
DRF
DigitalRightsFoundation
"KNOW YOUR RIGHTS"
CYBER HARASSMENT HELPLINE
REPORT 2023

DIGITAL RIGHTS FOUNDATION

Digital Rights Foundation (DRF) is a feminist, not-for-profit organization based in Pakistan working on digital freedoms since 2013. DRF envisions a place where all people, especially women, can exercise their right of expression without being threatened.

Digital Rights Foundation believes that a free internet with access to information and impeccable privacy policies can encourage a healthy and productive environment that would eventually help not only women but the world at large.

Contact Information:
info@digitalrightsfoundation.pk
www.digitalrightsfoundation.pk

Gender-sensitive, confidential & free helpline:
0800-39393
helpdesk@digitalrightsfoundation.pk

Our gender-sensitive, confidential, free of charge helpline aims to provide callers with a safe space where they can easily share their problems regarding online harassment. We can be reached through phone, social media and emails 7 days a week from 9 am to 5 pm.

Researched and Prepared by: Hyra Basit, Anmol Sajjad, Ayesha Sarwar, Ayesha Nooral
Reviewed and Edited by: Nighat Dad, Seerat Khan
Design and Layout: Ahsan Zahid, Talha Umar

TABLE OF CONTENTS

01 Message from the Executive Director

03 Note from the Helpline Manager

04 Online Harassment and the Helpline's Journey

09 Year in Review

12 Age Distribution

13 Geographical Distribution

15 Gender Analysis

17 Vulnerable Individuals

18 Platforms

20 Types of Complaints

25 Services Provided

27 Escalation Resolution

29 Impact and Feedback

38 Suspected Mental Health Issues

39 Policy Recommendations

46 References

MESSAGE FROM THE EXECUTIVE DIRECTOR

As we reflect on another year of serving the community through the Cyber Harassment Helpline, it is evident that the landscape of online violence, particularly targeting women and marginalized groups, is evolving rapidly. This year, we have witnessed a concerning increase in technology-facilitated gender-based violence (TFGBV), with more frequent and severe attacks on women's identities and participation in politics online.

This year was marked by a troubling political landscape, and not just because of the upcoming elections. We've witnessed that the personal is truly political, and we've seen women human rights defenders, journalists, as well as politicians, become the subject of immense gendered abuse and harassment. As online spaces offer people an accessible way to voice their opinions, they also become the stage for heightened abuse. But as women become the target of gendered violence, it not only stifles their voices but also undermines the democratic process by limiting their ability to engage freely in public discourse.

Despite our efforts to raise awareness of online safety and TFGBV, the total number of calls to the helpline continues to grow, indicating that violence against women and marginalized groups is perpetuating in various forms online. One alarming trend is the use of generative AI, which makes it increasingly difficult to spot authentic content. This poses a significant threat as dis- and misinformation, and manipulated content can have serious real-world consequences, particularly from a gendered perspective.

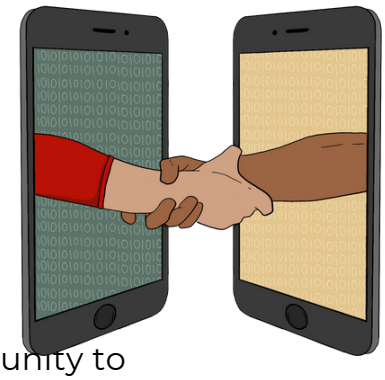
Furthermore, the rise in phishing attacks, unregulated apps, and wider data privacy breaches targeting individuals is a grave concern for online privacy. With data protection laws in place, there is a growing fear of how state and non-state actors may exploit digital data.

As everything becomes increasingly digital, it is imperative that steps are taken to protect users' privacy and security online. In the face of these challenges, the Cyber Harassment Helpline remains committed to providing support, guidance, and advocacy for victims of TFGBV. We will continue our efforts to raise awareness, provide online safety and digital literacy trainings, and advocate for policies that safeguard the rights of women and marginalized groups in the digital sphere.

Together, we can work towards creating a safer and more inclusive online environment for all.

Nighat Dad
Executive Director
Digital Rights Foundation

NOTE FROM THE HELPLINE MANAGER



Dear supporters,

During the drafting of this report, I got plenty of opportunity to reflect on the past year - the various cases we received, the hurdles we went through in trying to come up with ideal solutions for our complainants, our interactions with stakeholders, and of course, the strength and bravery exhibited by everyone facing technology-facilitated gender-based violence (TFGBV) who contacts us.

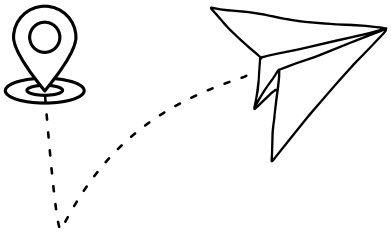
Now in our seventh year of operation, I am proud of the Helpline's strong commitment to providing sustained support to survivors of TFGBV, come rain or shine. At the same time, however, it is distressing that there is a need for this Helpline at all; the rising and evolving online harassment faced by women and transgender folks that necessitates the existence of the Helpline, should ideally not be a cause of concern at all. Until this ideal situation exists, though, the Helpline will hopefully be around to provide direct assistance to vulnerable individuals and communities in Pakistan (and around the world) facing TFGBV.

I would like to take this space to acknowledge the efforts of my team members without whom the Helpline would not be as successful as it is today. They are the heart and pillar of not just the Helpline, but DRF as well. They cope with the emotional burden of our callers with the strongest sense of empathy, and do not take the responsibility of being the first point of help to women under dire circumstances lightly. The importance of their work is exemplified by the sense of gratitude and relief expressed by our callers every day, so here's to them.

Sincerely,

Hyra Basit
Cyber Harassment Helpline Lead
Digital Rights Foundation

ONLINE HARASSMENT AND THE HELPLINE'S JOURNEY



Pakistan is consistently ranked among the world's most perilous countries for women. As internet usage has surged, with mobile broadband penetration[1] now at 53.6%, the scourge of violence against women continues to extend into the online sphere, reflecting the prevailing patriarchal and misogynistic norms. With the advancement and increasing accessibility of technology, the forms of technology-facilitated gender-based violence (TFGBV) have also evolved; the recent elections in Pakistan fostered an environment where deepfake images and videos of women politicians and journalists were spread online[2]. Vulnerable groups, including gender minorities, are particularly at risk in the digital realm, partly due to the anonymity the internet affords.

According to recent data from a GSMA report[3], women's mobile internet use stood at 27%; however, the gender gap between mobile internet use stands at 38%. Research on women's access to devices and the internet indicates that family disapproval remains a significant barrier to women owning a cellphone and accessing the internet. Another notable factor is that only 16% of women in Pakistan reported using mobile internet regularly, and that the top barrier to owning a mobile phone is low literacy and digital skills. This aspect is crucial in understanding why online harassment is wielded against women and how they respond to such threats.

In societies where a woman's (and her family's) honor is closely linked to family and societal perceptions, and where women's public participation is often discouraged, owning a cellphone is perceived as gaining access to the 'outside world.' This poses a challenge for women and girls seeking empowerment through digital means. Additionally, women's access to education still remains limited in the country and many women aren't aware of the legal avenues and redressal available to them in case they need to protect themselves online.

Digital Rights Foundation's investigations into online harassment in Pakistan reveal concerning trends. In a survey involving women in media and information roles, 55% reported experiencing abuse or harassment online, yet only 14.2% sought help[4]. Another study by DRF found that 70% of respondents feared the misuse of their pictures if posted online, with 40% reporting instances of stalking and harassment on messaging apps[5].

The decision to establish the Cyber Harassment Helpline was reinforced by two key events in 2016. Firstly, during DRF's Hamara Internet project, a significant number of young women approached the organization via social media and in person, seeking advice on online harassment. Secondly, the tragic murder of Qandeel Baloch underscored the dangers of online harassment; individuals supporting her received similar threats, highlighting the urgent need for a more robust support system for women online.

The passage of the Prevention of Electronic Crimes Act (PECA) 2016 and appointment of the Federal Investigation Agency (FIA) coincided with the development of the Helpline, allowing DRF to garner support from partners and operationalize the Helpline. The Act recognized cybercrimes, including online harassment, as punishable offenses, providing a legal framework to address such crimes. This facilitated the Helpline in offering concrete legal advice and assistance, meeting a crucial need for those requiring legal and emotional support. Since its inception, the Helpline has expanded its services, including an expanded legal team and referral system.

The launch of the Cyber Harassment Helpline in December 2016 underscores the growing demand for a secure online environment, particularly for women, children, and vulnerable occupations, who often experience higher rates of online harassment. It also demonstrates organizations like DRF taking proactive steps to bridge the gap and provide support for those affected by these crimes.

Over the course of six years, the Helpline has received and responded to 16,849 cases. Consistently, women have been the largest group to report instances of online harassment, and overall, they make up 58.5% of the people we have assisted.

16,849

CASES IN 7 YEARS OF CYBER HARASSMENT HELPLINE

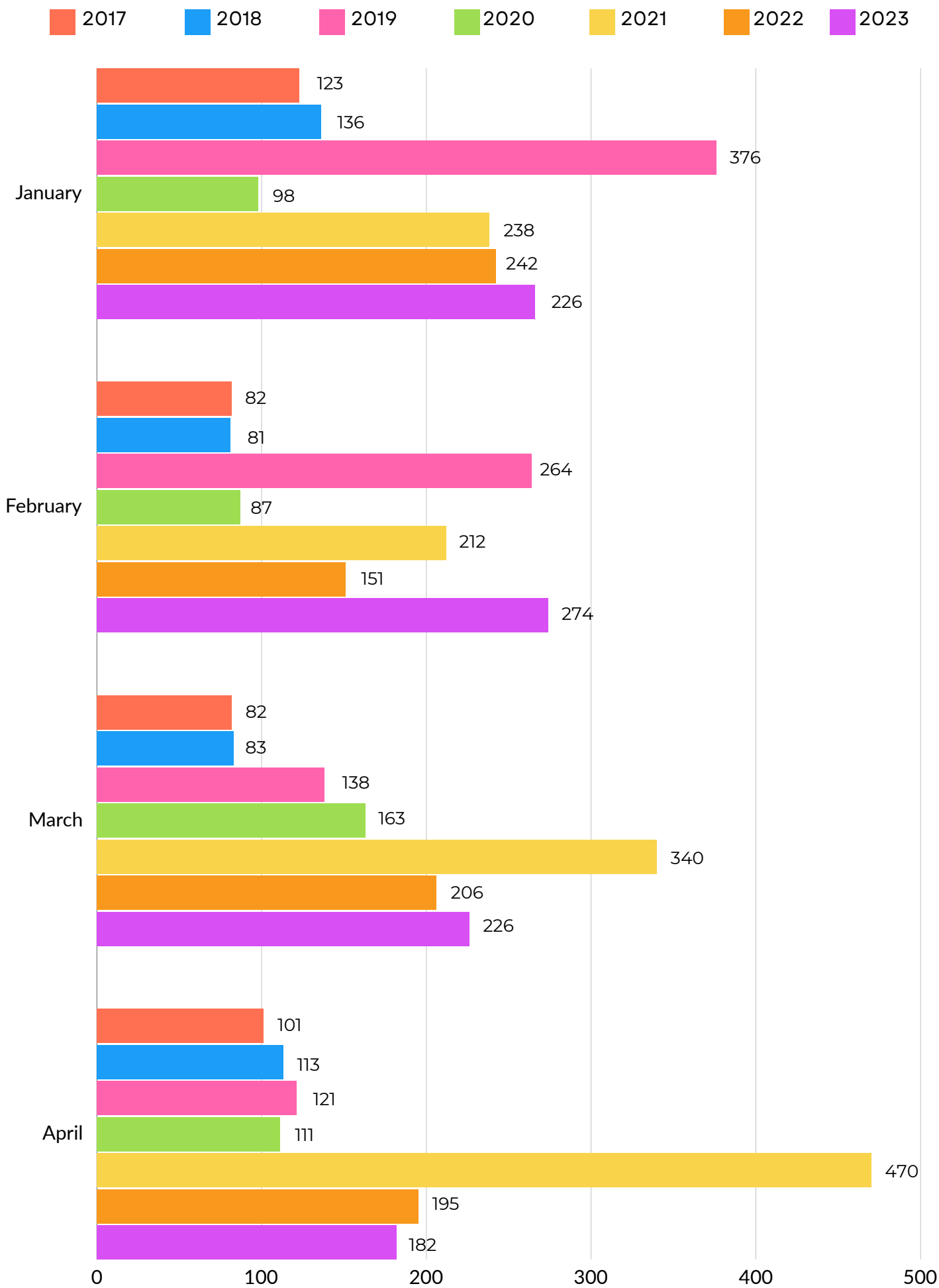


Fig 1.1: *Total number of cases received each year since the Helpline's initiation | Jan to April*

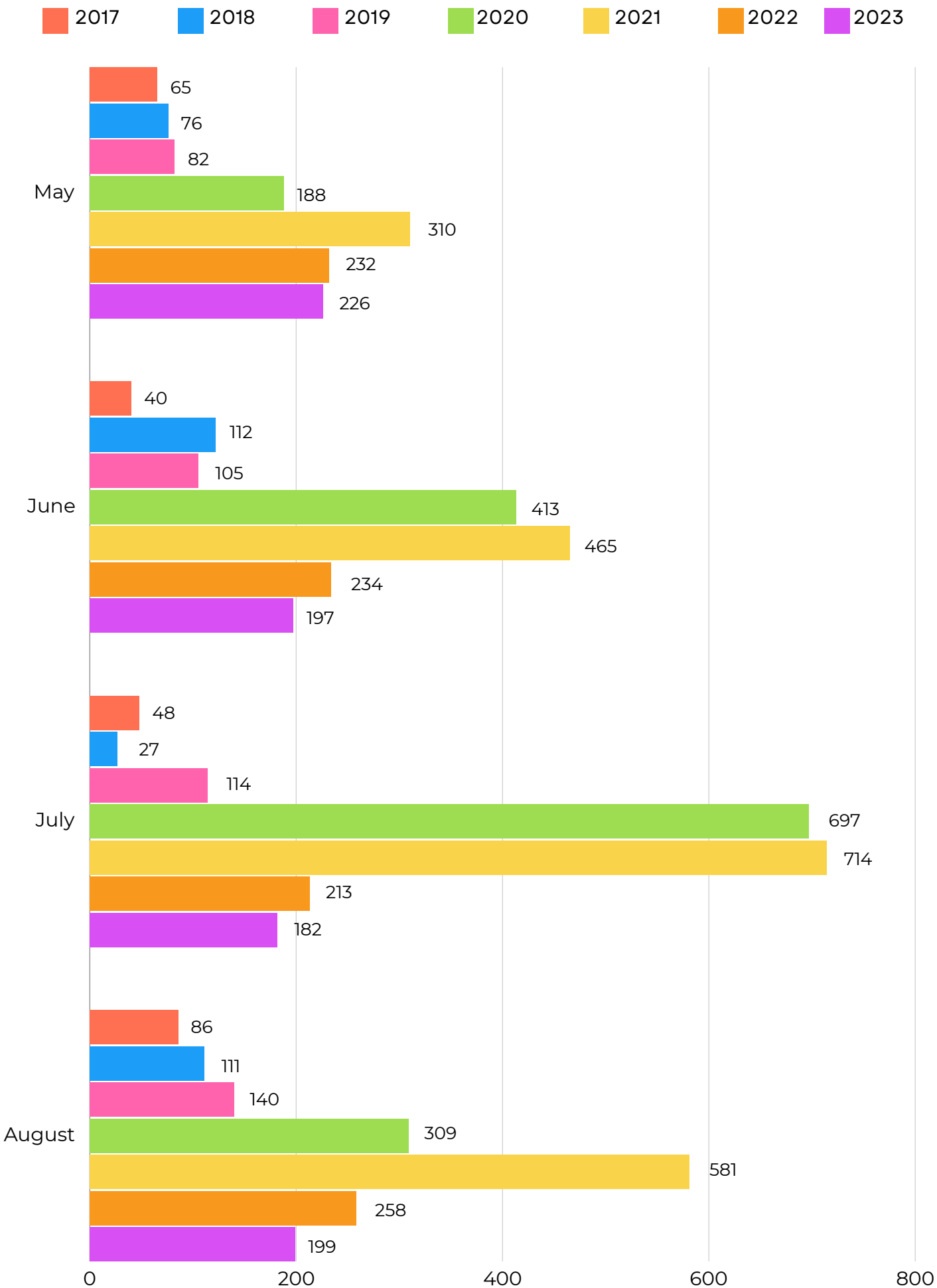


Fig 1.2: *Total number of cases received each year since the Helpline's initiation | May to Aug*

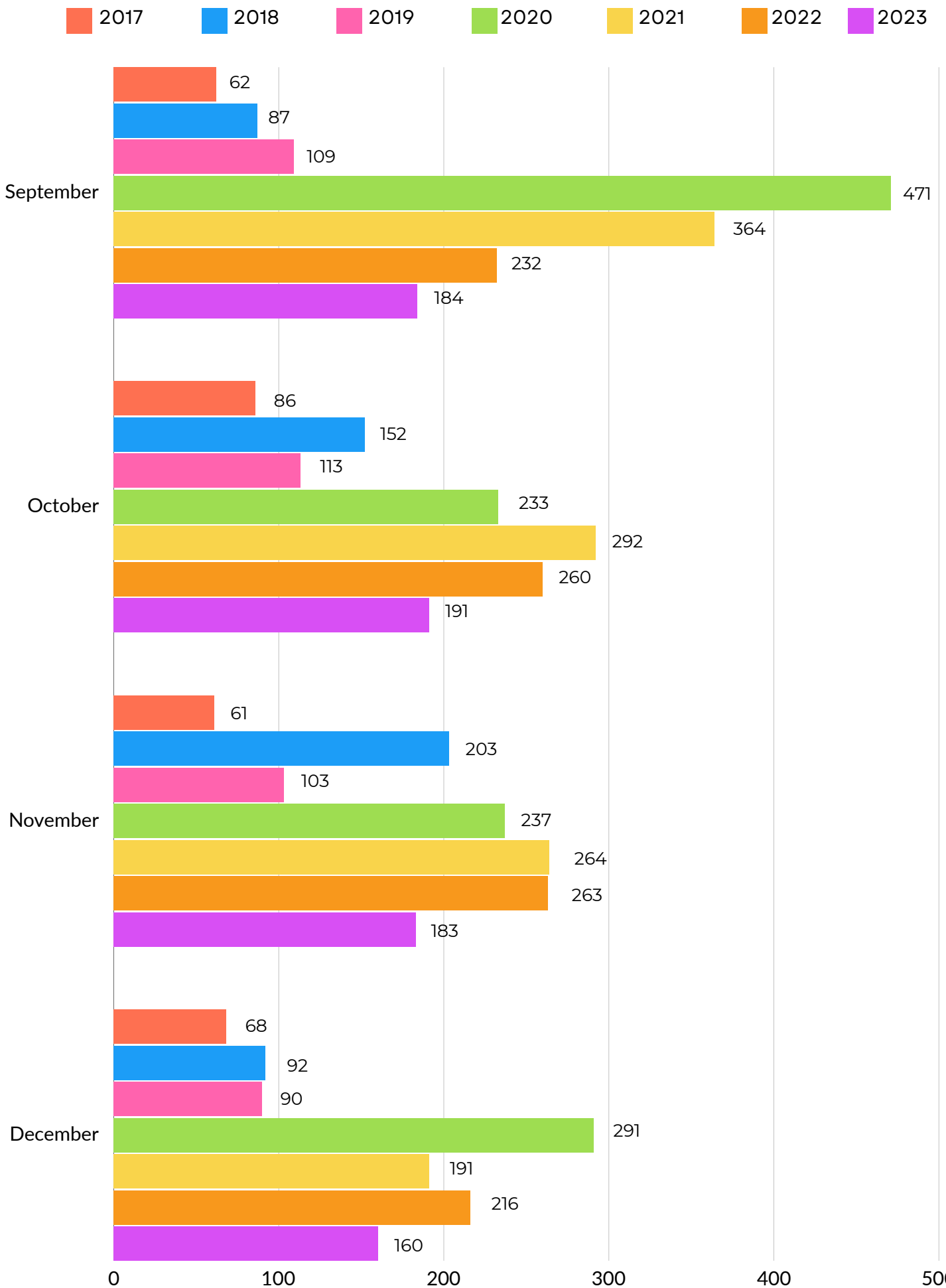


Fig 1.3: *Total number of cases received each year since the Helpline's initiation | Sept to Dec*

YEAR IN REVIEW

The Cyber Harassment Helpline receives cases primarily through three channels: the helpline phone number, DRF's social media channels, and the Helpdesk email. In 2023, a total of **2473** new cases were reported to the Helpline through these channels. The helpline is the primary mode of communication, with 2198 new callers. While the Helpline focuses on online harassment cases, it also considers other complaints depending on capacity, given the intersection of online harassment with other forms of violence. On average, 206 new cases were received each month, with February being the busiest.

During the coverage period, the digital gendered hate speech and gendered disinformation campaign targeting the transgender community in the country continued from the previous year. The response, or lack thereof, by social media platforms, where the campaign was orchestrated, is another troubling aspect of this trend. Although social media platforms showed a willingness to listen, the actions taken to resolve the matter were not satisfactory, resulting in harmful content remaining on the platforms. The Helpline team engaged with representatives from various social media platforms to explain the context of these campaigns and repeatedly requested more immediate action from platforms on the matter.

Also continuing from the previous year is the rise in financial fraud cases we received, despite these not being within the purview of the Helpline. However, it is pertinent to point out that a specific type of financial fraud committed through a surge of loan apps available in Pakistan was of interest to the Helpline. These loan sharks resorted to violating the privacy of several users; several complainants reported that the apps would gain access to users' contact lists and photo galleries, and would then use pictures to blackmail people, reach out to threaten and abuse their friends and family, or in certain cases, edit intimate pictures in order to blackmail people. Complaints regarding loan sharks dropped significantly after the Federal Investigation Agency (FIA) took notice of these predatory loan apps in July 2023[6].

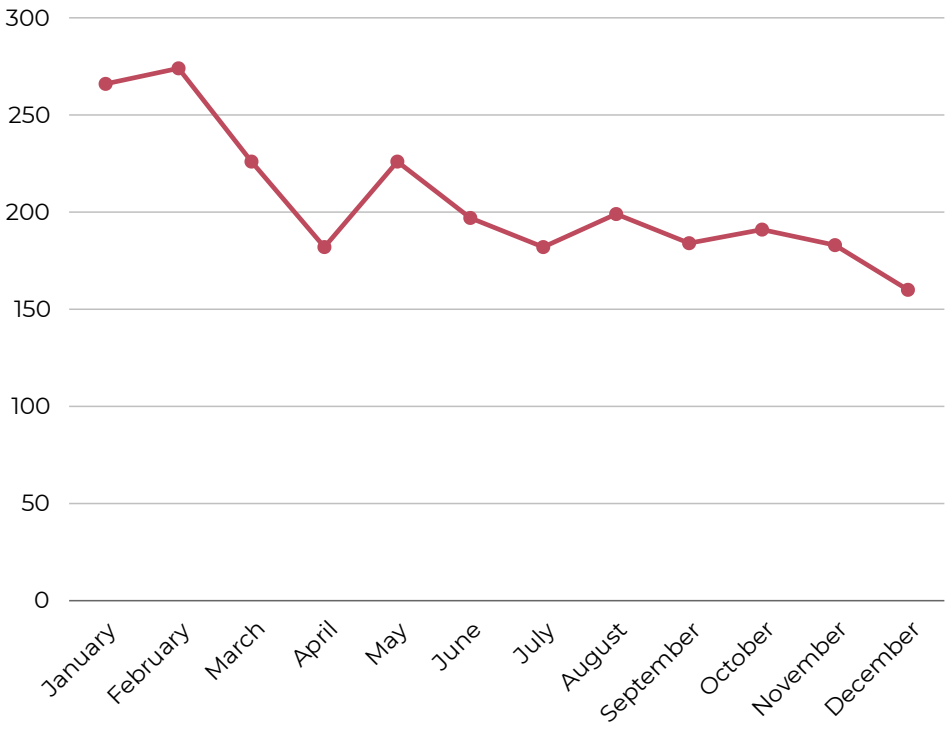


Fig 2.1: *Total calls received in 2023*

CATEGORY OF COMPLAINTS

2224

CYBER HARASSMENT

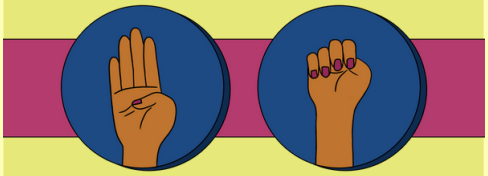
151

GENERAL INQUIRY

53

OTHER DIGITAL ISSUE

26



DOMESTIC ISSUE

10

PHYSICAL HARASSMENT

08

WORKPLACE HARASSMENT

AGE DISTRIBUTION

DRF's Cyber Harassment Helpline does not ask for complainants' personally identifiable information in order to preserve their privacy and identity. However, the Helpline does ask for certain details that would contribute to our research on how online harassment manifests in Pakistan.

The age distribution of our complainants indicates that young adults, particularly women, between the ages of 18 to 30, are most prone to facing some type of online harassment. Interestingly, for age groups above 30, complainants who are men outnumbered the women. This could indicate that younger women face greater instances of online harassment, or alternatively that they are more comfortable in reporting such instances although it cannot be ascertained for sure.

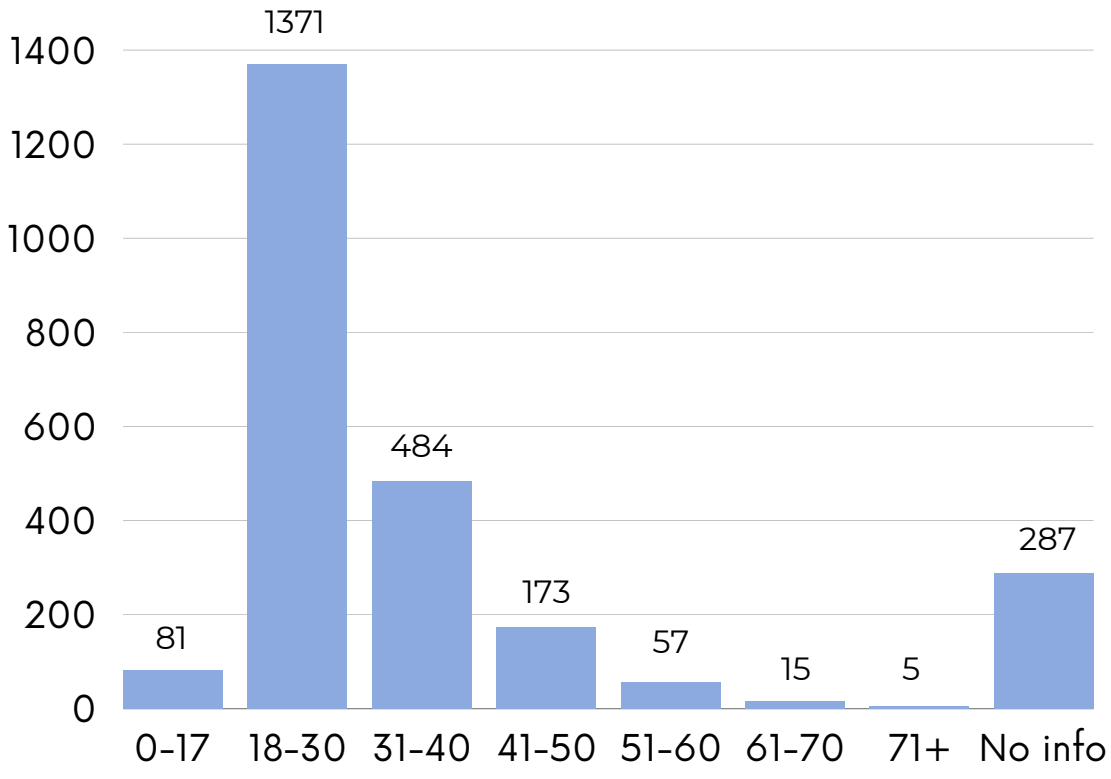


Fig 3.1: *Age distribution of complainants*

GEOGRAPHICAL DISTRIBUTION

We request information regarding the city and region of our callers to provide tailored advice and support, facilitating informed decision-making. Additionally, this data aids in mapping the accessibility of law enforcement and other support services, thereby enhancing our capacity to advocate effectively for individuals experiencing online and other forms of harassment.

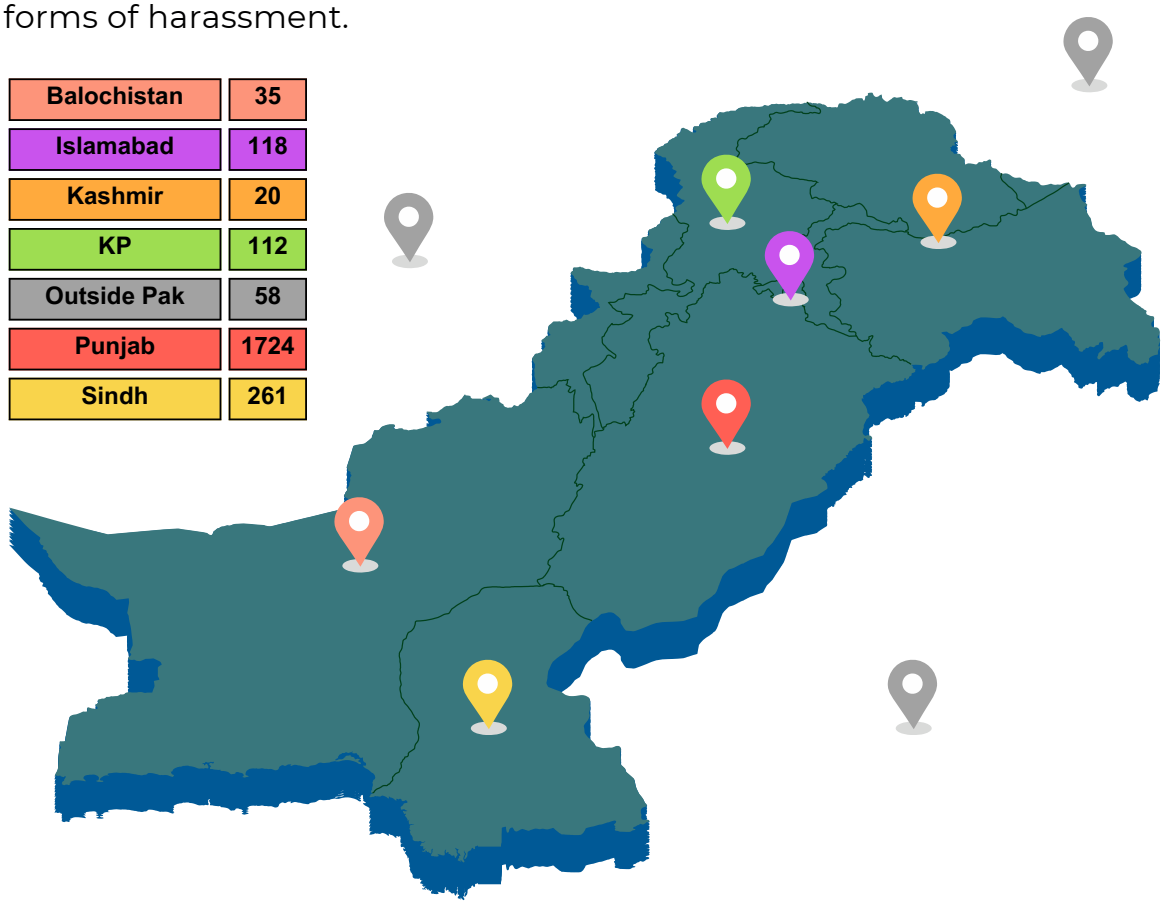


Fig 4.1: *Geographical Distribution of Helpline Calls 2023*

In 2018, the FIA announced[7] that it was expanding its services to 15 cybercrime wings in Pakistan. The option of registering a complaint online is available through their website, email and the FIA helpline; however, according to the feedback received from our complainants, these methods are nowhere near as efficient as visiting their office in person. According to the Georgetown Institute for Women, Peace and Security,[8] Pakistan scored 1.53 on a scale of zero to four on the access to justice scale which measures the degree to which women can file lawsuits, demand fair trials, and seek legal recourse when their rights are infringed.

Out of the 2224 cases of cyber harassment received by the Helpline, 1278 (57.5%) were eventually referred to the FIA because it was advised that taking legal action would be better for the long-term well-being of the survivors. 67.6% of the cases referred to the FIA originated from one of 15 cities where an FIA cybercrime wing was located, whereas 392 or 30% of cases originated from other locations, making it necessary for these complainants to travel across cities to file a report.

Complainants, especially women, have strongly objected to the scarcity of dedicated cybercrime units in their city. This logistical challenge is particularly acute for women and girls, who often prioritize maintaining privacy to avoid potential repercussions stemming from societal victim-blaming tendencies. Additionally, financial constraints serve as a significant deterrent, as individuals may find the prospect of traveling to lodge a complaint with the FIA financially burdensome. The associated costs of traveling to their nearest FIA office, including transportation expenses and accommodations, can impose a considerable burden, particularly for those with limited financial means. In Pakistan, pervasive gender norms often restrict women's financial and physical autonomy, leaving them dependent on seeking their family's permission. Furthermore, concerns regarding personal safety in public spaces, fueled by prevalent gender-based violence, compound the reluctance to embark on such trips. The necessity of physical travel to pursue legal remedies is therefore a significant barrier to pursuing legal remedies for women.

> However, five years after the expansion of cybercrime wings in 2018, amendments were made to PECA, that authorized the police to take notice of cybercrimes as proscribed under PECA, and to refer the matter to the FIA for due investigation.

In 2023, the Helpline received the highest number of complaints from within Punjab. In contrast, we received no complaints from Gilgit-Baltistan and Gwadar (Balochistan), despite the presence of FIA cybercrime wings in these two locations. This does not necessarily mean that these areas are devoid of complaints regarding online harassment or TFGBV; it may instead be an indication of the Helpline's uneven reach within the population, or that people are generally unaware of reporting mechanisms in these areas.

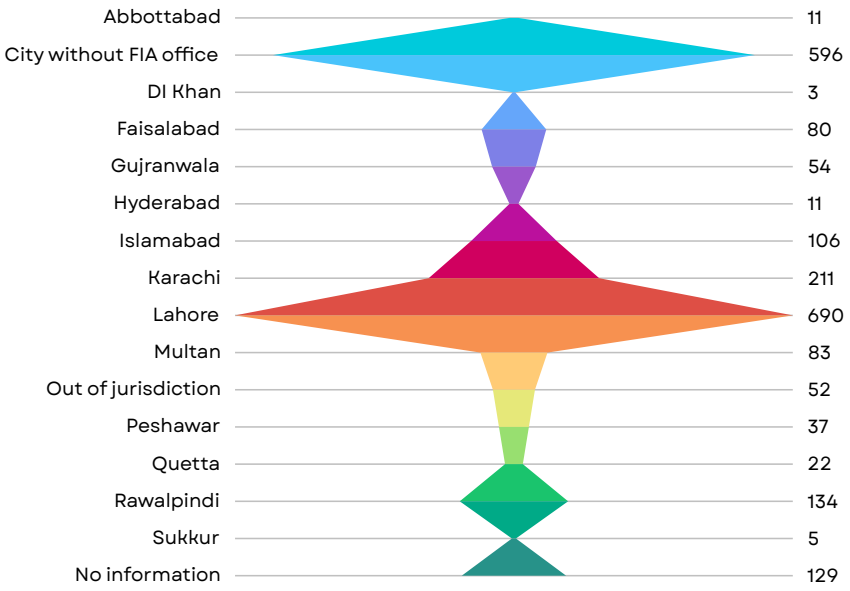


Fig 4.2: *Cases received from cities with established FIA Cyber Crime Wings*

GENDER ANALYSIS

Another category of non-personally identifiable information that the helpline records from complainants is their gender. Our aim at the Helpline is to provide a safe space for women and other gender minorities to seek guidance for the TFGBV that they experience in an environment where they won't be judged and to empower them to take back control.

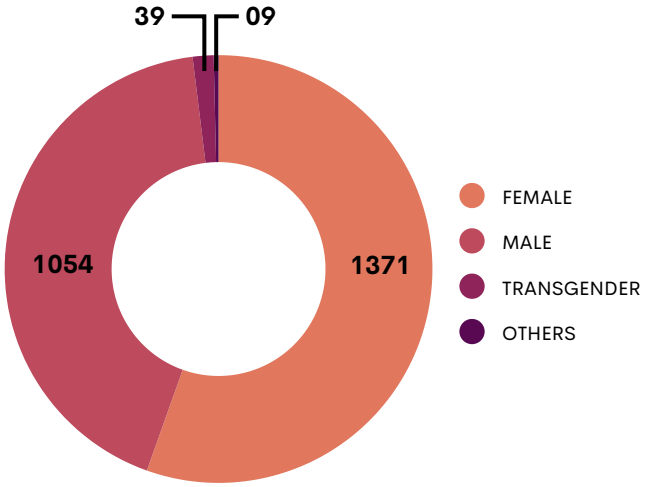


Fig 5.1: *Gender of Complainants*

Keeping in mind the taboo that is attached to being a victim of online harassment, especially in a conservative environment such as Pakistan, it can be difficult to confide in friends and family; according to the GSMA Gender Gap report[9], family disapproval counts as a major barrier to women's ownership of mobile phones. Many of our complainants (particularly women) report they are unable to share their circumstances with their family and cannot depend on them for support, which is also precisely one of the reasons the Helpline was established in the first place - to help women move past a sense of shame and secrecy. Out of the 1371 cases where a woman was targeted, 79% were reported to us by the complainant herself.

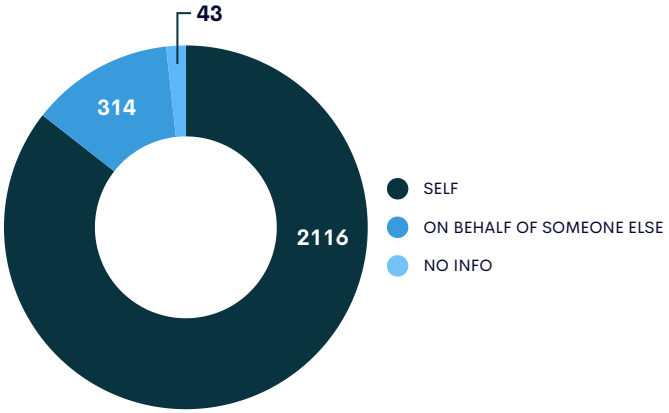


Fig 5.2: *Caller Segmentation*

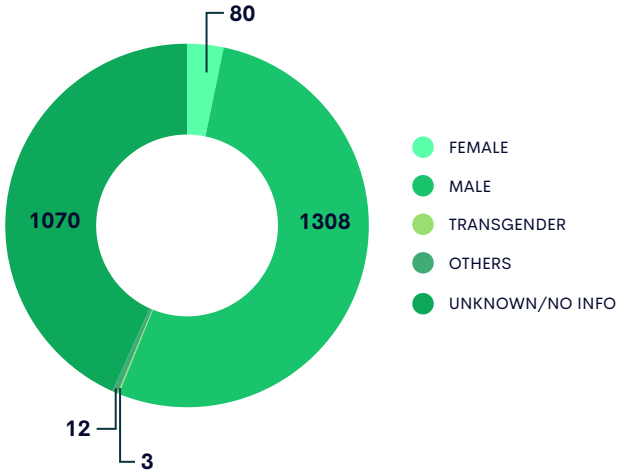


Fig 5.3: *Gender of the harasser*

From our analysis of the survivors' relationship with the harasser, about 30% were currently or previously in a romantic relationship with the harasser at the time of contacting the Helpline. This category includes relationships that started online. We have further categorized the various types of romantic relationships to better comprehend the influence each relationship type may have on resolving their case. This information is crucial as it influences the tactics the harasser might employ to intimidate the victim. Approximately 50% of the complainants reported being harassed by someone they knew in a personal capacity, including their friends, family, and (ex)partners.

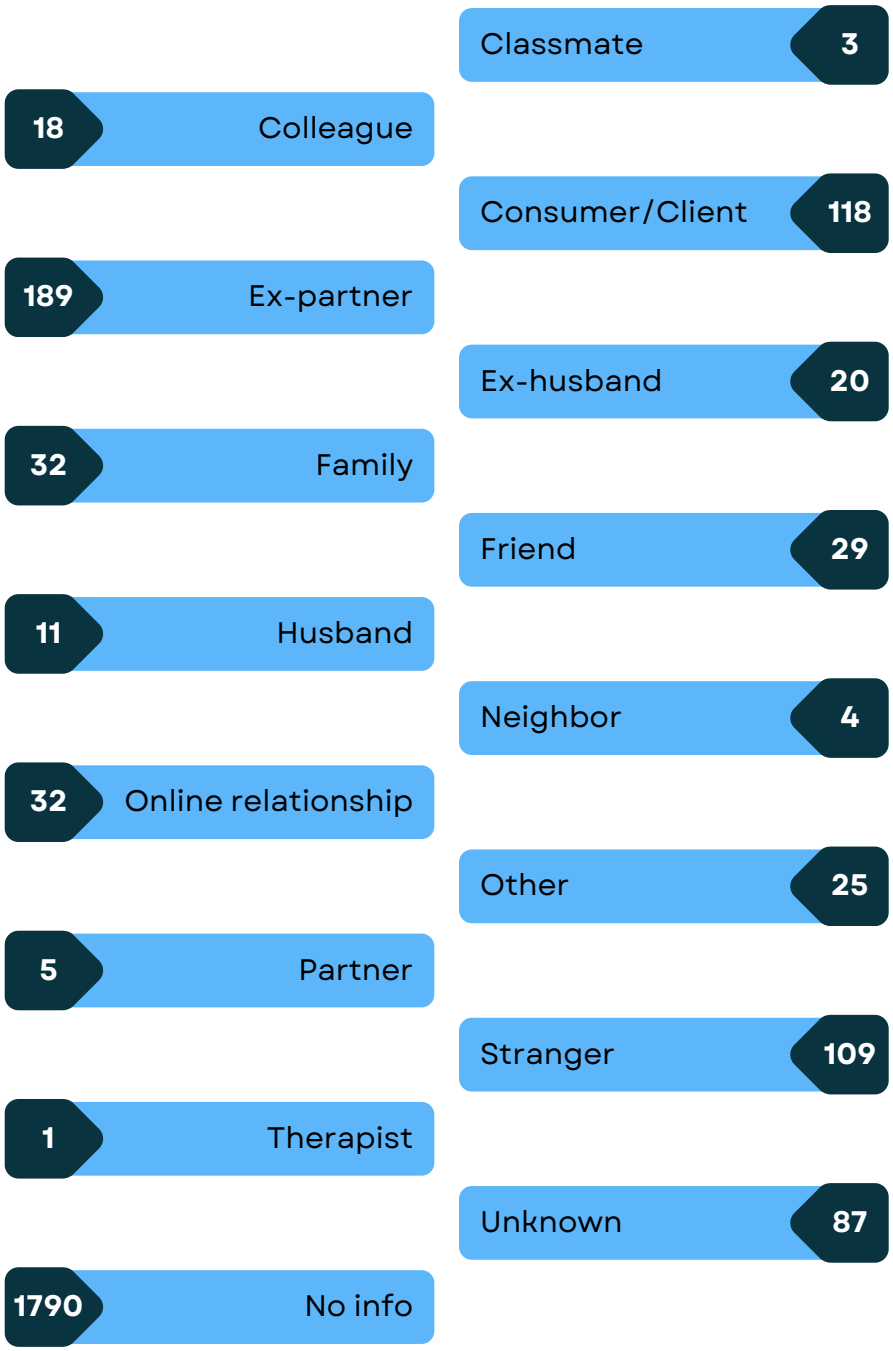


Fig 5.4: *Relation with the harasser*

VULNERABLE INDIVIDUALS

Certain segments of our society encounter heightened vulnerability to online harassment, either due to their identity or their profession. It is imperative for the Helpline to acknowledge and support these groups to mitigate the increased risks they face. The provision of specialized assistance becomes essential given the absence of adequate institutional safeguards available to these individuals. Notably, the past year witnessed the continuation of a concerted online hate campaign targeting the transgender community, comprising threats, abuses, and gendered disinformation, culminating in tangible threats of physical harm and legal action against the minority group.

In response to this alarming surge in hostility jeopardizing the safety and well-being of transgender individuals, the Helpline actively engaged with social media platforms, flagging cases and holding discussions to underscore the perilous misuse of their platforms. Furthermore, women journalists confront a heightened susceptibility to online harassment attributable to their gender, often enduring misogynistic and sexually explicit remarks. Moreover, they may encounter censorship and professional reprisals, which could have profound personal and career ramifications. Hence, it is imperative to furnish tailored support to individuals navigating such intricate and intersecting vulnerabilities.

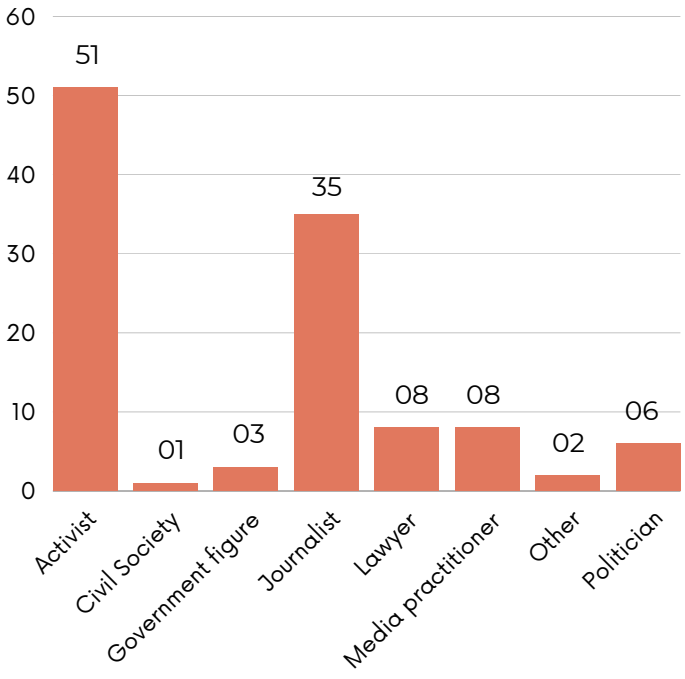


Fig 6.1: *Vulnerable Occupations*

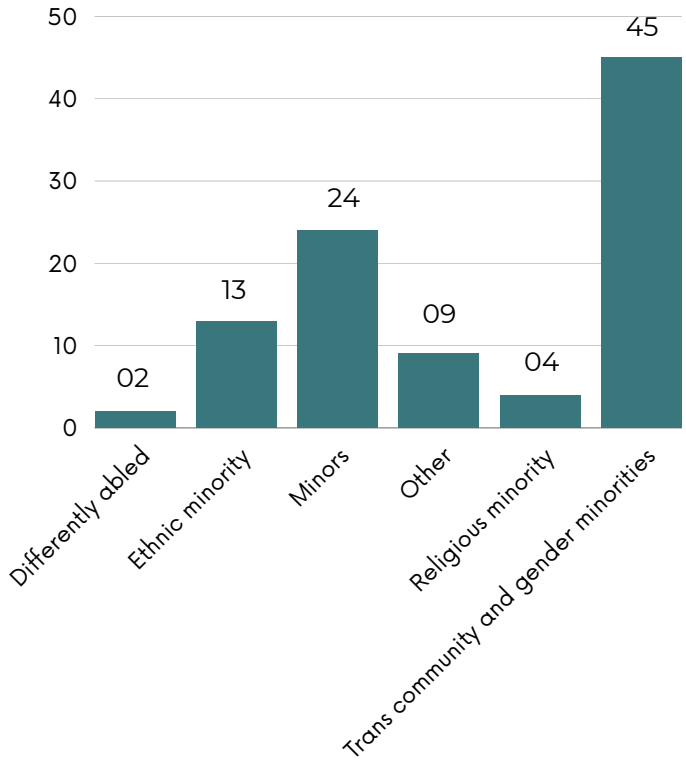


Fig 6.2: *Vulnerable Communities*

PLATFORMS

The Helpline monitors emerging patterns in online harassment by keeping track of the platforms where complainants report problems or harassment relating to online spaces. We then utilize this information to inform callers about preventative actions and conduct public awareness campaigns on DRF's social media channels. By highlighting the abuse and harmful content on these platforms, we get better equipped for further direct advocacy towards governmental agencies, social media companies, and tech businesses, and suggesting specific policies and safety initiatives to counteract the growing threats to users.

> With a combined 55.6% share of complaints (up by 3% since last year), WhatsApp, Facebook, and Instagram continue to be the platforms where users experienced the greatest levels of online harassment and other digital problems.

In order to close the gap between the community guidelines and policies focusing on the global north instead of the global majority and the use and abuse of these platforms with context-specific consequences in Pakistan, the Helpline has developed trusted partner relationships and escalation channels with a number of platforms. Platforms are constantly being pushed on how a universal policy application approach that depends on automated systems to review reports can frequently result in either too much or too little content moderation for cases from the global south/majority and in non-English language contexts. We engage in regular communication with these companies in order to flag emerging patterns and to prevent trends that could harm the most vulnerable communities.

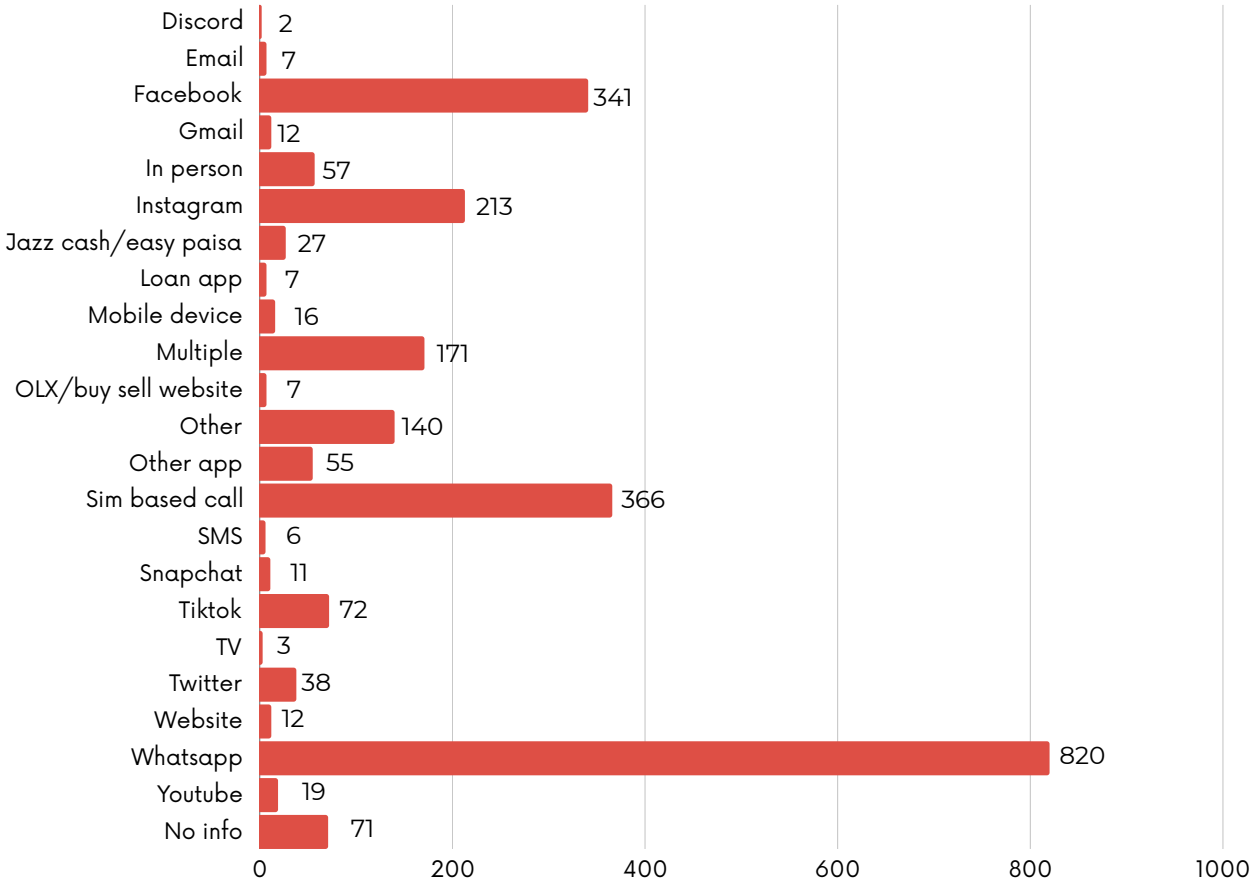


Fig 7.1: *Types of platforms*

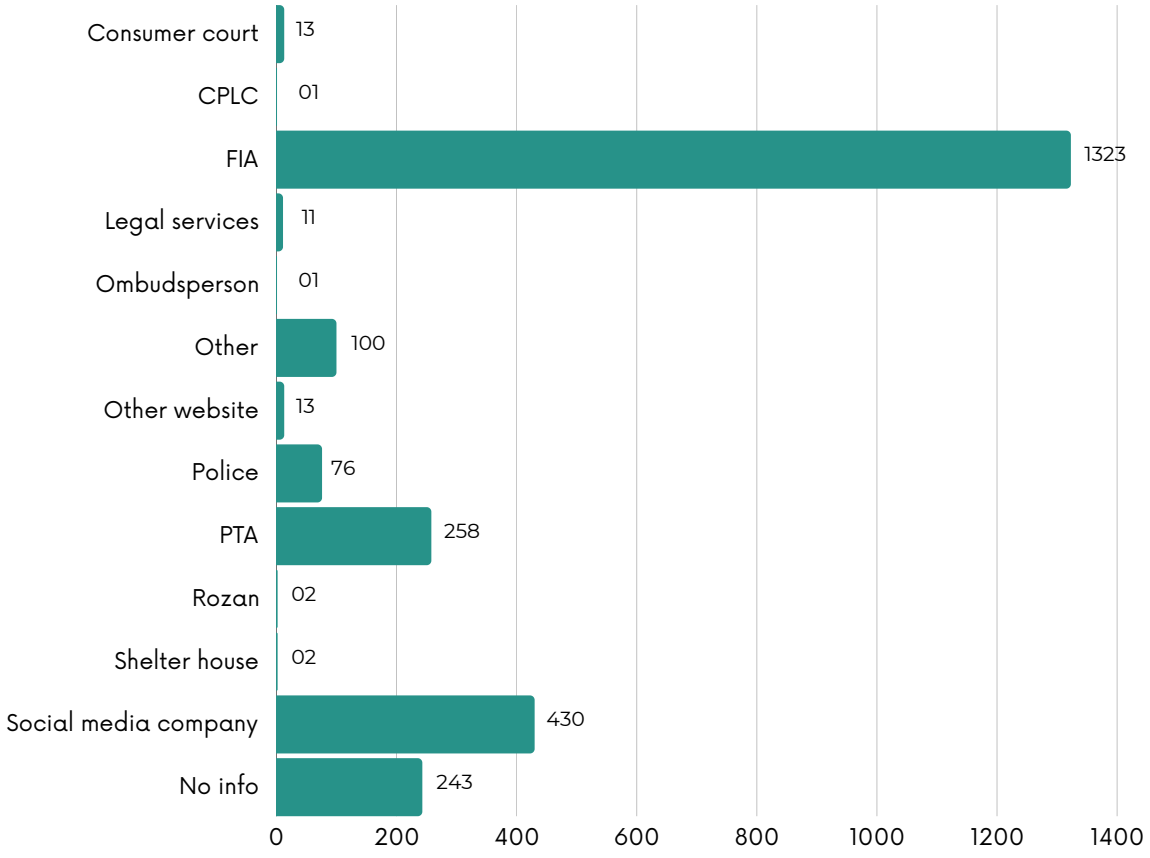


Fig 7.2: *Complaints Referral*

TYPES OF COMPLAINTS

The Cyber Harassment Helpline receives a diverse range of complaints, as illustrated by the data below, which can often be gender-specific in nature. Among the most common grievances reported by both men and women are blackmail, hacking, threats, and unsolicited contact. However, the manifestation of these complaints can exhibit gendered patterns. For instance, women frequently encounter sexualized comments or threats aimed at tarnishing their reputation.

Moreover, women often report cases involving defamation and the non-consensual use of intimate images/information (NCII and NCUI), which often exploit patriarchal honor-based norms. Consequently, women tend to lodge more complaints related to sexualized threats and comments, actions that undermine their reputation, especially in the eyes of their family and friends, or simply based on the fear of their family discovering their online presence. Conversely, men may face similar complaints, but these threats are not necessarily sexual in nature or aimed at defaming their character.

There are certain types of abuse that are reported simultaneously that exemplify the way in which TFGBV manifests in Pakistan. 87% out of the 178 cases of non-consensual intimate images (NCII) were reported by women. Similarly, 86% of the 460 blackmailing cases were reported by women. 48% of all cases that involved the non-consensual use of images, intimate or otherwise, reported by women also included an element of blackmailing.

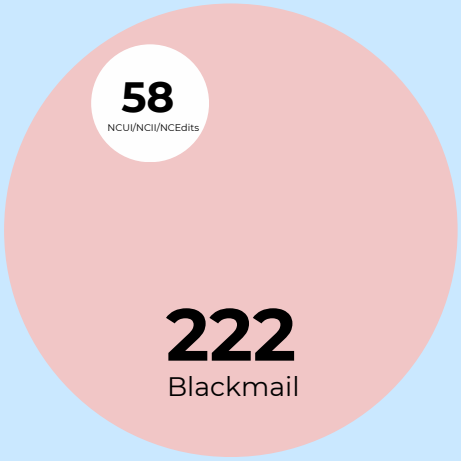


Fig 8.1: *26% of blackmail cases were NCUI/NCII/NCEdits*

Fig 8.2: *48% NCUI/NCII/NCEdits cases were blackmail*

TYPES OF COMPLAINTS

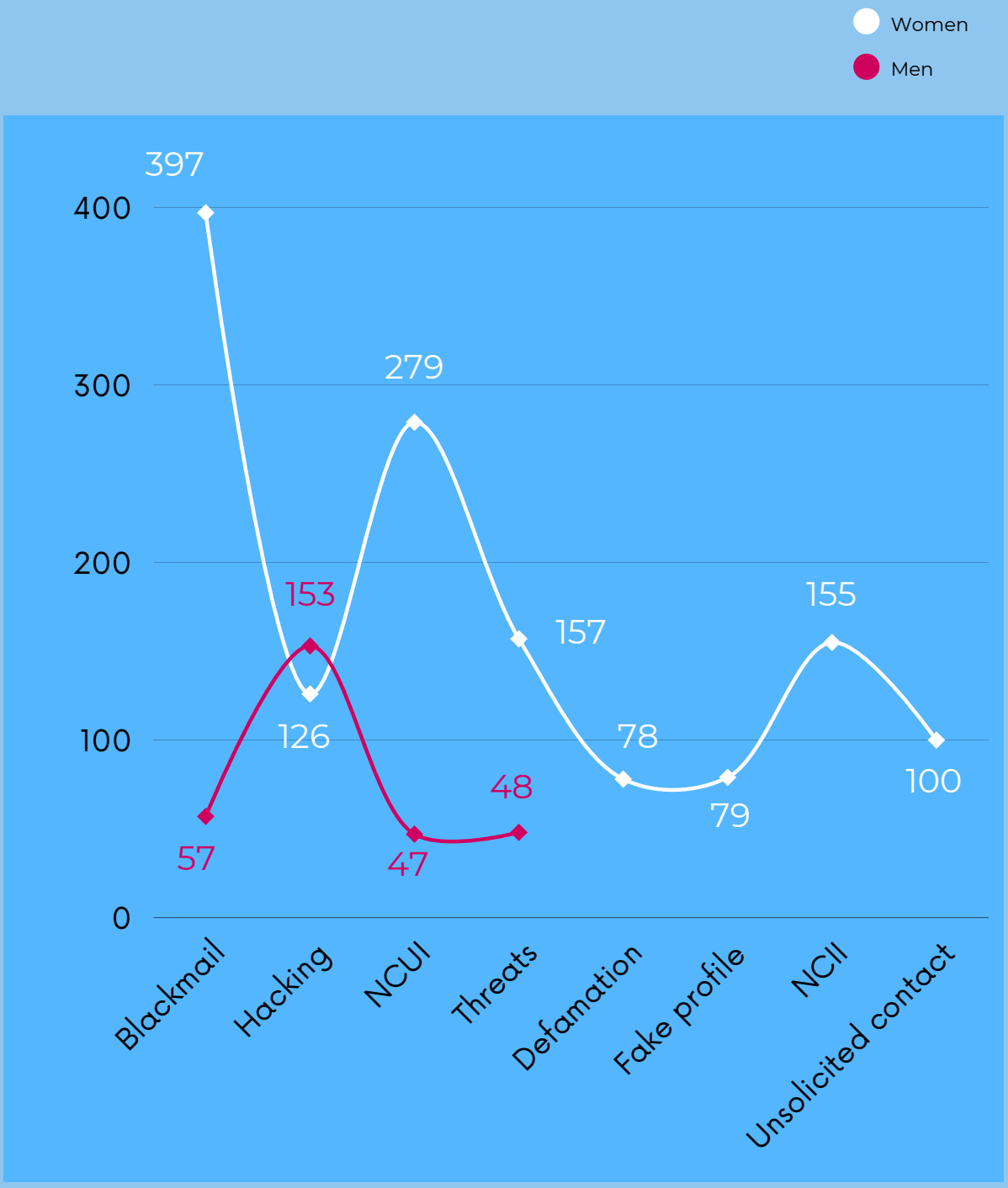


Fig 8.3: *Highest Incidents | Men Vs. Women*

TYPES OF COMPLAINTS

	TOTAL	FEMALE	MALE	NB	TRANS WOMAN	TRANS MAN
(THREAT OF) BLASPHEMY ACCUSATION	11	4	5		2	
ABUSIVE MESSAGES	64	42	19	1	1	
ACCOUNT DISABLED	25	16	6			
BLACKMAILING	460	397	57		2	
BULLYING	18	10	4		3	
CAPTURED ON CAMERA WITHOUT CONSENT	21	15	4		2	
CENSORSHIP	9	2	4		1	
COPYRIGHT ISSUE	2	1			1	
DEFAMATION	116	78	34		1	2
DOXING	29	20	9			
FAKE PROFILE	108	79	27		1	
FIA RELATED	22	6	13			
FINANCIAL FRAUD	742	227	506			
GBV	7	7				
HACKING	286	126	153		2	
HATE SPEECH	27	4	1	1	18	2
IMPERSONATION	69	49	20			

	TOTAL	FEMALE	MALE	NB	TRANS WOMAN	TRANS MAN
INFORMATION REQUEST	113	30	36			
LOGIN ISSUES	39	15	14		3	
NCII	178	155	23			
NCEDITS	35	33	2			
NCUI	334	279	47		7	1
ONLINE STALKING	31	27	4			
OTHER	81	32	42		1	
PHISHING	16	11	5			
PHYSICAL VIOLENCE	18	12	5			
SEXUAL HARASSMENT	27	23	3			1
SOCIAL ENGINEERING	59	16	43			
STALKING	23	20	2		1	
STOLEN DEVICE	12	5	7			
THREAT	213	157	48		8	
THREATS OF PHYSICAL VIOLENCE	35	21	13		1	
UNSOLICITED CONTACT	148	100	46			

Key:

*GBV: Gender based violence

NCII: non-consensual intimate images

NCEdits: non-consensual edited images

NCP: non-consensual pornography sent

NCUI: non-consensual use of information

'Blackmailing' may refer to asking for sexual or monetary favors in exchange for not distributing or tampering with a survivor's intimate images, or contacting the survivor’s family

SERVICES PROVIDED

The Helpline was established with a core mission of offering legal aid, digital security guidance, and basic counseling services to our valued callers. Supported by a proficient legal advisory team and digital security experts, our Helpline Associates are dedicated to meeting the diverse needs of our callers.

Our digital services encompass providing advice on digital security and best practices aimed at preventing or mitigating the impact of future instances of online harassment. We maintain direct channels of communication with major social media and technology platforms, facilitating mediation between them and local users, particularly when automated reporting mechanisms prove ineffective. These channels also enable us to identify and report dangerous and abusive trends targeting minority communities and public figures, effectively alleviating their mental distress and safety concerns. In scenarios where established escalation channels are absent, but content removal is imperative, such as cases involving intimate image abuse, we conduct independent and thorough research on all platforms hosting the offending content

As an accountable organization, we consistently strive to enhance our services in response to the evolving needs of our callers. In this regard, DRF's legal department has curated an online directory named 'Ab Aur Nahin,' featuring lawyers who volunteer to offer pro-bono legal assistance to complainants nationwide. Additionally, we have broadened our service scope to include in-person counseling and legal aid for complainants seeking to file legal complaints with the FIA cybercrime wing in Lahore.

In certain instances, we may need to gather and retain additional personal information from complainants to gain deeper insights into their cases and offer informed guidance. This may include details such as the complainant's name, contact information, and evidence photos. However, we assure our callers that such information is only retained for the duration of the Helpline lawyer's case follow-up and is not disclosed to external parties beyond the Helpline team.

Our commitment to upholding confidentiality and safeguarding data privacy is paramount. We employ stringent measures to ensure that the personal information of our callers is handled with the utmost security and confidentiality.

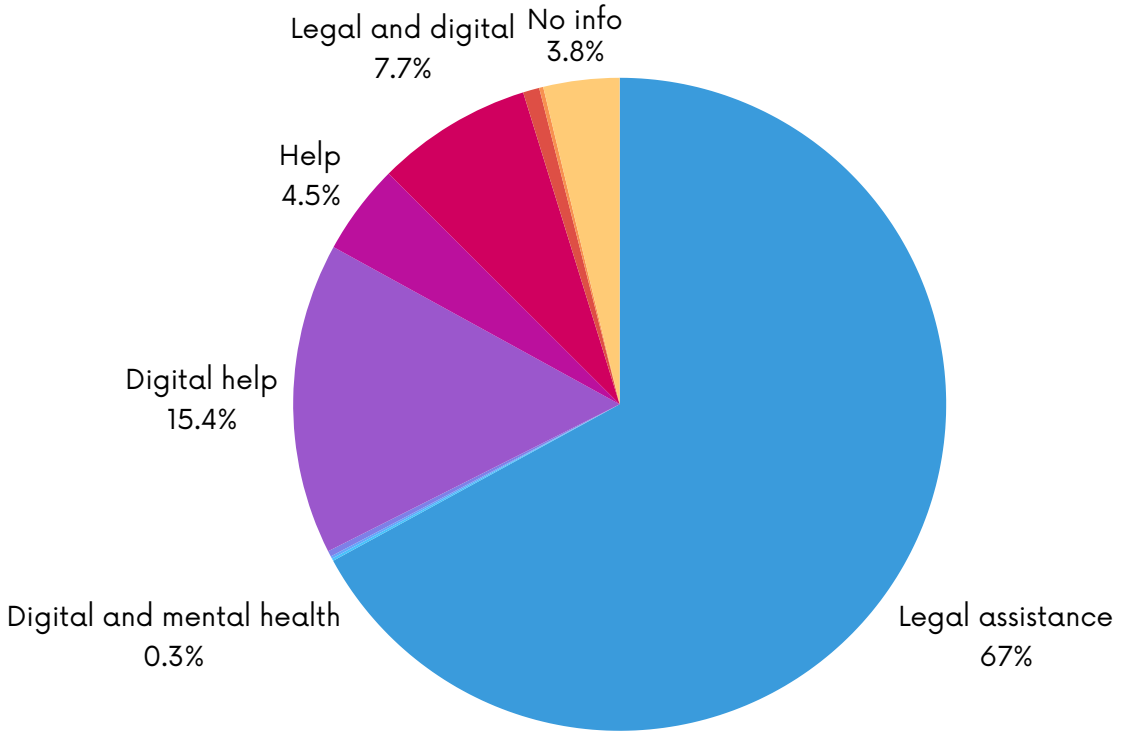


Fig 9.1: *Services provided by Helpline in 2023*

Summary of the Legal Team's engagement with the Helpline

Calls Received	Visits to Court/FIA	Survivors Assisted
140	77	43

ESCALATION RESOLUTION

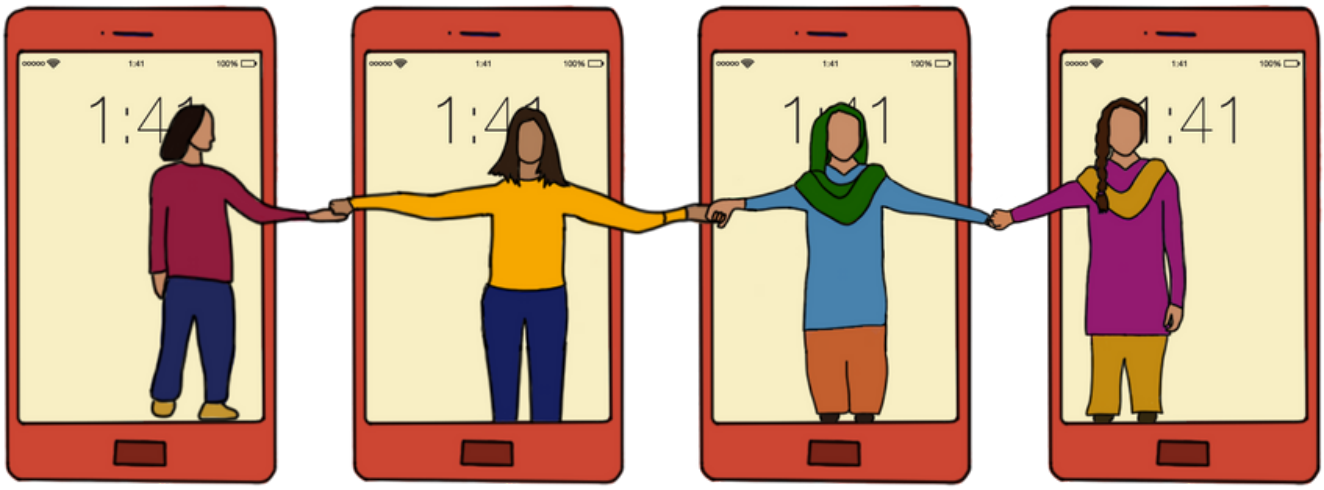
The Cyber Harassment Helpline has established escalation channels with various social media platforms. Where necessary, it also makes its own efforts to take down content on other websites that is harmful to a complainant and/or is violating laws. The kind of content we report through these channels generally pertain to intimate images or non-consensual use of images, fake or impersonating profiles, defamatory content that is inherently false, or the recovery of hacked accounts, particularly for vulnerable individuals.

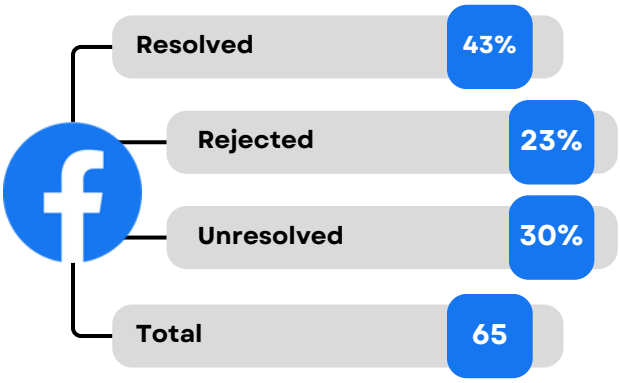
> In 2023, the Helpline made 177 escalations, and noticed several patterns in this process. The highest number of escalations were made regarding Meta platforms, totaling 124, but the highest resolution rate of the escalated cases was of TikTok at 77.8%.

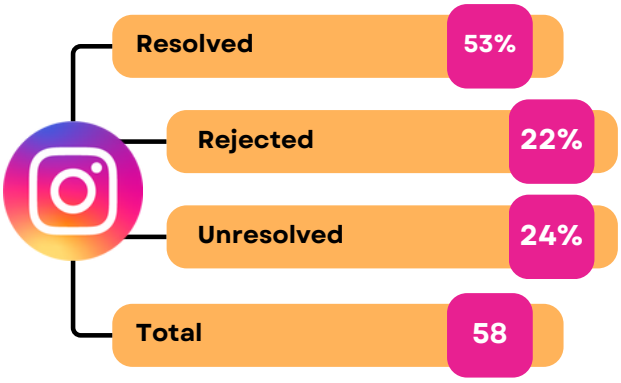
For several escalations made, there were many that were left unresolved which means either there was no answer or instructions were sent for complainants to fill out a form, which did not completely resolve the issue.

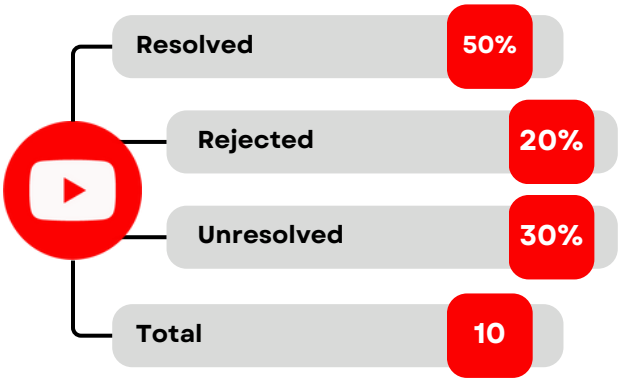
> After the recent changes in X's (formerly Twitter) internal structure, the escalation channel completely disintegrated after May, although they previously exhibited an appreciable level of cooperation.

Quite some content that fell under hate speech or disinformation against the transgender community in Pakistan was reported to Meta. As we mentioned in last year's report, Meta did not take this content seriously and was actively rejecting our requests, but after several meetings with their team in which we highlighted the gravity of the situation, their response improved slightly.

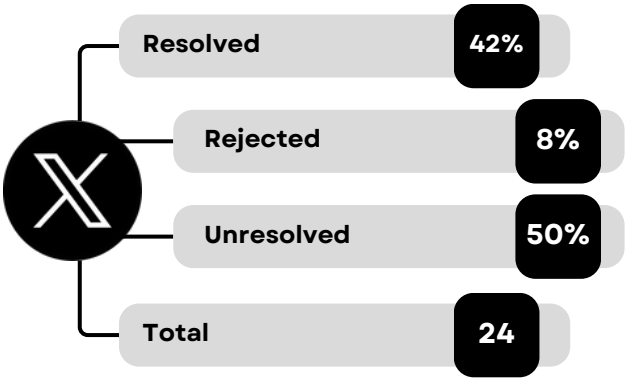



Resolved
43%
Rejected
23%
Unresolved
30%
Total
65


Resolved
53%
Rejected
22%
Unresolved
24%
Total
58


Resolved
50%
Rejected
20%
Unresolved
30%
Total
10


Resolved
78%
Unresolved
22%
Total
18


Resolved
42%
Rejected
8%
Unresolved
50%
Total
24

IMPACT AND FEEDBACK

To assess our impact, we have utilized various data sources to gain a comprehensive understanding of the Helpline's effectiveness. This includes tracking the number of cases that were successfully resolved, as well as evaluating the quality and impact of the support provided.

Feedback from our callers regarding how they learned about the Helpline serves as one metric for measuring our impact. Of the respondents, 4% mentioned being referred by a friend, and an equal proportion discovered the Helpline by reaching out to a DRF team member. The majority, 67%, learned about the Helpline through social media platforms. While DRF maintains an active presence on Instagram, Facebook, and Twitter, most of our promotion is through digital word of mouth. This indicates the level of trust, quality, and satisfaction callers experience with the Helpline, prompting them to recommend our services to others.

> It is important to note that the number of new cases received by the Helpline does not fully reflect the total number of calls handled by our associates. Follow-up calls constitute a significant portion of our daily activities, with 619 out of 3092 calls being follow-ups, accounting for approximately 20% of the year's total calls. This can be attributed to our ongoing support, reassuring responses, and proactive approach to seeking new solutions to recurring issues.

To respect our beneficiaries' privacy, we do not initiate contact unless we have their explicit permission. Consequently, our ability to measure impact is limited, as we often do not receive updates on case resolutions unless the callers reach out to us again.

Moreover, the definition of a "resolved" case can be subjective. Some issues may resurface over time, or beneficiaries may be content with a temporary solution rather than a permanent one. Additionally, when cases are referred to other institutions, we face a dilemma regarding whether to mark the case as resolved or continue to monitor its progress, for which we need express permission.

Given these challenges, we have not relied solely on direct feedback to measure impact. Instead, we conduct a feedback survey sent to select beneficiaries as well. However, this approach also has limitations, including a small sample size, respondents' backgrounds, and their access to technology, all of which can affect the survey's completeness and accuracy. We are actively working to make the feedback process more inclusive and informative.

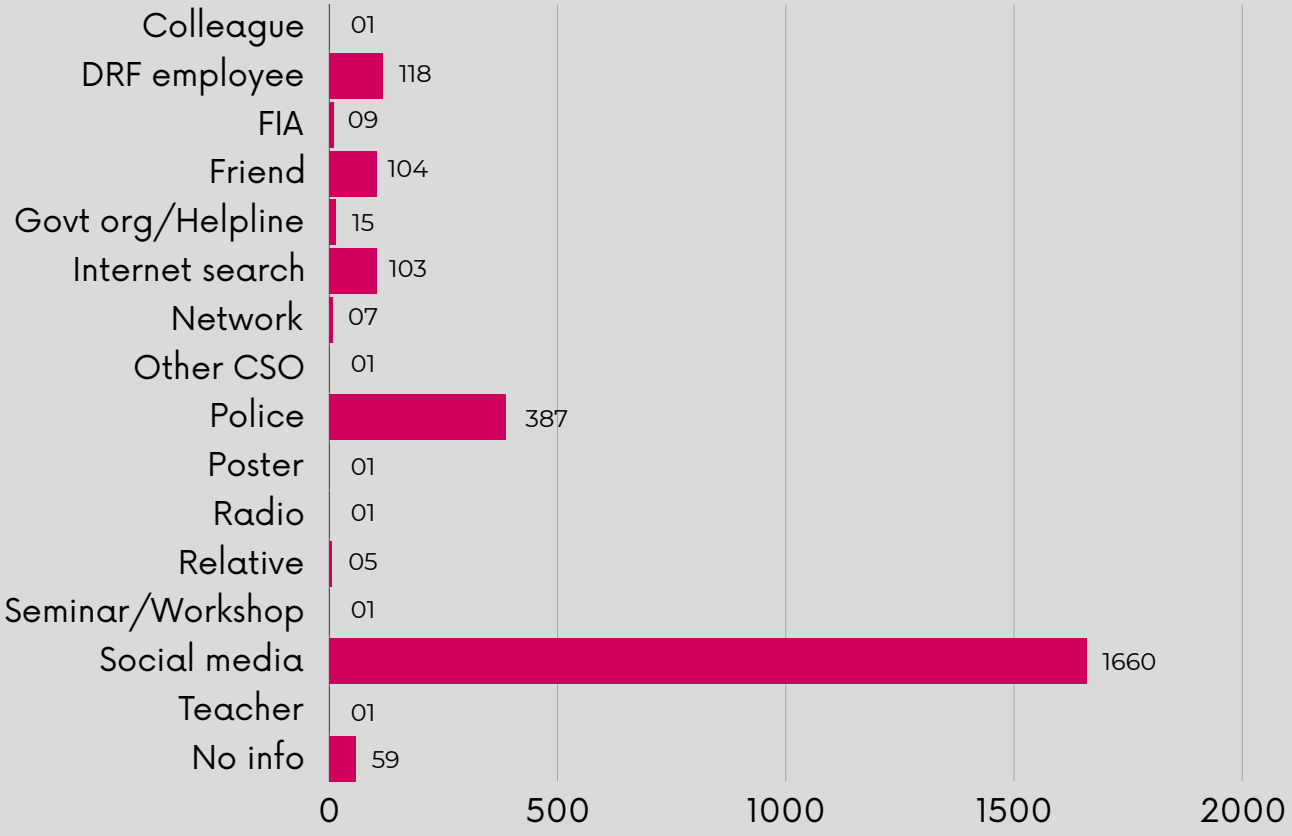


Fig 10.1: *Source of contact*

FEEDBACK QUESTIONNAIRE RESPONSES

01

How soon did you receive an initial response?

A few minutes: 12
A couple of hours: 10
1-2 days: 1
Within a week: 1

02

Do you identify as any of the following?

Activist: 3
Artist and minority business owner: 1
Civil society: 3
Government teacher: 1
Journalist: 6
None of the above: 9
Karkun: 2

03

Did you receive any digital safety advice or help with digital/social media platforms?

Yes: 22
No: 3

04

Did the digital help you received reduce the risk you were facing?

Yes: 22
No: 3

05

Did the digital assistance you received help in building short or long term capacity to protect yourself online?

Yes: 21
No: 4

06

Did you receive any legal guidance or help with how to contact law enforcement?

Yes: 17
No: 8

07

Did you choose to pursue legal action, if necessary?

Yes: 10
No: 13
No answer: 2

08

Did you feel more confident seeking legal help after speaking with the Helpline?

Yes: 25

09

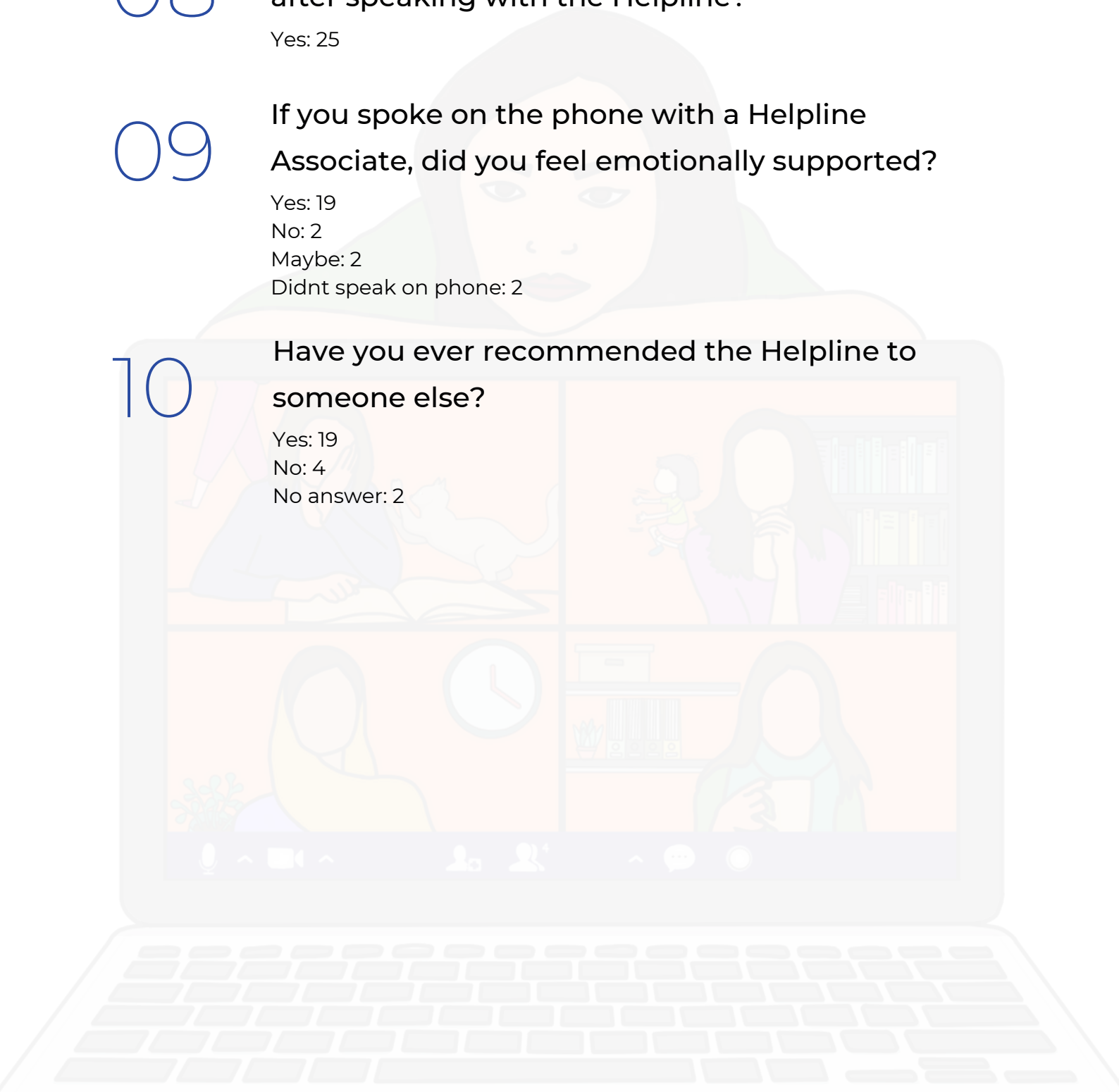
If you spoke on the phone with a Helpline Associate, did you feel emotionally supported?

Yes: 19
No: 2
Maybe: 2
Didnt speak on phone: 2

10

Have you ever recommended the Helpline to someone else?

Yes: 19
No: 4
No answer: 2



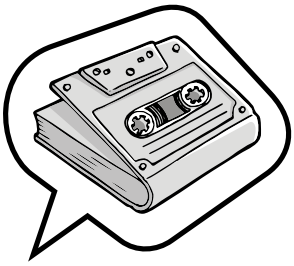
TESTIMONIALS

"I had comforting emotionally supported Quick and secure experience. Really helped me a lot. Great initiative for safe online experience
I will definitely recommend this platform to others"

"Timely response and action helped a lot. On time accurate scenario explanation. Forever grateful"

"I am so happy that the DRF exists. Without you, I would have had my hard work and future financial viability unjustifiably removed. Thank you so much. You are exactly the kind of organization that this world needs. You are all amazing."

"I feel safe talking about my experience."



FIRST RESPONDERS

For this edition of the Helpline's Annual report, we wanted to include the perspective of people who provide direct support to survivors of TFGBV. We interviewed one of our long-time collaborators at the FIA to whom we refer cases to and contact if and when we need advice or updates. With an experience of almost 30 years, he currently serves as an Assistant Sub-Inspector. His responses were received in Urdu and have been translated to English for this report. We also interviewed one of our Helpline Associates separately. This Associate has an experience of 3 years with the Helpline. Both interviewees were asked the same set of questions and their answers are being shared together to serve as a comparison. Their answers have been summarized but some direct quotes have been added that encompass the spirit of their answer.

To begin with, both the FIA representative and the Helpline Associate were in agreement that the highest number of complaints relating to TFGBV come from women.

Sub-Inspector

The cases we are receiving related to women are mostly about sexual harassment, alongside financial fraud cases. The majority of cases reported are indeed from women, with a minority being from men.

Helpline Associate

Most of the calls we receive are from women, and mostly, they are being blackmailed by those who are known to them regarding their private data, and they cannot even tell their families about it

When asked about whether women present any privacy concerns and feel at ease with the thought of traveling to FIA cybercrime wings for pursuing complaints, both seemed to be in agreement; Women have overwhelmingly expressed reluctance to travel, and this acts as one of the most important barriers to access to justice, and are equally concerned about not involving their families.

Sub-Inspector

Approximately 90 percent of women (in contact with the FIA) express concerns about their dignity. For instance, Multan's reporting center is for 14 districts, that's why women living far from FIA center have issues regarding travelling. Maximum women emphasize resolving their complaints discreetly, without involving "Thana, Kachahri" due to the cultural norms in Pakistan...only 10 to 15 percent women proceed with their cases legally.

Helpline Associate

When we receive calls on the helpline, we first ensure their privacy and reassure them that whatever they share with us will not reach their families; their information will remain confidential between us. They become so comfortable with us that they don't find it difficult to share their cases. Most women face the issue that they cannot travel from one city to another because their families do not permit them to go anywhere alone. However, then we have to encourage them that going to the FIA office is essential, and without it, they cannot overcome this difficulty.

They were also asked about vulnerable groups other than women that report cases to them as well.

Sub-Inspector

We receive cases involving minors, particularly those related to child pornography, which fall under a different section, Section 24. Overall, if we have received 100 cases of harassment, out of them two to three cases are of trans-gender and child pornography

Helpline Associate

Along with women, we also receive cases involving transgender individuals and minorities. In these cases, their pictures before and after transition are often posted on social media, leading to inappropriate comments and harassment. The helpline specifically prioritizes such cases and assists in removing their pictures and recovering their accounts. For complainants within the city, we also send our representatives to accompany them to the FIA to avoid any difficulties.

They were also asked about the hurdles when they receive cases, whether institutional or otherwise.

Sub-Inspector

Look, once a person becomes a government servant, they initially encounter hurdles and difficulties. However, over time, they get used to the system and gain a better understanding of their responsibilities. Priority is then given to cases where there is suspicion of causality or potential harm to victims, particularly females. I think the FIA should have offices in every district instead of just at the regional level. This way, victims wouldn't have to travel up to 400 km to reach us. In fact, their issues should be addressed within 50 km of where they are.

Helpline Associate

In Pakistan's current situation, we often face slow internet, technical issues with the phone lines, and backend problems. These challenges sometimes result in us missing calls, which can be frustrating. As helpline associates, we also need breaks to relieve ourselves from the stress of our work. We genuinely want to help in any way possible, and it can be disheartening when we're limited in our ability to assist. Working at the helpline can also affect our mental health. While we aim to support callers and ease their stress, absorbing their emotions can also impact our well-being. Since it's a helpline, we can't keep anyone on duty for extended periods. This often leads to having a limited number of support staff available, which puts extra pressure on us.

Moving from remedies to prevention, they were also asked about what can be done to empower women more, and the need for law enforcement and civil society to work in collaboration.

Sub-Inspector

We've organized awareness programs, delivered lectures at universities, participated in various forums, and spread awareness through social media and TV commercials. These methods have been proven successful in reaching our goals. This is a good effort from you. When individuals visit any channel and recognize that a particular domain belongs to a specific organization, they reach out to us. Numerous NGOs also direct cases to us, which is highly appreciated. It's great what these NGOs are doing.

I remember very clearly, from your reference a lady doctor reached out to me and her harasser was powerful, we obliged that case and now she’s living happily. She is praising us and NGOs and informing others as well from where she gets the relief.

Helpline Associate

It is crucial to reduce cases of increasing harassment against women to inform them about their legal rights and where they can report incidents. It's essential for women in small towns who may not have easy access to mobile phones or the internet. Setting up camps in these areas to provide awareness and education could be beneficial.
I came to know how our cyber harassment helpline helps people, listens to their problems, and advises them on how to get out of difficult situations by taking legal action. I felt the importance of the helpline in people's lives and also in my own life because it gives me inner peace knowing that I have helped so many people today, and afterward, I receive kind words and blessings from them, which give me a lot of comfort. I think there should be such helplines that guide people without asking for money, and if the helpline and FIA work together, we can quickly control this harassment and gradually reduce such crimes over time.

Finally, first responders also bear the brunt of other people's emotional burden and absorb the sadness, anger, and frustration of the people they are helping. We asked the FIA officer and Helpline Associate how they try to maintain a work-life balance and what they do for self-care.

Sub-Inspector

No, it doesn't impact our personal lives because it's part of our job, and that's a culture in Pakistan. When we take on a task, we're committed to completing it, even if it means working long hours even about 22 to 24 hours or days. It's our passion. For example, once we had to conduct a raid on a kidney transplant clinic. We were away from home for 40 days until the raid succeeded, but none of us felt upset about it because it was a unique and important case. Similarly, when people approach us with complaints of sexual harassment or financial fraud and we see their vulnerability, we feel compelled to help them immediately. Time isn't an issue in these situations. The fatigue fades away when we see them receive justice.

Helpline Associate

In the beginning, I used to find it quite difficult because I would become very emotional and wouldn't share with anyone how I was feeling. But then my team taught me how to balance my life and these real cases, and how to overcome my stress. I started discussing with my team or engaging myself in activities to cope with stress. Although it's very difficult, you have to understand yourself and reassure yourself that you have done your best to help and you have done everything in your power. However, over time, you do get used to it, like how doctors get used to hearing about their patients' illnesses repeatedly. But still, somewhere inside you, there is always a feeling. Besides this, we also have sessions on mental health and well-being, which help us in balancing our life and work.

SUSPECTED MENTAL HEALTH ISSUES

In recent times, there has been a rise in delusions and other mental health issues where the symptoms show a relation to technology. In 2023, we received 21 calls regarding such issues, such as fears of being monitored through mobile devices or concerns about someone accessing personal information. These fears arise from the perceived dangers of the internet and its potential consequences. Individuals are increasingly worried about breaches of their privacy and are experiencing delusions related to this. This phenomenon is now referred to as cyber paranoia,[10] which involves individuals having unrealistic fears about threats via information technologies and perceiving themselves to be vulnerable to attack, persecution, or victimization in some way.

It is also important to mention here that Pakistan, despite the excessive data breaches that it has received, still does not have a personal data protection bill to protect users' data. With few reporting avenues and paranoia about the internet keeping excessive information of users, some callers have been distressed about this monitoring without any concrete proof on their end.

POLICY RECOMMENDATIONS

Recommendations for Policy makers

The Pakistani government must take decisive action to eradicate online harassment and technology-facilitated gender-based violence. To achieve this, we recommend several measures.

Public Education
The government should collaborate with gender-based organizations to conduct gender sensitization workshops in schools and communities. These workshops should focus on digital literacy, raising awareness about online harassment and its impact, and promoting positive attitudes towards women's use of technology. Additionally, the government's public awareness campaigns and official curriculum should be updated to be more gender sensitized following consultations with these organizations. This will help ensure a comprehensive approach to addressing gender-based violence online.

Digital Literacy and Safety Integrated into Curriculum
Internet education and safety courses should be included in school curriculums. These courses should cover topics such as consent, social media ethics, safety practices, and what is illegal online. By including these topics in the curriculum, the government can empower the younger generation to be more confident and aware while exploring the internet. Furthermore, these courses should be regularly updated to reflect emerging trends and technologies.

Addressing the Digital Gender Divide
Pakistan has one of the widest digital gender gaps globally. According to the GSMA "Mobile Gender Gap Report 2023," women in Pakistan are 35% less likely than men to own a mobile phone due to economic inequality and patriarchal attitudes. Women report that family disapproval is the second most significant barrier to mobile internet usage, while only a negligible percentage of men report this as a hindrance. Policies must be introduced to eliminate the gender digital gap by removing financial, safety, and social barriers that women face when accessing digital devices and internet spaces. This includes improving literacy rates and making the internet more accessible in geographical areas that lack infrastructure. Additionally, the government should work with mobile network operators to offer affordable and accessible mobile internet packages targeted at women.

Gender Sensitization for Law Enforcers

The government must collaborate with gender-based organizations to conduct regular gender sensitization workshops with law enforcement, including police and the FIA. Staff handling complaints of online gender-based violence must overcome patriarchal attitudes and be trained to handle cases sensitively. These workshops should cover expansive issues relating to gender, including the risks and challenges faced by the transgender community. Civil society organizations, such as DRF, have conducted such workshops with the cybercrime wing of the FIA in the past, and are keen to work with law enforcement agencies in the future. Additionally, the government should establish mechanisms for regular monitoring and evaluation of law enforcement agencies' gender sensitization efforts to ensure their effectiveness.

Data Protection

The government must enact human rights-compliant legislation on digital privacy and protection after meaningful consultations with civil society and the general public. The right to dignity and privacy, as guaranteed under Article 14 of the Constitution of Pakistan, must be protected for every citizen. DRF's comments[11] to the Ministry of Information Technology and Telecommunications (MOITT) on the Personal Data Protection Bill 2021 should be taken into account when drafting the law. This legislation should establish clear guidelines for the collection, use, and sharing of personal data, as well as mechanisms for redress in case of data breaches or misuse. Additionally, the government should work with international partners to develop and implement standards for data protection that align with global best practices.

Supporting Civil Society Work

Policy makers must take measures to ensure the smooth functioning of civil society organizations and nonprofits working on digital rights and gender. This includes providing financial support, capacity building, and creating an enabling environment for their work. Additionally, the government should work with civil society organizations to develop and implement programs that promote digital rights and gender equality.

POLICY RECOMMENDATIONS

Recommendations for Law Enforcement

The following recommendations are provided for law enforcement agencies to enhance their capacity to address TFGBV cases in Pakistan.

Increase resource allocation

The FIA must receive more funding to meet the growing demand for its services, considering the rising incidence of TFGBV and increased awareness of cybercrime reporting mechanisms in the country. Additional resources must be allocated to hire and train more female officers, as well as to establish and expand forensic labs across the country. Furthermore, the government should work with international partners to provide technical assistance and capacity building to law enforcement agencies to improve their ability to investigate cyber harassment cases.

Establish a mechanism to handle cases in foreign jurisdictions

Despite being authorized to do so under Section 1(4) of the Prevention of Electronic Crimes Act (PECA), the cybercrime wing lacks the capacity to take action against individuals located outside Pakistan. DRF recommends that the MOITT and the Interior Ministry define "international cooperation" under Section 42 of PECA and appoint at least one officer in each branch with specialized training in international law and conflict of laws to handle cases involving foreign jurisdictions. Additionally, the government should work with international partners to develop and implement protocols for cross-border cooperation in cybercrime investigations.

Enhance the functionality of the online complaint portal

To facilitate complainants who cannot travel long distances to seek justice, the online complaint portal should be updated and enable identity verification to initiate an inquiry to better serve individuals, particularly women and young girls. The portal should also provide information on available support services and legal options for victims of cyber harassment. Additionally, the portal should be regularly monitored and evaluated to ensure its effectiveness and accessibility.

Develop protocols and coordination with police
In accordance with the recent amendments to PECA that allow local police stations in cities where there is no cybercrime wing of the FIA to receive relevant cases, the FIA should develop protocols that allow the police to acknowledge cases with empathy and in a sensitized manner. The protocols should also cover the coordination system between the police and the FIA, and designate a focal person within the police department who will receive cybercrime cases and work alongside the FIA for better management.

Collect gender-disaggregated data
The FIA must report the number of online harassment cases and cases registered by women and gender minorities under each section of PECA, particularly Sections 20, 21, and 24. These figures should be publicly available to aid policy-making, research, and resource allocation. Additionally, the government should work with civil society organizations and international partners to develop standardized data collection tools and methodologies for collecting gender-disaggregated data on cyber harassment.

Establish a dedicated desk for cyber harassment within the NR3C
Given the unique nature of cyber harassment cases and the gender sensitivity required for complainants/victims, a separate desk for cyber harassment should be set up within the cybercrime wing. This desk should be staffed by officers with specialized training in the nuances of online harassment, gender sensitivity, and counseling services. The desk should also work closely with civil society organizations and other stakeholders to ensure that victims receive the support they need.

Coordination with Other Departments
Channels of communication between police stations and cybercrime stations should be established to ensure that cases can be easily transferred and there is clarity as to where a particular case should be registered, investigated, and prosecuted. Given the intersecting nature of online and offline spaces, cases often involve both online and offline crimes, and complainants are given contradictory advice regarding the jurisdiction of the police and cybercrime wing. In certain trials, given that challans contain both sections of PECA and PPC, there is often back and forth between different courts and judges. It should also be ensured that each department knows what laws exist, which complaints need to be handled by which agency/department, so that complainants are not sent around when they are already in distress. Additionally, the government should establish a central coordination mechanism for cybercrime cases to ensure that information is shared efficiently and cases are handled promptly.

Coordination with Other Departments

Channels of communication between police stations and cybercrime stations should be established to ensure that cases can be easily transferred and there is clarity as to where a particular case should be registered, investigated, and prosecuted. Given the intersecting nature of online and offline spaces, cases often involve both online and offline crimes, and complainants are given contradictory advice regarding the jurisdiction of the police and cybercrime wing. In certain trials, given that challans contain both sections of PECA and PPC, there is often back and forth between different courts and judges. It should also be ensured that each department knows what laws exist, which complaints need to be handled by which agency/department, so that complainants are not sent around when they are already in distress. Additionally, the government should establish a central coordination mechanism for cybercrime cases to ensure that information is shared efficiently and cases are handled promptly.

Privacy and Confidentiality

It is observed that many complainants require the assurance of confidentiality to report an incident. Rule 9 of the PECA Rules outlines protections and requirements for confidentiality in cases involving women and intimate images. To ensure that the details of cases, personal information, and evidence are only accessible by authorized personnel, it is recommended that the case management system be reworked under strict SOPs. It is preferable to have a digital system that restricts access to authorized personnel only and has protocols in place for digital security and integrity of data. Additionally, the government should provide training to law enforcement officers on the importance of privacy and confidentiality in handling cyber harassment cases.

Greater Accessibility for Disabled Persons

To ensure that disabled persons do not face additional hurdles in registering and pursuing complaints, every cybercrime office must meet minimum requirements such as functioning elevators, ramps for wheelchairs, accessible toilet facilities, and in-person assistance in filing applications. Additionally, the government should work with disability rights organizations to develop guidelines and best practices for ensuring the accessibility of cybercrime offices and services for disabled persons.

Improve coordination between cybercrime wing branches
Measures should be taken to ensure that investigations can be carried out swiftly, even when complainants and accused individuals are in different cities. The FIA should evaluate all branches to ensure that they are following the same protocols. This would decrease the pressure on resources for travel, which serves as a significant hurdle in carrying out investigations at the moment, and would ensure faster action on holding perpetrators accountable. Additionally, the government should establish a central database for cybercrime cases to facilitate information sharing and coordination between branches.

Psychological services
The FIA should increase and improve the quality of psychological services at cybercrime offices to help complainants deal with the psychological trauma and distress that they experience due to online harassment and violence. All officers, especially those dealing directly with victims, should be trained on how to address trauma and when to refer to more experienced professionals. The cybercrime wing should offer a safe space for victims to help them process their trauma in a constructive and safe manner. Additionally, the government should work with mental health professionals and organizations to develop guidelines for providing psychological support to victims of cyber harassment.

Case management and tracking system
To improve the transparency and accessibility of the system, complainants should be able to track and receive regular updates on the status of their case through an accessible and easy-to-use case management system/portal. Digital copies of the case file and evidence filed should also be stored on a secure server to ensure reliable duplicates in case the original case file is lost or tampered with. Additionally, the government should establish a central case management system for cyber harassment cases to ensure that information is shared efficiently and cases are handled promptly.

Enhanced Technical Expertise

The Federal Investigation Agency (FIA) is facing a significant investigative delay, and some cybercrime complaints are being dropped due to the insufficient technical abilities of officers and inadequate technology available to the agency. In this regard, the Digital Rights Foundation (DRF) has recommended that the agency should be capacitated to address the current and future trends in cybercrime and forensic science, and evidence collection in the next five-year period. This capacity-building process should be continuous and ongoing. Consequently, DRF recommends substantial investment in research at the National Response Centre for Cyber Crimes (NR3C) to cater to the needs of the litigants and complainants. Additionally, the government should work with international partners to provide technical assistance and training to law enforcement agencies to improve their technical abilities in investigating cyber harassment cases.

Training for Judges on Cybercrime Law, Internet Governance, and Online Harassment

To ensure that judges are familiar with internet law and technology, the provincial judicial academies' curriculum should include internet governance and cybercrime. The lack of knowledge regarding the internet's governance and infrastructure results in bad jurisprudence and "unimplementable" orders. Additionally, the government should organize regular training workshops and seminars for judges on cybercrime law, internet governance, and online harassment to improve their understanding of these issues and their ability to adjudicate cases related to cyber harassment effectively.

REFERENCES

[1] Pakistan Telecommunication Authority. 2024. “Telecom Indicators.” Pakistan Telecommunication Authority. https://www.pta.gov.pk/en/telecom-indicators.

[2] Digital Rights Foudnation. 2024. “NWJDR condemns the use of technology-facilitated gender-based violence (TFGBV) and Generative AI to attack and silence women journalists.” Digital Rights Foundation. https://digitalrightsfoundation.pk/nwjdr-condemns-the-use-of-technology-facilitated-gender-based-violence-tfgbv-and-generative-ai-to-attack-and-silence-women-journalists/.

[3] Jeffrie, Nadia. 2023. “The Mobile Gender Gap Report 2023.” GSMA. https://www.gsma.com/r/wp-content/uploads/2023/07/The-Mobile-Gender-Gap-Report-2023.pdf.

[4] Digital Rights Foundation. 2019. “Fostering Open Spaces in Pakistan.” https://digitalrightsfoundation.pk/wp-content/uploads/2019/04/IMS-Study-Report.pdf.

[5] Digital Rights Foundation. 2017. “Measuring Pakistani Women's Experiences of Online Violence.” https://digitalrightsfoundation.pk/wp-content/uploads/2017/05/Hamara-Internet-Online-Harassment-Report.pdf.

[6] Qarar, Shakeel, and Muzhira Amin. 2023. “9 suspects rounded up after FIA launches probe against predatory loan apps.” Dawn.com. https://www.dawn.com/news/1764692

[7] Azeem, Munawer. 2018. “FIA allowed to open 15 centres to check cybercrime.” Dawn.com. https://www.dawn.com/news/1436438.

[8] Georgetown Institute for Women, Peace and Security. 2023. “Country Profile Pakistan.” Georgetown Institute for Women, Peace and Security. https://giwps.georgetown.edu/country/pakistan/.

[9] Jeffrie, Nadia. 2023. “The Mobile Gender Gap Report 2023.” GSMA. https://www.gsma.com/r/wp-content/uploads/2023/07/The-Mobile-Gender-Gap-Report-2023.pdf.

[10] Mason, Oliver, Caroline Stevenson, and Fleur Freedman. 2014. “Ever-present threats from information technology: the Cyber-Paranoia and Fear Scale.” National Library of Medicine. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4241818/.

[11] Digital Rights Foundation. 2023. “Analysis: Personal Data Protection Bill 2023.” Digital Rights Foundation. https://digitalrightsfoundation.pk/wp-content/uploads/2023/07/Legal-Analysis-Statement-on-PDPB-July-2023.pdf.

DigitalRightsFoundation

"KNOW YOUR RIGHTS"


@digitalrightsfoundation


@digitalrightsfoundation


@DigitalRightsFoundation


@digitalrightsfoundation


@DigitalRightsPK


@DigitalRightsPK