DigitalRightsFoundation
"KNOW YOUR RIGHTS"

CYBER HARASSMENT HELPLINE REPORT

Annual Report (January, 2020 – December, 2020)

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

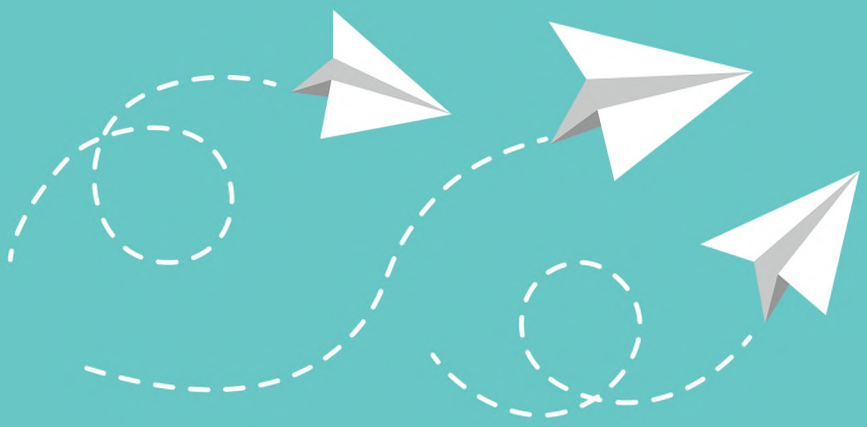
Gender-sensitive, confidential & free helpline
0800-39393

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, Facebook and emails five days a week from 9am to 5pm.

The report has been researched and authored by: Jannat Fazal
Reviewed and edited by: Shmyla Khan
Design and layout: Ahsan

TABLE OF CONTENTS



THE HELPLINE: THE ROAD SO FAR

In 2016, DRF team travelled to different colleges and universities in Pakistan to create awareness about digital safety and online harassment under our project, 'Hamara Internet'. The sessions led to women reaching out to us through word of mouth, and soon our inbox was swarmed with cases of women looking for advice and assistance for cases of online harassment. As there was no dedicated service delivery channel, the small team at DRF found itself unable to answer all the queries effectively, some cases started to slip through the cracks. This surge of cases laid the foundation for us to set up a helpline for online harassment complaints.

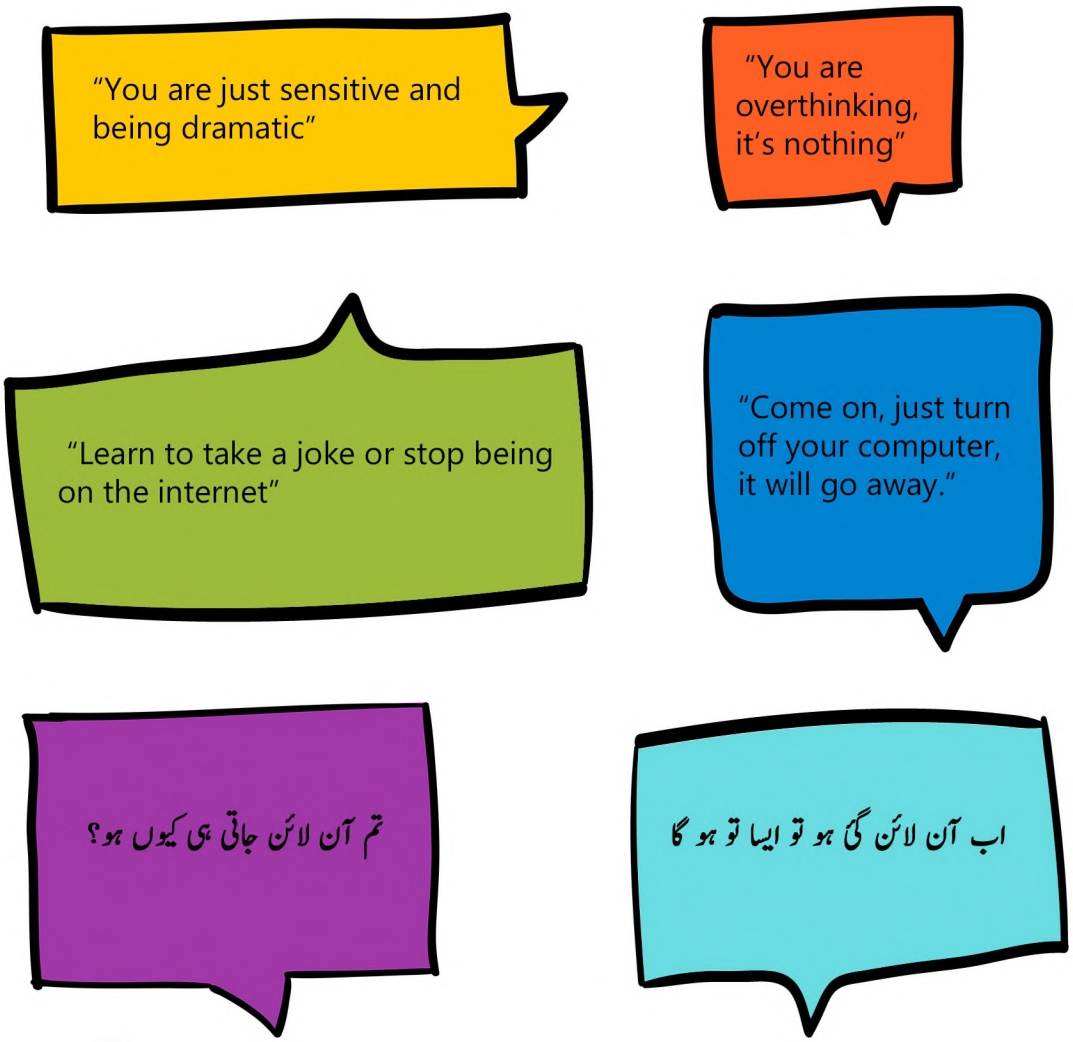
The need for a helpline was also precipitated by the brutal murder of Qandeel Baloch in 2016. This was not a one-off incident as it led to widespread online harassment and abuse against feminists speaking up online. Women were bullied and attacked in online spaces for their stances. This was part of a global phenomenon: gender-based online violence was emerging as a systematic trend all over the world, and Pakistan was no exception.

The stars aligned when Nighat Dad, the Executive Director of DRF, was nominated for the Dutch Human Rights Award in 2016. Seizing the moment, we launched an online campaign to mobilize votes with the aim of starting the region's first helpline for online harassment cases from the proceeds of the award. There was immense public support for Dad's nomination. Finally, in December 2016, as Dad received the Dutch Tulip Award in the Netherlands, the Cyber Harassment Helpline received its first call in Lahore.

Since 2016, our two-person team has grown in proportion with the needs of our callers. What had originally started with the aim of providing digital security support to victims of online harassment soon branched out into providing psychological counseling through a full-time counselor as well as legal assistance for callers through our dedicated legal officer.

Today, our helpline staff attends to an average of 212 calls per month. From cases of fake accounts and non-consensual use of personal data to financial scams, we strive to meet the needs of our callers on a daily basis during office hours (9am to 5pm) Monday to Friday.

INTRODUCTION TO ONLINE HARASSMENT



Have you ever heard any of the above statements when you or someone else spoke about their experience of online harassment? So have we.

This attitude is rooted in society's trivialization of online harassment and threats originating from digital spaces. The absence of or the lack of attention given to online harassment in mainstream discourse also contributes to this attitude of trivialization.

We at the DRF understand online harassment to be a form of violence. Our understanding emanates from the United Nations' comprehensive definition of harassment, which describes it as "any improper and unwelcome conduct that might reasonably be expected or be perceived to cause offence or humiliation to another person[1]". It further says that harassment can take place in the form of words, gestures or actions which tend to annoy, alarm, abuse, demean, intimidate, belittle, humiliate or embarrass another person or which create an intimidating, hostile or offensive work environment. Harassment can manifest in different forms: sexual harassment, workplace harassment, harassment in public spaces, and cyber-harassment.

Cyber-harassment is a term used to describe the use of cyberspace and digital technologies to harass, control, manipulate or belittle a target.

Even though online harassment is often not taken seriously as a form of violence, it has been DRF's mission to mainstream discourse around online harassment and the importance of online spaces. We think that harassment in online spaces is as real as harassment in physical spaces. We do not perceive online harassment as something confined to some unreal, virtual world from which you can opt out of. Online violence is deeply linked to and intertwined with larger structures of online gender-based violence and structural oppressions.

Understanding online harassment is important given the gravity of the situation. With the proliferation of the internet and digital technologies, there has been a gap between the lived experiences of women who are targeted in online spaces and the institutional attention being accorded to it. Extensive research has shown that online harassment can have serious and long-term repercussions on mental health. DRF's own research[2] illustrates how online harassment can take a toll on one's psychological wellbeing that can manifest in symptoms of depression, chronic stress, generalized anxiety, mistrust, withdrawal and insecurity. In the Pakistani context, the gravity of these cases is such that harassment and blackmailing have even led to cases of suicide.[3]

Meanwhile, despite the fact that cyber-harassment affects everyone including women, children, and men, it is a gendered phenomenon. This means that marginalized gendered groups are more vulnerable to it.

Furthermore, there also appears to be a link between physical violence and online violence. Those sections of the population that are more vulnerable to physical violence are also more likely to be targeted in acts of online violence, such as women, transgender individuals and children.

Physical violence is part of the lived experiences of women and gender minorities in Pakistan, and online spaces are no exception.[4] While women are frequently targeted in honor killings and social sanctions in the physical world, this violence seeps into the online sphere as well when threats of the said violence are enabled through digital devices. Harassment is gradually being normalized as an everyday experience for women using online spaces for social interaction. As many as **34%** of women who were surveyed in our Hamara Internet project reported they had experienced online harassment and abuse. Furthermore, a large percentage of women (55% of survey respondents) had witnessed other women being bullied and harassed by men online.[5] These experiences translated into almost **70%** stating that they were afraid of posting pictures online out of fear that they might be misused.

INTRODUCTION TO THE CYBER HARASSMENT HELPLINE

The helpline seeks to address the gaps in the legal system by providing a gender-sensitive, confidential and safe space to those facing online harassment. The helpline support staff has developed comprehensive policies around privacy, caller confidentiality and high-quality service.[6]

DRF's Cyber Harassment helpline is the region's first dedicated helpline that offers digital, legal, and mental health support to victims of online harassment and violence. The support team includes a qualified psychologist, digital security expert, and a lawyer, all of whom provide specialized assistance as and when needed. The helpline strives to help women, children, human rights defenders, minority communities and anyone who has been made to feel unsafe in digital spaces. Furthermore, we have developed a network of lawyers and practitioners who provide legal services and advice on a pro bono basis to complainants who cannot afford a lawyer. The network draws members from across Pakistan and can be accessed on our website called Ab Aur Nahin: **https://abaurnahin.pk/.**

The helpline officially began taking calls on December 1, 2016. It is operational five days a week from Monday to Friday between **9 AM to 5 PM** through our toll-free number. The helpline team can also be contacted outside of office timings via email at **helpdesk@digitalrightsfoundation.pk** and social media platforms (Facebook, Instagram, and Twitter).

This document is part of a series of annual reports by the cyber harassment helpline to ensure transparency of its operations, share its experiences and address the dearth of data around online harassment in Pakistan. The report seeks to document the data collected by the helpline and provide analysis of trends regarding online harassment as well as policy recommendations to make online spaces safer for all.

UNDERSTANDING CYBER HARASSMENT IN PAKISTAN THROUGH NUMBERS:

The main medium through which the DRF support team receives complaints regarding online harassment is its toll-free number, 0800-39393. However, we can also be reached on other platforms such as Facebook, Twitter and email. We try to promptly assist complainants and inquirers on any given means of communication. Nevertheless, the helpline's toll-free number remains the primary and most preferred mode of communication for complainants.

EXECUTIVE SUMMARY OF FOUR YEARS OF CYBER HARASSMENT HELPLINE

The figures outlined in this summary pertain to the four years of Cyber Harassment Helpline starting from December 1, 2016 until December 31, 2020.

Total number of complaints managed by the helpline in four years **7790**

Percentage of cases from women **(55%) 4214**

Percentage of cases from men **(32%) 2516**

Percentage of cases by gender and religious minorities **.01%**

Number of cases (received at the helpline) from cities without cybercrime office **(16%) 1232** cases.

Platforms regarding which most complaints were received **Facebook** and **WhatsApp**.

55%
WOMEN

32%
MEN

CYBER HARASSMENT DURING COVID-19 LOCKDOWN (MARCH – AUGUST)

When the government imposed lockdown to combat COVID-19 outbreak, many women were forced to stay in isolation at home with their abusers. The situation was made worse as services to support survivors had been disrupted or made inaccessible.[7] To address this issue, Cyber Harassment Helpline expanded its capacity and began operating 24/7 during lockdown (May- September) to provide timely relief and guidance to the recipients of online abuse. A continuous rise in cyber-harassment complaints, from 98 cases in January (before the lockdown) to 697 cases in July, has been observed since the COVID-19 pandemic outbreak in Pakistan. This pandemic has not only deepened economic and social stresses, restricted movement and increased social isolation, it has also contributed to an exponential rise in gender-based violence, which the United Nations has termed as the "shadow pandemic".[8]

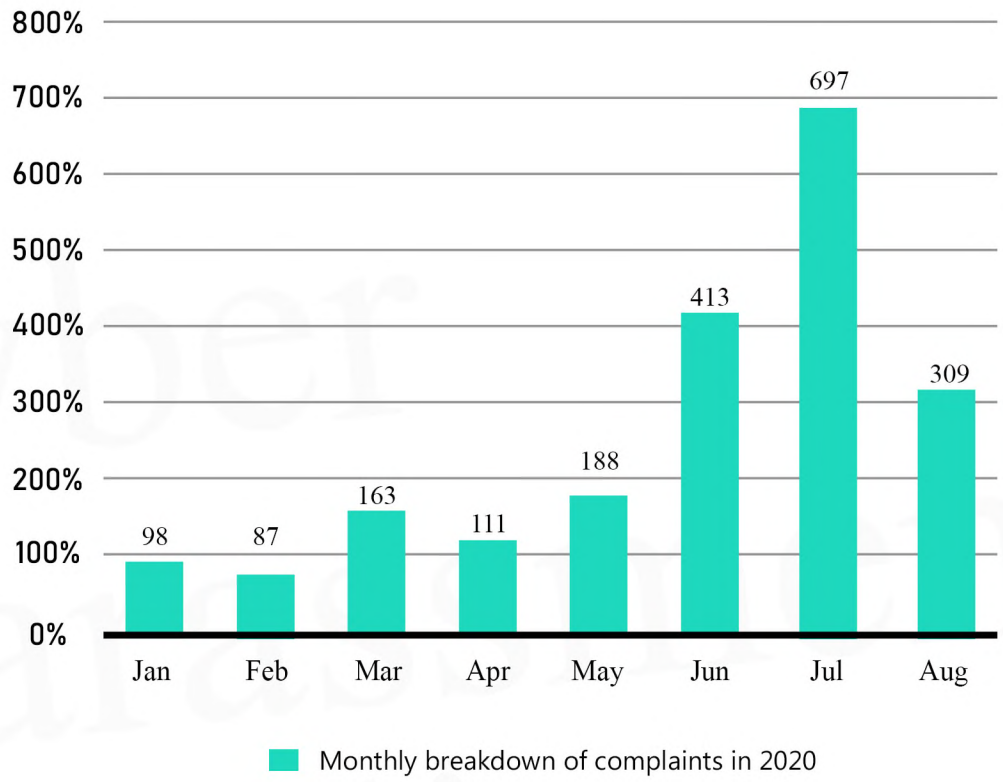


Table 2: Monthly Breakdown of Complaints during COVID-19 Pandemic from the Helpline. (Source: DRF Cyber Harassment Helpline data)

While the highest number of cases were received from Punjab, a great number of cases were from cities that had no Federal Investigation Agency (FIA) cybercrime wing offices. Given that physical presence is required to register a complaint, mobility issues meant that complainants from cities without FIA offices were unable to register their cases, highlighting the need for FIA to expand their operations into other cities and to have an online statement recording and identity verification process to register a case.

MENTAL HEALTH SERVICE DURING COVID 19 LOCKDOWN (MARCH- AUGUST)

The outbreak of the COVID-19 pandemic resulted in unprecedented levels of isolation and hardship, which led to the worsening of the overall mental health situation for many.[9] In order to respond to the specific challenges caused by the emergency situation DRF expanded its helpline's operations to 24/7 and extended the helpline's psychological services to vulnerable communities experiencing distress (women, children, religious and gender minorities). DRF also rolled out social media awareness campaigns on cyber harassment and mental health with the intent to sensitize masses on these issues.

During the months of lockdown, cyber harassment helpline provided mental health services to over 45 clients with **122 psychological counselling sessions,** which included young girls, minors and women.

CYBER HARASSMENT HELPLINE REVIEW 2020

Total Number of complaints in 2020

Following is the breakdown of complaints we received at the cyber harassment helpline from January 2020 to December 2020. In the early stages of the pandemic, calls were not taken because there was no way to access office during lockdown so the correspondence on Facebook or the phone were moved to email communication so that a smoother track of communication could be aligned.

Total complaints	Calls	Emails and social media queries
3298	2551	747

The following analysis is based on the total complaints received at the cyber harassment helpline.

The helpline only collects information that is not personally identifiable. Thus, phone numbers, names and other uniquely identifiable information are not collected. The process of data collection is guided by the Helpline's Privacy Policy that is publicly available on DRF's website and can be provided upon request. The collected information is also digitally secured, and precautions (data backup, password protection, restricted access, archiving and deletion) are taken to ensure data security.

However, in events where it has been assessed during a sensitive conversation that the call might drop, we store callers phone number so we can get back in touch with them if required. The numbers are not collected in permanent records.

AVERAGE NUMBER OF COMPLAINTS IN 2020

In the year 2020, the helpline has had a monthly average of 278 complaints including 212 calls on the toll-free helpline number. As can be observed from the monthly breakdown provided below, the average number of complaints has steadily increased over the years. This rise in online harassment is due to a complex set of factors, one reason is that as more and more people use online channels, they are bound to become susceptible to cybercrime and online harassment through such spaces. ICTs allow for anonymous communications, unprecedented access to private information, which is ripe for exploitation by criminals.[10]

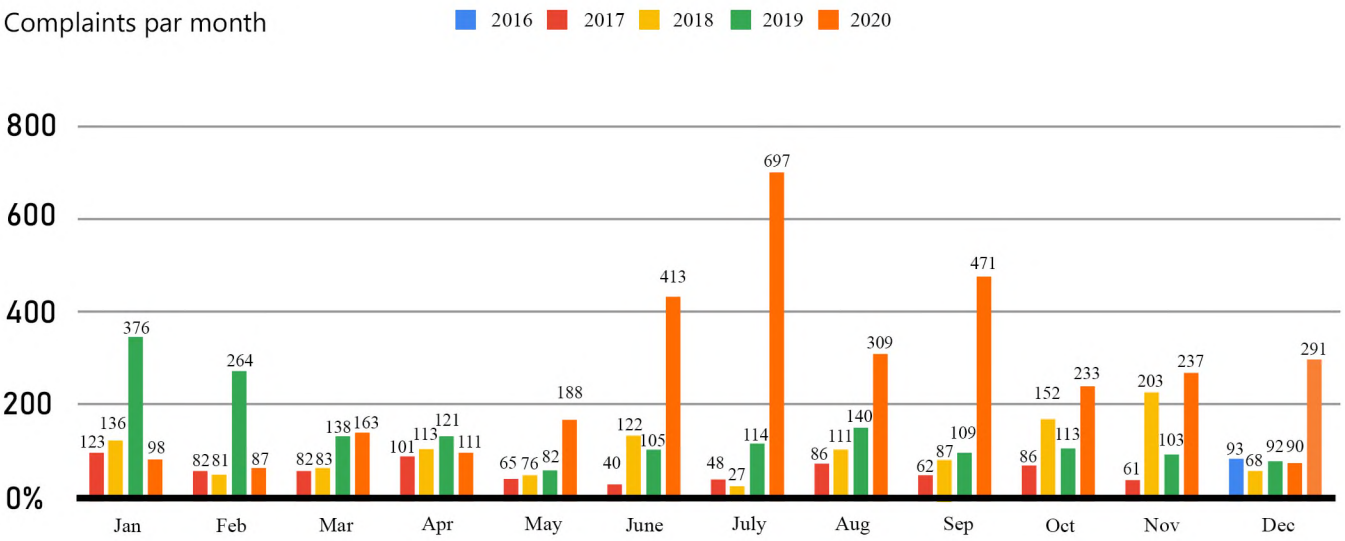


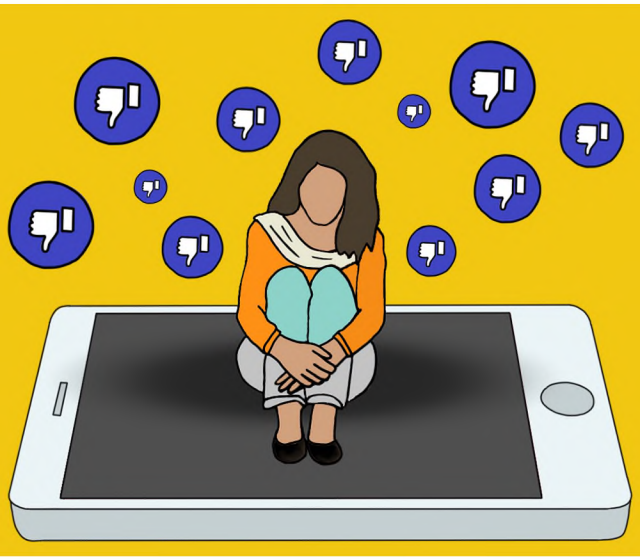
Figure 4: This data is based on the total number of complaints (3298)

278 **Average Number of Complaints** (Calls,Emails,Social Media) **Each Month in 2020**

212 **Average Number of Calls Each Month in 2020**

PERSPECTIVES AND IMPACT OF ONLINE VIOLENCE

Research suggests that online abuse directed at women reveals three important and related gaps. First, there is a lack of gendered analysis of this phenomenon. Second, the focus on online abuse as a form of communication overlooks commonalities with other forms of violence against women and girls. Third, the experience and impact of online violence on recipients is absent. Through our Cyber Harassment Helpline report we are trying to fill this gap.



Data collected from our earlier reports has shown that online harassment affected women more than men. The breakdown of this year's data also reveals that the most number of complaints received were by women (66%). Meanwhile, 33% of the helpline's cases were reported by men, >1% by gender non-binary people. Despite men having easier access to technology and the internet, which increases their numbers in online spaces, women experience more hate and vitriol online. This is particularly true in the context of Pakistan where one of the most common forms of harassment against women is use of their photos and information without consent. Women are blackmailed and threatened on the basis of their data, this is fundamentally used as a tactic to control, intimidate, shame, harm, extort and silence women.

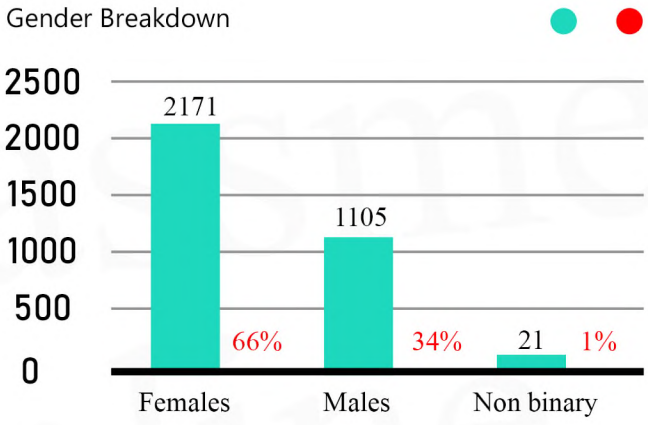


Figure 5: This data is based on the total number of complaints (3298)

Norwegian research illustrates that even though women and men are equally exposed to harassment directed toward group characteristics, targeted women are more likely than targeted men[11] to become more cautious in expressing their opinions publicly. This shows that even though the amount of harassment levelled at men can be more due to their greater presence on the internet, practical implications for women are far more severe as they are the ones more likely to censor themselves.

As per Duggan,[12] sexual harassment is more common in the case of women than men and the problem is exacerbated in the case of young women. Women are more than twice as likely as men to report experiencing sexual harassment online, 21% for women to men's 9%, among adults aged between 18 and 29. When the age bracket of 18-24 is analyzed, American women were found to be three times as likely to be sexually harassed online (20%) than men (6%).

There exists a nexus between online and offline spaces, while originating in virtual spaces, online harassment can result in physical violence. Research suggests that cyberbullying can often be motivated by sexual jealousy and problems in the offline context (Surat)[13] substantiated by another research suggesting linkages between digitally mediated and offline violence, including gender based and sexual violence (Ojanen et al.).[14] Cases of domestic, physical, and sexual violence overlapping with online violence received at the Cyber Harassment Helpline are reflective of these studies. In year 2020, the helpline received 45 such cases where online violence lead to domestic and physical violence, online and offline surveillance, and sexual harassment.

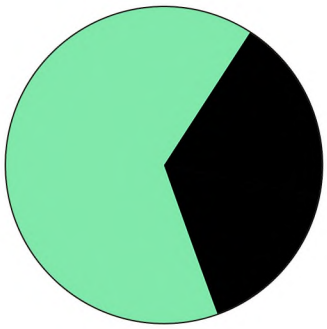
There are several cases of women in Pakistan being killed for their online presence or simply owning a phone. In 2016, a 16-year old girl was killed by her brother for using a mobile phone.[15] Also in 2016, a group of men shot a mother and two daughters in Gilgit-Baltistan for sharing a video of them playing in the rain.[16] A mother of two was stoned to death in 2013 after a tribal court in DG Khan convicted her of possessing a mobile phone.[17] In 2012, a video of a private gathering was leaked showing four women dancing in the presence of three men, all of whom were killed by their families in the name of honor.[18] Victims and survivors are often punished in other ways as well; in one case reported in the media, a woman was expelled from her home in 2017 by her husband as a result of a fake Facebook profile.[19]

Online harassment can have serious and long term repercussions on the lives of those experiencing it. DRF's research "Online Harassment: a Retrospective Review of Records" has demonstrated that online harassment can take a psychological toll that may manifest itself in the form of depression, anger, helplessness, chronic stress, generalized anxiety, mistrust, withdrawal, and insecurity.[20] Another study confirms that the impact of online violence can manifest physically or can lead to mental health consequences like symptoms of post-traumatic stress disorder.[21] Another research study posits that the victims of cyberbullying are 2.57 times more likely to attempt suicide,[22] increasing the overall rate of suicide worldwide.[23]

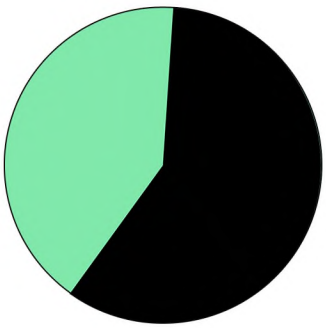
While online violence can result in physical violence from family members and society at large, there are also cases in which mental health and societal pressures have resulted in suicides. In 2017, a female student in Sindh died of suicide after experiencing online blackmailing and harassment.[24] In 2020, a girl died of suicide after experiencing continuous threats and blackmailing to withdraw her cyber harassment complaint that she had filed with the law enforcement. [25]

Gender Breakdown of the helpline's cases for the year 2020:

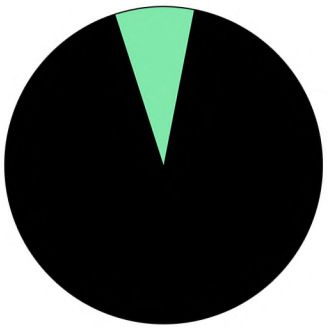
Women: 66%



Men: 34%



Marginalized communities: 1%



It is important to note that these numbers pertain to the cases received at DRF's cyber harassment helpline alone. They are certainly not a reflection of the total number of cases of online harassment in Pakistan or the ones that are reported to legal authorities in Pakistan.

INVISIBILITY OF MARGINALIZED COMMUNITIES

Our helpline has received a very low number of complaints from marginalized communities. This reflects a huge gap between instances of harassment in online spaces (that are publicly accessible on mediums such as Facebook, Instagram, TikTok and Twitter) and the number of complaints made about them. There are tremendous societal barriers in reporting cases for marginalized communities. The figures of the helpline do not reflect the extent of harassment the marginalised communities face in Pakistani online spaces as discriminatory abuse is rampant online as well as in offline spaces.

TYPES OF CASES

To analyze the general trends of online harassment in Pakistan in greater detail, we have categorized the cases according to predetermined typologies that can be found in the appendix.

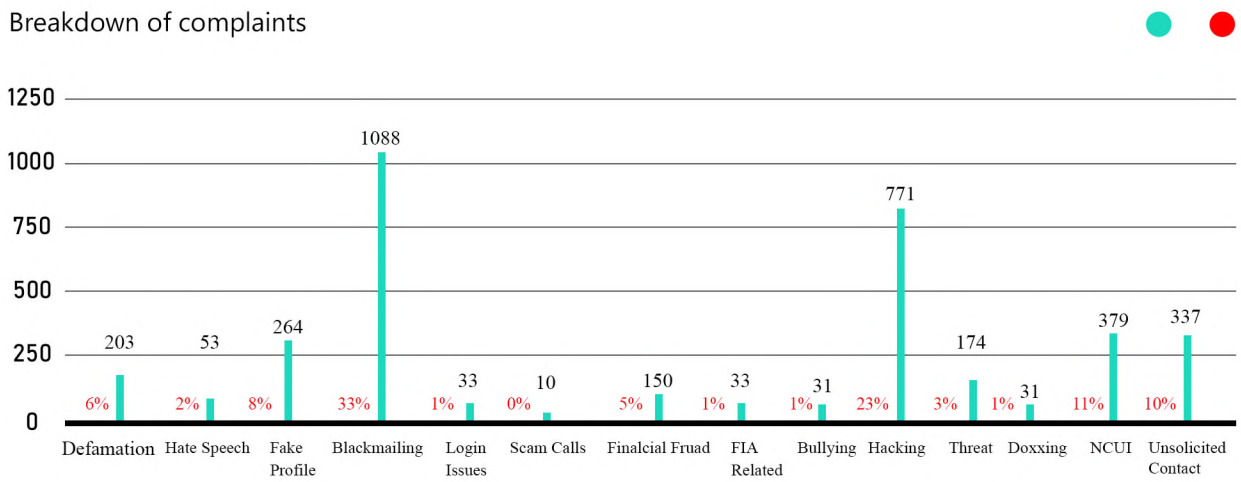


Figure 6: This data is based on the total number of complaints (3298). It must be noted that some callers reported more than one type of complaint. This data shows the types of cases reported to the helpline.

As the chart above shows, majority of the cases are related to **blackmailing,** which often entails the use of an individual's personal information, their photos, or psychological manipulation to make threats and demands, this is linked to **non-consensual usage of information (NCUI)** which involves using, sharing, disseminating and manipulating data such as photographs, phone numbers, contact details and other personal information on social media platforms or other websites such as classifieds or networking sites without the consent of the individual, which violates their right to privacy. Majority callers complain of being blackmailed on the basis of their information or data that the abusers have and use it as an intimidation tactic.

Other most common reported cases involve hacking/ social engineering and unsolicited contact.

Notably, in the past one year the helpline has experienced an influx of calls relating to mobile-based scams that prey on the trust of individuals. One of the most common types involves deception to gain WhatsApp codes of mobile users, which in turn leads to the hacking of their WhatsApp account. The scammers claim to be from well-known organizations, ranging from television game shows, Pakistan Army, government departments such as the Benazir Welfare Program and telecommunication companies.

GEOGRAPHICAL DISTRIBUTION

To understand the geographical patterns of harassment cases across the country and the outreach of the helpline itself, we maintain a database of demographics that includes information on the region where a complainant called from.

Keeping in line with the data privacy policy of the helpline, callers are neither required to provide their complete address nor does the helpline staff maintain a record of it.

We do, however, maintain a breakdown of how many cases were reported from the different provinces or regions of Pakistan. The breakdown can be seen in the table below.

A majority of the cases received by the helpline were from **Punjab (57%),** which is the most populous province in Pakistan. The second-highest number of cases were received from **Sindh (11%).**

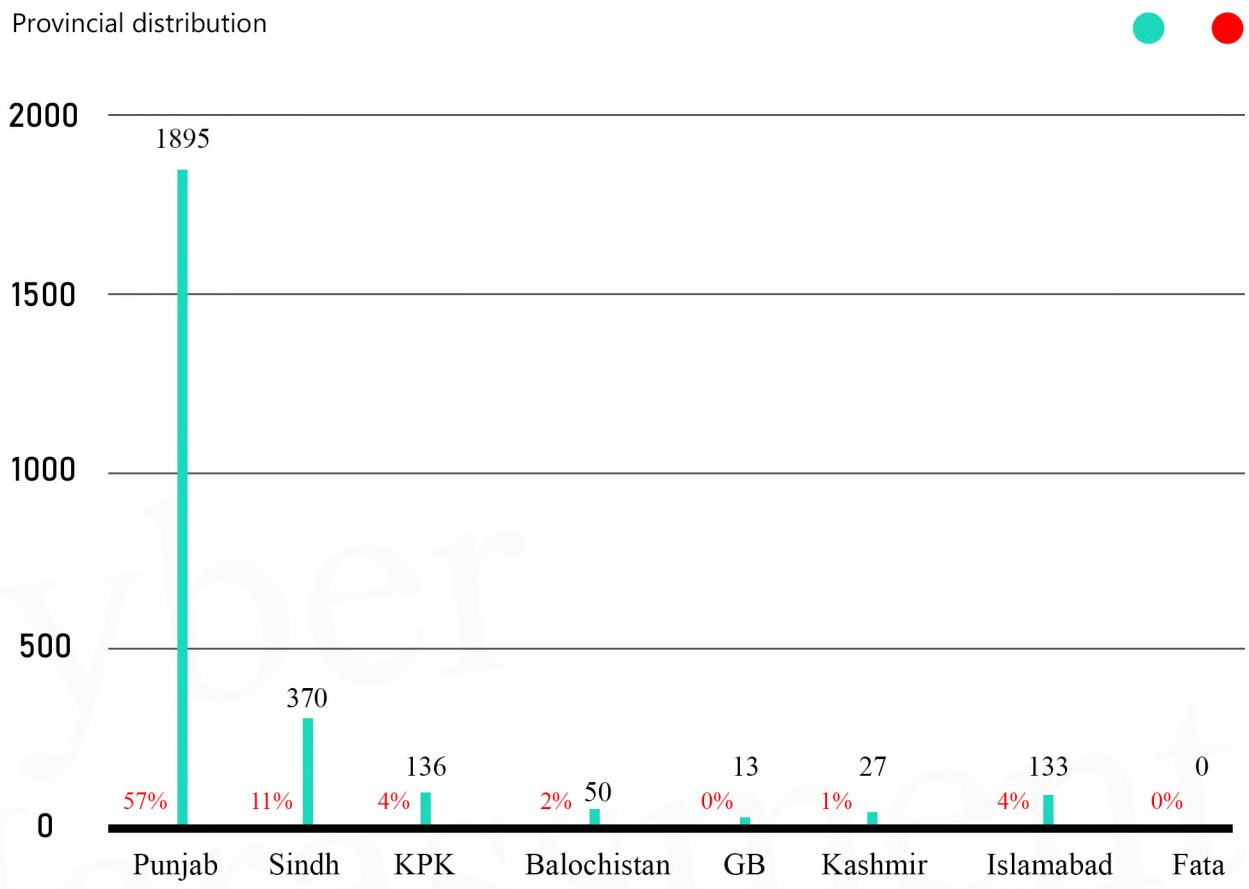


Figure 7: This data is based on the total number of complaints (3298). The number of missing data is in cases where either it was deemed inappropriate to ask for location data, or when the complainant refused to provide it.

INACCESSIBLE FIA OFFICES

Access to law enforcement agencies is one of the most important determinants of a smooth functioning criminal justice system. Lack of such access serves as a serious hindrance in reporting crime. These offices are still largely insufficient as well as ill-equipped to deal with the cases of a burgeoning population. To make matters worse, the procedure for reporting a cybercrime case to the Federal Investigation Agency (FIA) requires the complainant to travel to the cybercrime wing's office and register their case in person to commence legal proceedings. According to our figures, **53%** of the cases the helpline receives fall in the domain of the FIA.

The highest number of cases that the helpline received were from urban districts, with Islamabad, Karachi and Lahore in the top three. A vast majority of the cases were reported from areas where a cybercrime wing office did exist, and only **17%** of the cases were reported from areas where an office did not exist. This is a huge improvement from last year in the sense that the percentage of complainants living in cities without an office has gone down since the expansion of cybercrime wing offices in other areas namely Multan, Faislabad, Sukkur, Gawadar, Abottabad, Gujranwala, Gilgit, Dera Ismail Khan and Hyderabad besides Lahore, Karachi, Peshawar, Rawalpindi, Quetta and Islamabad.

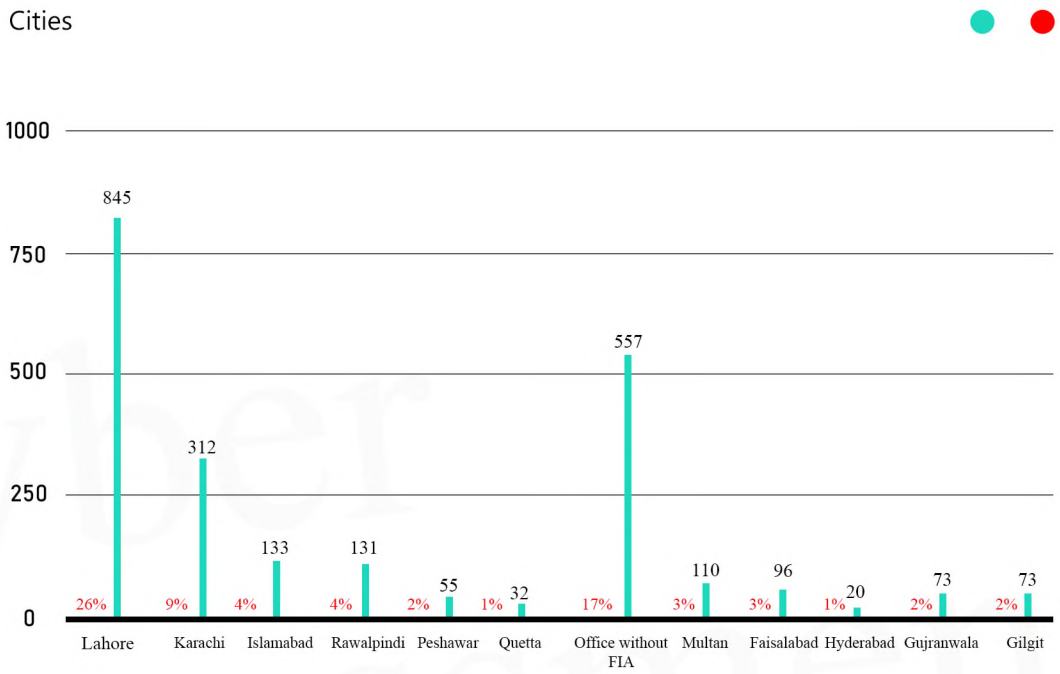


Figure 8: This data is based on the total number of complaints (3298)

AGE DISTRIBUTION

A majority of our callers **(28%)** were between the age of 21 and 25 years, followed by 26 to 30-year-olds and 18 to 20-year-olds. When read with the gender ratio discussed above, it can be deduced that the most vulnerable demographic regarding online harassment contacting the helpline are young women.

It is also interesting to note that **5%** of the complainants were under the age of 18, which is below the age of majority and consent. Callers under the age of 18 face complex challenges in terms of reporting since many of them do not receive support from their legal guardians. Cases become even more complicated in instances where the alleged harasser is also younger than 18.

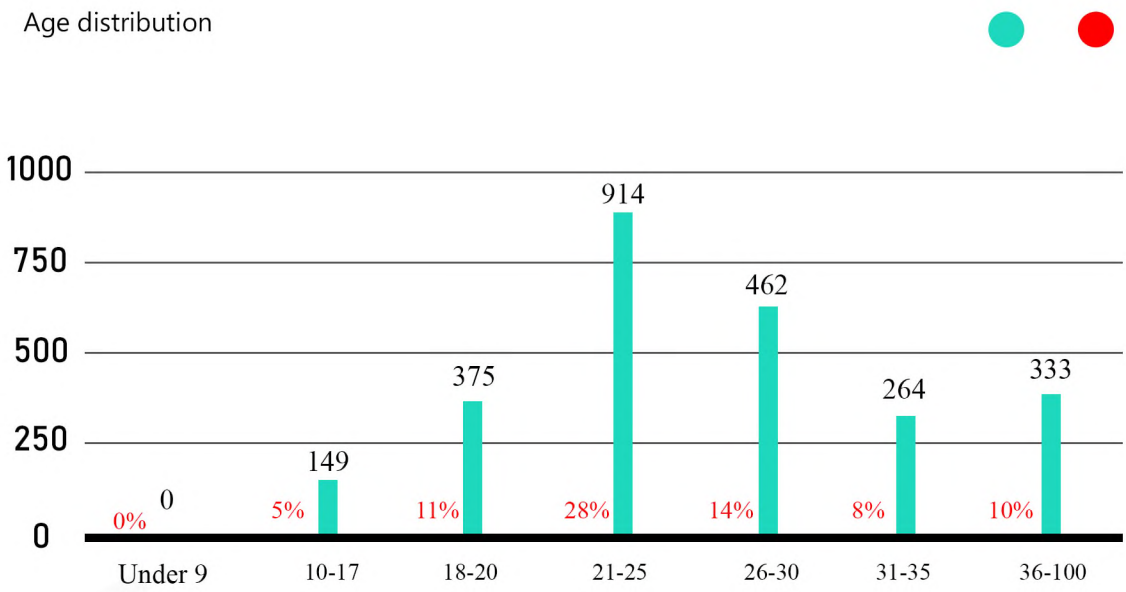


Figure 9: This data is based on the total number of complaints (3298)

SOCIAL MEDIA PLATFORMS: SPACES FOR NETWORKING OR SITES OF HARASSMENT?

The internet is increasingly becoming a complicated and multi-layered space with several dominant social media companies as well as smaller platforms. As a result, the helpline has to deal with cases of harassment experienced on multiple digital platforms. In Figure 11 below, we identify the mediums and social media platforms that are the most common sites for harassment. This distinction of platforms is important because it highlights not only the spaces most prone to harassment but also identifies which policies, sets of community guidelines and laws apply in certain cases.

The companies that own these platforms are diverse in their policies, community guidelines and mechanisms to address harassment. Furthermore, since most of these companies have offices in foreign jurisdiction, there is often a cultural, language and legal barrier when it comes to reporting cases of online harassment. By far, the biggest number of complaints at the helpline relate to Facebook (833 complaints). As many as 25% of our callers reported experiencing problem or harassment on Facebook.

Recently, there has been an influx of cases regarding WhatsApp (25%) and e-mobile wallets that have been found to be more prone to hacking attacks.

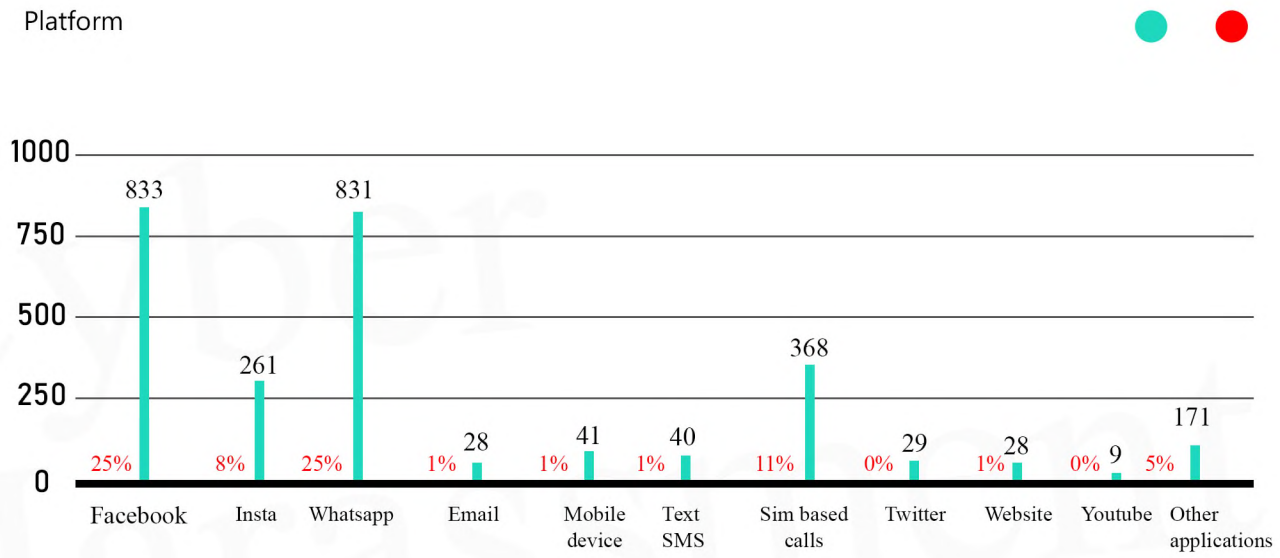


Figure 10: This data is based on the total number of complaints (3298)

REFERRALS

DRF is a non-governmental organization and, therefore, there are limitations to our investigative and intervention powers. When a caller wants to pursue a legal case or investigate into the identity of their harasser, the helpline staff informs them about the Cybercrime Wing of the FIA. This is the designated law enforcement agency for such crimes under Section 29 of the Prevention of Electronic Crimes Act 2016 (PECA). Nevertheless, the final decision about whether or not they want to follow through with the referral lies with the caller. As the data below shows, **53%** of our cases were either fully or partially referred to the FIA. For cases within Lahore, our legal officer accompanies the complainant to the FIA offices and actively follows up on cases in the Lahore branch. In 2020 **direct legal assistance** was provided to **78** such callers, out of which **55** were women. This assistance included drafting and filing of complaints, following up and taking updates from the FIA, and giving accurate legal advice. For other cities, we refer cases to lawyers from our network of legal practitioners.

In sensitive situations, emergencies that require immediate action from law enforcement agencies or when specialized services are needed, our staff refers the case to other relevant government authorities or NGOs for further assistance such as the PTA, Punjab Commission on the Status of Women (PCSW), and Rozan among others.

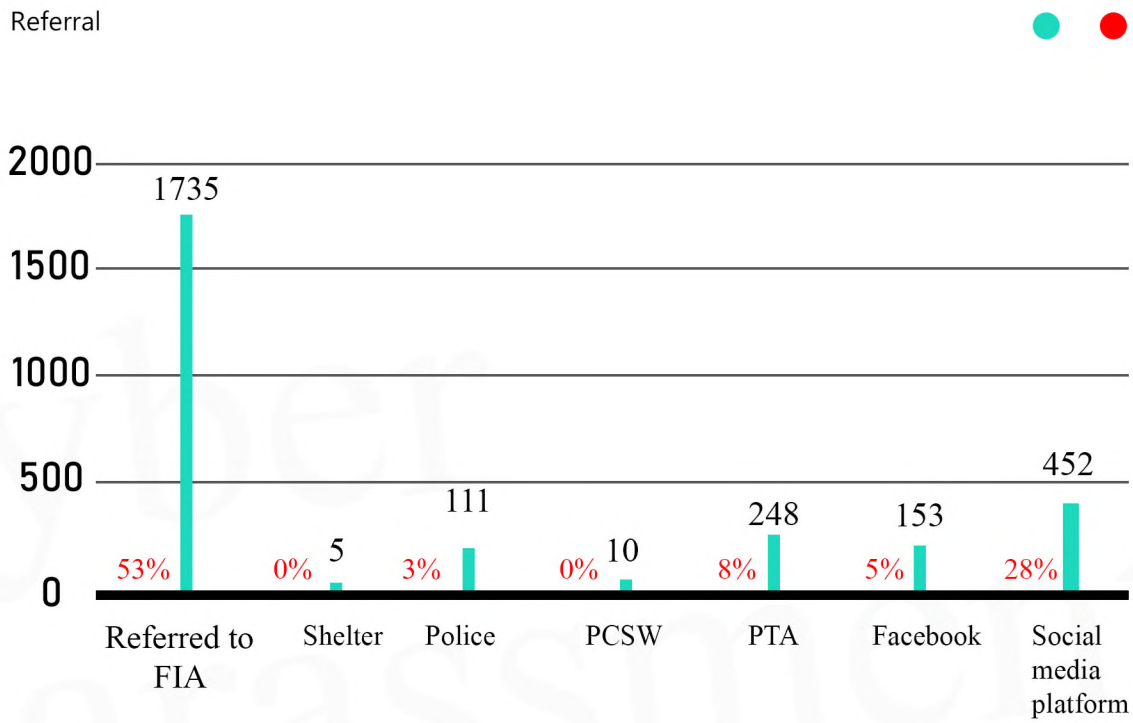
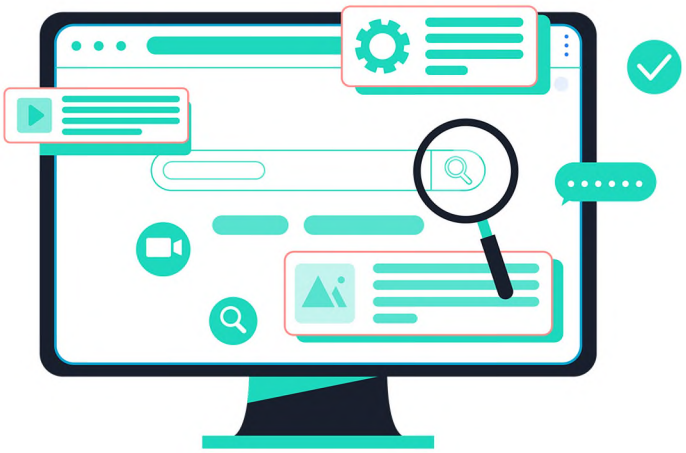


Figure 11: This data is based on the total number of complaints (3298)



WHERE DO PEOPLE HEAR ABOUT OUR HELPLINE?

To understand the awareness and impact of our communication efforts, we ask our callers about where they first heard about our helpline. A majority of our callers indicated that they heard about us through their friends/word of mouth and through police helpline. The helpline team, along with our advocacy officer, regularly runs awareness campaigns online to educate users about digital safety and for outreach regarding our helpline.

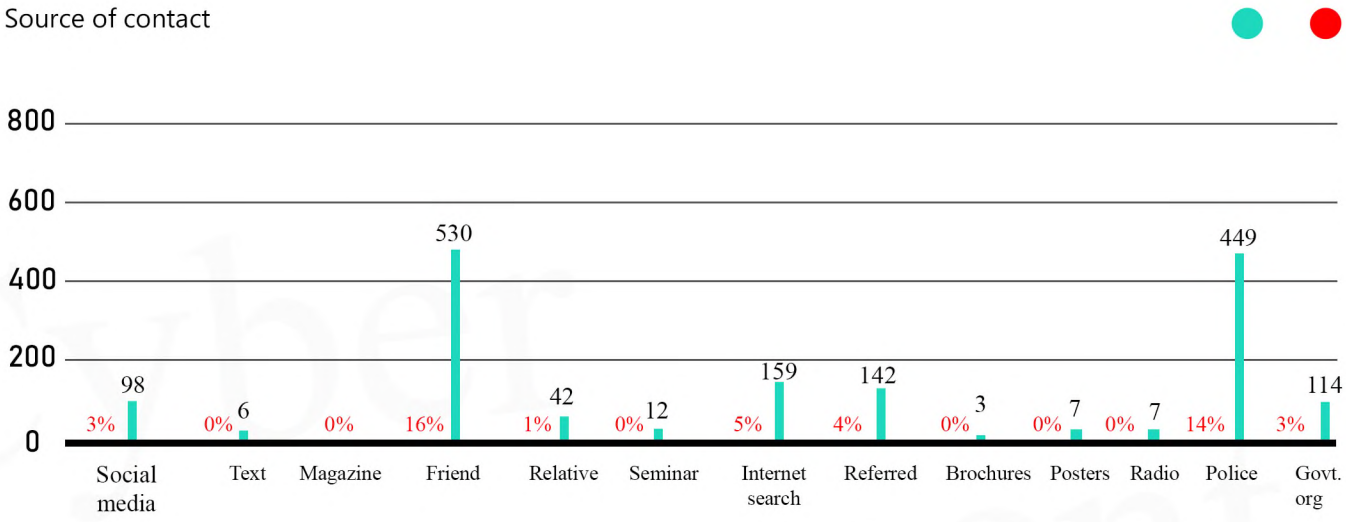


Figure 12: This data is based on the total number of complaints (3298)

TYPES OF SERVICES WE PROVIDE:

Our cyber-harassment helpline provides one or a combination of the following services:

1. **Legal counsel:** We inform people about their rights,the options they have under the cybercrime law and how to report cases to law enforcement.

2. **Digital safety support:** We provide relevant digital support required to secure the individual in an online space.

3. Mental health counselling: We lend a non-judgmental ear to distressed individuals to help them cope with their situation.

Below is a breakdown of the services provided on cases:

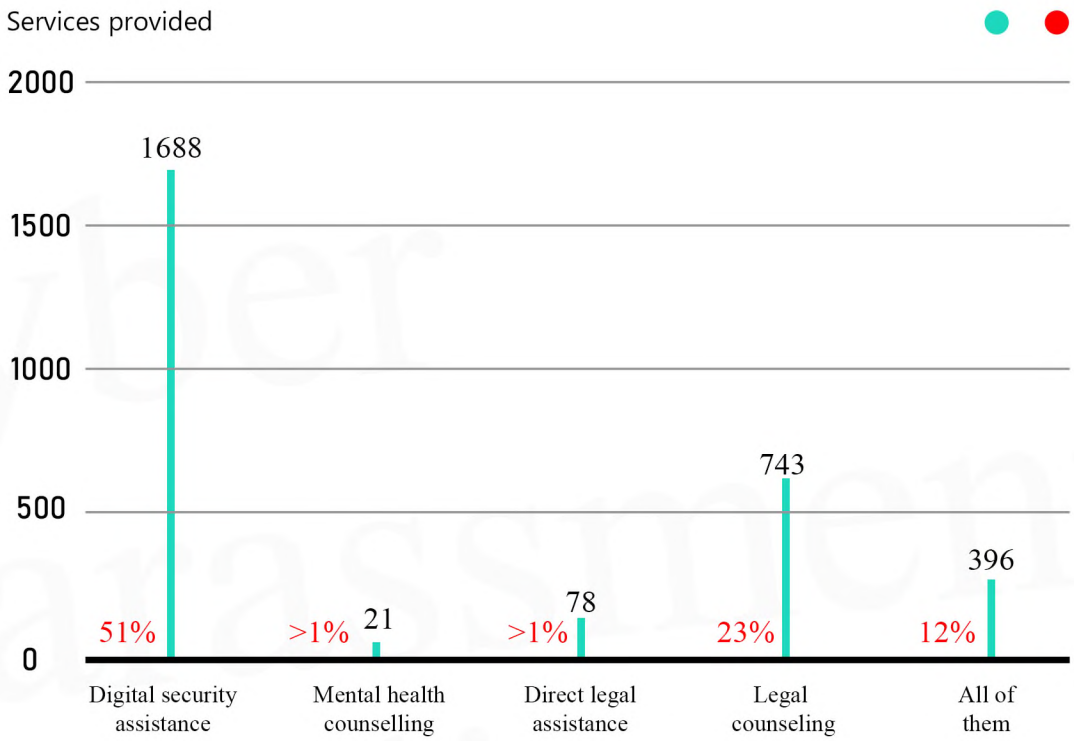


Figure 13: This data is based on the total number of complaints (3298)

A majority of our cases deal with complainants requiring digital security assistance, which is provided by the helpline staff trained in basic digital security and well-versed with the community guidelines of social media companies to facilitate reporting and escalating complaints with Facebook, Instagram, Google, YouTube, Twitter, Dailymotion, TikTok, and various other online platforms

In cases requiring legal counsel or assistance, our dedicated legal officer provides telephonic and in-person services as well. Our "Ab Aur Nahin" network acts as a network of lawyers who can represent complainants pro bono and provide them quality and affordable counsel.

CALLERS AT RISK

The helpline has received a number of cases in which we assessed that our callers were at risk. We have identified two main categories:

Individuals suffering from poor mental health

Our helpline team assesses every distressed caller against mental health indicators and looks out for signs in individuals for minimal or extreme suicide ideation. Suicidal ideation means thinking about or planning suicide. Thoughts can range from a detailed plan to a fleeting consideration. Three of our callers were noted to have suicidal ideation this year.

Our helpline support staff are specifically trained to offer psychological support to the callers. In cases when the individual is deemed to have extreme suicide ideation, they are immediately referred to our in-house psychologist.

We have observed that men don't come out with their psychological issues within their family or peers due to internalised roles of masculinity that contradict the concept of asking for help or support when dealing with emotions. Thus, men are more likely to reach out for help outside their support circles.

Individuals from marginalised communities

We received calls from complainants who experienced heightened vulnerability online due to the fact that they belonged to marginalized groups (gender and sexual minorities and religious minorities). 21 such cases were received from members of these groups . Some of these callers were specifically targeted by individuals for personal reasons, while others were victims of harassment both online and offline simply because of prejudice against their gender and/or sexuality. It has been observed that members of vulnerable communities are common targets of such hate crimes.

Receiving calls from communities that are stigmatized or marginalized, highlights the fact that issues of harassment are not endemic to women alone but speak to a concerted targeting of groups deemed as vulnerable or different in these spaces. Members of marginalized communities are less likely to reach out and have access to resources for assistance, which means that the statistics here are not representative of the extent of threats faced by them.

Members of the marginalized communities find it difficult to report such issues to the law enforcement agencies as these institutions lack sensitization.

Individuals from vulnerable professions

We have also received complaints from individuals working on human rights issues, supporting democracy, and advancing universal human rights in order to create a more secure, stable and just society. 48 such cases were received from members of these groups including, but not limited: to journalists, media workers, lawyers, human rights defenders and development workers. We feel that these professionals are more at risk of online attacks given their visibility and the nature of their work, thus requiring specialized support.

There exists a culture of impunity against killings of human rights defenders in Pakistan and this has fueled further violence against them.[26]

EMERGING CHALLENGES

Online spaces are extremely dynamic and trends emerging within Pakistan are evolving with the techno-legal landscape. We have delineated emerging challenges that we have observed through the cases we receive:

Blackmailing through pictures and information: the most worrying trend observed in the year 2020 was the dissemination of non-consensual pictures and information through different WhatsApp groups. Firstly, perpetrators remain anonymous. Secondly, unlike other platforms, content moderation is not as pervasive in WhatsApp, therefore, filing complaints for breach of community guidelines becomes ineffective.

Social engineering attacks/phishing: Hackers evolve with technology and introduce new phishing strategies to scam and blackmail people. A burgeoning trend we have seen at the helpline is social engineering/phishing attacks to hack WhatsApp accounts of people. In these attacks, hackers trick people by impersonating government officials or game show personnel offering prizes to give up their security codes. Once hackers have access to one account, they are able to embed themselves and use it to send malicious messages to others in groups/ contacts, expanding their access and making others susceptible to attack as well.

Mobile wallet/e-cash: Another emerging trend is financial fraud and scams through mobile wallets and e-cash accounts, such as Jazz Cash and Easy Paisa. Hackers scam people by obtaining their e-wallet codes, in turn gaining access to their accounts and finances. These scams are usually perpetrated by impersonation of telecommunication companies, government officials or schemes like Benazir Income Support Program or Jeeto Pakistan TV game show. By the time victims realize that their account have been hacked, it is usually too late and they have already lost a significant amount of money from their account. For victims belonging to low-income groups, who are more likely to use these services, these losses can be significant.
It is important to address the gravity and expanse of these problems. We urge users to be mind-ful of the information they share with strangers and also understand that passwords and codes are personal data and should not be shared with anyone.

RECOMMENDATIONS

For individuals experiencing cyber harassment

Online harassment, much like physical (offline) harassment, is not only inappropriate conduct but also an unlawful form of discrimination that should be reported. Following are the tips for dealing with online harassment and reporting it effectively:

1. Seek Support: online harassment and its after-effects are difficult to process. Reach out to supportive and trusted friends, family members, teachers and/or organisations who can provide you much-needed support and help to process what has happened. You should not be made to feel alone.

2. Keep the evidence : Keep the abuser's account details and any evidence of abusive messages in the form of screenshots. Do not delete your chats without saving the evidence. Do not remove your social media accounts immediately without preserving evidence.

3. Do not engage with the harasser/abuser: Do not give them the satisfaction that they can control you with fear and blackmail. If disengaging is not an option then try to neutralize the situation and gain enough time to lodge a complaint against the abuser.

4. Exercise your rights: block the harassers and report them using the mechanisms given by the social media sites. You can also lodge a complaint against them with the relevant authorities.

PREVENTATIVE TIPS FOR INDIVIDUALS

Breach of privacy on social media platforms is a serious concern. While online security will not eliminate cyber harassment completely from your life, you can limit it to an extent by grabbing the steering wheel of your digital life. Here are some basic preventive tips for your online safety.

1. **Don't overshare:** When making a public post, be careful about the information you share. Information that can be used to identify you should be shared with caution online as doing so can endanger your privacy. Make informed decisions taking into account all the risks.

2. **Control your privacy:** Keep checking your security and privacy settings to update them. This helps ensure that changes made by social media platforms do not affect your security and privacy. You need to be in control of your privacy settings so as to minimize chances of cyber harassment.

3. **Go anonymous:** You can maintain anonymity by changing your privacy settings to prevent users from looking you up through your email address or phone number. You can also prevent users from sending you messages by adjusting your privacy settings. The fewer people can look you up online, the fewer chances of cyber harassment.

4. **Review your login information:** Facebook and Google allow you to see where you are logged in and which browsers you are logged on to. Review this information regularly to ensure that you have not accidentally left a session logged in anywhere, or that your account has not been compromised. If you are careless about where you leave your account logged in, you are basically leaving your account and by extension your data vulnerable to misuse. This can lead to potential online violence against you.

5. **Targeted ads:** Ensure that social media websites cannot personalize ads, or track you online. Check your Facebook ad preferences - you will be shocked to see the large number of keywords used to identify your "ad preferences". When social media companies can collect your personal data, they can very well distribute and/or sell it. Therefore, it's best to keep it in check.

6. **Never share your location:** Do not let social media websites track your location. Make sure that you disable the option in your settings. Similarly, be very careful about announcing where you are via the "check-in" option on social media. Stalkers in particular can use this information against you.

7. **Control your tags:** Check and control your tag settings to ensure that you are not tagged in irrelevant photos or updates. Protect your privacy!

8. **Strong Password:** Protect your accounts using strong passwords. Use a phrase instead of a word with symbols or numbers, as it will be difficult for hackers to guess and easier for you to remember. If you don't want to think of a combination of words for your password, you can use one of the online password generators.

9. Two Factor Authentication (2FA): 2FA authentication is used to provide your account with additional protection. When you sign into your account with 2FA, you must not only enter the correct password, but also an additional code generated earlier or sent to your device. If someone just gets a password for your account, they will not be able to access it without entering this additional code. Enable 2FA for all your social media accounts especially WhatsApp.

REMEMBER: Cyber harassment or any form of online violence is never your fault - just like potential theft of your valuable jewellery is never your fault. Precautions taken to avoid any form of theft should not be taken to mean that it is your fault if you, unfortunately, fall victim to any form of violence.

FOR POLICY MAKERS

The Government of Pakistan needs to take concrete steps to root out online harassment and make digital spaces safe for all. We recommend the following steps in achieving that:

1. Transparency: Ensure that the bi-annual report by the FIA, required under section 53 of PECA, is submitted regularly and without delay to Parliament. In the past, the FIA has failed to submit its report in the first two years of PECA's enactment. So far only two reports have been submitted by the FIA since 2016.

2. Sensitize society: The government should collaborate with organizations working on gender issues to conduct gender sensitization workshops with teachers – as they have the power to influence students' minds – and community leaders. Such workshops should also become part of the government's public awareness campaigns. They should also be introduced at all workplaces so as to change society's mindset in general. Futhermore, policies should be introduced to address the gender digital gap by removing the financial, safety and social barriers that women face when accessing digital devices and internet spaces.

3. Gender Sensitization of the law enforcers: The government should collaborate with organizations working on gender issues to conduct gender sensitization workshops with law enforcement agencies so that staff dealing with complaints of gendered online violence can overcome patriarchal attitudes. Victim blaming and intrusive questions are a deterrent for victims/survivors reporting online harassment. DRF has conducted such workshops with the FIA in the past and welcomes all such future collaboration.

4. Data protection: DRF urges the government of Pakistan to enact meaningful legislation on digital privacy or data protection after consultation with civil society and the general public. The right to dignity and privacy as guaranteed under Article 14 of the Constitution of Pakistan for every citizen should also be protected. Strict action must be taken against sexual harassment, surveillance, unauthorized use and dissemination of personal information, and manipulation of personal information including photos and videos.[27]

5. Decriminalize defamation laws: Online defamation is criminalized under section 20 of PECA and has been used to silence survivors of sexual harassment and assault, especially those using social media to share their experiences of harassment. We strongly recommend that the online defamation section in PECA be repealed, and those aggrieved by online speech against their person can seek alternate remedies under civil defamation laws.

6. Training for judges on cybercrime law, internet governance and online harassment: Internet governance and cybercrime should be included in the curriculum of provincial judicial academies to ensure that judges are not only familiar with the law regarding the internet, but also have a thorough understanding of the technologies involved in the process. It has been observed that judges are not only ignorant of the law regarding the internet and cybercrime -- they also fundamentally misunderstand governance and infrastructure of the internet itself, which leads to bad jurisprudence and, at times, "unimplementable" orders.

7. Allocate funds for NR3C: DRF urges policy makers to **push the government to create more funding for the Cybercrime Wings,** especially by recruiting trained women staff and trained mental health counselors to address online violence against women.

8. Allow smooth functioning of NGOs: DRF urges policy makers to take measures to ensure the smooth functioning of NGOs working on digital rights and **gender**.

FOR FEDERAL INVESTIGATION AGENCY

We commend the government and the FIA for expanding its resources for tackling online harassment by increasing the number of offices for the Cybercrime Wings. Nevertheless, there is a long way to go in terms of addressing online harassment, and we hope that the incumbent government continues to see online harassment as a serious and pressing issue.

1. Greater resource allocation: While there has been a vast improvement in the resources allocated to the NR3C than in the past, we posit that more needs to be done to keep up with the exponential growth in cybercrime cases at the NR3C in order to resolve them in a timely manner. With the increased access to ICTs and awareness regarding cybercrimes, the FIA will need to respond to an unprecedented number of complaints and a higher future demand. The allocation of resources, thus, needs to take into account these unique circumstances and DRF urges the concerned government departments to increase grants allocated to the FIA.

2. Mechanism to deal with cases in foreign jurisdictions: In many cases where either the accused or the complainant is located outside Pakistan, the FIA lacks the capacity to take action despite being empowered to do so under Section 1(4) of PECA. DRF recommends that there be at least one officer in each branch dealing with cases in foreign jurisdictions, with specialized training in international law and conflict of laws. Both the Ministry of Information Technology and Interior Ministry are urged to define "international cooperation" under Section 42 of PECA while upholding the spirit of the rights of Pakistani citizens.

3. Introduce online portal for cybercrime-related complaints: It is not possible for everyone who experiences online violence to **go in person to the NR3C offices** and report the crime, particularly because of the mobility issues that arose during the COVID mandated lockdown. Therefore, DRF urges the FIA to invest in the establishment of a digitally secure online portal that citizens could use to file their complaints and to record their statements without having to visit the office **in person**. Furthermore, necessary changes to the law should be made to ensure that such digital reporting is possible.

4. Sex-disaggregated data: The FIA, while fulfilling its statutory obligation to report to Parliament under Section 53 of PECA, is requested to produce data regarding the number of online harassment cases and the number of cases registered by women under each section of PECA, particularly Sections 20, 21 and 24. These figures should be **public** as it will allow for better policy-making and allocation of resources.

5. Creation of a separate desk for online harassment within the cybercrime wing: Given the specific and complex nature of online harassment cases and the gender sensitivity required for complainants/victims, DRF recommends that a dedicated desk for cyber-harassment be set up within each cybercrime wing to handle cases under Sections 21 and 24 of PECA. This desk should be the first point of contact for complainants of online harassment and equipped with officers specifically trained in the nuances of online harassment, its various forms and gender sensitivity as well as counseling services.

6. Rapid Response Cell: Given the urgent nature of certain cases of online harassment, where leaked information can harm personal safety or cause immediate reputational harm, a rapid response cell that is operational 24/7 should be established in addition to the regular operations of the FIA. Cases marked as urgent should be expedited and dealt with on a priority basis.

7. Privacy and confidentiality: One of the biggest barriers for reporting cases of cybercrime, particularly online harassment, to law enforcement is the fear of leaked information and a further breach of confidentiality. Many complainants require the assurance of confidentiality as a prerequisite to reporting. Rule 9 of the PECA Rules lay down protections and requirements for confidentiality for cases involving women and intimate images, it is urged that concrete measures be taken to ensure that these rules are followed in their letter and spirit.

8. Greater accessibility for people with disablities: Functioning elevators, ramp for wheel-chairs, accessible toilet facilities and in-person assistance in filing applications are minimum requirements that every cybercrime wing office should meet to ensure that disabled persons do not have to face additional hurdles in registering and pursuing complaints.

9. Coordination with other departments: 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 FIA. In certain trials given that challans contain both sections of PECA and the Pakistan Penal Code (PPC), **there is often back and forth between different courts and judges**. DRF recommends that channels of communi-cation between police stations and cybercrime wings 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.

10. Empower local police to process cases of online harassment: While cases under PECA fall in the jurisdiction of the FIA, the role of the police and its infrastructure can and should be harnessed to ensure that cybercrime case is processed at the local level.

11. Psychological services: DRF urges the FIA to make provision for psychological services at cybercrime wings to help complainants deal with the psychological trauma and distress that they experience due to online harassment and violence. All officers at the FIA, especially those dealing directly with victims, should be trained on how to **address trauma**. The cybercrime wing should offer a safe space for victims and help them process their trauma in a constructive and safe manner.

12. Case management and tracking 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 be stored on a secure server to ensure reliable duplicates in case the original case file is lost or tampered with.

13. Gender sensitization: Several female complainants who have approached the NR3C have reported being shamed for their choices and discouraged from pursuing cases by officers at the cybercrime wing. DRF has observed that while higher officials, such as deputy directors and assistant directors, are sensitive to these issues and proactively reassure complainants, this attitude is not always reflected in the behavior of individual investigation officers. Since many cases involve sharing of intimate data and gendered harassment, there is a need to ensure that officers, particularly those directly dealing with complainants, as well as the overall environment of the offices, are conducive to female complainants and provide a safe and judgment-free space. DRF has conducted gender-sensitisation training with the FIA in Islamabad and Karachi and hopes that these engagements will continue in the form of regular trainings. DRF recommends that a quota of at least 40% female and transgender investigation officers and prosecutors be instituted, and all officers—including the female ones—be given extensive gender sensitivity training. It is also recommended that women's rights organisations be included and allowed to assist in developing these training sessions. Gender sensitisation does not only mean taking into account the specific needs of women but different genders and marginalized communities. Often gender-nonconforming individuals are the most vulnerable to harassment and are subsequently discouraged from reporting the same.

14. Check on the performance of investigators and prosecutors: Internal mechanisms should be in place to review the performance of investigators and prosecutors. Incompetence and insensitive behavior on part of officers can lead to a miscarriage of justice in certain cases. Complainants should be able to register concerns and complaints regarding their assigned officers to a senior presiding officer for each regional zone, which should automatically trigger an independent and transparent inquiry. A new officer should be assigned immediately in case of misconduct or failure to perform duties.

15. Greater technical expertise: Several complaints to the cybercrime wing experience a substantial investigative delay or are dropped altogether due to lack of technical abilities of officers and technologies available to the FIA. DRF recommends that measures be taken to capacitate them to not only meet current trends in cybercrime but also keep abreast with developments in forensic science and evidence collection in the five-year coverage period. This capacity-building should be an on-going and constant process. Thus, DRF recommends substantial investment in research at the cybercrime wing to address the needs of litigants/-complainants.

16. Collaboration with civil society organizations: DRF recommends more public-private partnerships by the government to ensure that public institutions work collaboratively with civil society and academia to complement each other's work. A mutually beneficial memorandum of understanding (MOU) between DRF's cyber harassment helpline and FIA will be in the best interest of victims and will ensure the complainants obtain timely and comprehensive support.

REPORTING MECHANISMS

Cyber Harassment can be reported to the relevant authorities.

1. Cyber Harassment Helpline - Digital Rights Foundation: a referral and redressal helpline that connects cyber harassment affectees with law enforcement agencies. It also helps in getting content removed from social media sites through its established escalation channels.

2. FIA Cyber Crime Wing: In order to register complaints with the law enforcement agency for investigation, the complainant will have to go to the nearest FIA cybercrime wing office with a written application (in Urdu or in English), all the evidence in hard copy, and their original CNIC. In cases of minors, they need to be accompanied by their parent or guardian to register their complaint.

APPENDIX:

Types of Cases:

In order to analyse the needs of the helpline as well as general trends of online harassment in Pakistan in greater detail, we categorise the cases according to predetermined typologies. The following are definitions that we use to sort the cases:

General Inquiry:
These are inquiries we receive regarding cyber harassment, digital security and the work of Digital Rights Foundation. This category also includes inquiries that we get outside the realm of digital rights, in which case our Helpline Support Staff redirects the caller to the relevant authorities and organisations through the referral network.

Impersonation:
Complaints under this category involve an individual's identity being appropriated without their permission. This manifests in profiles purporting to belong to someone on social media websites and contacting people through texts or calls pretending to be someone else.

Blackmailing:
This often involves using personal information or psychological manipulation to make threats and demands from the victim. Blackmailing using sexually explicit videos or pictures is criminalised under Section 21 of the Prevention of Electronic Crimes Act 2016 (PECA).

Stolen Device:
These complaints involve loss of information, data, and identity in cases where digital devices are stolen or misplaced. Assistance provided involves helping complainants in recovering and securing their accounts as well as assisting them in filing criminal complaints about theft.

Fake Profile:
Fake profile on a social media platform or application is an account pretending to be someone or something that doesn't exist.

Scam Calls:
Fraudulent calls that pretend to be an individual or from an authority to make a quick profit. Mostly such scam calls lead to a potential financial fraud being committed.

Abusive Language:
Using harsh, hurtful, explicit or insulting language to attack another person.

Unsolicited Contact:
Unsolicited contact involves unwanted and repeated calls and messages by the accused/abuser, which may include spam, repeated requests for contact, personalised threats, blackmail or any unwanted contact that makes the receiver feel uncomfortable. If this rises to the level of criminal liability, cases in this category can fall under the ambit of Section 24 of PECA.

Login Issues:
These involve difficulties in accessing accounts and devices where the user has been locked out or has limited/compromised access due to a known or unknown reason.

Hacking:
Gaining unauthorised access to someone's electronic system, data, account and devices, which can result in loss of data, loss of identity and blackmailing.

Federal Investigation Authority (FIA)-related Inquiry:
These are queries we get regarding the complaint procedure of the National Response Centre for Cyber Crime (NR3C) of the FIA. These callers often want to file a formal, legal complaint. It also includes individuals who are contacting the helpline after they have dealt with the FIA, either to get advice on their case or to complain about the FIA officials or process.

Non-Consensual Usage of Information (NCUI):
This involves using, sharing, disseminating and manipulating data such as photographs, phone numbers, contacts, and other personal information without consent and in violation of the privacy of a person.

Online Stalking:
Online stalking is keeping track of someone's online activity in a way that it makes the subject of the stalking uncomfortable. For the purpose of this report, online stalking also refers to (repeatedly) contacting a person's friends and/or family.

Doxxing:
Doxxing is the practice of leaking and publishing information of an individual that includes personally identifiable information. This information is meant to target, locate and contact an individual, usually through social media, discussion boards, chat rooms and the like, and more often than not, is accompanied by cyberbullying and cyberstalking.

Gender-based Bullying:
Any actions, statements, and implications that targets a person based on their gender identity or sexual orientation. Evaluations for gender-based bullying take into account the overall connotations attached to actions and verbal communications within the larger system of gendered oppression and patterns of behavior that signify abuse.

Bullying:
Any actions, statements, and implications that targets a person in order to intimidate, silence, threaten, coerce or harass them. This category is distinguished from the one above, where the complainant is targeted specifically on the basis of their gender.

Non-Consensual Use of Pornographic Information (NCUPI):
This is obtaining, using, distributing or retaining pictures, videos or graphic representations without a person's consent that violate their personal dignity.

Financial Fraud:
Intentional actions of deception perpetrated by a person for the purpose of financial gain and profit; this includes using someone's financial data to gain access to accounts and make purchases. For the purpose of our operations, we confine our definition to fraud conducted through electronic means.

Stalking:
This category includes monitoring, physical following, and harassment that occurs outside of online spaces. A majority of the cases received by the helpline relate to non-consensual use of information, which include pictures, videos, and personal data. In cases of online harassment, this information is weaponized by harassers to cause harm, reputational damage or to blackmail victims. This information is also manifested in fake profiles or used on various forums without the consent of the victim. Another major form of harassment experienced by our callers is unsolicited messages, usually containing lewd or threatening content.

Non-Consensual Photoshopped Pictures/Doctored Pictures:
The manipulation, distortion or doctoring of images without the permission of the person to whom they belong. This is often accompanied by distribution and sharing, or threat to share, of such pictures as well.

Threats of Sexual/Physical Violence:
An action or verbal communication that results in a reasonable fear of sexual or physical attack.

Non-Cooperation from Social Media Platforms:
These complaints refer to a situation when a person has reported a case of cyber harassment to the relevant social media team but has not received a decision in their favor.

Threats:
These are all threats directed at the victim of online harassment that do not fall under the category of gender-based threats or sexual/physical violence.

Defamation:
Any intentional, false communication purporting to be a fact that harms or causes injury to the reputation of a natural person.

Hate Speech:
Any communication that targets or attacks an individual on the basis of their race, religion, ethnic origin, gender, nationality, disability, or sexual orientation. Hate speech becomes a matter of urgent action when it puts its target in physical danger or the reasonable apprehension of physical danger. However hate speech is not restricted to just incitement to violence, it is hate speech if it leads to the exclusion of or creation of a hostile online environment for its target.

BIBLIOGRAPHY

“Prohibition of discrimination, harassment, including sexual harassment, and abuse of authority”, UN Women, https://www.un.org/womenwatch/uncoordination/antiharassment.html

Jannat Fazal et al, “Online harassment: a retrospective review of records”, F1000 Research, 2017, https://f1000research.com/slides/6-785.

Mohammad Hussain Khan, “Sindh University student Naila Rind 'committed suicide after exploitation, blackmail': police”, Dawn, December 4, 2017, https://www.dawn.com/news/1374502.

Imtiaz Ali, “Engaged couple murdered for 'honour' over accusation of taking pictures together”, Dawn, December 3, 2018, https://www.dawn.com/news/1449194/engaged-couple-murdered-for-honour-over-accusation-of-taking-pictures-together.

Sanayah Malik, “Measuring Pakistani Women's Experience of Online Violence”, Digital Rights Foundation,2017,http://digitalrightsfoundation.pk/wp-content/uploads/2017/05/Hamara-Internet-Online-Harassment-Report.pdf.

Digitalrightsfoundation.pk. 2021. [online] Available at: <https://digitalrightsfoundation.pk/wp-content/uploads/2020/06/DraftPolicy_1.8_02.06.2020.pdf>.

Shehryar Warraich. 2020. "Domestic Violence Increases Amid Coronavirus Lockdown | Dialogue | Thenews.Com.Pk". Thenews.Com.Pk. https://www.thenews.com.pk/tns/detail/678152-locked-down-and-vulnerable.

“The Shadow Pandemic: Violence against women during COVID-19,” UN Women, https://www.unwomen.org/en/news/in-focus/in-focus-gender-equality-in-covid-19-response/violence-against-women-during-covid-19.

Alradhawi, Mohammad, Nour Shubber, Jack Sheppard, and Yousif Ali. "Effects of the COVID-19 pandemic on mental well-being amongst individuals in society-a letter to the editor on “The socio-economic implications of the coronavirus and COVID-19 pandemic: A review”." International journal of surgery (London, England) (2020)

Viano, E., n.d. Cybercrime, Organized Crime, and Societal Responses.

Marjan Nadim & Audun Fladmoe, “Silencing Women? Gender and Online Harassment”, Institute for Social Research, Oslo, Norway, 2019 https://journals.sagepub.com/doi/full/10.1177/0894439319865518

Maeve Duggan, “Online Harassment 2017”, Pew Research Center, 2017 https://www.pewresearch.org/internet/2017/07/11/online-harassment-2017/

Surat P. Master's thesis. Faculty of Graduate Studies, Mahidol University; Thailand: 2010. Cyberbullying behaviors among youth: Case studies on high school and vocational school youth in Bangkok.

Ojanen, T., Boonmongkon, P., Samakkeekarom, R., Samoh, N., Cholratana, M. and Guadamuz, T., 2015. Connections between online harassment and offline violence among youth in Central Thailand. Child Abuse & Neglect, 44, pp.159-169.

Chris Summers, "Man stabs his 16-year-old sister to death in Pakistan 'honour killing' - because she was using a mobilephone," Daily Mail, April 28, 2016, http://www.dailymail.co.uk/news/article-3563679/Pakistan-police-arrest-man-honourkillingsister.html.

"Two Girls, Mother Killed Over Family Video," Dawn, June 25, 2014, http://www.dawn.com/news/1020576/two-girls-motherkilled-over-family-video;"Pakistani

"Woman Stoned to Death on Panchayat's Orders," Pakistan Today, July 10, 2013, http://www.pakistantoday.com.pk/2013/07/10/woman-stoned-to-death-on-panchayats-orders/;
Emma Batha, "Special Report: The Punishment was Death by Stoning. The Crime? Having a Mobile Phone," The Independent, September 29, 2013, http://www.independent.co.uk/news/world/politics/special-report-the-punishment-was-death-by-stoning-the-crime-having-amobile-phone-8846585.html.

Naveed Siddiqui, "Kohistan video case: Girls declared alive by SC had actually been killed, says Bari", Dawn, October 21, 2016, https://www.dawn.com/news/1291398.

"Husband 'kicks out' wife from house over 'fake' Facebook ID", The Express Tribune, March 27, 2017, https://tribune.com.pk/story/1367115/husband-kicks-wife-house-fake-facebook-id/.

Jannat Fazal, "Online harassment: a retrospective review of records", DRF, 2017, https://doi.org/10.7490/f1000research.1114142.1

Lewis, R., Rowe, M., & Wiper, C. (2017). Online abuse of feminists as an emerging form of violence against women and girls. British journal of criminology, 57(6), 1462-1481.

John, A., Glendenning, A. C., Marchant, A., Montgomery, P., Stewart, A., Wood, S., ... & Hawton, K. (2018). Self-harm, suicidal behaviours, and cyberbullying in children and young people: Systematic review. Journal of medical internet research, 20(4), e129.

Nikolaou, Dimitrios. "Does cyberbullying impact youth suicidal behaviors?." Journal of health economics 56 (2017): 30-46..

Ali Hasan, " Suspect arrested in 'suicide' case of Sindh University student a 'repeat offender': police", Dawn, January 6, 2017, https://www.dawn.com/news/1306787/suspect-arrested-in-suicide-case-of-sindh-university-student-a-repeat-offender-police.

The News. 2020. "Girl Commits Suicide After Threats Over Harassment Case", 2020.

2021. Frontline Defenders [online] Available at: <https://www.frontlinedefenders.org/en/location/pakistan>

2021. Digital Rights Foundation's Legal Analysis of the 2020 Personal Data Protection Bill -. [online] Available at: <https://digitalrightsfoundation.pk/digital-rights-foundations-legal-analysis-of-the-2020-personal-data-protection-bill/> [Accessed 10 February 2021].

CYBER HARASSMENT HELPLINE

0800-39393

helpdesk@digitalrightsfoundation.pk

MONDAY TO FRIDAY

9AM - 5PM

www.digitalrightsfoundation.pk

info@digitalrightsfoundation.pk

DigitalRightsFoundation

DigitalRightsFoundation

DigitalRightsPK