Cyber Harassment Helpline Report 2019

DRF

DigitalRightsFoundation

"KNOW YOUR RIGHTS"

www.digitalrightsfoundation.pk

info@digitalrightsfoundation.pk

DigitalRightsFoundation

DigitalRightsFoundation

DigitalRightsPK

About

Digital Rights Foundation (DRF) is a feminist, not-for-profit organisation 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.

www.digitalrightsfoundation.pk

DRF

DigitalRightsFoundation

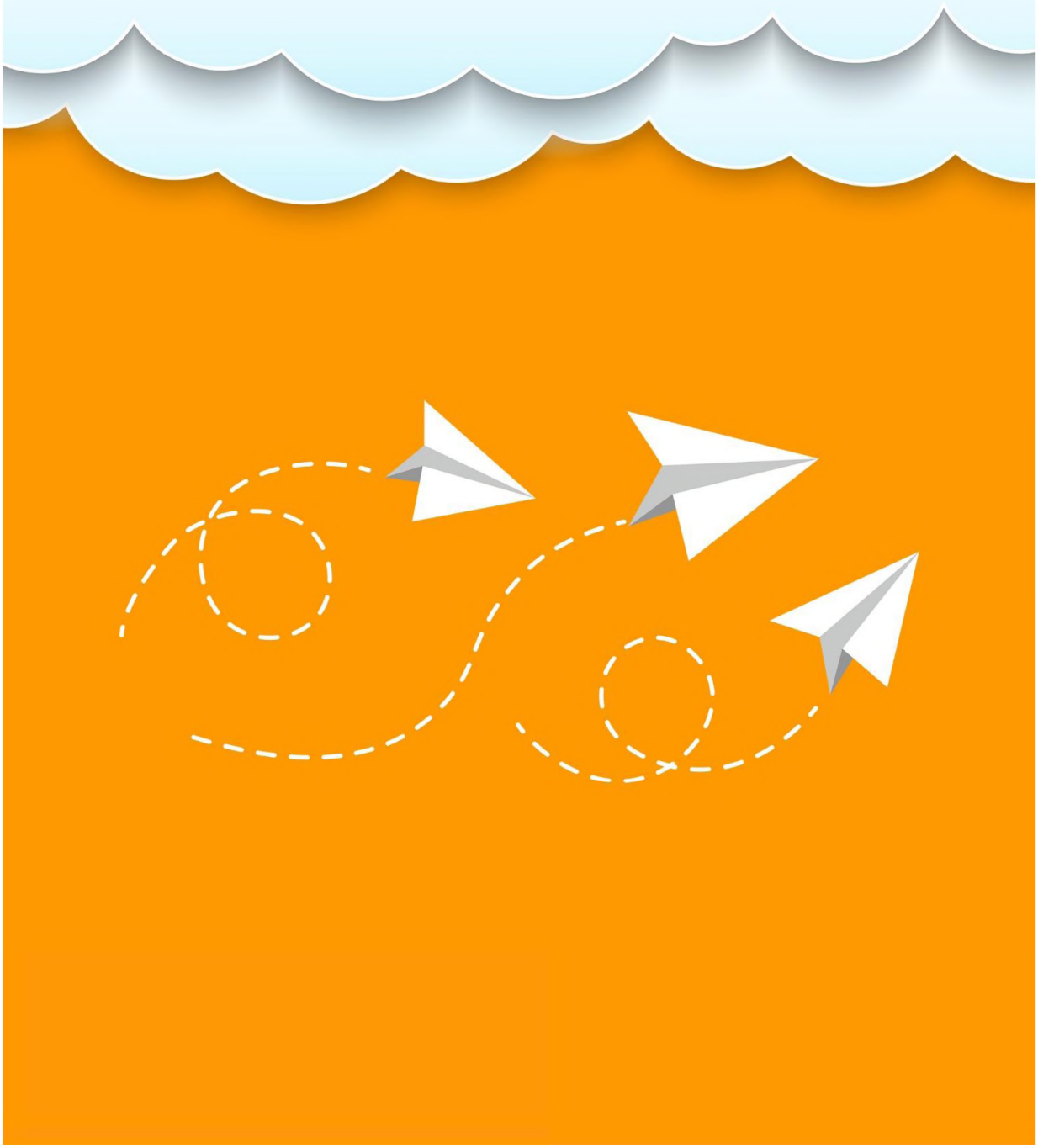
"KNOW YOUR RIGHTS"

Gender-sensitive, confidential & free helpline
0800-39393

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. Callers will speak to a helpline support staff trained in handling cases of cyber-harassment, who will assess the best means of helping the caller with their problem. The helpline is dedicated to helping vulnerable and marginalised communities in Pakistan.

Table Of Contents

The Helpline: The Road So Far



In 2016, we travelled to different colleges and universities in Pakistan to create awareness about digital safety and online harassment under our project, Hamara Internet. Little did we know then that this would finally lead us to setting up a helpline for online harassment complaints.

The sessions led to women reaching out to us through word of mouth, our inbox teeming with cases of women looking for advice and assistance in cases of online harassment. As there was no dedicated service delivery channel, the small team at DRF would find itself unable to answer all the queries effectively. Some cases started to slip through the cracks.

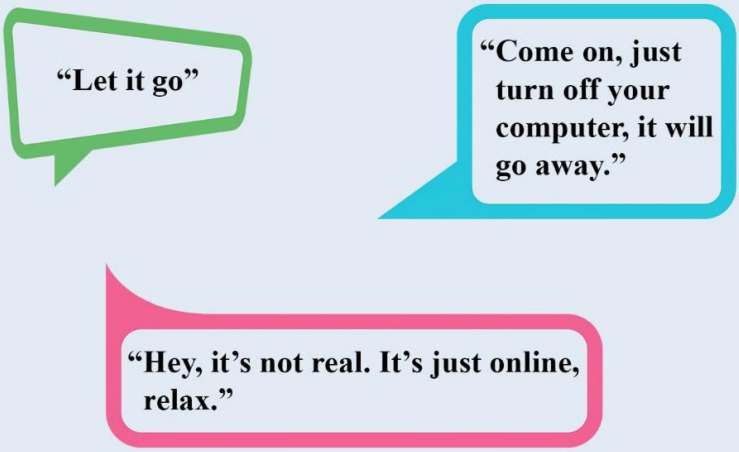
The summer of 2016 then saw the brutal murder of Qandeel Baloch. This was not a one-off incident as it led to widespread online harassment and abuse against feminists . Women were bullied and attacked in online spaces for their stances. This was part of a global phenomenon: gender-based online violence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

Serendipity would have it that Nighat Dad, the Executive Director of DRF, was nominated for the Dutch Human Rights Award in August 2016. Seizing the moment, we launched an online campaign to mobilise 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 would soon branch out into providing psychological counseling through a full-time counselor as well as legal assistance for callers through our legal officer.

Today, our helpline staff attends to an average of 146 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 trivialisation 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 trivialisation.

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.[2] Harassment can manifest in different forms: sexual harassment, workplace harassment, harassment in public spaces, and cyber-harassment.

---

[1] "Prohibition of discrimination, harassment, including sexual harassment, and abuse of authority", UN Women, https://www.un.org/womenwatch/uncoordination/antiharassment.html
[2] ibid.

What is 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.

Why do we think understanding online harassment is important? It is because of 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 illustrates how online harassment can take a toll on one's psychological wellbeing that manifests in depression, chronic stress, generalised anxiety disorder, mistrust, withdrawal and insecurity.[3] In the Pakistani context, the gravity of these cases is such that harassment and blackmailing have even led to cases of suicide.[4]

Meanwhile, despite the fact that cyber-harassment affects everyone including women, children, and men, it still remains a gendered phenomenon. This means that certain marginalised gendered groups are more vulnerable.

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.

---

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

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

Physical violence is part of the lived experiences of women and gender minorities in Pakistan, and online spaces are no exception.[5] While women are frequently targeted in honour 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 normalised 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. These experiences translated into almost **70%** stating that they were afraid of posting pictures online out of fear that they might be misused.[6]

---

[5] 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.

[6] 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.

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.

DRF's cyber-harassment helpline is the region's first dedicated helpline for cases of online harassment and violence. The support team includes a qualified psychologist, digital security expert, and a lawyer, all of whom provide specialised 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 can be contacted for pro bono representation of a complainant 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 9am to 5pm through our toll-free number. The helpline team can also be contacted outside of office timings via email at **helpdesk@digitalrightsfoundation.pk.**

This document is part of a series of bi-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 an analysis on trends regarding online harassment as well as policy recommendations to make online spaces safer for all.

Understanding cyber-harassment in Pakistan in numbers:

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

[7] Caveat: While we entertain cases on Facebook, if the complainant wants to reveal confidential or sensitive information switch to a more secure mode of communication.

Executive summary of three years

The figures outlined in this summary pertain to the three years starting from December 1, 2019 until December 31, 2019.

Total number of complaints managed by the helpline in three years **4492**

Percentage of cases from women **40% 1785** 

Percentage of cases from men **32% 1411** 

Percentage of cases reported by men on behalf of someone else **6% 258** 

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

Number of cases from cities without cybercrime office **15% 654 cases**

Platform on which most complaints were received **Facebook and WhatsApp**

Total Number of complaints in 2019

Total complaints	Total Calls	Total Emails	Facebook	Total Cases
2023	1805	218	170	1960

"We reassure our callers to keep in touch with us. This gives them a sense of security and builds a trusting relationship between the caller and the Support Officer"

-Anonymous Helpline Support Staff-

The following analysis is based on the two main mediums provided by DRF's cyber-harassment helpline: **calls** and **email.**

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.[8] The collected information is also digitally secured, and precautions 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.

[8] "Cyber Harassment Helpline Policy", Digital Rights Foundation, http://digitalrightsfoundation.pk/wp-content/uploads/2017/02/Public-Policy-for-Helpline_30.11.2016-1.pdf.

a. Average Number of Calls

In the last three years, the helpline has had a monthly average of 146 calls. As can be observed from the monthly breakdown provided below, the average number of calls has steadily increased over the years.

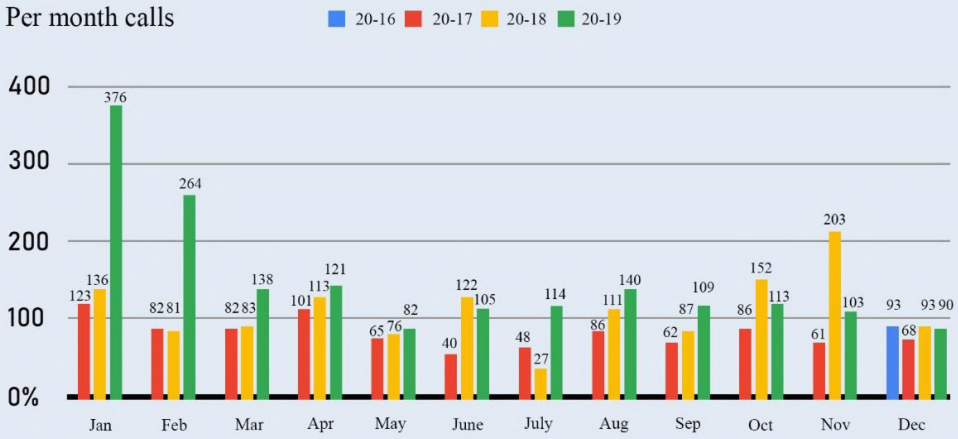


Figure 4: This data is based on the total number of cases (1960), not the number of calls attended.

b. Gendered aspect of online harassment

Data collected from our earlier reports has shown how online harassment has affected women more than men.[9] The breakdown of this year's data excluding the social engineering cases (Whatsapp hacks) reveals that the most number of complaints were received by women (58%) as well. Meanwhile, 40% of the helpline's cases were reported by men, 1% by non-binary people and 1% by callers whose data could not be collected.

How can the fact that men reported more cases than women inclusive of social engineering cases be explained? Does that mean that cyber-harassment has ceased to be a gendered phenomenon? Both ground realities and research show that none of that is true. In Pakistan, men have easier access to technology and the internet,[10] which increases their presence in numbers in online spaces. As a result, the bulk of harassment levelled at men (Whatsapp hacks) is bigger should come as no surprise.

Research shows that as against popular expectations, more men than women have experienced online harassment in Norway.[11] They explain this unexpected occurrence by the fact that "men receive more comments directed at their opinions and attitudes".[12] Their analysis further illustrates that even though women and men are equally exposed to harassment directed toward group characteristics, targeted women are more likely than targeted men to become more cautious in expressing their opinions publicly.[13] This shows that even though the amount of harassment levelled at men can be bigger due to greater presence owing to easier access to internet, computers and cellular devices, practical implications for women are far more severe as they are the ones to censor themselves.

---

[9] "Cyber-Harassment Helpline", Digital Rights Foundation, 2018 www.digitalrightsfoundation.pk/wp-content/uploads/2019/01/Booklet-Helpline.pdf

[10] "AfterAccess: ICT access and use in Asia and the Global South", AfterAccess, 2018 https://lirneasia.net/wp-content/uploads/2018/11/AfterAccess-Asia-Report-2.0.pdf

[11] 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

[12] Ibid.

[13] Ibid.

Similarly, another study on Americans' experience of online harassment shows that men are slightly more likely to experience any form of online harassment (44%) as compared to women (37%).[14] Duggan, however, complicates their analysis by explaining the differences in the types of online harassment men and women experience.

According to them, men are slightly more likely to be called offensive names (30%) as compared to women (23%) and to receive physical threats online (12% vs. 8%).[15] However, 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%) than men (9%) among adults aged between 18 and 29.[16] When the age bracket of 18-24 is analysed, American women were found to be three times as likely to be sexually harassed online (20%) than men (6%).[17]

Our own gender-segregated information consists of two sets of data:
(1) gender ratio of the callers
(2) a gender breakdown as per "caller type" that determines whether the caller was calling on someone's behalf or not

Our standard practice is to not assume the gender of someone unless they mention it themselves or if it is explicitly confirmed. Creating a safe space for our callers is a process, and we hope to do more towards creating a truly gender-inclusive and welcoming space. The category of marginalized individuals was added in the second year of the helpline's operations.

Why do we maintain a gender breakdown of our data as per "caller type"? This is because it is important in situations where there is a need to understand the disparity between the caller's gender and the victim's gender. Out of our total number of callers, [number] were categorised under "self", i.e. calling about their own case.

---

[14] Maeve Duggan, "Online Harassment 2017", Pew Research Center, 2017 https://www.pewresearch.org/internet/2017/07/11/online-harassment-2017/
[15] Ibid.
[16] Ibid.
[17] Ibid.

According to our analysis, **57%** of female callers and only 30 % of male callers were calling to complain about their own case. Ten transgender persons reached out to us regarding their own cases as well.

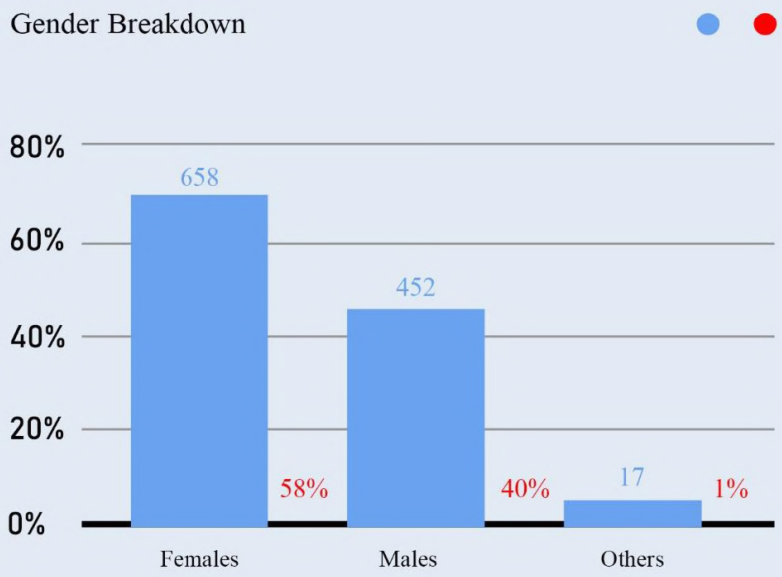
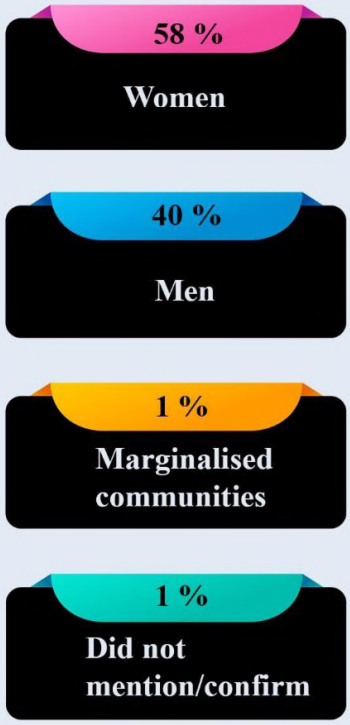


Figure 5: This data is based on the total number of calls (1134) excluding social engineering (WhatsApp hacks) , and not the number of calls attended.
The number of female complainants was 658 and male callers was 452 . A discrepancy of cases exists due to the inability to confirm information given the sensitive nature of certain calls.

Breakdown of the helpline's cases for the past one year is as follows:



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.

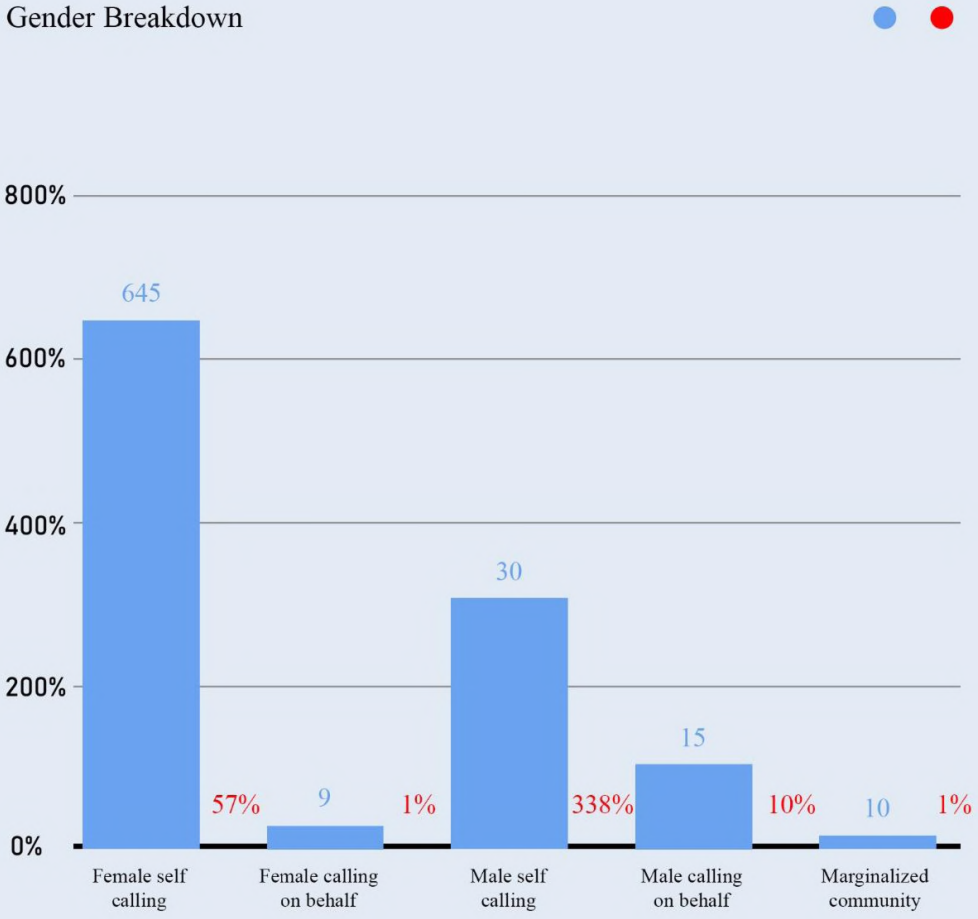


Figure 6: This data is based on the total number of calls excluding social engineering (WhatsApp hacks) (1134), not the number of calls attended. The number of female complainants were and male callers were . A discrepancy of cases exists due to the inability to confirm information given the sensitive nature of certain calls.

Invisibility of marginalised communities

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

Figure 6: This data is based on the total number of individual cases (1960), not the total number of calls.

How do we then explain the slightly higher number of online harassment cases reported by men as compared to women?

This question reveals a limitation in our data set. Unlike the research quoted above by Duggan, we have yet to start classifying our various online harassment cases into explicitly defined categories that are ranked in order of gravity of the crime such as name-calling, physical threats, stalking and sexual harassment. This makes offering an analysis all the more difficult. Yet there are certain observations that the helpline staff has made while speaking to the complainants, such as the fact that some complainants are hesitant to call for themselves. There are a number of factors contributing to this phenomenon. Due to a victim-blaming culture perpetuated by patriarchy in Pakistan, many victims are overwhelmed by a sentiment of shame or a fear of losing out on potential opportunities if they report harassment. Meanwhile, access to means of communication is a serious hindrance in women's reporting of online harassment.[18] According to a study, 37% of women aged between 15 and 65 years are less likely than men in Pakistan to own a mobile phone.[19] As many as 43% of women in the same age group are less likely to use the internet.[20]

---

[18] Haneen Rafi, 'There is a sense of shame attached to reporting harassment', Dawn, August 4, 2018, https://www.dawn.com/news/1424761

[19] "AfterAccess: ICT access and use in Asia and the Global South", AfterAccess, 2018 https://lirneasia.net/wp-content/uploads/2018/11/AfterAccess-Asia-Report-2.0.pdf

[20] Ibid.

In certain cases, complainants who have experienced trauma prefer that someone else speaks on their behalf. In cases like these, either a close friend or family member leads the call. Encouragingly, over the past few quarters, the proportion of complainants calling for themselves has risen. We have observed that this reluctance to report their own experiences becomes a challenge for accessing legal remedy since that requires statements from the victim and in-person reporting in cases of cyber-crime.

In short, research and our observations suggest that the higher number of harassment complaints filed by men can be explained by two main factors: one, lack of access to means of communication for women in Pakistan, and two, patriarchy instilling a reluctance in women to speak out.

c. Types of Cases

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

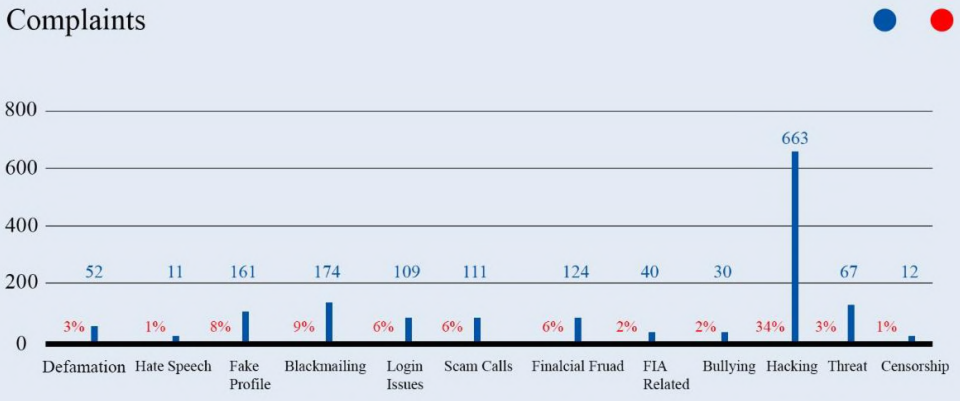


Figure 7: This data is based on the total number of cases (1960), not the number of calls attended. It must be noted that some callers reported more than one type of complaint. The helpline support staff categorised the nature of the complaint as "secondary" and "primary" according to the facts of each individual case--this data shows the top ten types of cases reported to the helpline.

As the chart above shows, a majority of the cases are related to **non-consensual usage of information (NCUI).** These cases involve 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.

The second most common type of complaints pertained to **blackmailing,** which often entails the use of an individual's personal information or psychological manipulation to make threats and demands. Other most commonly reported cases involved **hacking** and **unsolicited contact.**

Notably, in the past two months, 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 involve 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 organisations, ranging from television game shows, Pakistan Army, government departments such as the Benazir Welfare Programme and telecommunication companies.

d. 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 administered by 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 was received from **Sindh (15%).**

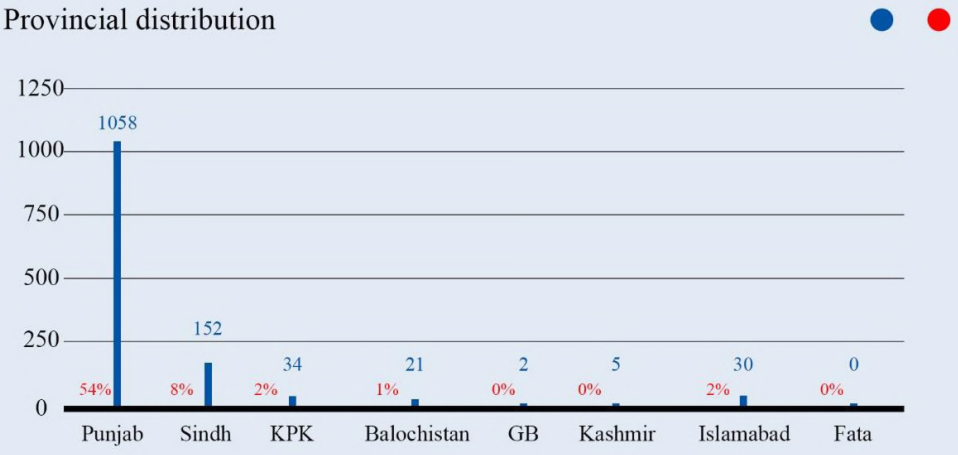


Figure 8: This data is based on the total number of cases (1728), not the number of calls attended. The significant number of missing data is in cases where either it was deemed inappropriate to ask for location data, or when the complainant refused to provide it.

e. (In)accessibility to 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 to the FIA requires the complainant to travel to the NR3C's office and register their case in person to commence legal proceedings. According to our average, **37%** 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. Compared to areas where an NR3C office did not exist, the vast majority of the cases were reported from areas where an office did exist. Only **19%** of the cases were reported from areas where an office of the NR3C 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 NR3C offices in other areas.

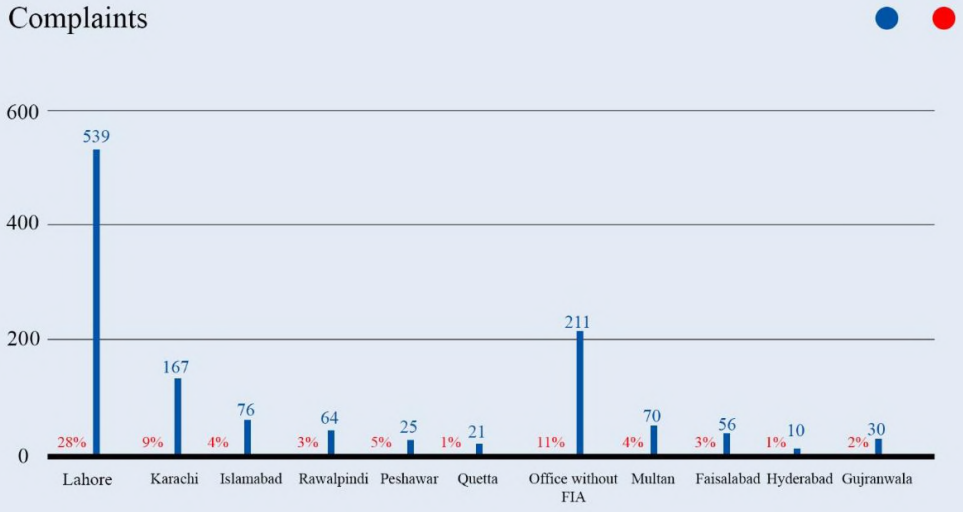


Figure 9: This data is based on the total number of cases (1728), not the number of calls attended.

f. Age Distribution

A majority of our callers (**21%**) were between the ages 21 and 25 years, followed by 26-30-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 **2%** 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 are not receiving support from their legal guardians. Cases become even more complicated in instances where the alleged harasser is also younger than 18.

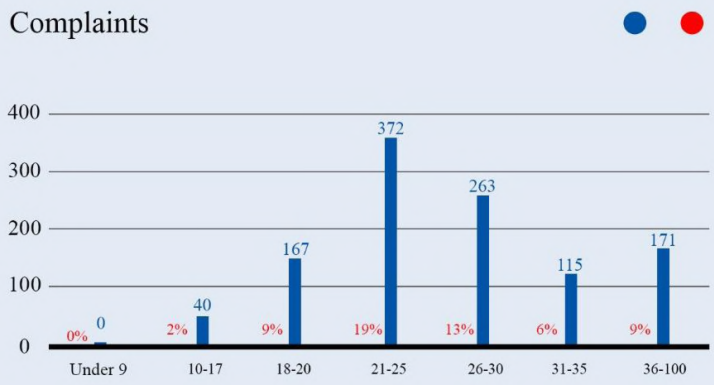


Figure 10: This data is based on individual cases, not the total number of calls

g. 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 (**660** complaints). As many as **29%** of our callers reported experiencing harassment on Facebook.

Recently, there has been an influx of cases regarding **WhatsApp,** with cases rising from 2.6% to 9.5% in the past six months (with the total number of cases rising from 29 to 220).

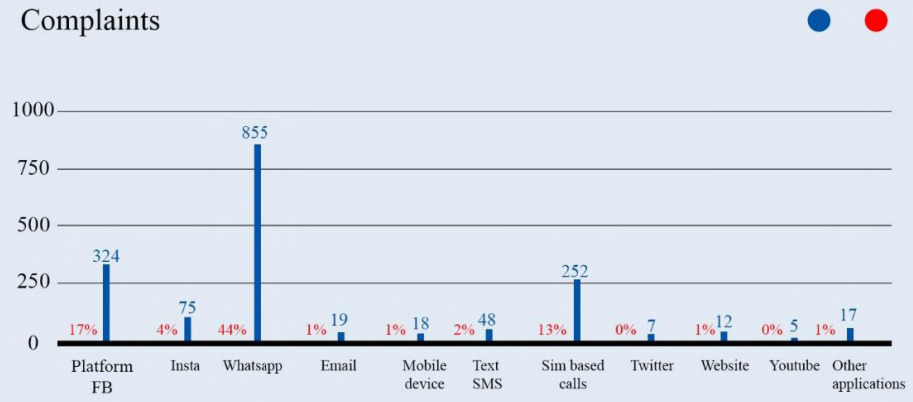


Figure 11: This data is based on individual cases, not the total number of calls.

h. Referrals

DRF is a non-governmental organisation 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 National Response Centre for Cyber Crime (NR3C) of the Federal Investigation Agency (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, **37%** 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. For other cities, we have contacts in the legal fraternity who refer cases effectively in other branches.

In sensitive situations or emergencies that require immediate action from law enforcement agencies or when specialised services are needed, our staff refers the case to other relevant government authorities or NGOs for further assistance such as the PCSW, Rozan and LoBono in Karachi.

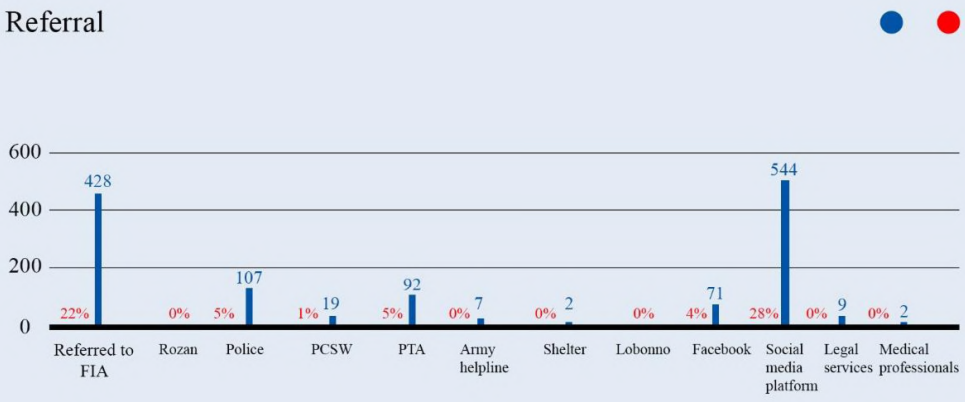


Figure 12: This data is based on the total number of individual cases, not the number of total calls attended.

i. 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 has indicated that they heard about us on social media or through word of mouth. 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.

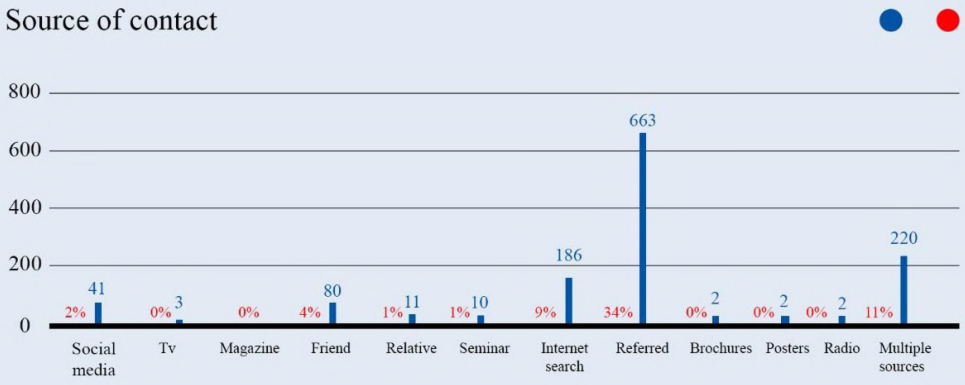


Figure 13: This data is based on individual cases, not the total number of calls.

j. 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 and the options they have under the cybercrime law.

2. Digital security 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:

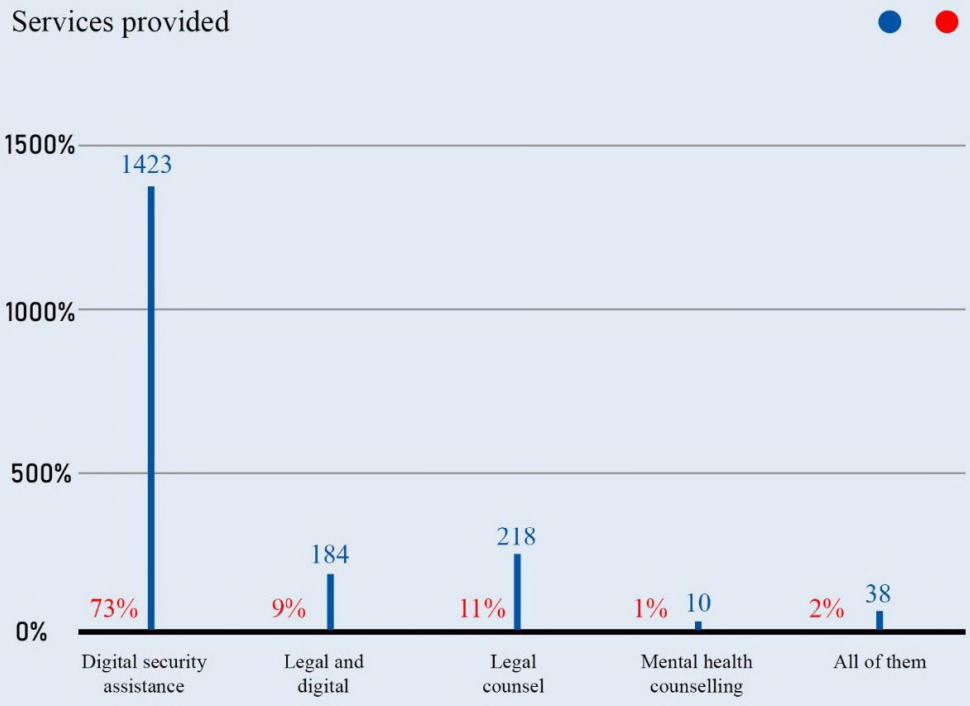


Figure 14: This data is based on individual cases, not the total number of calls.

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.

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.

k. 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 were deemed to experience heightened vulnerability online due to the fact that they belonged to marginalised communities and groups. **Two** such cases were received from members of the marginalised community. Some of these callers were specifically targeted by individuals for personal reasons, while others were victims of harassment online and offline simply because of prejudice against their gender and/or sexuality. It has been observed that members of the vulnerable community are common targets of such hate crimes.

Similarly, we received **two** calls from callers who identified themselves as belonging to religious minority groups. **One** caller who reached out to us was physically disabled. Receiving calls from communities that are stigmatised or marginalised, even though not many, 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 marginalised 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 sensitisation.

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:

. Social engineered attacks/phishing: Every year hackers get more advanced and introduce new phishing strategies to scam and blackmail people. A burgeoning trend we have seen at the helpline is social engineering/phishing attack to hack Whatsapp accounts of people. In this attack hackers trick people by impersonating government officials or game show personnels offering prizes. Once a hacker has 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 as well.

. Mobile wallet/e-cash: Another emerging and worrying trend is Financial fraud and scams through mobile wallets and e-cash accounts are 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 Programme or Jeeto Pakistan TV game show. By the time a victim realises that their account has been hacked, it is usually too late and they have already lost all the money that was there in their account.

It is important to address the gravity and expanse of these problems. We urge users to be mindful 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 harassment is not only inappropriate and immoral but also an unlawful form of discrimination that should be reported. Following are the tips for dealing with the online harassment and reporting it effectively:

1. Seek Support: online harassment and its after effects are difficult to process. Tell supportive and trusted friends, family members , teachers and/or organisations who can give you much-needed support and help needed to process all that has happened. You shouldn't be made to feel alone.

2. Keep The evidence: Keep the abusers 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, however do exercise caution.

3. Do not engage with the harasser/abuser: Don't 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 this person.

4. Exercise your rights: block the person and report them to 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 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 minimise chances of cyberharassment.

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 controlling 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 hence your data vulnerable ,open to misuse. This can lead to potential online violence against you.

5. Targeted ads: Ensure that social media websites cannot personalise 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!

REMEMBER: Cyber-harassment or any form of online violence is never your fault - just like potential theft of your valuable jewelry 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

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

1. Ensure that the6 months report by the FIA, required under section 53 of PECA, is submitted regularly and without delay. In the past, the FIA has failed to submit its report in the first two years of PECA's enactment. So far only only two reports have been submitted by the FIA since 2016.

2. Sensitise society: The government should collaborate with organisations working on gender to conduct gender sensitisation 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 the society's mindset in general. 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 Sensitisation the law enforcers: The government should collaborate with organisations working on gender to conduct gender sensitisation workshops with law enforcement so that staff dealing with complaints of gendered online violence can overcome patriarchal attitudes. DRF has conducted such workshops with the FIA 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, unauthorised use and dissemination of personal information, and manipulation of personal information including photos and videos.

5. Decriminalise defamation laws: Online defamation is criminalised 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 aggreived by online speech against their person can seek alternate remedies under civil defamation laws (that too be safeguards for survivors of sexual violence).

6. Allocate funds for NR3C: DRF urges policy makers to push the government to create more funding for the National Response Centre for Cyber Crime (NR3C), especially in the form of trained women dedicated staff to address online violence against women as well as trained mental health counselors.

7. 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 NR3C. DRF also appreciates the inclusion of civil society groups in the planning stage, which gave the civil society a voice at the table and ensured diverse representation and better decision-making. 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. The Interior Ministry has given approval for 15 new reporting centers to be built across the country, some of which are already operational.[21] According to the FIA's figures, not only have the number of cases increased, the rate of growth of complaints has also grown (complaints rose 20% from 2015 to 2016, while there was a 30% rise from 2016 to 2017). Since the NR3C's Phase 3 proposes to cover the next five years, it means that the increase in resources should neither be limited to meet the current demand nor the current rate of growth. 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 jurisdiction: In many cases where either the accused or the complainant is located outside Pakistan, the NR3C 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 specialised 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.

---

[21] Munawer Azeem, "FIA allowed to open 15 centres to check cybercrime", Dawn, October 3, 2018, https://www.dawn.com/news/1436438.

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 given the mobility issues that women face. Therefore, DRF urges the FIA to invest in the establishment of a digitally secure online portal that citizens could use to file their complaints.

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 NR3C: 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 the NR3C 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 NR3C. 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 out 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 disabled persons: Functioning elevators, ramp for wheelchairs, accessible toilet facilities and in-person assistance in filing applications are minimum requirements that every NR3C 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 NR3C. In certain trials given that challans contain both sections of PECA and PPC, there is often back and forth between different courts and judges. DRF recommends that channels of communication between police stations and cybercrime stations 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 is processed at the local level.

11. Psychological services: DRF urges the FIA to make provision for psychological services at NR3C offices to help complainants deal with the psychological trauma and distress that they experience due to online harassment and violence. All officers at the NR3C, especially those dealing directly with victims, should be trained on how to address trauma. The NR3C should offer a safe space for victims and help them process their trauma in a constructive and safe manner.

12Case 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 sensitisation: Several female complainants who have approached the NR3C have reported being shamed for their choices and discouraged from pursuing cases by officers at the NR3C. 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 33% female 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 behaviour 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 NR3C 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 NR3C to address the needs of litigants/complainants.

16. 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.

17, Collaboration with civil society organisations: 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 NR3C will be in the best interest of victims and will ensure the complainants obtain timely and comprehensive support.

Reporting Mechanism

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 for investigation, 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 case of minors they need to be accompanied by their guardian or older sibling 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.

Cyber Harassment Helpline

0800-39393