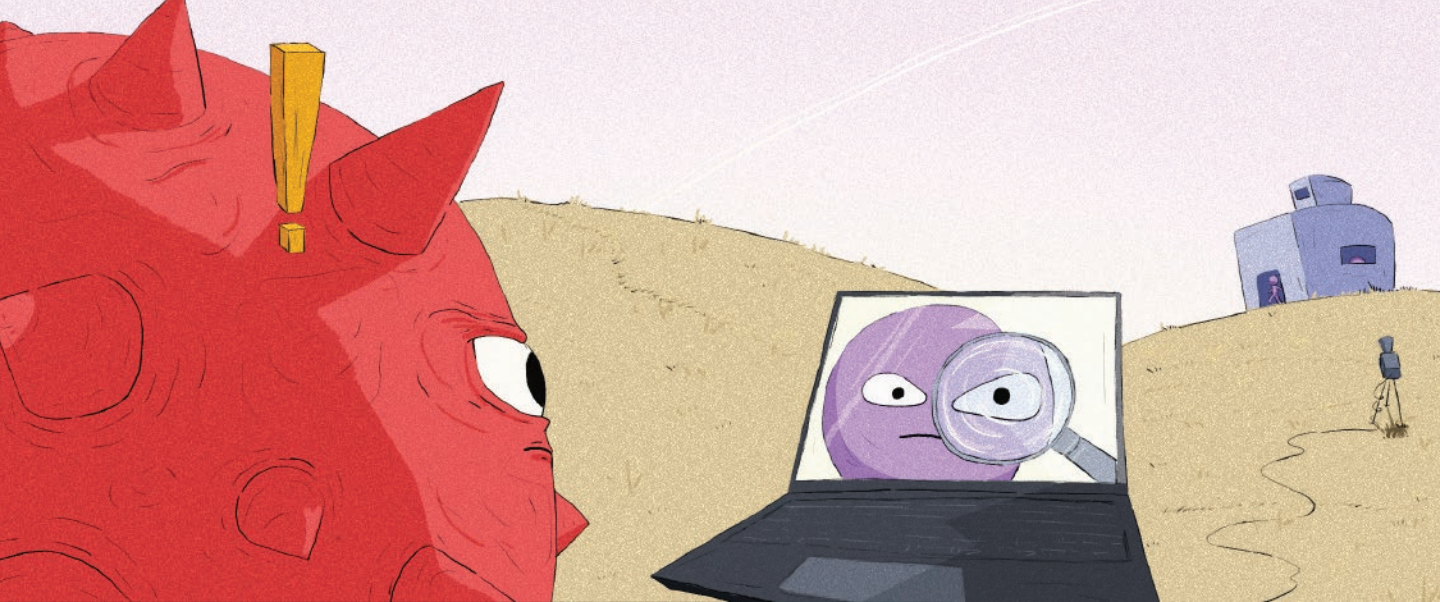
1. Harm through sexualised imagery
2. Harm through child sexual abuse and exploitation material (CSAEM)
3. Harm through digitally manipulated content
4. Harm through denigration and reputational targeting
5. Harm through coercion and intimidation
6. Harm through identity exposure and manipulation

¹²Citron, D. K., & Franks, M. A. (2014), Criminalizing Revenge Porn, 49 Wake Forest Law Review 345.

¹³McGlynn, C., Rackley, E., & Houghton, R. (2017), Beyond 'Revenge Porn': The Continuum of Image-Based Sexual Abuse, Feminist Legal Studies, 25(1), 25-46.

¹⁴Dragiewicz et al. (2018), Technology Facilitated Coercive Control: Domestic Violence and the Competing Roles of Digital Media Platforms, Feminist Media Studies.

¹⁵Henry, N., & Powell, A. (2016), Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research, Trauma, Violence, & Abuse.



1 HARM THROUGH SEXUALISED IMAGERY

Sexualised imagery in this report refers to the creation, capture, or circulation of visual material depicting individuals in sexually suggestive or explicit situations without their consent. These categories are examined together because they share a common mechanism: visual material is used as leverage to damage reputation, enable coercion, and cause sustained psychological harm.

The material documented in this section consists of real images and videos of identifiable individuals rather than synthetically generated content. Although material was often edited or repurposed, its harm was closely tied to the fact that it depicted actual people and actual acts.

✿ 1.1 Frequency

In Year 3, 68 victim-survivors reported harms involving sexualised imagery. The Trustline reported 239 pieces of harmful content, links, or associated accounts in these cases, which was the highest volume of content-related intervention recorded across any harm category.

This cluster includes five related forms of categorised harm:

1. Erotic posing was reported by 23 victim-survivors and involved 84 pieces of content depicting sexualised presentation without explicit sexual activity.
2. Imagery depicting solo sexual activity was reported by 20 victim-survivors and involved 61 pieces of content.
3. Penetrative sexual content was reported by 12 victim-survivors and involved 47 pieces of content.
4. Non-penetrative sexual interaction was reported by 8 victim-survivors and involved 29 pieces of content.
5. Partial nudity was reported by 5 victim-survivors and involved 18 pieces of content.

Table 7: Frequency of Harms Through Sexualised Imagery (Year 3)

Type of sexualised imagery harm	Victim-survivors	Harmful links/ accounts reported	
Erotic posing	23	84	3.7
Solo sexual activity imagery	20	61	3.1
Penetrative sexual content	12	47	3.9
Non-penetrative sexual interaction	8	29	3.6
Partial nudity	5	18	3.6
Total sexualised imagery cases	68	239	3.5

A notable finding is that material with less explicit sexual content, such as that categorised as erotic posing and partial nudity, accounted for a substantial share of reported content. This suggests that perpetrators frequently relied on imagery that could evade automated moderation systems while still causing significant harm to the victim-survivor.

Year 3 saw both a higher number of victim-survivors and a larger volume of content per case than in previous years. On average, each affected victim-survivor was associated with 3.5 separate uploads or accounts. In many cases, imagery reappeared after removal through reposting, new accounts, or migration to less-regulated websites.

✿ 1.2 Survivor Profile

Adolescents and younger adults were more frequently represented in cases involving erotic posing and solo sexual activity imagery.

Cases involving penetrative or non-penetrative sexual interaction were relatively more visible among older adolescents and adults.

Female victim-survivors constituted the majority across most sub-categories. Male victim-survivors were also present, particularly in cases involving financially motivated coercion.

Across age groups, victim-survivors described distress shaped by the perceived permanence and loss of control over visual material once circulated. Anxiety was often linked not only to immediate reputational consequences but also to the anticipation that the content may resurface in the future, get discovered by family or employers, and its long-term social implications.

✿ 1.3 Perpetrator Profile

When perpetrators were known, they were typically current or former intimate partners or acquaintances who had prior access to private images or communications. Abuse in these cases was often connected to relationship breakdown, betrayal of trust, or attempts to maintain control after separation.

Where perpetrators were unknown, case records pointed to networks of actors—often anonymous—who shared, edited, archived, or monetised sexualised material.

In several instances, the primary source of a leak was a known person, and that violation was then followed by secondary actors who reposted, repackaged, or aggregated imagery to attract engagement, expand follower bases, or generate revenue. This distributed circulation chain contributed significantly to the persistence of harm and complicated containment efforts.

✿ 1.4 Platforms

Sexualised imagery was reported across both mainstream and unregulated platforms. Instagram and Facebook were common initial sites of circulation or amplification. WhatsApp and Telegram featured in cases involving distribution within peer groups or closed networks.

A substantial share of harmful content was traced to a variety of websites hosting pornography, including tube sites, fringe unregulated platforms, and file-hosting services. Once content reached these platforms, takedown efforts became significantly more complex and time-consuming.

✿ 1.5 Patterns Noted

The severity of harm and the ease of removal have an inverted dynamic. Less explicit material such as erotic posing, partial nudity, and suggestive presentation, proved harder to remove than overtly sexual content because it was less consistently identified as violating platform policies. Automated moderation systems are calibrated primarily to detect explicit sexual content. Material that fell below that threshold but was still used to humiliate, coerce, or expose a victim-survivor circulated longer, reached wider audiences, and generated more repeated intervention cycles.

Removal of individual pieces of content rarely ended the harm cycle. Imagery reappeared through new accounts, compilation uploads, and migration to less regulated platforms. This pattern indicated that single-point intervention is structurally insufficient for sexualised imagery cases, and that sustained monitoring and repeated reporting are operational requirements.

In a significant number of cases, an identifiable primary source of a content leak was followed by networks of secondary actors who reposted, repackaged, or monetised the material. These actors had no prior relationship with the victim-survivor and no interpersonal motive. Their participation was driven by attention and revenue.

✿ 1.6 Case Study: Recurring Circulation of Sexualised Imagery

Victim-Survivor Age: 20 (female survivor), 27 (male survivor)

Location: Cuttack, Odisha

Timeline: November 2024 – February 2026 (ongoing)

Incident

In November 2024, a 27-year-old man from Odisha contacted Meri Trustline after learning that intimate content involving him and his former partner had begun circulating online without their consent. The material had been recorded privately earlier that year. Its availability in public circulation first came to his attention through messaging platforms, after which it was found on multiple pornographic websites and social media accounts.

Impact

As the number of links increased, the survivor struggled to understand the scale and speed of dissemination. Friends, extended family, and acquaintances had already come across the content. The possibility of continued circulation within their local networks generated intense shame and fear of recognition. They reported avoiding public spaces and altering aspects of their appearance to reduce the likelihood of being identified.

Over the months that followed, circulation became more complex. Edited versions began appearing on short-video platforms, repackaged with music overlays and manipulated audio that increased shareability and renewed attention. Links were simultaneously routed through file-hosting services, mirror browsing sites, and encrypted group channels, making the spread difficult to track or contain.

The case also involved complicated interpersonal dynamics. Blame and pressure came from individuals connected to the incident. Communication with the female survivor especially became limited after her family came to know of the leak and restricted her access to digital devices.

Intervention

The Trustline supported both survivors through systematic identification and reporting of links across pornographic websites and social media platforms, reverse-image search and evidence documentation, escalation through platform grievance and copyright mechanisms, and coordination of a reporting spreadsheet to manage high link volumes. Psychosocial support focused on stabilisation, expectation-setting about the likelihood of recurrence, and sustained accompaniment through repeated intervention cycles. The victim-survivors were also taught strategies of self-reporting so they could feel empowered to take action.

By early 2026, the content had resurfaced in an altered form, underscoring the persistence of harm even after repeated removal efforts. The case remains open.

Nature of harm: Non-consensual intimate imagery resulting in reputational, emotional, and social harm.

Form of circulation: Initial private leak followed by multi-platform uploads, repost networks, and remix edits that enabled recurring visibility.

Sphere of spread: Encrypted messaging channels, pornography hosting websites, short-video platforms, and mirror browsing services.

Relationship between survivor and perpetrator: Previously known intimate partner; subsequent circulation involved multiple unknown actors.

Primary support needs identified:

- Removal of content across platforms
- Containment of ongoing circulation
- Psychosocial reassurance and expectation-setting
- Guidance on documentation and reporting processes

Key Insight

This case demonstrates how sexualised imagery abuse increasingly unfolds as a prolonged process of circulation and re-emergence rather than a single incident. Less explicit edited versions evaded moderation thresholds and circulated longer than the source material. New uploads continued to appear months after initial removal. Secondary actors with no relationship to either survivor drove sustained amplification through remix, redistribution, and keyword-based discovery. Together, these dynamics produced harm experienced not as a single incident but as a condition of ongoing exposure with no definitive endpoint.



2 HARM THROUGH CHILD SEXUAL ABUSE AND EXPLOITATION MATERIAL (CSAEM)

Child Sexual Abuse and Exploitation Material (CSAEM) in this report refers to visual material depicting minors (below the age of 18 years) in sexually implicit or explicit situations, including sexual activity, sexualised posing, or contexts that sexualise the child. The term reflects the framing increasingly used in Indian jurisprudence, including observations by the Hon'ble Chief Justice of India emphasising that such material constitutes exploitation, rather than merely "pornography"¹⁶.

The creation, possession, circulation, or facilitation of access to such material constitutes a serious criminal offence under the Protection of Children from Sexual Offences (POCSO) Act, 2012, and is treated as a zero-tolerance category by most digital platforms.

CSAEM-related harm, similar to other forms of image-based abuse, often unfolded through rapid and uncontrolled circulation following initial recording or content leak. Material was commonly reshared within peer environments before moving to wider digital spaces, including public social media accounts and external hosting sites. In some instances, existing material was edited, combined with other media or reposted with new captions or audio overlays, contributing to renewed circulation and complicating removal efforts.

2.1 Frequency

In Year 3, 10% of victim-survivors (n = 13 of 130) whose cases required intervention were affected by CSAEM-related harms. Trustline's intervention in these required action on 53 pieces of harmful content, links, or associated digital accounts.

On average, each affected minor was associated with approximately four separate uploads or circulation points, reflecting repeated dissemination across digital spaces.

Cases were reported from multiple states, including Maharashtra, Assam, Punjab, Telangana, Uttar Pradesh, and West Bengal.

¹⁶LiveLaw, *Desire to Sexually Exploit Children Inherent in the Act of Watching Child Sexual Exploitative Materials*: Supreme Court, 23 September 2024.

✿ 2.2 Survivor Profile

The majority of reported CSAEM cases in Year 3 involved adolescent minors in the 13 to 17 age group. Two cases involved children who were below the age of 10.

Female victim-survivors constituted 92% (n = 12) of the cases, while 1 case involved a male minor.

In several instances, circulation began within peer or school-based digital networks before expanding into wider online environments. Victim-survivors and their caregivers frequently described distress shaped by the loss of control over how widely the material might circulate and who might encounter it over time.

Concerns were often linked to disruption of schooling, withdrawal from social participation, and the fear of long-term stigma.

✿ 2.3 Perpetrator Profile

In 69% of the CSAEM cases (n = 9), victim-survivors reported knowing the perpetrator, all of whom were male. This marks CSAEM as one of the harm categories in which abuse more frequently emerged from proximate social environments rather than anonymous online actors. Perpetrators included peers, neighbours, relatives, etc.

In the remaining 31% of the cases, circulation was driven by unknown individuals with anonymous profiles, aggregation accounts, and participants in closed sharing groups, who had no direct connection to the child but contributed to the spread of the material.

✿ 2.4 Platforms

It was observed that 75% of the documented circulation (n=40) occurred on unregulated or pornographic hosting websites, where removal was slow, inconsistent, and frequently required multi-channel escalation. Instagram accounted for 15% of the instances. Telegram, WhatsApp, Facebook, and Snapchat were also reported, typically in cases involving peer-group sharing.

✿ 2.5 Patterns Noted

Within the CSAEM cases documented, most material involved sexualised posing and non-penetrative imagery, alongside a smaller but significant subset involving more explicit forms of abuse. Across these forms, harm typically unfolded through rapid and uncontrolled circulation following initial recording or content leak.

Material was commonly reshared within peer environments before moving to wider digital spaces, including public social media accounts and external hosting sites. In some instances, existing material was edited, combined with other media or reposted with new captions or audio overlays, contributing to renewed circulation and complicating removal efforts.

The replicability and perceived permanence of such imagery contributed to sustained psychological strain for both victim-survivors and caregivers. Effective response, therefore, required prioritising speed of reporting, preservation of digital evidence, and ongoing monitoring to detect resurfaced content, coupled with ensuring appropriate emotional support to both the child and caregiver.

In CSAEM-related cases, response pathways consistently involved ensuring that knowledge of the incident was communicated both to the criminal justice system and to a trusted adult responsible for the child's care. Reports were typically initiated through statutory channels, alongside parallel efforts to inform or involve caregivers where they were not already aware. In several instances, a parent or guardian was the first point of contact with the Trustline and remained closely engaged throughout the intervention process.

✿ 2.6 Case Study: Circulation of Sexual Content Involving a Minor

Age: 17

Gender: Female

Location: Delhi

Timeline: May 2025 – August 2025

Incident

In May 2025, a 38-year-old medical professional contacted Meri Trustline after discovering sexually explicit content bearing her 17-year-old niece's facial features on multiple adult websites. The minor reported that the material had been digitally manipulated and that she had not participated in the sexual activity depicted. The intervention proceeded on the basis of her account with a primary focus on content takedown.

Subsequently, it was discovered that the imagery was already hosted across several pornographic platforms and intermediary file-hosting services. Available timestamps suggested the content had been online for a significant period before discovery. This delay complicated efforts to establish the origin of the content and identify those responsible for the uploads.

Impact

The delayed discovery shaped the survivor's experience in specific ways. Uncertainty about how long the material had been circulating, who had encountered it and how widely it had spread, generated sustained anxiety that was difficult to contain because it had no clear starting point.

The survivor initially preferred that all communication with the Trustline pass through her aunt who acted as a mediator and coordinator throughout the early stages of support. Establishing direct contact required repeated reassurance about confidentiality and the non-judgemental nature of the assistance being offered.

The family's response added a layer of complexity. There was a strong desire to identify and pursue the perpetrator. But there was also reluctance to independently engage with law enforcement.

Intervention

Content removal involved coordinated reporting through DMCA takedown notices, the National Cybercrime Reporting Portal and the Aarambh India–IWF Hotline for child sexual abuse material. Within two weeks, 28 links were removed from hosting platforms and the content was hashed to reduce the likelihood of re-uploads. Search thumbnails and indexed traces continued to surface after initial removals, requiring repeated reporting to search engines.

Alongside removal efforts, the Trustline provided counselling-oriented guidance focused on online safety, adolescent vulnerability in digital interactions and strategies for securing personal data and devices. Safety planning emphasised identifying trusted adults and establishing clear pathways for seeking support when encountering distressing online content.

By August 2025, immediate circulation risk had stabilised.

Nature of harm: Digitally manipulated sexual imagery involving a minor, resulting in risks of reputational injury, emotional distress, and persistent digital traceability.

Form of circulation: Initial discovery through peer sharing followed by identification of distributed hosting across pornography websites and file-hosting services.

Sphere of spread: Public adult content platforms and various content hosting platforms that enabled extended visibility.

Relationship between survivor and perpetrator: Unknown; no clear indicators of prior relationship or identifiable motive.

Primary support needs identified:

- Rapid removal of harmful content
- Legal guidance
- Trust-building to facilitate survivor engagement
- Safety education and psychosocial reassurance

Key Insight

This case illustrates how child sexual abuse and exploitation material may continue to shape a minor's digital footprint even after primary removals, particularly when residual indexing, mirrored hosting and delayed detection prolong visibility. Such dynamics increase the emotional and procedural burden on survivors and families. This highlights the need for coordinated, multi-layered response systems that address both removal and ongoing discoverability.

It also highlights the legal challenges since the perpetrators were not being identified and the source of the leak was unknown. Families face significant uncertainty in pursuing legal recourse. The absence of identifiable offenders complicates the filing of complaints, limits the ability of law enforcement to initiate targeted action, and often leaves families navigating unclear or prolonged legal processes with limited recourse.



3 HARM THROUGH DIGITALLY MANIPULATED SEXUAL CONTENT/DEEPFAKES

A deepfake is a digital photo, video, or sound file of a real person that has been created with artificial intelligence (AI) to make an extremely realistic but false depiction of them doing or saying something that they did not actually do or say. Deepfakes are created using AI software that draws on real photos or recordings of the person to model and produce new content.¹⁷

In Year 3, Meri Trustline documented deepfake-related harm across two distinct forms. The first involved sexually explicit synthetic imagery such as AI-generated or face-swapped content depicting victim-survivors in sexual situations without their participation or consent.

The second involved the manipulation of real incidents such as AI-altered material circulated in connection with actual events of violence against women, used to reconstruct, sensationalise or fabricate narratives around those events. The harm in these cases, therefore, was not limited to sexual exposure but they undermined confidentiality of victims, distorted factual records, and intensified public scrutiny of survivors and their families.

✿ 3.1 Frequency

In Year 3, digitally manipulated content was reported by 10 victim-survivors. Interventions in these cases required action on multiple links, reposts, and associated accounts involved in the circulation of fabricated material.

Although the number of victim-survivors reporting deepfakes is smaller than other image-based harm categories, it reflects the growing ease with which such material can now be created and circulated. The tools required are widely available, free to use and require no technical expertise.

¹⁷Office of the eSafety Commissioner, *Deepfake Trends and Challenges*,

✿ 3.2 Survivor Profile

Adolescents and young adults, mostly female victim-survivors constituted the majority of survivors who reported this form of abuse. In some instances, manipulated content intersected with experiences of prior sexual harassment or assault, causing distress and violations through renewed exposure and loss of confidentiality.

✿ 3.3 Perpetrator Profile

Perpetrators were typically unknown to victim-survivors and operated through anonymous or pseudonymous accounts. Creating harmful content in this category required no prior relationship with the target. Publicly available photographs or social media images were sufficient.

Also, secondary amplification was common. These included individuals seeking online visibility or attempting to capitalise on sensational news events.

✿ 3.4 Platforms

Digitally manipulated content circulated primarily through mainstream social media platforms including Instagram, Facebook, YouTube, and X (Twitter) as well as messaging applications such as WhatsApp and Telegram.

✿ 3.5 Patterns Noted

Unlike other forms of image-based abuse, the production of harm in these cases did not always require prior intimacy, access to private material or sustained interpersonal interaction. Publicly available photographs, news footage or social media images were sufficient to enable manipulation and circulation.

Across cases, victim-survivors described anxiety linked to the plausibility of manipulated imagery and uncertainty about whether viewers would recognise the material as fabricated. Harm was, therefore, shaped not only by circulation but also by the erosion of trust in the authenticity of digital visual evidence.

A further pattern observed was the creation of synthetic visuals to participate in ongoing public discourse around high-visibility incidents. In such cases, manipulated material functioned as sensational or attention-seeking content. The resulting spread nevertheless generated reputational harm, confusion, and emotional distress for affected individuals.

✿ 3.6 Case Study: Synthetic Media and the Attention Economy in the R.G. Kar Case

Age: Adult female (victim of violent crime)

Gender: Female

Location: Kolkata, West Bengal

Timeline: August 2024 – January 2025

Incident

In August 2024, the rape and murder of a trainee doctor at a major medical college in Kolkata triggered widespread national outrage in India and sustained protest mobilisation. The incident generated media attention and high levels of online engagement with social media feeds rapidly filling with user-generated content referencing the case. As public discussion intensified, the dynamics of virality began to shape how information and misinformation about the victim-survivor circulated in digital spaces.

Impact

Numerous accounts were created across Facebook, Instagram, and YouTube using the victim's name and photographs sourced from her personal online profiles. While some positioned themselves as expressions of solidarity or calls for justice, others disseminated misleading visual material and speculative narratives that blurred the boundary between public commentary and impersonation. Judicial directions¹⁸ issued by the Hon'ble Supreme Court of India restricting disclosure of the victim's identity proved difficult to enforce within fast-moving social media platforms, which are characterised by rapid resharing.

Case records also identified the circulation of digitally altered and synthetic material appearing to reconstruct aspects of the assault including edited video fragments, AI-generated image sequences and dramatised re-enactments designed to simulate the victim's experience. Fabricated voiceovers were layered onto such visuals to suggest imagined conversations or final moments, heightening emotional engagement and increasing the likelihood of viral dissemination. Some widely shared posts misidentified unrelated individuals as the victim, demonstrating how speculative storytelling gains traction during moments of heightened public attention.

In certain instances, impersonating accounts were also associated with promotional or sexually suggestive advertising content, indicating how attention surrounding gender-based violence can be appropriated for opportunistic monetisation.

Intervention

Over the reporting period between August 2024 to May 2025, Meri Trustline identified and escalated 31 accounts connected to identity misuse, harmful speculation or synthetic media circulation. All were successfully taken down through platform escalation mechanisms.

Nature of harm: Identity misuse and digitally manipulated content linked to a victim of gender-based violence, resulting in risks to dignity, confidentiality, and the emotional well-being of affected families.

¹⁸Kinori Ghosh & Anr. v/s Union of India & Ors., (2023), Supreme Court of India, Order dated 20 August 2024

Form of circulation: Creation of impersonating accounts, synthetic visual reconstructions, misleading narratives, and opportunistic reposting during a high-attention news event.

Sphere of spread: Mainstream social media platforms and short-video platforms shaped by algorithmic visibility and rapid user engagement.

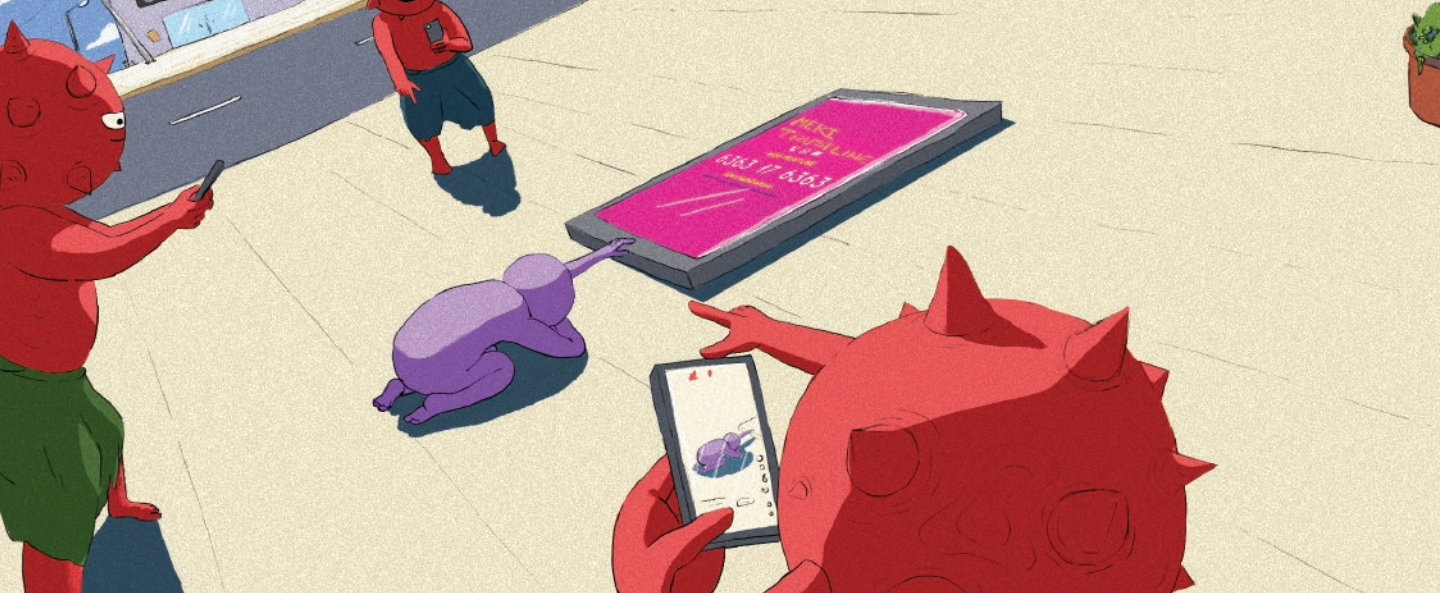
Relationship between survivor and perpetrators: Unknown and diffuse; circulation driven by multiple opportunistic actors rather than a single identifiable source.

Primary support needs identified:

- Rapid reporting and removal of impersonating content
- Containment of speculative and misleading narratives
- Protection of victim identity in line with legal safeguards

Key Insight

Rapid sharing, algorithmic amplification, and speculative user participation can generate secondary waves of circulation that extend beyond verified information. This creates difficulty in enforcing confidentiality protections or containing identity exposure. In such moments, the speed and emotional intensity of online engagement can transform public outrage into a parallel ecosystem of harmful visibility.



4 HARM THROUGH DENIGRATION AND REPUTATIONAL TARGETING

Denigration refers to the circulation of images, videos, or information intended to ridicule, humiliate, or socially discredit a victim-survivor. Unlike image-based abuse with sexual intent, which derives its harm primarily from the intimate or sexual nature of the content, denigration operates through the social meaning attached to material through its framing, the audience, and the networks through which it travels. The content itself may be innocuous but the context of circulation and the intent behind it constitute the harm.

4.1 Frequency

In Year 3, this form of harm was reported by 42 victim-survivors and involved 86 pieces of harmful content documented by the Trustline. Based on simple averages, each affected victim-survivor was associated with approximately 2 instances of denigrating content.

The difference between the number of victim-survivors and the volume of harmful content reflects the recurrent nature of reputational abuse. In many cases, the same individual was targeted through repeated reposting, reframing, or re-uploading of content across multiple digital platforms.

Table 8: Denigration/Damaging Reputation Cases Across Three Years

	Year 1	Year 2	Year 3
Victim-survivors	24	30	42

Reports of denigration have increased steadily across reporting cycles. The number of victim-survivors reporting this form of harm rose by 75% over 3 years—from 24 in Year 1 to 30 in Year 2, and finally to 42 in Year 3.

✿ 4.2 Survivor Profile

Adults aged 28 years and above constituted the largest share within this category, followed by adolescents and young adults. Female victim-survivors represented the majority of those affected. In several cases, the circulation of defamatory or compromising content intersected with concerns related to employment, marriage prospects, family reputation or social standing.

✿ 4.3 Perpetrator Profile

In a majority of the reported instances, perpetrators were unknown to victim-survivors, indicating the role of anonymous digital environments in enabling reputational attacks. Where perpetrators were identified, they were overwhelmingly male and were often situated within existing interpersonal or social relationships.

✿ 4.4 Platforms

Denigration-related content circulated across Instagram, Facebook, WhatsApp, X (Twitter), YouTube, and Telegram. In some cases, content migrated to unregulated websites and message boards.

✿ 4.5 Patterns Noted

In this category, visibility itself is the mechanism of violence. Harm is produced not through the existence of damaging content alone but through its repetition, its contextual framing and its circulation within socially meaningful networks.

In a significant proportion of cases involving known perpetrators, harm originated in interpersonal disputes such as workplace conflicts, neighbourhood tensions, and relationship breakdown. These were subsequently digitised and circulated. A localised incident became a public event through the act of recording and uploading content.

In several cases, denigrating content was accompanied by slurs referencing the victim-survivor's caste, religion, gender, or community background. Denigration in these cases was not only personal but communal and designed to mark the victim-survivor as an outsider or legitimate target within a broader social hierarchy.

Some accounts with history of politically motivated or communally inflammatory content expand the reach and the perceived legitimacy of the attack. Victim-survivors described sustained emotional fatigue linked to the scale of reporting required and uncertainty about the social consequences of having been publicly humiliated within networks that mattered to them.

🌟 4.6 Case Study: Viral Circulation of Hate Crime Footage

Age: 35

Gender: Male

Location: Thane, Maharashtra

Timeline: March 2025 – May 2025

Incident

In March 2025, a 35-year-old man from Maharashtra contacted Meri Trustline after footage of his physical assault at his workplace began circulating widely on social media. The incident stemmed from a workplace dispute. It escalated when individuals associated with local political groups were deliberately brought into the workplace premises by some of those involved under the pretext of “settling the dispute”.

The confrontation subsequently took on a communal and xenophobic shade. During the assault, perpetrators used identity-based slurs that framed the survivor as an “outsider” and physically assaulted him. Members of the political group as well as bystanders recorded the incident. The footage was widely disseminated online.

Impact

Within days, the footage spread rapidly across Facebook, Instagram, YouTube, and X (Twitter), reposted as short-form videos accompanied by abusive captions and inflammatory commentary. In some instances, the clip was incorporated into compilation reels featuring other acts of communal violence, extending its visibility beyond the original context. The viral spread exposed the survivor and his family to ridicule, scrutiny, and social pressure from acquaintances and extended networks who had encountered the video online.

The repeated reappearance of the footage contributed to sustained emotional strain. The survivor reported anxiety about how he was being perceived by colleagues and relatives, and distress linked to encountering the clip in new forms each time he believed it had been contained.

Intervention

Reverse searches were conducted to map the spread of the footage and identify accounts responsible for reposting. Multiple instances were reported under categories related to harassment, hate speech and privacy violations. Several platforms removed content promptly. Others required sustained monitoring, repeated reporting and, in one instance, formal escalation through grievance channels alongside identity verification before the content was taken down.

Alongside technical intervention, the Trustline counsellors provided psychological first aid, encouraged the survivor to reduce direct viewing and checking the circulating content constantly and supported him in maintaining a daily routine while response efforts continued.

By May 2025, most identified uploads had been removed following coordinated platform reporting and escalation.

Nature of harm: Viral circulation of assault footage accompanied by identity-based harassment, resulting in reputational damage, psychological distress, and social stigma.

Form of circulation: Recording of offline violence followed by rapid reposting as short-form videos, compilation edits, and inflammatory commentary.

Sphere of spread: Mainstream social-media platforms characterised by algorithmic amplification and high engagement with provocative content.

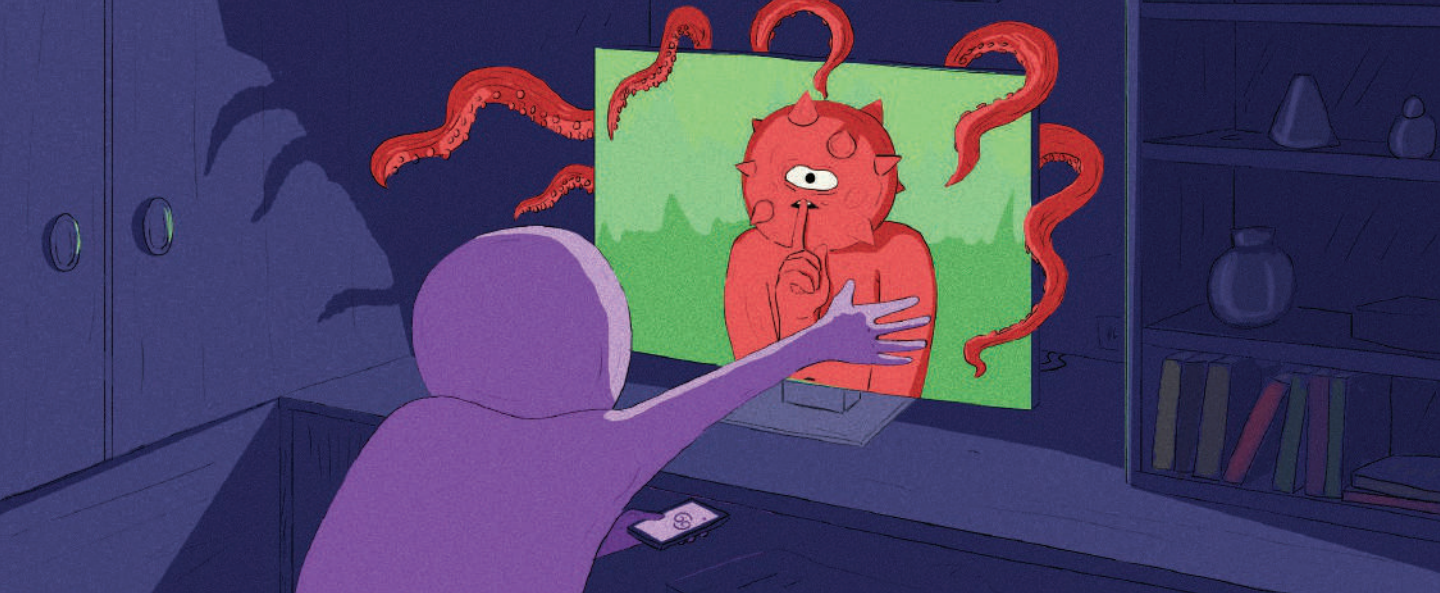
Relationship between survivor and perpetrators: Known individuals connected to a workplace conflict; subsequent online harassment involved multiple opportunistic actors.

Primary support needs identified:

- Removal of harmful content across platforms
- Containment of identity-based harassment
- Psychosocial reassurance and coping support
- Guidance on escalation through formal grievance mechanisms

Key Insight

This case illustrates how offline acts of violence and communal faultlines can be transformed into prolonged digital harm through viral circulation. Once recorded and widely shared, such footage may continue to shape public perception and emotional well-being long after the immediate conflict has subsided.



5 HARM THROUGH COERCIVE INTIMIDATION

This category captures forms of harm in which victim-survivors were subjected to pressure through the threat of exposure, continued harassment or anticipated reputational consequences.

Coercive intimidation operated through two closely related pathways:

- Threats of online consequences refer to situations in which victim-survivors were warned that private communication, images, or personal information would be circulated within social networks such as family groups, peer circles, or workplaces.
- Sextortion or blackmail refers to cases in which such threats were used to demand financial payment, continued interaction, sexual content, or other forms of coercive non-consensual compliance to demands made.

5.1 Frequency

Table 9: Coercive Intimidation Harms (Year 3)

Type of coercive harm	Victim-survivors	Harmful links/ accounts reported	Avg. content per survivor
Threats of online consequences/ intimidation	21	26	1.2
Sextortion/ blackmail	17	29	1.7
Total coercive intimidation cases	38	55	1.4

In Year 3, 38 victim-survivors reported harms falling within these combined categories. Threats of online consequences were reported by 21 victim-survivors, while 17 victim-survivors experienced sextortion or blackmail.

Across these cases, the Trustline documented 55 pieces of threatening or extortion-related content or associated digital accounts. Of those, 26 were linked to threat-based intimidation and 29 linked to sextortion-related coercion.

The higher number of accounts relative to victim-survivors reflects repeated contact through multiple profiles and cross-platform escalation.

Coercive intimidation has remained a persistent feature of Trustline's casework. Comparable categories were reported by 24 victim-survivors in Year 1, 31 in Year 2, and 38 in Year 3, indicating a gradual increase across reporting cycles.

✿ 5.2 Survivor Profile

Threats of online consequences were more frequently visible among adolescents and younger adults, where intimidation was often linked to peer networks, early romantic interactions, or school-based social environments. The fear in these cases was typically about humiliation within known social circles.

Sextortion and blackmail were more visible among older adolescents and adults, particularly in cases that began through social media or dating platforms. Male victim-survivors appeared more frequently in sextortion cases than in most other harm categories—a pattern seen in international data on financially motivated online sexual coercion as well.¹⁹

✿ 5.3 Perpetrator Profile

Perpetrators in both categories were more often unknown to victim-survivors. Anonymous profiles, rapidly created accounts, and cross-platform communication enabled intimidation without prior social proximity. In minority of the cases where perpetrators were known, they were typically situated within peer or interpersonal networks.

Female victim-survivors were more likely to face coercive intimidation from known perpetrators, while male victim-survivors were more likely to be targeted by unknown perpetrators.

✿ 5.4 Platforms

Threat-based intimidation and sextortion incidents were reported across social media platforms and private messaging applications, including Instagram, Facebook, WhatsApp, and Telegram. Case records suggest that perpetrators often used multiple accounts and cross-platform communication to sustain intimidation even after blocking or reporting. Dating applications were also noted as initiation points in some financially motivated sextortion cases.

¹⁹ Eaton, A. A., Ramjee, D., & Saunders, J. F. (2022), *The Relationship between Sextortion during COVID-19 and Pre-pandemic Intimate Partner Violence, Victims & Offenders*.

🌟 5.5 Patterns noted

In sextortion-related cases, the victim-survivor was entrapped with a sense of manufactured urgency. Apparently consensual interactions were quickly followed by threats of exposure and demands for payment. Pressure of time running out, repeated and escalating messaging of threat and consequences, and the circulation of screenshots were commonly used to intensify fear and induce compliance.

Across both threat-based and financially motivated incidents, intimidation was sustained through the use of multiple accounts and continued contact. This produced a sense of inescapability and heightened emotional strain.

Victim-survivors frequently reported anxiety shaped not only by the immediate threat, but by the continuing possibility of future circulation. In several cases, even after content removal or account takedown, the anticipation of renewed contact remained a significant source of distress.

These patterns indicate that in coercive intimidation, harm is produced less through the actual circulation of content and more through the anticipation of exposure, which functions as a powerful mechanism of psychological control.

🌟 5.6 Case Study: Sexual Coercion Through Threats of Circulating CSAEM

Age: 17

Gender: Female

Location: Chandigarh

Timeline: April 2024 – August 2025

Incident

In April 2024, a 17-year-old girl contacted Meri Trustline after being approached online by an unknown individual who claimed to possess intimate images obtained from her former partner's device. When she challenged this, the perpetrator threatened to distribute the images widely unless she agreed to video calls with him.

Impact

During these calls, the perpetrator coerced the survivor into sexual posing and undressing while recording the interaction. He then sent her brief clips from the recordings to demonstrate what he held and to reinforce the threat. Each encounter followed the same sequence: anonymous contact, threat of exposure, forced compliance, withdrawal, and the assurance that he would return. The cycle repeated.

The emotional impact was significant. The survivor described intense guilt and fear about potential exposure. She was reluctant to approach law enforcement, worried about how her family would react if the situation became known. At times, she expressed sympathy for the perpetrator after he indicated remorse. It's a common response that counsellors recognised as a feature of the coercive dynamic itself rather than evidence of genuine ambiguity about what was happening to her.

Intervention

Intervention focused first on the survivor's immediate emotional safety. A complaint was filed through the National Cybercrime Reporting Portal and known accounts were reported to platforms. Crucially, the Trustline identified additional accounts the perpetrator appeared to have created in anticipation of future contact and had these taken down proactively. Thus, disrupting the cycle before it could resume. This was done by identifying a pattern that the perpetrator was employing: anonymous accounts incorporating the victim's name alongside sexually suggestive wording.

The survivor was supported in maintaining complete disengagement from the perpetrator, blocking all known accounts and preserving evidence of communication for legal purposes. Counselling continued through this period.

Nature of harm: Sexual coercion through threats of non-consensual image circulation, resulting in psychological distress and reputational vulnerability.

Form of circulation: Threat-based control combined with extraction of further sexualised material during recorded video interactions.

Sphere of spread: Anonymous social-media accounts and private messaging applications.

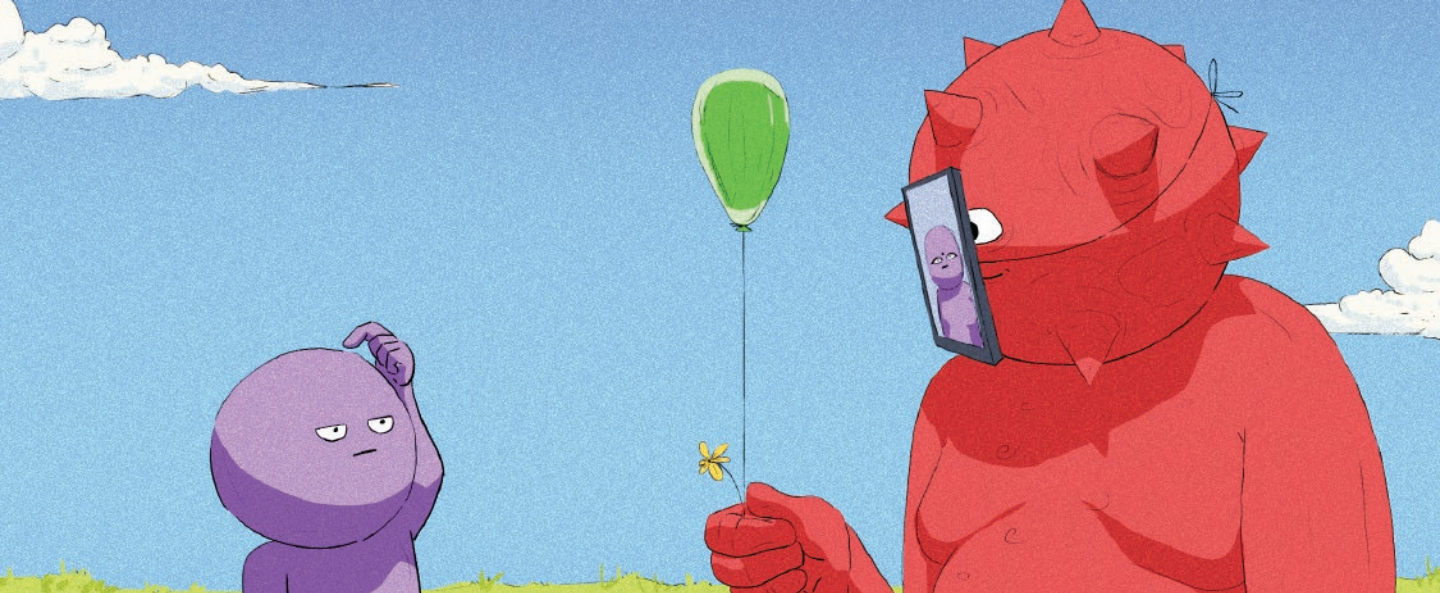
Relationship between survivor and perpetrator: Unknown individual claiming access to intimate material through a prior relationship context.

Primary support needs identified:

- Safety planning centred on strict disengagement and evidence preservation
- Psychosocial reassurance to address guilt, fear, and self-blame
- Guidance on reporting coercive threats through formal cybercrime mechanisms
- Pre-emptive containment of repeated anonymous contact attempts

Key Insight

This case demonstrates how digital coercion may operate through sustained emotional manipulation and grooming rather than immediate public exposure of intimate material. The perpetrator's repeated pattern of anonymous contact, threats, intermittent withdrawal, and expressions of remorse functioned to destabilise the survivor's sense of agency and normalise compliance. Such tactics can create confusion, self-blame, and misplaced sympathy towards the abuser, particularly among adolescents with limited support networks. The resulting emotional entrapment becomes a central mechanism of control.



6 IDENTITY EXPOSURE AND MANIPULATION

Identity exposure and manipulation in this report brings together two categories: impersonation and doxxing. Both share a common mechanism of harm involving the use of a person’s own information: their name, photograph, contact details or personal circumstances, to manipulate how others see and perceive them.

Impersonation refers to the creation or use of fake digital accounts that falsely represent the victim-survivor in order to harass, mislead, or damage reputation.

Doxxing refers to the unauthorised disclosure or circulation of personal information such as phone numbers, home addresses, workplace details or family information with the intent to enable harassment, intimidation, or reputational harm.

6.1 Frequency

Table 10: Identity Exposure & Manipulation Harms (Year 3)

Type of identity-related harm	Victim-survivors	Harmful links/ accounts reported	Avg. content per survivor
Impersonation	15	39	2.6
Doxxing / forced identity exposure	14	28	2.0
Total identity exposure & manipulation-related harm cases	29	67	2.3

In Year 3, identity-related harms were reported by 29 victim-survivors, comprising 15 cases of impersonation and 14 cases involving doxxing or forced identity exposure.

Trustline's intervention in these cases required action on 67 pieces of harmful content, links, or associated digital accounts. Of those, impersonation-related incidents involved 39 offending accounts or links, while doxxing-related incidents involved 28 circulation points.

On average, each affected victim-survivor encountered two to three instances of harmful circulation, reflecting repeated reposting of personal information, or the creation of multiple fake profiles.

✿ 6.2 Survivor Profile

Identity-related harms were reported across age groups but were particularly visible among adolescents and young adults.

Female victim-survivors constituted a larger share of impersonation-related incidents, especially where fake profiles were used for sexualised harassment, reputational targeting or solicitation.

Male victim-survivors were more frequently represented in doxxing-related cases involving disclosure of contact details or misuse of identity within peer environments.

✿ 6.3. Perpetrator Profile

In a majority of reported instances, perpetrators were unknown to victim-survivors and operated through anonymous or pseudonymous accounts.

Where perpetrators were identified, they were often situated within peer groups, neighbourhood environments or existing interpersonal relationships.

In several adolescent cases, impersonation was carried out by individuals from the same school or social circle and patterns of repeat behaviour, including the creation of fake accounts targeting more than one individual, were observed.

Identity manipulation in such contexts frequently followed offline disputes that later migrated into digital spaces.

✿ 6.4 Platforms

Fake profiles and impersonation accounts were most commonly reported on Instagram and Facebook, while WhatsApp, Telegram, Snapchat and Gmail also featured.

🌟 6.5 Patterns Noted

The more credible the impersonating profile, the more confusion it generated. Profiles that closely mimicked the victim-survivor in tone, content, and appearance were more likely to deceive existing contacts and cause sustained reputational damage. In some cases, perpetrators purchased verified badges to make fake accounts appear authentic—a direct misuse of a platform feature intended to establish identity. At the other end of the spectrum, null accounts (profiles bearing only the victim-survivor's name with no content or activity) also proved difficult to take down, as platforms did not consistently treat inactive impersonation as a violation requiring removal.

In the majority of the cases involving known perpetrators, identity manipulation followed an offline dispute such as a conflict at school, within a neighbourhood, or in an interpersonal relationship, which was subsequently extended into digital spaces. The fake profile or disclosed information became a tool for continuing and amplifying a conflict that had begun elsewhere.

Several minor victim-survivors expressed reluctance to inform parents or teachers, citing fear of being blamed or not taken seriously.

Harm in this category was shaped less by the nature of individual posts and more by the social consequences of identity distortion within networks the victim-survivor could not easily leave or avoid. Victim-survivors described ongoing vigilance, reputational strain, and uncertainty about how widely misleading content had circulated.

🌟 6.6 Case Study: Online Impersonation and Reputational Distress Within Adolescent Peer Networks

Age: 14

Gender: Female

Location: Ghaziabad, Uttar Pradesh

Timeline: December 2024 – January 2025

Incident

In December 2024, a 14-year-old girl contacted Meri Trustline after discovering that a fake Instagram account had been created using her photograph and personal details. The account was actively posing as her and interacting with individuals from her school and social circles. She suspected the person behind it may have been connected to an earlier impersonation incident targeting one of her friends, suggesting a pattern of repeated identity-based targeting within the same peer network.

Impact

The incident took place during her exam season, intensifying existing anxiety and fear of reputational damage at a particularly vulnerable time. She was reluctant to inform teachers or family members, having seen other students in similar situations blamed rather than supported. She requested that all communication with the Trustline take place through email.

As the situation developed, she shared screenshots showing conversations between a senior student and the impersonating account, illustrating how the misuse had begun to affect her

standing within the school network. The harm was not in any single post but in the accumulating confusion about how she was being represented before people she knew.

Intervention

Counsellors reassured her that she was not responsible for the impersonation and guided her in collecting evidence including screenshots, URLs, and records of interactions. Despite a report to the platform, the account remained active. Therefore, a second, more detailed report highlighting specific policy violations was submitted. Following escalation, the account was taken down.

She confirmed the removal and expressed relief. Follow-up communication focused on reinforcing safety practices and supporting her emotional wellbeing through the remainder of the exam season.

Nature of harm: Digital impersonation involving misuse of a minor's identity, resulting in reputational vulnerability, emotional distress, and disruption to peer relationships.

Form of circulation: Creation of a fake profile that engaged with the survivor's social network, generating confusion about authenticity, and amplifying humiliation through indirect peer interactions.

Sphere of spread: Mainstream social media platforms, where identity replication and networked visibility enable rapid dissemination of misleading representations.

Relationship between survivor and perpetrator: Unconfirmed but suspected peer-network actor, indicating how interpersonal tensions within adolescent social environments may manifest through online impersonation.

Primary support needs identified:

- Prompt removal of impersonating content
- Guidance on documenting and reporting identity misuse
- Confidential psychosocial reassurance
- Safety planning that respects the survivor's communication preferences

Key Insight

The case highlights how fear of institutional or family blame can be as significant an obstacle to seeking help as the harm itself. Support pathways that are confidential, flexible, and on the survivor's terms are a primary condition that needs to be fulfilled if victim-survivors are to access support.

*Hacking and Financial Fraud

When incidents related to account compromise or financially motivated fraud were reported to the Trustline, support was typically informational and facilitative in nature. Many such approaches were not logged as full cases because victim-survivors primarily sought recovery of lost funds and accounts — an outcome that falls outside the Trustline’s operational mandate. In these situations, individuals were guided on steps to secure compromised accounts, preserve digital evidence, and access appropriate reporting pathways, including referral to the national cybercrime helpline (1930) and the cybercrime reporting portal. Legal guidance was also provided when requested. Consequently, only a small number of cases ($n = 6$) relating to hacking or financial fraud were formally recorded during the reporting period.

At the national level, however, the scale of such harms is substantial. Data from the National Crime Records Bureau²⁰ indicate that financial fraud constitutes the majority of recorded cybercrime incidents in India. Account hacking and related digital compromise also form a significant share of harms experienced by Indian internet users. This contrast highlights an important service gap.

There is a need for clearer referral pathways and more integrated response systems for individuals navigating financial and account-security harms. Strengthened customer-support mechanisms across platforms, financial institutions, as well as stronger systemic responses will be essential to ensure timely and survivor-centred resolution.



²⁰ Wani, S. (2025), Economic Offences Surge in India, While Convictions Lag, Forbes India, 1 October 2025

IX. Platform Response and Content Removal Outcomes

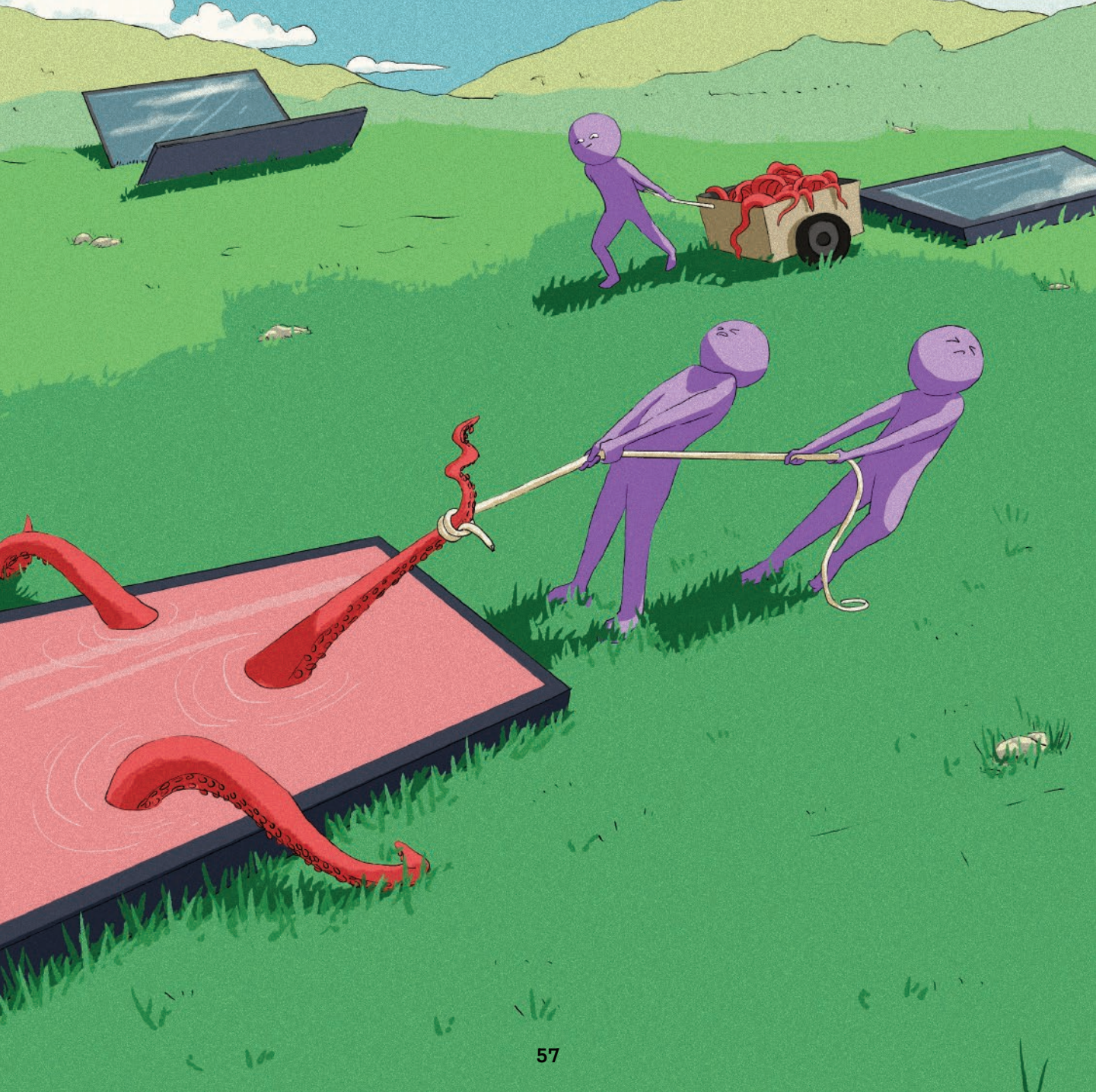


Table 11: Platform Occurrence Across Cases (n = 130)

Platform/ Category	Number of Cases Where Harm Occurred on the Platform	Share of Cases (%)
Instagram	90	69.2%
WhatsApp	25	19.2%
Telegram	20	15.4%
Facebook	20	15.4%
Pornographic websites*	14	10.8%
YouTube	7	5.4%
Google services	6	4.6%
Snapchat	5	3.8%
X (Twitter)	5	3.8%
Discord	3	2.3%
Reddit	3	2.3%
Messenger	2	1.5%
Others / Unspecified	2	1.5%

*Note: Values represent the proportion of cases in which each platform appeared. Percentages do not sum to 100% as multiple platforms may be involved in a single case.

The distribution of online harm across platforms spans multiple digital environments rather than remaining confined to a single platform. Instagram appears in over two-thirds of cases (69.2%), which is consistent with its position as one of the most widely used social media platforms and a central site of user interaction and content sharing.

A second layer of platforms, particularly WhatsApp (19.2%) and Telegram (15.4%), illustrates how incidents may evolve across more private or semi-private communication channels.

Notably, pornographic websites (10.8%) represent a growing area of concern both in frequency

and in their role within the broader harm ecosystem. While each individual domain may appear in relatively fewer cases, their collective presence and persistence make them significant. As regulatory and policy attention in India has largely focused on significant social media intermediaries, this segment of the ecosystem remains comparatively under-addressed, despite its role in hosting, recirculation, and prolonged availability of harmful content.

Differential Patterns of Platform Responsiveness

During Year 3, a total of 1,137 offending accounts and content instances were reported of which 981 (86.3%) were successfully taken down. This represents a substantial increase from the previous reporting cycle, when 537 accounts were reported and 409 (76.2%) were removed.

The increase in reporting reflects both the expanding scale and diversification of technology-facilitated abuse. However, the persistence of the removal gap indicates that crisis relief remains uneven and shaped by governance structures, moderation capacity, and escalation accessibility of concerned platforms.

Instagram and Facebook demonstrated comparatively higher responsiveness in cases escalated through structured reporting workflows, including Grievance Officer channels under IT Rules and established trusted-partner relationships.

WhatsApp, although part of the same corporate ecosystem, presented distinct intervention constraints. Even the Grievance Officer mechanisms were not always perceived as consistently effective and outcomes in many cases depended on survivor-led reporting and blocking strategies, rather than harm-based escalation.

Among other platforms, Telegram, Snapchat, and Discord demonstrated relatively effective response patterns in instances where policy violations were clearly documented. However, Telegram and Discord also allowed for high recidivism with alternate accounts emerging almost immediately following takedown action.

Moderation outcomes varied across other services. While clearly violative sexual content on YouTube was often removed promptly, contextual harms such as reputational targeting were less consistently taken down.

Content reported on X (Twitter) was among the least responsive platforms encountered, with repeated instances of delayed takedowns or non-removal despite escalation.

Pornographic Websites

Adult content hosting websites represented a significant proportion of reported accounts, estimated at around 10.8%.

Since July 2024, the Trustline recorded an increase in incidents where non-consensual intimate imagery was uploaded simultaneously across multiple adult content websites

Across widespread-circulation incidents, harmful material was typically identified on a mix of large commercial adult content platforms such as Pornhub, XVideos, and XNXX and a growing ecosystem of lower-visibility websites.

While established pornographic platforms generally maintained functional abuse-reporting pathways, intervention outcomes on smaller or newly emerging sites were far more inconsistent. Reporting interfaces were frequently non-responsive or altogether absent, requiring escalation to hosting providers or domain registrars. This significantly increased removal timelines and procedural complexity.

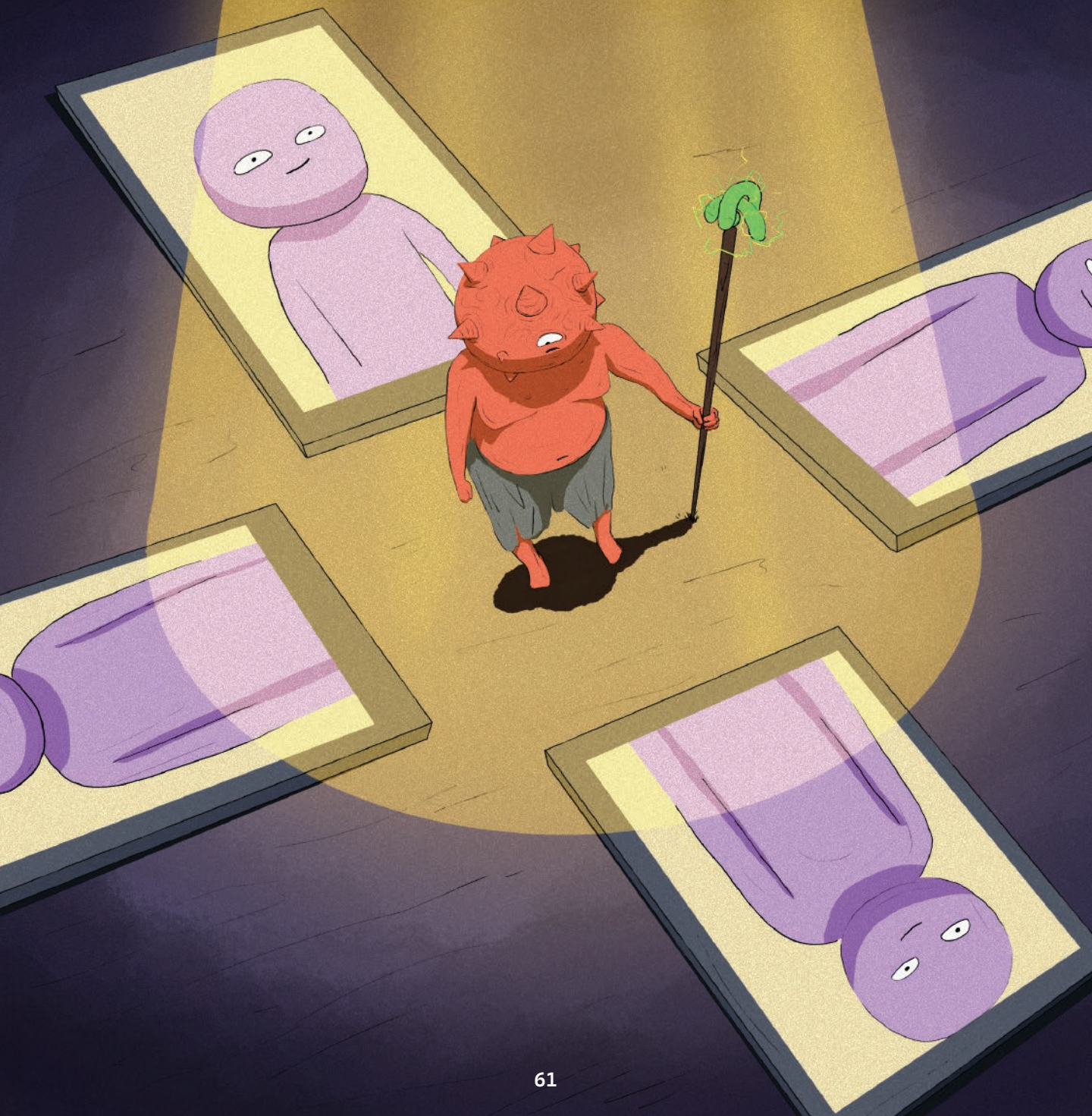
File-Sharing Infrastructures

Circulation of NCII was further sustained through embedded cloud-storage infrastructures.

Full-length files were commonly hosted on third-party file-sharing services such as **TeraBox**, **DropGalaxy**, and **Upfiles**, with preview clips or thumbnails displayed on social media as well as other webpages. These platforms frequently operate on monetisation incentives, including pay-per-view access and referral-based payouts—creating structural motivations for continued dissemination of content. There were also multiple downstream websites that embedded videos from these links.

These dynamics demonstrate how monetised content infrastructures actively sustain the persistence and scale of technology-facilitated abuse.

X. Trend Spotlight



Beyond the core harm categories, Year 3 casework surfaced several patterns that warrant closer attention. Each reflects a distinct dynamic in how technology-facilitated abuse is evolving in its methods, its targets, and the gaps it exploits.

Spotlight 1: Widespread Dissemination and Recidivism in Image-Based Abuse

Trustline’s casework indicates that certain incidents of non-consensual intimate imagery (NCII) evolve into situations of **widespread digital circulation**, where harmful material travels rapidly across multiple digital platforms and persists through repeated sharing, modification, and reposting. Two interlinked patterns characterise these cases.

The first is **networked dissemination**. Content that begins circulating within closed or semi-private spaces such as messaging groups or peer networks can migrate rapidly into publicly searchable platforms through reposting, format adaptation, and cross-platform sharing. As circulation expands, containment becomes harder and incidental exposure more likely. The wider the spread, the greater the recognition risk for victim-survivors.

The second is **temporal recurrence or recidivism**. Even after successful takedown, harmful material frequently reappears through newly created accounts, altered formats or shifts to less regulated platforms. This reappearance is termed ‘recidivism’ and each instance may require survivors to restart documentation and reporting processes that are often not designed to recognise prior takedowns.

Together, these dynamics mean that harm is defined not only by the original violation but by its persistence—the ongoing uncertainty of not knowing where material may appear, who may encounter it, or whether circulation has truly ended.

Circulation Across Platforms

Research on image-based sexual abuse similarly notes that material often moves from semi-private spaces into highly searchable public platforms, intensifying both the reach of exposure and perceptions that harm is difficult to contain.^{21,22}

In the case involving the most extensive dissemination during Year 3, the intervention involved identifying over 300*(case ongoing) harmful links through systematic mapping across two reporting cycles. The case remains ongoing with new instances continuing to emerge.

An intimate video, originally created within a consensual relationship, first leaked within closed peer messaging networks before appearing on publicly visible social media accounts. Subsequently, it spread across a wider digital ecosystem including:

- Private or semi-private communication networks such as encrypted messaging groups
- Mainstream social media platforms
- Informal file-sharing infrastructures, including cloud storage links or download repositories
- Commercial adult content hosting websites

²¹Powell, A., & Henry, N. (2017), *Sexual Violence in a Digital Age*. Palgra ve Macmillan.

²²Bates, S. (2017), *Revenge Porn and Mental Health: A Qualitative Analysis of the Mental Health Effects of Revenge Porn on Female Survivors*, *Feminist Criminology*.

After ten months of dedicated case work, the majority of links containing the NCII were taken down. But a year later, more links appeared almost as if the intervention process was back to square one.

Manipulation of Content and Viral Adaptation

Recidivism frequently involved deliberate tactical shifts. Once enforcement processes began, perpetrators modified either the content or the distribution strategies to sustain visibility or evade moderation thresholds or both.

Rather than remaining static, the video was repeatedly reformatted in ways that increased shareability, reduced the likelihood of being detected during moderation, or it was aligned with platform-specific content styles.

Observed transformations included:

- Shortened suggestive clips extracted from longer recordings
- Still images captured from video frames and shared as standalone posts
- Blurred or cropped versions re-uploaded after takedown actions
- Meme-based edits and compilations incorporating humour or defamatory captions
- News clips or roast videos combining the NCII with commentary
- Sensationalised thumbnails that gave away identity of the victim-survivors

Such practices indicate that perpetrators and secondary actors actively **construct virality**. Content framed through sexualised captions, provocative thumbnails, trending keywords, or suggestive edits was more likely to surface in recommendation feeds, search rankings or high-traffic discovery interfaces. These algorithmically mediated visibility incentives contributed to the rapid expansion of audience reach.

Research on platform governance has highlighted that offenders frequently exploit differences in enforcement standards by shifting material between services or altering its presentation to remain below formal violation thresholds²³. By adjusting explicitness, tone or framing, they attempt both to evade moderation systems and to keep content visible within algorithmically curated feeds.

Even where full-length uploads were removed, residual visual traces often remained in the form of cached previews or cropped thumbnails appearing in search results and platform interfaces.

Procedural Burden and the Limits of Linear Takedown Models

Cases involving widespread circulation create substantial procedural demands. Large volumes of links across multiple platforms require coordinated reporting through platform grievance systems and statutory cybercrime pathways. Trustline's interventions, therefore, involved structured guidance to victim-survivors on documenting URLs, prioritising reporting actions, and pacing engagement to reduce cognitive overload.

²³Henry, N., & Flynn, A. (2019), *Image-Based Sexual Abuse: Online Distribution Channels and Illicit Communities of Support, Violence Against Women*.

Conventional linear crisis-response models, which assume that removing a single post or account is sufficient to stop the spread of harm, are frequently inadequate. While the spread of harm is networked, reporting systems remain manual and instance-based.

Each resurfacing instance may require victim-survivors to re-engage with systems that treat recurrence as isolated complaints, rather than as part of an ongoing pattern of abuse. Survivors often described this experience as having to “start from the beginning again,” contributing to emotional fatigue and diminishing trust in formal redress mechanisms.

These challenges are compounded by broader systemic gaps. Approaching law enforcement can be difficult for victim-survivors and even when engaged, systems are often not equipped to enable timely and coordinated takedowns across platforms, particularly in high-volume cases, when the content appears in waves.

As a result, much of the burden of tracking and reporting harm continues to fall on victim-survivors rather than being absorbed by the systems meant to support them.

Psychosocial Consequences of Persistent Circulation

High-visibility dissemination was associated with intensified and cyclical psychological distress. Periods of relative quiet were disrupted by discovery of new links or reposted material, generating renewed anxiety and undermining confidence in earlier intervention efforts.

Victim-survivors reported fear of recognition by peers, extended family members, or professional networks. In several cases, this uncertainty contributed to withdrawal from educational or social settings and disruption of routine activities.

In one instance, a survivor who had begun resuming normal life reported a sharp escalation in anxiety after encountering a repost of previously removed imagery on a widely used platform.

The unpredictability of recurrence reinforced the perception that digital exposure could continue indefinitely. Studies indicate that the persistence and searchability of intimate imagery can sustain trauma responses long after initial removal, reinforcing feelings of shame, vulnerability, and loss of control.^{24,25}

Recommendation

These patterns suggest that containment cannot be achieved through platform-specific action alone. Effective response requires coordinated cross-platform accountability alongside sustained survivor-centred navigation support across the wider digital ecosystem.

²⁴Walker, K., & Sleath, E. (2017), *A Systematic Review of the Current Knowledge Regarding Revenge Pornography and Non-Consensual Sharing of Sexually Explicit Media, Aggression and Violent Behavior*

²⁵Ruvalcaba, Y., & Eaton, A. A. (2020), *Nonconsensual Pornography among U.S. Adults: A Sexual Scripts Framework on Victimization, Perpetration, and Health Correlates for Women and Men, Psychology of Violence.*



Spotlight 2: Audio-Mediated Abuse in Short-Form Video Ecologies

Emergence of Audio as a Vector of Harm

Year 3 shows an increase in cases of technology-facilitated abuse operating through audio as the carrier of harm. In several cases, the primary harm did not lie in what was visually shown but in how sound was used to sexualise, denigrate, or recontextualise otherwise neutral imagery.

Audio functioned as a vector of harm in two interconnected ways: by sexualising or denigrating existing imagery through voiceovers, background tracks, or defamatory narration; and by enabling large-scale replication of abusive messaging through reusable sound assets that could be attached

to new visual content across hundreds of posts.

How Perpetrators Use Platform Audio Design to Scale Harm

On short-form video and social media platforms, audio increasingly functions as an indexing mechanism through which users discover, repurpose, and amplify content.

Abusive actors frequently relied on pre-existing soundtracks. Many such tracks were originally produced as standalone creative content, including songs or spoken-word clips containing sexually explicit humour, misogynistic commentary or suggestive narratives. The original creators did not target specific individuals at the point of production.

However, once these audio assets entered wider circulation, they were repurposed by former partners, cyberstalkers, or acquaintances seeking to humiliate or sexualise identifiable victim-survivors.

Typologies of Audio-Based Abuse

Trustline's case documentation points to several recurring patterns in which audio functioned as the primary carrier of harm.

Abusive voiceovers and reputational framing: In multiple instances, everyday visuals such as college photographs, vacation selfies, or other social media posts were paired with abusive audio tracks implying sexual availability or moral deviance. Victim-survivors reported videos in which their images were accompanied by voiceovers suggesting involvement in sex work or multiple intimate relationships. In one case, sexually suggestive audio was overlaid onto visuals of a minor, thereby contributing to the creation of exploitative content within a child-sexual-abuse context.

Synthetic or AI-generated audio content: The growing accessibility of generative media tools has been lowering the barriers to producing convincing fabricated audio-visual content, thus, expanding the repertoire of technology-facilitated abuse. Cases involved fabricated songs or voice-cloned speech that simulated victim-survivors making sexually explicit statements or narrating fictional encounters. These productions were often highly explicit and designed to enhance believability. In one instance, a single account producing synthetic audio functioned almost as a shared resource for multiple perpetrators who used it to dox and target several women across platforms.

Remixing of non-consensual recordings: Some cases involved extraction of voice segments from private calls or leaked intimate videos, which were then transformed into music loops or meme-style audio clips. For example, fragments of speech from a non-consensual intimate recording were incorporated into a DJ-style remix that circulated independently of the original visual material.

Moderation Challenges in Audio-Dominant Abuse

Audio-mediated harms present distinct enforcement difficulties. Moderation systems that prioritise visual detection or keyword-based reporting categories may fail to recognise abuse encoded primarily in sound.

Moderation can also struggle with dialect variation, code-mixing, and culturally specific slang, creating detection gaps in multilingual environments.

Platform reporting interfaces also don't provide clear options for users to identify audio as the primary site of violation.

Recommendation

Effective response may, therefore, require recognition of audio as an independent object of moderation. Clearer reporting pathways for sound-based abuse and mechanisms to identify derivative reuse of harmful audio across uploads may be necessary to ensure durable containment.

At the same time, regulating audio raises complex normative questions. Content that later functions as a template for harassment may also originate within mainstream entertainment cultures including music, comedy, or influencer-led trends. Determining when such material becomes actionable, therefore, requires careful balancing of harm prevention with freedom of expression.



Spotlight 3: Harassment of Emerging Creators

Visibility Without Protection

‘Emerging creators’ refers to individuals in the early stages of building a publicly visible social media presence.²⁶ These individuals were often still building their audience. Their visibility was usually concentrated within local or regional networks, where online reputation was closely tied to offline social standing, livelihood opportunities, and personal safety. Despite their visibility, they lacked the institutional protection that more established public figures may have, such as professional management, legal support or platform contacts.

Trustline’s casework during Year 3 indicates that perpetrators often exploited this transitional stage of visibility to initiate impersonation, sexualised defamation, and coordinated reputational targeting.

Reputational attacks could quickly translate into family pressure, community-level stigma and disruption to emerging career opportunities. Structural inequalities, including those linked to gender, caste, class, religion, or regional marginalisation, often intensified these risks.

Impersonation, Sexualised Defamation, and Networked Targeting

A common pattern involved the creation of fake accounts using publicly available photographs or short-form videos taken from the influencer’s own content. These accounts frequently circulated sexually suggestive captions, fabricated narratives of sex work, or defamatory insinuations designed to damage credibility.

The attack often did not remain limited to one profile. Perpetrators created clusters of accounts across platforms, reposted the same material with minor changes and sustained visibility through tagging, resharing, and coordinated commenting.

In several cases, impersonating accounts also acquired authenticity signals such as paid verification badges or professional-looking layouts. Since such markers are widely read as signs of legitimacy, they made false accounts appear more credible to audiences unfamiliar with the original profile.

In many cases, the goal was not only to shame the influencer publicly, but also to expose them before the audience they had built and before their family or community.

Perpetrators also targeted existing fault lines. Influencers who posted progressive or feminist content were subjected to misogynistic backlash. Others from historically marginalised communities

²⁶Cunningham, S., & Craig, D. (2019), *Social Media Entertainment: The New Intersection of Hollywood and Silicon Valley*. NYU Press.

were harassed using caste, religion, or locality as tools of humiliation. In some cases, young women from communities historically associated with sex work were falsely framed through that lens, with their caste location itself being weaponised online.

Consequences for Participation and Livelihood

For many emerging influencers, online visibility represented a significant investment of labour, aspiration, and identity. Harassment threatened future work, as well as audience trust.

A central difficulty in these cases was the tension between privacy and livelihood. Typical safety advice such as going private, logging off, or deleting content were often not practical. When visibility was directly linked to income, collaboration opportunities, or public recognition, stepping back from the platform could itself produce loss. As a result, influencers were often forced to remain online under conditions of heightened exposure and stress.

Victim-survivors described anxiety, withdrawal, reputational fear, and disruption to emerging career pathways in digital promotion, entertainment, or content creation.

In several cases, impersonation-based harassment also triggered sexually explicit messages, solicitation attempts, and stigma within offline networks.

Recommendation

People who are publicly recognisable but structurally unprotected may face some of the most disproportionate burdens of technology-facilitated abuse. The backlash is not only social but also economic and tied to their livelihoods. There is a need for platform governance frameworks that recognise different levels of visibility-related risk.

Spotlight 4: Voyeurism as Networked Sexual Exploitation

Defining Voyeuristic Harm in Digital Contexts

Voyeurism in digital environments refers to the covert observation, recording, and circulation of visual material depicting individuals in situations where privacy, bodily integrity, or contextual dignity would ordinarily be expected.

Trustline's casework during Year 3 identified multiple instances where sexualised filming of fully clothed women through strategic framing of intimate body areas, suggestive captions, or contextual editing, transformed everyday moments into material for voyeuristic consumption.

Recent news reporting from Indian cities has similarly documented covert filming of women in public transport systems and the circulation of hospital surveillance footage online, suggesting that voyeuristic harm is increasingly widespread and monetised.²⁷

²⁷Women Secretly Filmed on Bengaluru Metro: Instagram Account Sparks Outrage, FIR Filed, The Indian Express, 21 May 2025.



Capture, Packaging and Distribution

Case analysis suggests that voyeuristic content often followed a structured distribution pathway.

Covert recordings captured in homes, markets, transport systems, or clinical settings were first uploaded as short clips on high-visibility social media platforms. These clips functioned as promotional “bait”, directing viewers toward encrypted groups or niche websites offering longer videos through subscription or pay-per-download models.

Everyday Surveillance and Domestic Proximity

A particularly disturbing pattern involved recordings made by individuals within close social proximity.

Several videos appeared to be filmed inside homes by relatives or acquaintances, often staged under routine pretexts such as asking the woman to bend or retrieve objects while the camera focused on specific body areas.

Other clips were recorded in crowded public environments such as marketplaces or streets, where perpetrators followed women while filming them without consent.

These dynamics indicate that voyeuristic abuse is not confined to anonymous urban surveillance, but may also emerge from violations of trust embedded within everyday social relationships.

Clinical Vulnerability and Institutional Breach

Trustline’s casework also revealed circulation of voyeuristic material originating from medical environments.

Short clips appearing to depict gynaecological exams or patient preparation areas were circulated online as teaser content linking to external channels advertising longer footage.

Investigations into hospital surveillance misuse in India have highlighted how CCTV systems may be compromised and exploited for online distribution.²⁸ Such incidents illustrate how institutional failures can be transformed into sustained digital exploitation when voyeuristic material enters commercialised circulation networks.

Network Replication and Moderation Challenges

Voyeuristic content networks demonstrated strong recidivism patterns. Accounts removed following reporting frequently reappeared under new identities, while related profiles continued circulating similar material. Keyword-driven discovery mechanisms, including terms associated with hidden cameras, candid filming, or taboo sexual themes, enabled rapid reconstruction of distribution networks even after enforcement action.

In the documented case, containment required escalation of more than forty accounts alongside submission of keyword clusters and hashtag patterns to platform safety teams. This highlighted the importance of addressing underlying network structures, rather than isolated posts.

²⁸*Hackers Steal Maternity Ward CCTV Videos in India Cybercrime Racket, BBC News, 17 November 2025.

Recommendations

Understanding voyeurism as a distributed digital phenomenon is essential for designing interventions that move beyond episodic takedowns toward durable disruption of exploitative content infrastructures. Effective response, therefore, requires:

- Recognition of sexualised non-consensual recording as a dignity-based harm even where individuals are clothed or located in public contexts.
- Network-level moderation strategies capable of identifying clusters of related accounts.
- Stronger safeguards in institutional environments characterised by high expectations of privacy.



XI. Mental Health Support



Psychosocial care constitutes a core dimension of support provided through the Trustline. The mental health response operates along a continuum: from immediate stabilisation at intake to structured long-term counselling, where required.

Support in this report is discussed across two broad modalities:

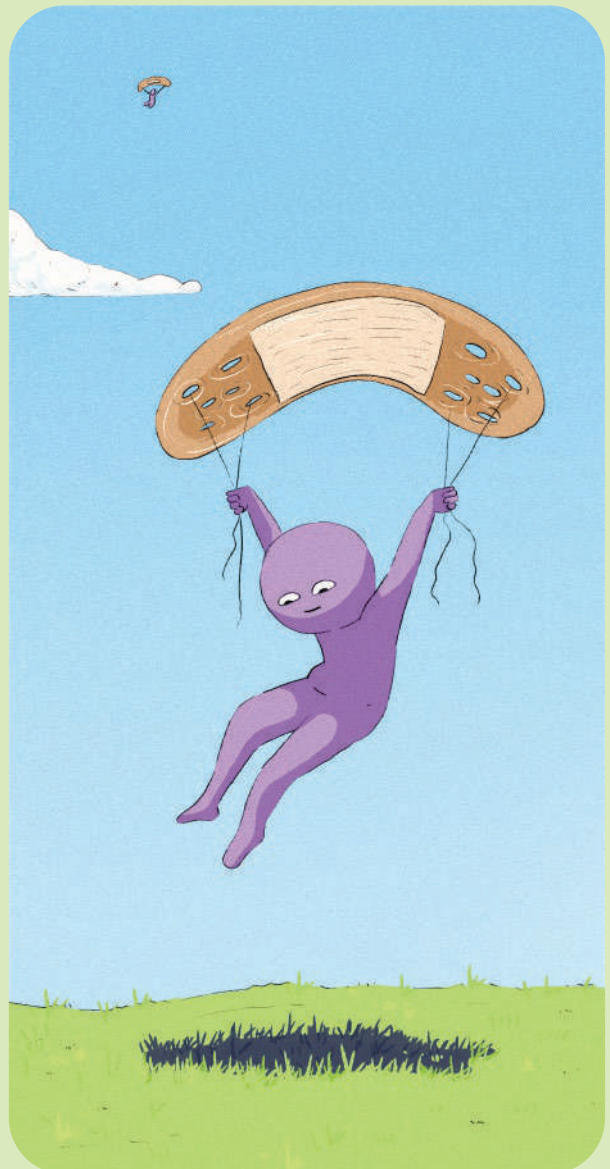
1. Psychological first aid (immediate stabilisation)
2. Long-term mental health support (structured counselling and extended accompaniment)

1) Psychological First Aid

All victim-survivors requiring intervention in Year 3 (100%, n = 130) received some form of psychological first aid by trained psychologists at the point of intake.

This initial response was not limited to individuals reporting direct victimisation. In several cases, distress was also expressed by individuals who had witnessed incidents or were supporting an affected person. At intake, callers frequently described acute fear, panic, confusion, shame, and anticipatory anxiety linked to the possibility of further exposure or escalation.

Psychological first aid is focused on grounding, reassurance, and restoration of immediate safety. Counsellors supported victim-survivors in slowing crisis reactions, identifying practical next steps and understanding available technical or reporting remedies. At this stage, the objective was stabilisation rather than therapeutic processing—enabling individuals to move from acute distress towards more anchored engagement with the support process.



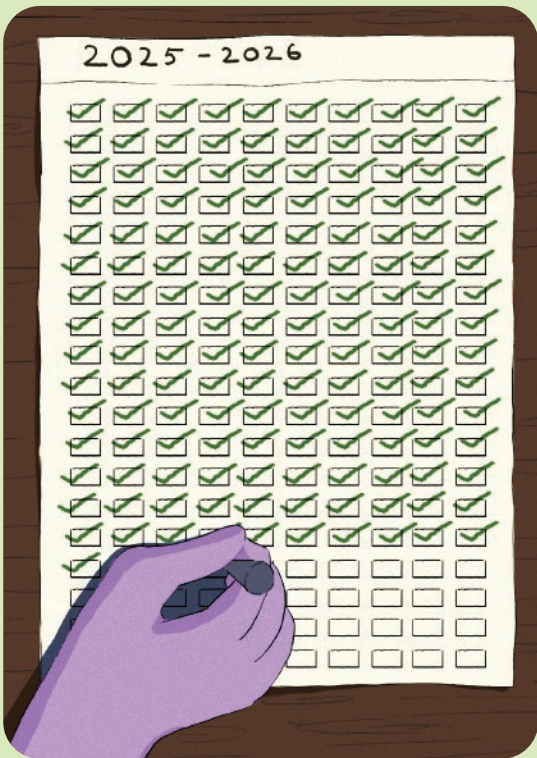
2) Long-Term Mental Health Support

A smaller proportion of cases required structured and sustained mental health intervention beyond initial intake.

In Year 3, 36 victim-survivors received counselling support that spanned across multiple sessions over two months or more. These cases were characterised by prolonged distress, disruption in academic, occupational or social functioning, or the need for continued emotional accompaniment as technical and legal processes unfolded.

Support in such situations involved scheduled counselling sessions, periodic reassessment, and extended handholding across the lifecycle of the incident.

Cases where remote counselling (via phone or video) was not feasible or where more intensive support was required, referrals for in-person care were facilitated. These included psychiatrists and psychologists who were thoroughly vetted to ensure sensitive, non-retraumatising engagement. The clients' paying capacity was also taken into consideration. Referrals spanned both private practitioners and public healthcare systems.



Nature of Reported Mental Health Concerns

Table 12: Subcategories of Mental Health Concerns (Year 3)

Mental health concern category	Instances of concern (n)	Share (%)
Emotional distress – fear and anxiety problems	28	77.8%
Concerns about the self	5	13.9%
Emotional distress – mood problems	1	2.8%
Emotional distress – anger problems	1	2.8%
Self-harm/suicidal ideation concerns	1	2.8%
Total mental health concern instances	36	100%

Across the reporting period, instances explicitly coded as mental health concerns were most frequently associated with emotional distress.

Approximately 77.8% (n = 28) of such instances involved fear and anxiety-related symptoms. These were followed by concerns relating to self-perception and self-blame, anger responses and broader mood-related difficulties.

Psychological Impact of Tech-Facilitated Abuse

The psychological impact of technology-facilitated abuse was closely shaped by anticipated social consequences by the survivors and the persistence of harm across digital platforms.

Heightened psychological distress was particularly visible in cases involving socially proximate perpetrators, including acquaintances, peers, or former partners. In such contexts, online harm intersects with ongoing offline relationships, intensifying fear of continued interaction, and widening social repercussions.

Adolescents and young adults were more likely to report **acute anxiety** linked to peer exposure, reputational fallout, and uncertainty regarding institutional response. Among older victim-survivors, distress was more frequently connected to concerns about livelihood security, family expectations, and community standing.

3) Intervention Spotlight: Tech-Enabled Crisis Counselling (TECC)

Emerging global frameworks on technology-facilitated violence recognise that digitally mediated harms can generate significant psychological, social and economic consequences rather than remaining confined to online environments.²⁹

Conventional response systems that separate technical redress from psychosocial care, therefore, do not fully reflect the lived experience of victim-survivors. International practice guidance addressing online sexual abuse increasingly emphasises the need to combine safety planning, removal pathways, and psychological recovery support, while acknowledging that complete digital containment may not always be achievable.³⁰

Drawing on this understanding, the Trustline employs an integrated response model called **Tech-Enabled Crisis Counselling (TECC)**. The model combines:

1. Digital incident response
2. Crisis stabilisation
3. Sustained psychosocial accompaniment



²⁹UN Women (2023), *Technology-Facilitated Violence against Women: Taking Stock of Evidence and Data Collection*

³⁰Office of the eSafety Commissioner, *How to Help Someone Deal with Image-Based Abuse*

The Trustline’s experience across reporting cycles suggests that visible technical action such as the first successful removal or reporting of harmful content can function as an early mechanism of crisis de-escalation by restoring a sense of agency and reducing emotional intensity. At the same time, uncertainty surrounding removal outcomes requires support processes that extend beyond technical intervention.

Operational Continuum of Tech-Enabled Crisis Counselling

In practice, TECC involves a sequenced yet flexible set of actions designed to address both the digital drivers of harm and the victim-survivor’s psychosocial safety.

Although presented as stages, these processes frequently overlap and may be revisited depending on recurrence of harm, evolving risk, or survivor readiness.

Intake and Immediate Stabilisation

The first point of engagement prioritises rapid containment of crisis.

Counsellors assess the intensity of distress, including panic reactions, dissociation, inability to perform daily activities, or indicators of self-harm risk.

Grounding techniques, reassurance, and simple, actionable steps are introduced to restore a sense of immediate safety and control. Particular attention is given to identifying safe channels of communication, recognising risks associated with shared devices, monitored accounts, or coercive control within interpersonal relationships.

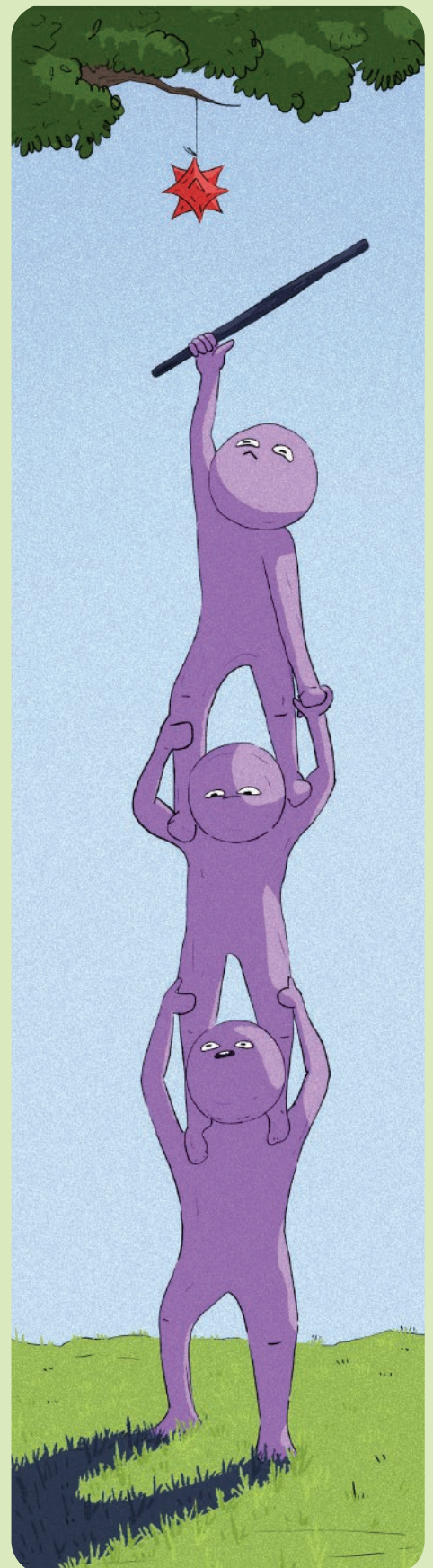
Information collection at this stage is deliberately limited to what is necessary for action. This approach reduces the likelihood of retraumatisation and supports individuals who may be overwhelmed by the immediate crisis.

Digital Incident Triage

Once initial stabilisation is achieved, attention shifts to understanding the digital architecture of harm.

Counsellors work with victim-survivors to identify the type of abuse involved and map potential circulation pathways.

Where feasible, individuals are guided in preserving available evidence through practical steps such as saving links or capturing screenshots but without increasing exposure or distress. Since digital evidence is often incomplete or already deleted, emphasis is placed on procedural sufficiency rather than technical perfection.



Reporting strategies are prioritised based on urgency, visibility of content, age of the victim-survivor, and likelihood of further harm. In cases involving image-based abuse, platforms employing hash-matching technologies may be identified as part of containment strategies.

Trustline's casework frequently involves guiding individuals through fragmented reporting ecosystems, including platform grievance mechanisms, national cybercrime processes, and on-ground socio-legal services. During periods of acute distress, coordinating multiple procedures can itself become a source of burden. TECC, therefore, functions as a navigation mechanism that reduces cognitive load on the victim-survivor by supporting decision-making and facilitating appropriate referrals.

Communication on Timelines and Limitations

Transparent communication regarding expected timelines, procedural constraints, and the possibility of content resurfacing forms a critical component of response.

Counsellors provide realistic expectations based on prior case experience, while also ensuring that survivor's concerns are acknowledged and validated.

The discussion of recidivism risks is framed as harm-reduction guidance, rather than as a negation of the survivor's fears.

Psychosocial Support and Functional Recovery

Psychological first aid continues alongside technical intervention during acute phases of the crisis.

Victim-survivors may also require assistance in addressing secondary consequences of abuse such as withdrawal from academic engagement, workplace disruption, or strained relationships within family and peer networks.

Sessions during this phase focus on emotional regulation, coping strategies and rebuilding confidence in institutional and interpersonal environments.

Accompaniment and Continuity of Care

Technology-facilitated abuse frequently lacks a clear endpoint. Harmful material may resurface across platforms, circulate within closed messaging networks, or continue to shape social perceptions even after initial removal.

Periodic follow-ups are undertaken with survivor consent to reassess emotional wellbeing, emerging risks, and subsequent reporting needs.

Continued support may include intervention in cases of recidivism, facilitation of legal or mental health referrals, and assistance in navigating institutional processes that often remain fragmented or difficult to access.

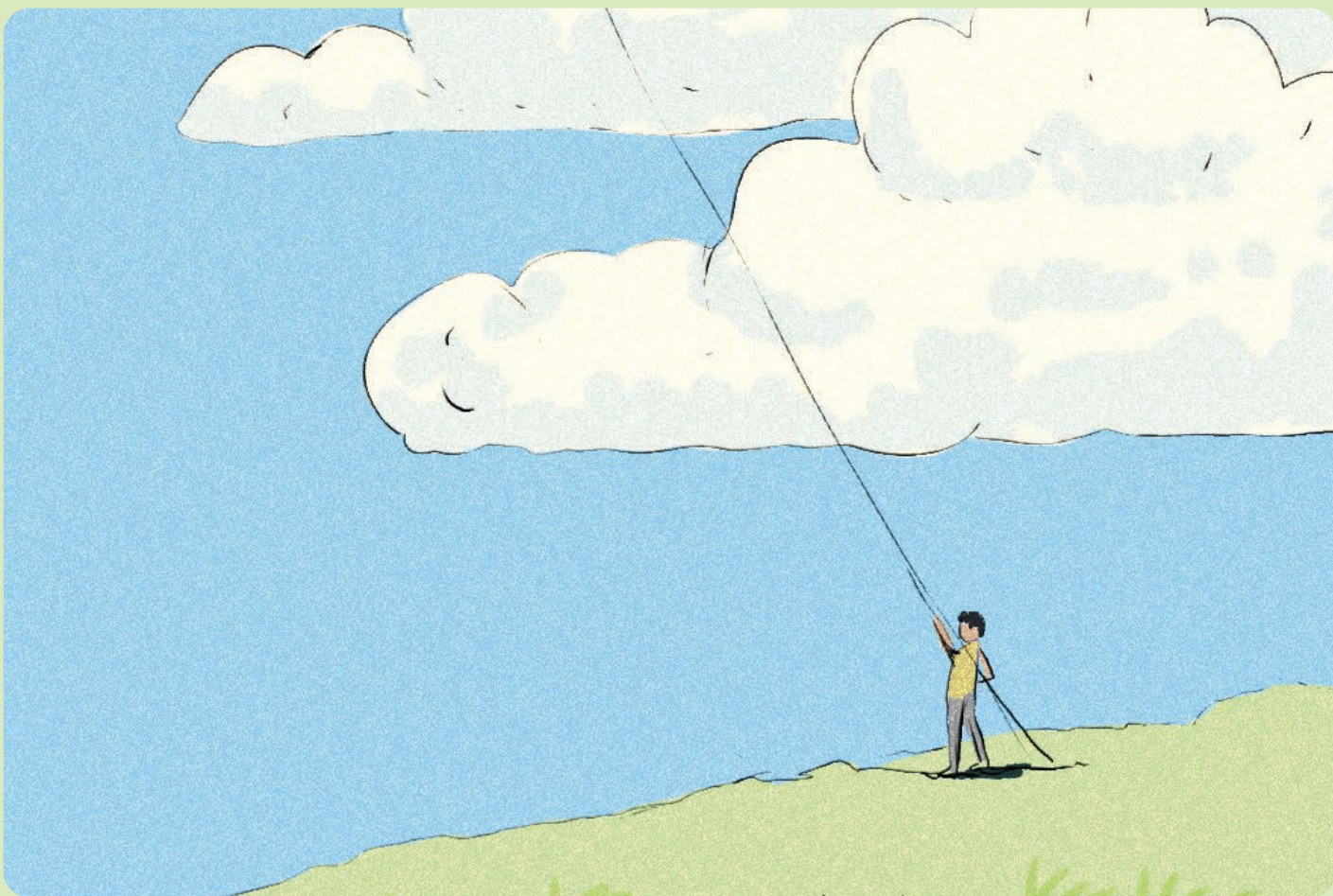
A critical dimension of accompaniment involves strengthening the victim-survivor's offline support ecology. Where stigma, victim-blaming, or fear of reputational loss inhibit disclosure,

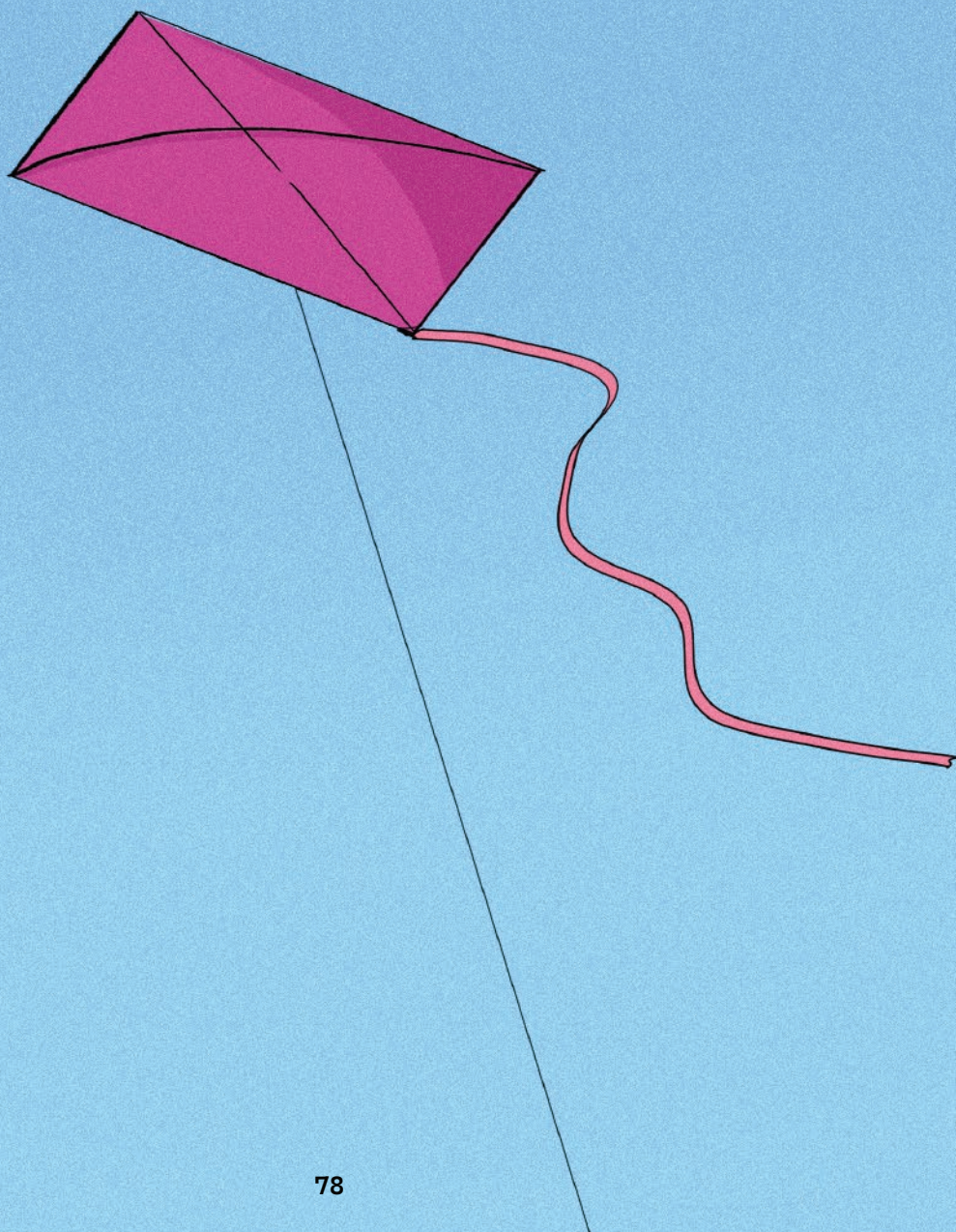
counsellors may assist victim-survivors in identifying trusted individuals and preparing for safe conversations about the abuse. This may include helping them articulate the nature of the violation, anticipate possible responses, and establish practical safety plans.

With informed consent, counsellors may also engage family members, partners, or other close actors to help them understand the need to process the incident as a form of harm, rather than a moral failing and to support the victim-survivor.

Such relational work serves multiple functions. It reduces isolation, redistributes the burden of coping, and enables the rebuilding of everyday routines that are often disrupted during crises. Evidence from the Trustline practice suggests that when immediate social environments are sensitised and supportive, victim-survivors are better able to sustain engagement with technical and legal processes and demonstrate greater emotional stabilisation over time.

By supporting both victim-survivors and their close networks to process the incident, reinterpret responsibility, and restore a sense of agency, the TECC practice recognises recovery as a socially embedded and frequently non-linear process. In this sense, continuity of care functions not only as crisis management but as an enabling condition for long-term psychosocial restoration.





The TECC Checklist

Intake & Immediate Stabilisation

- Assess distress intensity (panic, dissociation, daily functioning, and self-harm risk)
- Apply grounding techniques and reassurance
- Identify safe communication channels
- Check for shared devices, monitored accounts, and coercive control
- Limit information collection to only what's needed for immediate action

Digital Incident Triage

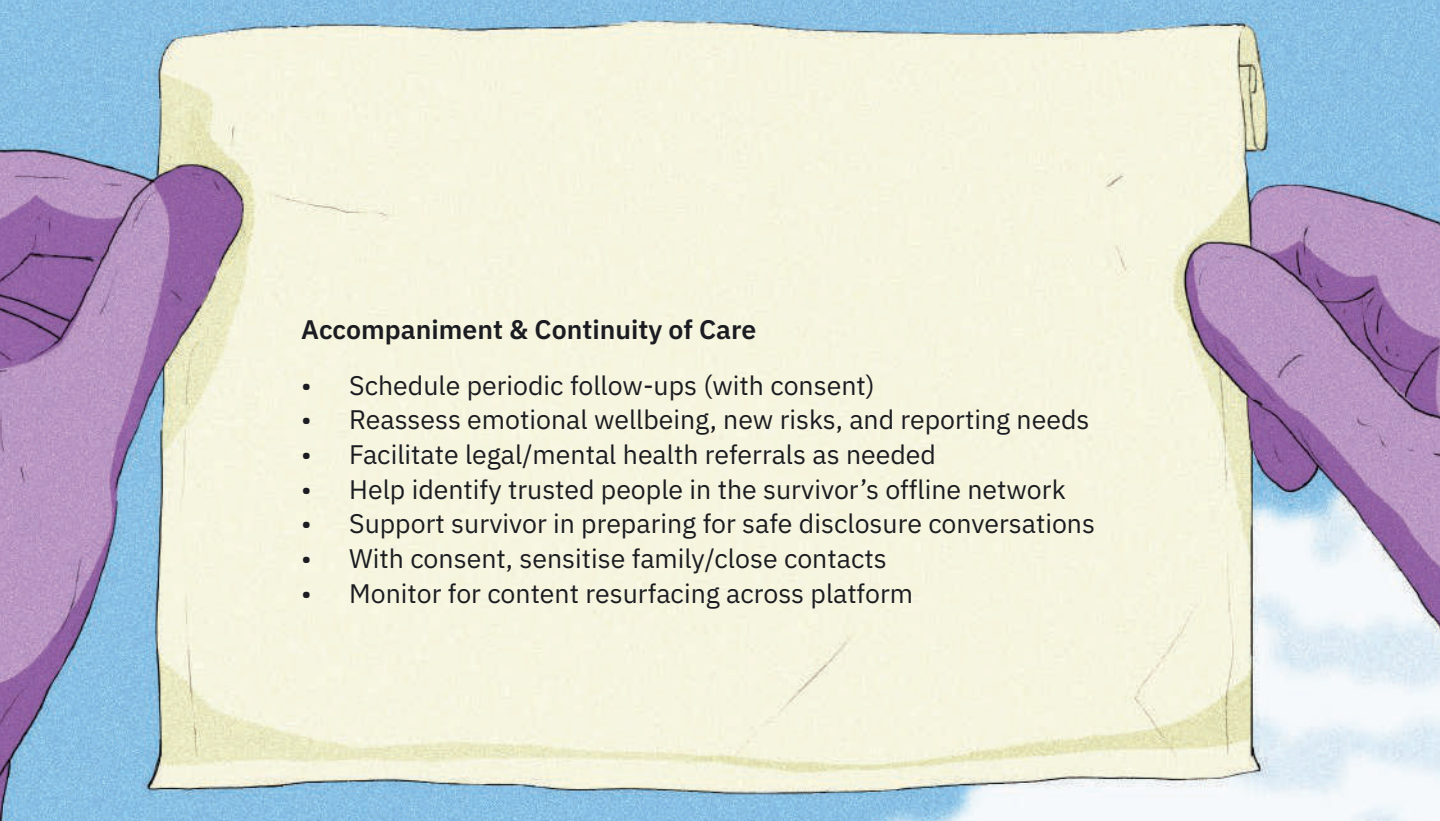
- Identify type of abuse and map circulation pathways
- Guide evidence preservation (screenshots, links) without increasing distress
- Prioritise reporting based on urgency, content visibility, age, and recurrence risk
- Identify relevant platforms (including those with hash-matching for Image-Based Abuse cases)
- Coordinate across platform grievance mechanisms, cybercrime portals, and socio-legal services

Communication

- Set realistic expectations on timelines and outcomes
- Acknowledge and validate survivor concerns
- Frame recidivism risk as harm-reduction guidance, not dismissal

Psychosocial Support

- Continue psychological first aid alongside technical work
- Address secondary consequences (academic, workplace, relationships)
- Focus on emotional regulation, coping, and rebuilding institutional confidence



Accompaniment & Continuity of Care

- Schedule periodic follow-ups (with consent)
- Reassess emotional wellbeing, new risks, and reporting needs
- Facilitate legal/mental health referrals as needed
- Help identify trusted people in the survivor's offline network
- Support survivor in preparing for safe disclosure conversations
- With consent, sensitise family/close contacts
- Monitor for content resurfacing across platform

✿ Case Study: Navigating Psychological Crisis During Persistent Circulation of NCII

Age: 26

Gender: Female

Location: Northeast India (Specific locational details have been intentionally withheld to safeguard survivor's identity in this case.)

Timeline: July 2025 – January 2026

Intake

In July 2025, a 26-year-old schoolteacher from Northeast India approached Meri Trustline after discovering that intimate images and videos depicting her were circulating across a private online Discord server and associated messaging channels. The material had been created within a past relationship, and later shared without her consent. Over time, screen recordings appeared on adult websites and local messaging groups, extending the reach of the content into her immediate social and professional environment.

As awareness of the circulation spread, she experienced stigma, strained relationships, and eventual loss of employment. The repeated resurfacing of the material created ongoing uncertainty about whether the harm would end. This uncertainty began to shape her daily routines, contributing to withdrawal from social interactions and heightened vigilance in public spaces alongside intense intrapersonal shame.

Digital Triage & Containment

Initial intervention focused on mapping the content and initiating reporting across relevant platforms. Reverse searches confirmed the presence of the material on multiple hosting platforms. Early takedown actions were prioritised to reduce immediate visibility and demonstrate that response was possible.

The first confirmed removal of identified content coincided with a noticeable shift in counselling sessions. The survivor described a temporary reduction in panic and an increased willingness to engage in discussions about coping strategies. However, continued risk of recurrence required ongoing monitoring and periodic escalation, making digital containment an extended intervention spanning over multiple months rather than one-time engagement.

Communication & Psychosocial Support

Alongside technical response, counselling sessions addressed the survivor's escalating psychological distress. She reported persistent anxiety, disrupted sleep, and difficulty concentrating. As the situation progressed, she disclosed experiencing suicidal thoughts linked to shame, perceived loss of future opportunities, and social isolation.

Crisis-response strategies focused on validating her emotional reactions, reducing self-blame, and establishing safety plans for periods of acute distress. She was encouraged to identify concrete personal reasons to remain safe. In a subsequent session, she shared a document titled "reasons.pdf" containing messages of affection and encouragement from children she had previously taught. She described revisiting these messages during moments of crisis as helping her remain grounded and manage impulses towards self-harm.

Accompaniment & Continuity of Care

Support extended beyond immediate crisis management. Counselling sessions gradually shifted towards rebuilding daily structure, setting manageable goals, and preparing for safe engagement with trusted individuals. At the same time, the Trustline responders continued to monitor potential recirculation and assisted with additional reporting where required.

This coordinated approach enabled the survivor to regain a degree of predictability in her routine. Over several months, she resumed academic preparation and later cleared a competitive examination. Although reputational challenges within her community persisted, her emotional stability improved and indicators of acute crisis reduced. By early 2026, almost six months after the initial intervention, the immediate risk environment had stabilised and the case was closed following sustained follow-up.

Primary Psychological Impact:

Acute anxiety, social withdrawal, and suicidal ideation associated with persistent online exposure and reputational harm. The survivor described a sustained sense of vigilance linked to uncertainty about whether the material would resurface.

Stress Amplifiers:

- Repeated digital resurfacing of intimate content
- Hyperlocal circulation within closely connected social networks
- Stigma and victim-blaming responses within family and community environments
- Loss of employment and diminished confidence in future opportunities

Protective Factors Identified:

- Meaningful relational connections and sense of responsibility towards former students
- Consistent crisis-oriented counselling support
- Gradual re-establishment of routine activities and future-oriented goals
- Visible takedowns in a time bound manner that reduced immediate exposure and restored limited control

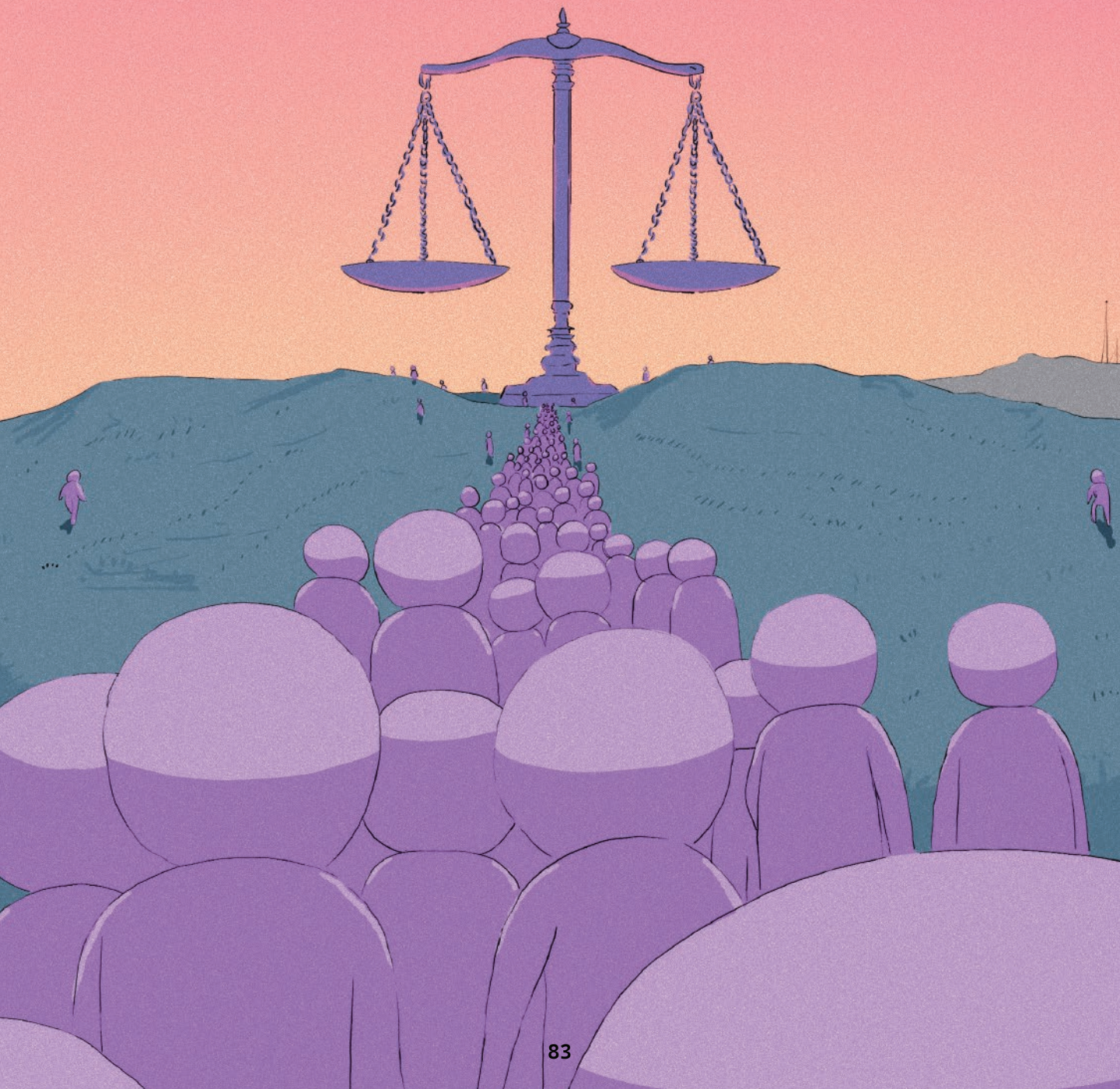
Barriers to Recovery:

- Fear of continued circulation and long-term reputational consequences
- Limited access to trusted support within immediate social surroundings
- Emotional exhaustion linked to prolonged uncertainty and the need for ongoing monitoring

Integrated TECC Insight:

This case demonstrates how technology-facilitated abuse can generate overlapping digital and psychological crises that require coordinated intervention. Early technical containment contributed to emotional de-escalation by making response visible, while sustained counselling support addressed the longer trajectory of stigma, uncertainty, and recovery. Within this continuum, TECC functioned as an integrated system that linked content takedown response, stabilisation of survivors, the rebuilding of their resilience, and restoring a sense of agency.

XII. Legal Support



In Year 3, 95 cybercrime reports were filed by Trustline on behalf of the survivors, while a smaller group of victim-survivors (n=10) sought structured legal guidance before deciding whether to pursue formal action. These patterns suggest that survivors are not disengaged from legal remedies.

For many victim-survivors of technology-facilitated abuse, the decision to engage with formal legal processes is not straightforward. It involves weighing the possibility of redress against the costs of pursuing it. Common fears include procedural unfamiliarity, jurisdictional uncertainty, social stigma including the fear and risk of having one's own conduct scrutinised and the sustained emotional burden of legal processes that may extend over years.

Survivors typically approach formal institutions when the situation has already intensified i.e. when intimate content is circulating, threats are escalating or the abuse begins to affect physical safety, livelihood or family relationships. Many seek reassurance that their complaint will be taken seriously before committing to steps such as FIR registration. Others move in and out of legal engagement over time, filing complaints, withdrawing or re-approaching authorities as they assess whether the system is able to respond effectively.

1 Challenges faced by Victim-Survivors

Several structural challenges recurred across Year 3 cases involving legal engagement.

The portal-to-police loop: In multiple cases, victim-survivors arrived at police stations only to be redirected to the cybercrime portal. Others who had called the 1930 helpline number were told that in-person visits were required for further action only for them to be redirected back to the portal. This circular referral between systems, each directing survivors toward the other generated delay, frustration, and, in some instances, abandonment of the formal process.

Jurisdictional uncertainty: Where survivors and perpetrators were located in different cities or states, determining which Police Station held jurisdiction to register an FIR often involved repeated visits to police stations, referrals across jurisdictions and delays linked to the transfer of Zero FIRs. These delays frequently occurred while the abuse continued. In most cases,



victim-survivors were also required to bear logistical and financial burdens associated with travel for investigative procedures.

Complaint closure without action: Multiple victim-survivors reported that cybercrime complaints were closed by the concerned police department without tangible follow-up or explanation.

Device seizure and collateral burden: In cases where offending content had been circulated to the survivor's contacts, devices belonging to family members or acquaintances were sometimes seized as evidence. This disrupted household routines and imposed financial strain. While the devices are meant to be returned after the trial, the process of recovering them is so cumbersome that, in practice, they are often lost for good.

Preference for physical over digital provisions: In cases involving both physical and digital abuse, law-enforcement responses often tended to prioritise provisions related to physical harm. This was partly because police were often less familiar with the applicable legal sections and evidence-collection requirements in cases of tech-assisted abuse. As a result, digital evidence and the harms it documented were not always adequately reflected in the legal record. This has consequences beyond the immediate case. In at least two Trustline matters, the documented presence of harmful content online was later used to oppose bail, showing that when digital harm is properly recognised, it can materially shape outcomes.

Scrutiny within legal processes: Victim-survivors who pursued formal complaints frequently described feeling scrutinised during investigative and court proceedings. Questions about relationships with perpetrators, the circumstances in which intimate material had been created and subsequent communication patterns were experienced as emotionally taxing. Concerns about the handling and privacy of sensitive digital evidence also shaped willingness to remain engaged with legal processes over time.

2 The Trustline's Role in Legal Engagement

RATI's legal team provides two kinds of services to victim-survivors who approach the Trustline:

- I. Legal guidance to victim-survivors navigating procedural steps.
- II. Direct legal representation if the cases are from Mumbai or nearby districts. Where cases fall beyond this scope, victim-survivors are connected with appropriate legal resources and verified referrals. In some cases, RATI's legal team works closely with the lawyers and other agencies supporting victim-survivors. Our legal intervention in such cases includes translating legal procedures for survivors and their families, supporting evidence preservation and documentation, coordinating with investigating officers and prosecutors and providing sustained psychosocial support through proceedings that may extend over months or years.

In Year 3, this accompaniment included

- assistance with FIR registration and jurisdictional transfers
- drafting responses / replies to bail applications on behalf of the survivor
- coordination with public prosecutors on evidentiary requirements
- real-time support to victim-survivors appearing as witnesses in court.

The following case illustrations demonstrate how legal engagement unfolds in practice in matters where digital harassment intersects with reputational harm, physical threats, and prolonged institutional processes. They also show that legal support extends beyond mere representation and involves helping survivors & families understand processes, timelines and possible outcomes.



3 Case Study: Jurisdictional Challenges & Escalating Risk in a Case of Intimate Partner Abuse

Age: 23

Gender: Female

Location: Mumbai, Maharashtra

Timeline: November 2024 – ongoing

Incident

Following the end of a two-and-a-half-year-long relationship in November 2024, a 23-year-old woman from Mumbai began receiving threats from her former partner. He warned her that he would circulate intimate photographs taken during the relationship, if she refused to resume contact.

Over the following months, these threats were repeatedly carried out. The perpetrator sent explicit images to members of her family and professional contacts she had previously taught. He used WhatsApp’s “view-once” feature and private Telegram accounts to transmit the material and then deleted evidence of having done so. In parallel, he issued a fabricated legal notice claiming that she owed him money, a document, he later admitted, that had been created to intimidate her.

Impact

The circulation of intimate content within her social and professional networks resulted in significant reputational harm. Her employment contract was not renewed. In December 2024, she filed a complaint through the cybercrime portal. The complaint was subsequently closed without visible action.

In an attempt to contain the situation, she resumed communication with the perpetrator. The harassment intensified. Images were distributed simultaneously to multiple contacts, leading to repeated calls and questions from people within her network. Experiencing acute distress and perceiving no immediate pathway to safety, she attempted suicide by consuming pills. Her family intervened then and accompanied her to the police station the following day.

Intervention

After contacting Meri Trustline in April 2025, the survivor received coordinated technical, legal, and psychosocial support. The perpetrator's accounts were reported to WhatsApp and Telegram, both of which confirmed takedown. Counselling sessions were initiated and continued throughout the legal process to address trauma, anxiety, and safety concerns.

When the investigation required travel across jurisdictions, the Trustline advised the survivor on her rights regarding investigation-related expenses and supported her in asserting these. The team also assisted her in preparing documentation for legal proceedings, including her response to the bail application filed by the perpetrator.

Legal Journey

An FIR was initially registered as a Zero FIR in Mumbai in March 2025 due to jurisdictional uncertainty as the survivor resided in Mumbai, while the perpetrator was based in Delhi. Following deliberations between police authorities, the case was formally transferred to a police station in Delhi in May 2025.

Once the perpetrator was aware that the FIR was registered, he arrived at the survivor's residence in Mumbai in the early hours of the morning in May 2025 and threw firecrackers through a window into her living room, where her siblings were sleeping. Two devices exploded inside the house, narrowly avoiding serious injury. A second FIR was subsequently registered, and the perpetrator was traced and arrested the same day in Mumbai.

Between 27 May 2025 and 29 August 2025, multiple bail applications were opposed and rejected by the court. While the survivor had separate legal representation before the court, Trustline continued to provide legal guidance and psychosocial accompaniment during this period. As of today, the accused remains in custody and proceedings are ongoing.



4 Case Study: A Three-Year Journey to Conviction

Age: 17 years old at the time of the incident

Gender: Female

Location: Mumbai, Maharashtra

Timeline: 2019 – ongoing

Incident

In June 2022, the father of a 17-year-old girl contacted Meri Trustline after discovering that her former partner had created impersonating social media accounts using her photographs and was circulating private images online. At the same time, the former partner had also issued threats of an acid attack.

When the family initially approached the police, registration of an FIR was refused on the grounds that the situation appeared to arise from a consensual relationship. Subsequent counselling engagement revealed a longer and more serious pattern of abuse. Beginning in 2019, the survivor had experienced grooming, coercion, abduction and sustained sexual assault. The case therefore involved both digital harms addressed under the Information Technology Act and grave offences punishable under the Protection of Children from Sexual Offences Act and then Indian Penal Code.

Impact

By the time the case reached the Trustline, the survivor had been living with the consequences of the abuse for nearly three years. She was preparing for her Class 12 board exams, while impersonating accounts continued to circulate within her peer network. The threat of an acid attack by the perpetrator also created an immediate sense of physical danger.

The family, too, faced sustained pressure from the perpetrator's family, associates, and later from local political actors seeking an out-of-court settlement. During the legal process, the survivor encountered conflicting expectations within her own household, including periods when her parents urged her not to testify. These dynamics contributed to significant psychological strain at a time when she was also navigating key educational transitions.

Trustline Response

In 2022, the Trustline accompanied the child and family to the Police Station to ensure the registration of an FIR and advocated for digital harms to be recognised as evidentiary components of the broader case. We were also appointed by the Child Welfare Committee as Support Persons for this child under the Protection of Children from Sexual Offences Act, 2012. The legal team coordinated with the Public Prosecutor, facilitated child-friendly procedures as prescribed by the law such as audiovisual testimony and oriented key witnesses for examination and cross-examination

Throughout the 3 year trial period, multiple disruptions occurred. A panch witness turned hostile, the investigating officer was transferred, FIR documents were temporarily untraceable in court records and the presiding judge was reassigned mid-trial. The perpetrator applied for bail twice in the Sessions Court and even in the High Court, but was not granted. The Trustline maintained continuity across each of these procedural breaks, ensuring that the survivor and her family remained informed and supported.

Counsellors and social workers provided sustained psychosocial accompaniment, including accompanying the survivor to court hearings, supporting her during a four-hour cross-examination in which she broke down and maintaining regular contact as she prepared for examinations, applied to college and began rebuilding daily routines.

Legal Journey

Following a formal complaint in 2022, the impersonating accounts were removed from online platforms. The survivor received victim compensation under the Maharashtra Government's Manodhairya Scheme. In December 2024, the accused was convicted and sentenced to twenty years' imprisonment. His bail applications were rejected at multiple stages of the proceedings.

As of July 2025, the survivor is enrolled in a fashion designing course and attending college regularly. In her own words, she is "finding her way towards her future." However, the perpetrator has appealed against the conviction in a higher court and the case remains ongoing.



XIII.

Feedback: What did Clients Say About the Services Provided by Meri Trustline?

The Trustline requests its clients for feedback on their experience after engaging with our services. Clients whose cases have been closed are sent a form for this purpose, which is available in English, Hindi, and Marathi.

In Year 3, a total of 69 clients completed the form. Key findings are as follows:



Timeliness of response

100%

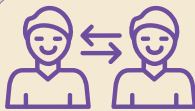
reported that Meri Trustline responded to their call or message in time.



Quality of listening

100%

felt that their concerns were listened to patiently.



Understanding of concerns

100%

felt that their concerns were understood.



Comfort in sharing concerns
(Comfortable/Neutral/Uncomfortable)

75%

reported feeling comfortable

25%

reported feeling neutral



Overall service rating

94%

rated the service as Excellent

5%

rated it as Good

1%

rated it as Fair

100% said they would reach out to Meri Trustline again if they, their family members, or friends faced online issues.

Below are testimonials from some of the victim-survivors supported by Meri Trustline in Year 3:

"Whatever help I am getting from your organisation, is best and excellent and I don't have words to express my gratitude. Your organisation is best."

"I liked the way meri Trustline responded and helped to me."

"तुम्ही दिलेल्या सर्व सेवा या खूप छान होत्या त्या तुम्ही खूप छान नियोजन केल्या असून मला व इतर केसेस मध्ये त्याचा खूप लाभ झाला आहे."

"Always helping person and good man."

"The speed was excellent."

"You were up to the level, thank you very much."

"You are better enough."

"Thank you apne hamare liye bahut kuch kiya hai"

"You guys have did your very best and there's no need for an Improvement because your already doing very well I'm really thankful to you guys for saving my life."

"आपने बहुत अच्छे से हेल्प की मुझे आपका नम्बर खोजना पड़ा । आपको लोग ओर easily कॉन्टेक्ट कर सके।"

"Already aapne meri bahut help ki hain dil se thank you."

"It would helped alot if you could've recovered my instagram account."

"You were just the help that was needed. Efficient, wise, resourceful."

"Their message helped a lot to calm me down when I was very stressed."

"I personally have no complaints my problem was solved and I am very thankful to that."

"No need already at good level."

"That's enough thanks."

"By prioritising everyone's issue."

"Very great thank you."

"Very great help. Thank you."

"Jaisa mere saath hua hai mene aap ki help li waise log aap tak ponche aur apni problem share kare uske liye aap ki jo team hai sabhi ko aap tak pahoonche ke liye asaani ho uske liye kaise aap tak pahoonche."

"Ur help was good enough."

"jaise kr rhe ho wo he sbse bahter h."

"You've helped me to understand every step :)"

"I shared my issues and received a prompt response. My problem was resolved within just one day. Thank you for your excellent service and for helping me with the harassment and abuse I experienced on social media."

"I received all the help I could get, maybe opening more offline centres across India would be a progress towards helping more people, just a suggestion."

"नाही धन्यवाद जितकं केल त्या बदल"

"आप पहले ही सभी की मदद कर रहे हैं। अल्लाह आपके ट्रस्ट को ऊँचा मुकाम दे। जो काम आप कर रहे हैं, लोगों की मदद करना, वह बेहद नेक और बेहतर है। मैं तो बस आपके लिए दुआ ही कर सकता हूँ। आपने मेरी पूरी तरह से मदद की, इसके लिए दिल से धन्यवाद।"

"May be they can evaluate and come up with solutions faster"

"I think the effort they have put in helping me is more than enough. I think they have tried every measure possible."

"It is the best of service."

"Contact the victim, because she is not sharing anything with anyone.. this incident must have impacted her very much but she is silent."

"I don't think there is another better way to help, you provided me with a very quick response so thank you."

"They are already doing a commendable work."

"Treating the problem in a very good way and handling also. Thanks for understanding my issue and for the resolution you gave."

"तुम्ही देत असलेल्या सेवा यांचा खूप लाभ होत आहे. तरी आपले मार्गदर्शन असंच मिळत राहो धन्यवाद"

"मेरी राय में सर को एक ऐसा सहायक व्यक्ति साथ रखना चाहिए, जो उनकी तरह काम को समझे और भविष्य में ज़िम्मेदारियाँ संभाल सके।"

"Great and excellent work, full marks"

"थैंक्यू सो मच"

"इतनी मदद करने के लिए दिल से धन्यवाद"

"Keep up the good work. Take care :)"

"Meri trust line is best."

"Excellent services"

"Having your service in all languages will make your service a little easier for everyone."

"They acted upon it very quickly and the issue was resolved within a couple of days."

"I am happy and would like to say that this is a good platform for online cases and it is much better than cyber report, fast action is taken and you can clear your concern to them. But I would specially like to focus on this thing that no action should be taken against those who report the users, otherwise those who report the users will also never dare to report."

"Thank you so much Meri trustline for helping me"

"No comments everything is just awesome."

"आपकी हेल्पलाइन सेवा बहुत ही सराहनीय और उपयोगी है।"

"आपकी हेल्पलाइन वास्तव में बहुत अच्छी है। मेरी बहुत मदद हुई है। ऐसा हेल्पलाइन मैंने कहीं और नहीं देखा। आपने मेरी पहले भी और इस बार भी बहुत मदद की है। इसके लिए मैं दिल से आभार व्यक्त करता हूँ।"

"Excellent"

"Need more reach so the needy gets your help"

“जो काम आप कर रहे हैं, वह सबसे बेहतर है। अल्लाह आपको और आपके ट्रस्ट को ऊँचा मुकाम दे।”

“The Trustline has been very helpful for me. When I reached out for support, they listened carefully and provided helpful suggestions. My issue was resolved in just one day. I truly appreciate their trust, support, and quick response. Thank you for helping me.”

“I got out of a huge situation and traumatic experience, and in a world where women are desensitized about crime and illegal stuff saying that it's their responsibility to take care of themselves and not the perpetrators' fault, the trustline helped me come out of that mentality and accept whatever happened, and deal with it the best way i could, providing with the legal support as well as mental support even when I stopped checking in on myself, the trustline was checking up on me, it's really important. Thank you!”

“Doing great job”

“माझी ट्रस्टलाईन खूप छान संस्था आहे त्यांनी माझी information खूप जास्त private ठेऊन मला खूप शांत पद्धतीने guide त्या बदल धन्यवाद माझी ट्रस्टलाईन”

“I was really impressed with the prompt intervention by the Meri Trustline team and appreciate your tireless efforts to protect children from online harms. I would like to know more about whether the Meri Trustline service and mechanism also extends to addressing offline sexual abuse against children that has happened before recorded content is posted online or that might continue even after content takedown.”

“Thank you soo much for helping us.. and I am glad we have such a platform for resolving the issues in which no one can help. You people are doing a great job... Thankyou is such a small word.”

“I am already suggesting meri to other people as well”

“I am glad that they solved the problem so quickly and with such patience”

And 1 two-star review: “Had an unpleasant experience.... The councellors in question chose to discuss my intimate matters with a former friend. As well as failed to cater to my needs and stall my standing over my case. Simply worse”



Thank you!

Author: Siddharth Pillai

Co-Authors: Salman Mujawar, Sameer P, Ritu Jain, Ruta Sawant

Editors: Uma Subramanian & Tanim Saha

Advisor: Tarunima Prabhakar

Contributing Former Team Member: Dr. Nisha Bharti

Legal Guidance & Support: Adv. Persis Sidhva, Adv. Pranalee Thakoor, Adv. Shivani Pundhir

Design & Illustrations: Entho Designs

Program Support: Urmila Sawardekar

Proofreader: Renuka Pal

Feeling **UNSAFE** online?
#DaroNahiDialKaro
Meri Trustline
63631 76363
9am to 5pm



India's
bharosemand
online safety
helpline