POLICY BRIEF

CYBER HARASSMENT HELPLINE

DRF

DigitalRightsFoundation

"KNOW YOUR RIGHTS"

Cyber Harassment and ICTs in Pakistan

The UNWomen fund for Tackling violence against women implemented by Digital Rights Foundation (DRF) in Pakistan was conceived with the aim to ensure access to justice, services and safe spaces for women vulnerable to cyber harassment in the target areas thereby helping to end violence against women in the country.

It is crucial to uphold and preserve the right of women to freedom of expression online and offline while also recognizing the limits set in place by international and national laws in terms of speech that instigates violence or hate

This policy brief delineates the current trends of online harassment, gender-based violence and current laws in Pakistan protecting women and girls from cyber violence and harassment and bringing criminals to justice. It makes recommendations on addressing existing gaps in the adequate dealing of online harassment by various institutions in Pakistan.

Introduction

Harassment is defined in the United Nations policy brief as ' any improper behavior by a person that is directed at and is offensive to, another individual and which the person knew or ought reasonably to have known would be offensive. It comprises objectionable or unacceptable conduct that demeans, belittles or causes personal humiliation or embarrassment to an individual. Mildly offensive comments or behavior can rise to the level of harassment if they are repeated; a single incident can be considered harassment if it is so severe that it has a lasting negative impact on the individual(s) concerned.'[1]

It has many forms viz. Sexual harassment, workplace harassment, harassment in public spaces and cyber harassment.

Cyber harassment is a term used to describe the use of cyberspace to harass, control, manipulate or belittle a target. It affects everyone including women, children, and men but it is more of a gendered issue, as technology-related violence against women has become prevalent, according to the two-year report of DRF's cyber harassment helpline.

---

[1] United, Nations. Policy on the Prevention of Harassment. www.un.org/women watch/osagi/UN_system_policies/(FAO)Policy_on_the_prevention_of_harassment.pdf.

Prevalence and Gender Distribution:

The use of technology-based harassment is not specifically the concern of one gender, however, victims of cyber harassment are more likely to be women when compared to men and children. In Pakistan, 70% of female population experience sexual or physical violence at least once in their lifetime by their intimate partners and 93% of the female population experiences some form of sexual violence in public places.[2] Moreover, child sexual abuse cases in Pakistan have increased from nine cases per day to 12 cases per day in 2018, and an alarming total of 2322 child abuse cases was reported in newspapers in only six months.[3] The complexity of these issues lies on a continuum where offline violence is interlinked with online harassment and should not be viewed independently. Out of the 2302 cases reported to Digital Rights Foundation's Cyber Harassment Helpline between 2016-2018 53% (1225) were by women.[4] Furthermore, data provided by the FIA reports that 90% of the cases reported to the Cyber Crime section of the FIA were women. [5]

The forms of female-targeted-violence include sexual harassment, surveillance, unauthorized use and dissemination of personal information, and manipulation of personal information including images and videos. This form of violence acts as a significant barrier to women's meaningful engagement with the internet. Issues pertaining to cyber harassment include cyberstalking, blackmailing, hacking, doxing, non-consensual usage of information, online stalking, bullying, impersonation, and manipulation of personal data and images. Cyber harassment and blackmailing through the use of and forwarding of private and sensitive information, pictures and videos are becoming more and more common and being reported by women and girls who use the internet in Pakistan. Out of the cases reported to cyber harassment helpline, 14 % (323) were of non-consensual use of information and 14% (323) were of blackmailing.[6]

Another form of harassment faced by women in Pakistan is sexualized violence with their nude or doctored pictures circulated on social media platforms without their consent. This information is also used to create fake profiles on social media that lead to reputational and psychological harm. Digital Rights Foundation's cyber harassment helpline received 4% (92) cases of non-consensual sharing of intimate images and videos. [7]

---

[2] Kazi, Mudaser. "'93% Of Pakistani Women Experience Sexual Violence'." The Express Tribune, The Express Tribune, 8 Mar. 2017, tribune.com.pk/story/1348833/93-pakistani-women-experience-sexual-violence/.

[3] Wasif, Sehrish. "Child Sexual Abuse Cases Surge in 2018: Report." The Express Tribune, The Express Tribune, 31 Aug. 2018, tribune.com.pk/story/1791931/1-child-sexual-abuse-cases-surge-2018-report/.

[4] Digital Rights, Foundation. Cyber Harassment Helpline Two Year Report. digitalrightsfoundation.pk/wp-content/uploads/2019/01/Booklet-Helpline.pdf.

[5] Imran, Warda. "Of Consent and Copyrights: Women Lodge 90% Complaints in FIA Cybercrime Circle." The Express Tribune, The Express Tribune, 9 Apr. 2018, tribune.com.pk/story/1681027/1-consent-copyrights-women-lodge-90-complaints-fia-cybercrime-circle/.

[6] Digital Rights, Foundation. Cyber Harassment Helpline Two Year Report. digitalrightsfoundation.pk/wp-content/uploads/2019/01/Booklet-Helpline.pdf.

Prevention and Protection:

Prevention may not always avert the onset of cyber harassment, however, it is always better to be knowledgeable about precautions while making use of technology. The first step to prevention is awareness and education. It has been observed that awareness regarding digital spaces is quite low, both in terms of digital security practices as well as the laws governing them. According to our research, only **28%** of women in our sessions were aware of the Prevention of Electronic Crimes Act.[8] Lack of awareness is one of the primary reasons for the under-reporting of online harassment. It is imperative to be aware of cyber crimes and to seek professional aid from law enforcement personnel or concerned agencies such as the FIA in Pakistan when any cybercrime occurs. It is also crucial that law enforcement agencies be well-informed and supportive of the victims. Social networking platforms and law enforcement strategies can play a massive role in preventing incidents of cyber harassment.

Current Law in Pakistan:

Pakistan's legal landscape regarding cybercrime is in its nascent stage and is evolving at a grim pace, especially given the leaps and bounds of development that have been made in the arena of crimes that can be committed using the internet as a tool.

The Electronic Transactions Ordinance came about in 2002 brought in provisions, specifically s.36, that dealt with the violation of privacy information and has been the main section used by law enforcement agencies for issues relating to privacy violations. This section has been repealed by the Prevention of Electronic Crimes Act in August 2016.

The first piece of legislation with regards to criminalizing acts committed online has been the Prevention of Electronic Crimes Act (PECA) which was passed in 2016. Prior to this, a Prevention of Electronic Crimes Ordinance was passed in 2009 which lapsed due to non-confirmation by the Parliament.

[7] Digital Rights, Foundation. Cyber Harassment Helpline Two Year Report. digitalrightsfoundation.pk/wp-content/uploads/2019/01/Booklet-Helpline.pdf.

[8] Sanayah Malik, "Measuring Pakistani Women's Experience of Online Violence", 2017, http://digitalrightsfoundation.pk/wp-content/uploads/2017/05/Hamara-Internet-Online-Harassment-Report.pdf.

The pivotal sections of PECA include:

s. 20 Offenses against the dignity of a natural person which criminalizes the exhibition, display or transmission of any information through any information system which they know to be false and using which, harms the reputation or privacy of that person.

s. 21 Offenses against the modesty of a natural person criminalize the manipulation of pictures of a natural person with sexually explicit images, intimidation or enticement of a natural person to engage in sexually explicit acts through an information system.

s. 22 Child pornography criminalizes the transmission of material depicting a minor or a person appearing to be a minor engaging in or realistic pictures of sexually explicit conduct or discloses the identity of the minor.

s. 24 Cyberstalking criminalizes monitoring, following, spying of a person despite a clear and repeated desire not to do so. It also covers taking a photograph or making a video of a person without their consent, in a manner that harms that person.

A number of other acts have also been penalized under the ambit of PECA, which also seeks to criminalize the writing and transmission of malicious code, spamming, electronic fraud and hate speech. It also contains a provision, **s. 32** (Retention of traffic data), which directs telecom companies to ensure retention of consumer data for the past year, at a minimum which can be accessed through a court-issued warrant by LEAs and their officials.

Recommendations

1. PECA Rules: The government is under an obligation to ensure that the forthcoming PECA Rules are compatible with principles of human rights—particularly the right to freedom of expression, the right to privacy and protection of minorities.

2. Greater resource allocation: To amount to extreme and DRF urges the concerned government departments to increase grants allocated to the FIA.

3. Mechanism to deal with cases in foreign jurisdictions: 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.

4. Regular reporting and performance review of the FIA: DRF urges the FIA to fulfill its obligations u/s 53 and submits bi-annual reports, assessments and reviews on FIA's performance. These reports should also be made available online.

5. Sex-disaggregated data: The FIA is requested to produce data regarding the number of online harassment cases and the number of cases registered by women. These figures should be public and will allow for better policy-making and allocation of resources.

6. Creation of a separate desk for online harassment within the NR3C: Given the specialized 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 u/s 21 and 24 of PECA.

7. Rapid Response Cell: A rapid response cell that is operational 24/7 should be established in addition to the regular operations of the NR3C.

8. Privacy and Confidentiality: The FIA is thus urged to develop clear, accessible and publicly available Standard Operating Procedures (SOPs) on privacy, confidentiality, and protection of evidentiary data and identity of the complaints.

9. 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.

10. Coordination with other departments: 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 be registered, investigated and prosecuted.

11. Empower local police to process cases of online harassment: While cases under PECA are under the jurisdiction of

11. Empower local police to process cases of online harassment: While cases under PECA are under 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.

12. 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.

13. 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.

14. Gender sensitization: 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 organizations be included and allowed to assist in developing these trainings. Furthermore, gender sensitization does not only mean taking into account the specific needs of women but different genders such as non-binary and transgender.

15. Check on the performance of investigators and prosecutors: Complainants should be able to register concerns and complaints regarding their assigned officers to a senior presiding officer to 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.

16. Greater technical expertise: DRF recommends that measures be taken to capacitate them to not only meet current trends in cybercrime but also keep abreast with developments 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 to litigants/-complainants.

17. 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.

18. Collaboration with civil society organizations: DRF recommends more public-private partnerships by the government to ensure that the public institutions work collaboratively with civil society and academia to complement each other's work. A mutually beneficial 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.

DigitalRightsFoundation

"KNOW YOUR RIGHTS"

www.digitalrightsfoundation.pk

digitalrightsfoundation

digitalrightspk

digitalrightsfoundation