Human Rights Council: Submission on online violence against women

Digital Rights Foundation, Pakistan

1. This report will explore the laws and institutions that are in place within Pakistan to deal with issues of online violence against women. Facts and figures will be used to gauge the extent of the problem and its nature, relying on data provided by the government, law enforcement agencies and collected by DRF. A legal analysis of the legislation will be accompanied by an appraisal of the implementation of the laws and the functioning of institutions on the ground. Reported judgments will also be analysed to gauge jurisprudence (interpretations of the laws) as well as legal principles developed by local courts. The purpose of the report will not only be to analyse the existing structures, but to situate them within the lived experiences of women facing online violence. This experience will be elucidated through case studies as well as analysis done by DRF's cyber harassment helpline team.
2. We hope that this submission will provide a sufficient overview of the regulatory and social landscape in Pakistan with relation to online violence against women.

A. About: Digital Rights Foundation

3. Digital Rights Foundation (DRF) is a non-government non-profit organization registered legally in Pakistan in 2013 under the Societies Registration Act 1860. DRF focuses on ICTs to support human rights, inclusiveness, democratic processes and digital governance through advocacy, research and direct services. The organization works on issues of privacy, surveillance, free speech, political participation, digital security, gender & tech and online harassment.

B. Introduction: Online Violence in the Pakistani Context

4. The use of Information and Communications Technologies (ICTs) has experienced an exponential growth in Pakistan, however there is still a long way to go. Pakistan's internet penetration was 18% in mid-2016, as per ITU's ICT Facts and Figures.[1] With the popularisation of mobile internet (3G and 4G), it is expected that this 18% will rise.
5. Access to these technologies is not equal; factors such as geographical location, economic status, gender and disability determine the level of access. Pakistan's digital gender gap is among the highest in the world, as "men are twice as likely as women to own a mobile phone in Pakistan" as only 64% of women owned mobile phones, while 81% Pakistani males owned cellular devices in 2015.[2]
6. Even when women do have access to technologies, they are subjected to online violence that is markedly different from the experience of men. Online violence against women includes an array of behaviour, such as and not limited to, blackmailing, non-consensual access and distribution of personal information, impersonation, defamation, threats and

[1] International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2015," http://bit.ly/1cblxxY

[2] Measuring the Information Society Report 2016, *International Telecommunications Union*, http://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2016/MISR2016-w4.pdf

gender-based bullying. While there are several motivations behind online violence, gender is the primary one and women are often the main target of it.

7. According to data collected by the Digital Rights Foundation's cyber harassment helpline, an overwhelming majority of victims of online harassment are women.[3] There are no official figures on this subject however. Despite demands by Senators, gender disaggregated data is not provided by the Pakistani government. It has been reported that out of the 3027 cybercrime cases reported to the Federal Investigation Agency (FIA) during August 2014 - August 2015, 45% involved electronic violence against women.[4]

a. Experiences of Pakistani Women

8. Online is often trivialised and harms associated with it are not considered tangible enough. While the harassment should be taken seriously in and of itself, its real life consequences are quite evident and worrying. Online harassment can lead to suicide,[5] physical assault,[6] emotional distress[7], women leaving jobs and online spaces. Online harassment cannot be dismissed as merely because it occurs in a "virtual" space.
9. In our "*Measuring Pakistani Women's Experiences of Online Violence: A Quantitative Research Study on Online Gender-Based Harassment in Pakistan*", 70% of the surveyed women posited that they were afraid of their pictures being posted online. Furthermore 40% of the women reported that they had been stalked or harassed through messaging apps. These numbers, though based on a sample size of 1400 women, are representative of the experiences that women have when navigating online spaces.[8]

b. Types of Online Violence in Pakistan

10. There is a serious dearth of data in terms of online harassment in Pakistan, even when it comes to reported cases. The Federal Investigation Agency (FIA), tasked with investigating cybercrime and registering cases of online violence, have repeatedly failed to submit a report to parliament regarding their operations as required under section 53 of the *Prevention of Electronic Crimes Act 2016*. Other organisations have attempted to fill in the gaps, according to data collected by DRF's Helpline, the main types of harassment experienced by Pakistani women are blackmailing (20%), impersonation (21%), non-consensual information (19%) and unsolicited messages (12%).

---

[3] 63% women self-reported harassment, whereas 107 of the 153 men were calling on behalf of women; "Cyber Harassment Helpline: Six Month Report", *Digital Rights Foundation*, July 2017, https://digitalrightsfoundation.pk/wp-content/uploads/2017/07/Cyber-Harassment-Helpline-Six-Month-Report.pdf

[4] Rafia Zakaria, "The web and women's harassment", *Dawn*, October 12, 2016, https://www.dawn.com/news/1289530

[5] Nighat Dad and Shmyla Khan, "Naila Rind killed herself because Pakistan's cybercrime laws failed her", *Dawn*, January 7, 2017, https://www.dawn.com/news/1306976

[6] "Two Girls, Mother Killed Over Family Video," *Dawn*, June 25, 2014, http://www.dawn.com/news/1020576/two-girls-mother-killed-over-family-video; "Pakistani Women Shot in 'Honour Killings,'" *BBC*, http://www.bbc.co.uk/news/world-asia-23084689

[7] Jannat Fazal, "Online harassment: a retrospective review of records", *Médecins Sans Frontières (MSF) Scientific Day South Asia 2017*, https://f1000research.com/slides/6-785

[8] "Measuring Pakistani Women's Experiences of Online Violence: A Quantitative Research Study on Online Gender-Based Harassment in Pakistan", Digital Rights Foundation, May, 2017, http://digitalrightsfoundation.pk/wp-content/uploads/2017/05/Hamara-Internet-Online-Harassment-Report.pdf

c. Case Studies

11. Given the lack of quantifiable data, it would be instructive to look at some prominent cases of online violence against women to understand its manifestations in the context of Pakistan. DRF's cyber harassment helpline has also highlighted certain case studies of harassment in its report.
12. In 2016, Qandeel Baloch, a social media star, was murdered by her own brother as a direct result of her online content. He deemed that her online activity brought dishonour on the family.[9] This case explicitly highlighted the continuum of violence from online spaces to offline as well. Given the high profile nature of the case, it was both influential in terms of awareness raising as well as sparking a divisive debate online. Encouragingly, the state became a party/complainant to the case to ensure that no pardon, under Islamic law, was possible in this case.[10]
13. In 2012, one of the first cases of honour killings and digital technology was reported in the Kohistan video case. In this incident, a video of a private gathering was leaked showing four women dancing in the presence of three men. All the individuals shown in the video were murdered by their families in the name of honour. While the Supreme Court of Pakistan took up the case via its *Suo Moto* jurisdiction, the case was side-lined when a fact-finding team visiting the area were actively misled by locals and it was concluded that the women were still alive. Eventually, it was discovered that the investigation team was shown four different women. The case was reopened in 2016 following doubts raised by some members of the commission.[11] This case highlights the ineptitude to investigate and provide timely justice in cases of online violence against women, even at the highest level of the judiciary.

C. Legislative Models in Pakistan

a. A History of Legislation around Online Harassment

14. The prevailing law dealing with online harassment is the *Prevention of Electronic Crimes Act 2016* (which will be discussed in detail later on). Pakistan has been slow to enact legislation regarding digital spaces and several offline laws are being used to regulate these spaces.
15. Several other laws have started to reflect online crimes. The *Punjab Protection of Women against Violence Act 2016* defines violence as "any offence committed against the human body of the aggrieved person including abetment of an offence, domestic violence, sexual violence, psychological abuse, economic abuse, stalking or a cybercrime".[12] Acknowledgment of online violence by the law is an important step towards a viable solution. However the phrase "cybercrime" as a stand-alone offence with no further

[9] Imran Gabol and Taser Subhani, "Qandeel Baloch murdered by brother in Multan: police", *Dawn*, July 16, 2016, https://www.dawn.com/news/1271213
[10] Imran Gabol, "State becomes complainant in Qandeel's murder, bars family from pardoning killers", *Dawn*, July 18, 2016, https://www.dawn.com/news/1271588
[11] 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
[12] Punjab Protection of Women against Violence Act 2016, Section 2(r).

explanation if a reflection of bad legal draftsmanship and the lack of understanding of internet spaces that exists.

16. Furthermore, several laws that precede the digital era are also applied to address online harassment. The *Pakistan Penal Code* has sections for harassment[13] and defamation[14]. The *Telegraph Act 1885* also addresses harassment using communication systems in section 25-D.[15] However these laws are clearly outdated and do not anticipate the specificities that inhere in online harassment.
17. The *Electronic Crimes Ordinance 2002 (ETO)* has been used to address online harassment, is still being used for cases registered prior to August 2016. The ETO is not specficially a criminal legislation as it was passed "to recognize and facilitate documents, records, information, communications and transactions in electronic form, and to provide for the accreditation of certification service providers."[16] However, Chapter 8 of the Ordinance did deal with creation of certain offences, such as "violation of privacy of information" (section 36)[17] and "damage to information system" (section 37).[18] These sections are employed by the National Response Centre for Cyber Crime (NR3C) to tackle online harassment. Since the passage of PECA, these sections have been superseded through section 54 which specifically repeals these two provisions.

---

[13] Section 509: "insulting modesty or causing sexual harassment": "(i) Intending to insult the modesty of any woman, utters any word, makes any sound or gesture, or exhibits any object, intending that such word or sound shall be heard, or that such gesture or object shall be seen, by such woman, or intrudes upon the privacy of such woman; (ii) conducts sexual advances, or demands sexual favours or uses written or verbal communication or physical conduct of a sexual nature which intends to annoy, insult, intimidate or threaten the other person or commits such acts at the premises of work place, or makes submission to such conduct either explicitly or implicitly a term or condition of an individual's employment, or makes submission to or rejection of such conduct by an individual a basis for employment decision affecting such individual, or retaliates because of rejection of such behavior, or conducts such behaviour with the intention of unreasonably interfering with an individual's work performance or creating an intimidating, hostile, or offensive working environment."

[14] Section 499: "Defamation: Whoever by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said except in the cases hereinafter excepted, to defame that person".

[15] Section 25-D: Penalty for causing annoyance, etc: "Any person, including a Telegraph Officer, who uses any telephone, public or private, for causing annoyance or intimidation to any person, whether a subscriber or not, or for obnoxious calls shall, without prejudice to any other action which the Telegraph Authority is competent to make under this Act, be punishable with imprisonment for a term which may extend to three years, or with fine, or with both."

[16] Preamble of Electronic Transactions Ordinance, 2002.

[17] "Any person who gains or attempts to gain access to any information system with or without intent to acquire the information contained therein or to gain knowledge of such information, whether or not he is aware of the nature or contents of such information, when he is not authorised to gain access, as aforesaid, shall be guilty of an offence under this Ordinance punishable with either description of a term not exceeding seven years, or fine which may extend to one million rupees, or with both."

[18] "(1) Any person who does or attempts to do any act with intent to alter, modify, delete, remove, generate, transmit or store any information through or in any information system knowingly that he is not authorised to do any of the foregoing, shall be guilty of an offence under this Ordinance. (2) Any person who does or attempts to do any act with intent to impair the operation of, or prevent or hinder access to, any information contained in any information system, knowingly that he is not authorised to do any of the foregoing, shall be guilty of an offence under this Ordinance. (3) The offences under sub-section (1) and (2) of this section will be punishable with either description of a term not exceeding seven years or fine which may extend to one million rupees, or with both."

b. Prevention of Electronic Crimes Act 2016 (PECA)

18. The *Prevention of Electronic Crimes Act (PECA)* was passed in August, 2016 amid criticism from civil society and digital rights organisations.[19] The vaguely-worded nature of the law meant that it could, and ultimately was, be used to silence opposition and clamp down on free speech.[20]
19. Nevertheless, PECA has several sections that pertain to online harassment and protection of women in online spaces. Section 21 of PECA ("*offences against modesty of a natural person and minor*") address the exploitation of sexual imagery without consent:

> "Whoever intentionally and publicly exhibits or displays or transmits any information which,
> (a) superimposes a photograph of the face of a natural person over any sexually explicit image or video; or (b) includes a photograph or a video of a natural person in sexually explicit conduct; or (c) intimidates a natural person with a sexual act, or any sexually explicit image or video of a natural person; or (d) cultivates, entices or induces a natural person to engage in a sexually explicit act, through an information system to harm a natural person or his reputation, or to take revenge, or to create hatred or to blackmail".[21]

20. Section 21 regulates sexually explicit content, be it digital photographs or videos, taken or distributed without consent. This also covers sexually explicit images or videos that are used to intimidate or blackmail someone. However given that it exclusively deals with sexually explicit content, it can overlook other material that is often used to blackmail women. In certain cases, an otherwise innocuous picture or conversation can be used to intimidate women. Furthermore, there are no guidelines as to what constitutes "sexually explicit" under this section.
21. Another provision that is often used to address online harassment is section 20 of PECA. While not explicitly designed to deal with online harassment, several kinds of online harassment are captured under this section. The inclusion of criminal defamation in the law has its problems in terms of human rights law,[22] it does cover the reputational harm that inheres in cases of online harassment:

> "20. Offences against dignity of a natural person:
> (1) Whoever intentionally and publicly exhibits or displays or transmits any information through any information system, which he knows to be false, and

[19] See: "Pakistan: New Cybercrime Bill Threatens the Rights to Privacy and Free Expression", http://digitalrightsfoundation.pk/wp-content/uploads/2015/04/Pakistan-Cybercrime-Joint-Analysis_20-April-2015.pdf
[20] "Free speech in danger", Dawn, May 23, 2017, https://www.dawn.com/news/1334762
[21] Section 21 of the Prevention of Electronic Crimes Act (2016).
[22] Article 19, known for its advocacy around freedom of expression, terms criminal defamation as "disproportionate", "Criminal defamation", Article 19, https://www.article19.org/pages/en/criminal-defamation.html

> intimidates or harms the reputation or privacy of a natural person."

22. Another provision of PECA dealing with online harassment is section 24: "*cyberstalking*". The definition of "cyberstalking" in PECA is vague and criminalises a wide range of activity that might not otherwise be considered a crime. This includes:

> "Section 24: Cyberstalking:
> (1) A person commits the offence of cyber stalking who, with the intent to coerce or intimidate or harass any person, uses information system, information system network, the internet, website, electronic mail or any other similar means of communication to:
> (a) follow a person or contacts or attempts to contact such person to foster personal interaction repeatedly despite a clear indication of disinterest by such person;
> (b) monitor the use by a person of the internet, electronic mail, text message or any other form of electronic communication;
> (c) watch or spy upon a person in a manner that results in fear of violence or serious alarm or distress, in the mind of such person; or
> (d) take a photograph or make a video of any person and displays or distributes it without his consent in a manner that harms a person."

23. Section 24 suffers from many of the pitfalls as the other sections. Phrases like "clear indication of disinterest" are not clearly defined and have the potential of placing the onus on women. Furthermore, since there has not been a lot of litigation around PECA these are interpretations are merely conjecture.

D. Institutional Response to Online Violence

a. Law Enforcement Agencies

24. While there are several issues with the existing legislation, its implementation and the institutions tasked with the implementation create several hurdles for women and other victims of online violence.
25. The National Response Center for Cyber Crime (NR3C) of the Federal Investigation Agency (FIA) is the designated authority to conduct investigations under PECA.[23] The NR3C is severely understaffed and under-resourced, which hampers its ability to effectively deal with the scale of the problem at hand. The offices of the NR3C are limited to only major cities within Pakistan (Quetta, Peshawar, Lahore, Karachi, Rawalpindi and Islamabad). The lack of geographical access of these offices is a real concern, as it means that women living outside these select cities will have to leave their

[23] Section 29 of the Prevention of Electronic Crimes Act 2016.

area of residence to simply file a complaint—which has the effect of particularly disadvantaging women in remote areas. While the NR3C does have an online complaint mechanism in place, it still adheres to a paper-based system and thus a formal complaint requires at least one visit to the office to start one's application.

26. Furthermore, the NR3C offices are criminally understaffed. For instance, the office in Lahore only has 13 investigators (field officers), which includes 2 assistant directors, 4 inspectors and 5 Sub-Inspectors.[24] The Deputy Director of the Lahore branch admits that these "13 men have to cover territorial jurisdiction within 32 districts within Punjab with only one available official vehicle."[25] These officials are tasked with handling a plethora of cybercrimes cases, not just online harassment. The NR3C has received 4030 complaints just between January and June 2017. The sheer volume of complaints compared to the amount of resources available means that it is riddled with a severe backlog and institutional delays.
27. The procedures of the NR3C also raise several concerns in terms of evidentiary requirements, gender-sensitisation and confidentiality. While it is understandable that the standards of proof in criminal law are adhered to, the evidentiary requirements do not take into account the unique nature of online violence. In the instance of website-based harassment, the FIA requires an active IP address so as to trace and verify the identity of the perpetrator. In cases where sensitive information is leaked online, women are torn between keeping material online to act as traceable evidence and taking it down immediately to minimize the harm that it can cause. The PECA requires that the same standards laid down under the *Qanoon-e-Shahadat, l984*, which precedes the internet and does not take its special procedures in mind when tackling such cases.
28. The verification systems of the NR3C are often too slow and bureaucratic to address more urgent cases. The nature of certain cases of online violence is such that copies can readily be made and shared instantly, which can cause irreparable reputational harm within a very short span of time. There is a minimum lag of 2 weeks in between filing an application with the NR3C and being assigned an Investigative Officer. In cases that require urgent attention, there is no special procedure in place.
29. Another concern is that there are no Standard Operating Procedures (SOPs) in place to ensure data privacy and confidentiality of cases. Complainants have often noticed that evidentiary files, often containing sensitive and personal information, are lying around at the office without any data security mechanisms in place. This concern is a real one, as DRF's cyber harassment helpline has received several cases where data breach on part of the NR3C has led to additional harassment of the complainants.
30. The lack of gender-sensitisation of the NR3C staff and its public interface in terms of filing of complaints is a deterrent for several women. Women do not feel comfortable sharing details of past relationships and sexually explicit content with male officers. Several of the offices of the NR3C do not have female officers, and even the ones that do are limited to one and two in number. Furthermore, DRF's helpline has received complaints regarding victim-blaming from female IOs as well. Several callers have expressed reluctance to visit the NR3C offices because of their environment.

---

[24] Shahid Aslam, "Dealing with cyber crime needs more resources", *The News*, October 23, 2017, https://www.thenews.com.pk/print/238972-Dealing-withcyber-crime-needs-more-resources
[25] *Ibid*, 25.

b. Courts

31. The "cybercrime" courts under PECA were notified by the Ministry of Information Technology in March, 2017 and trials under the law began shortly afterwards through powers given to it under section 44 of PECA. Under the notification, judges have been designated to try cybercrime cases. 2 judges have been designated in Balochistan, 2 in Khyber Pakhtunkhwa, 4 in Punjab and 27 in Sindh.
32. Since the notifications, a heavy sentence of 12 years imprisonment for blackmailing a woman online was passed.[26] Given the volume of cases that are expected to come through, concerns have been raised regarding the number of judges. Furthermore, no details have been provided regarding the training provided to these judges especially with reference to online violence against women. No reported judgments have come through from these judges so it is difficult to access their effectiveness with reference to online violence against women.

c. The Pakistan Telecommunications Authority

33. The Pakistan Telecommunications Authority (PTA) is tasked with regulating content online. It is authorised, under section 37, to take down content that pertains to offences under PECA or the criteria laid out under its mandate as follows:

> "Section 37. Unlawful online content:
> l) The Authority shall have the power to remove or lock or issue directions for removal or blocking of access to an information through any information system if it considers it necessary in the interest of the glory of Islam or the integrity, security or defence of Pakistan or any part thereof, public order, decency or morality, or in relation to contempt of court or commission or incitement of an offence under this Act."

34. This section has been criticised by human rights groups for being too vague and having the potential to be used as a pretext for online censorship. Furthermore, despite its wide ambit, the PTA lacks the capacity to act on individual cases and is notoriously non-transparent in its content removal processes.[27] DRF's report "*Case Study: Experiences of Online Harassment in Pakistan*,"[28] highlights certain instances of online violence where there has been institutional failure to provide appropriate relief. One of the cases highlights the injustice that can occur in the absence of a Mutual Legal Assistance Treaty

---

[26] Izhar Ullah, "Peshawar man gets 12-year jail term for blackmailing woman on Facebook", *The Express Tribune*, July 11, 2017, https://tribune.com.pk/story/1455517/man-peshawar-gets-12-years-creating-womans-fake-facebook-profile-blackmailing/.

[27] When a satirical website, "Khabaristan Times", was blocked in Pakistan no notice to served to its owners or reasons given. "Satire website Khabaristan Times blocked in Pakistan," *Dawn*, January 30, 2017, https://www.dawn.com/news/1311656.

[28] "Case Study: Experiences of Online Harassment in Pakistan", Digital Rights Fondation, November, 2017, https://digitalrightsfoundation.pk/wp-content/uploads/2017/11/Case-Study-Experiences-of-Online-Harassment-in-Pakistan.pdf.

(MLAT) to allow for data sharing and content removal. Cases are most likely to be abandoned by the NR3C or PTA if social media companies are non-compliant.

d. Service Providers

35. Internet Service Providers (ISPs) are guaranteed limited liability under section 38 of PECA.[29] The section ensures that ISPs will not be held liable for activity on their servers unless it can be proven that they had "actual knowledge" and "wilful intent" to "proactively and positively participate". The burden of proof for "wilful intent" and "actual knowledge" shall lie with the alleger. This insulates service providers from effectively incurring any liability for online harassment on their servers and means that law enforcement agencies cannot hold ISPs responsible for online harassment that occurs on their servers.
36. Nevertheless, ISPs do not have an absolute free hand, they are required to remove material that is objectionable under section 37 of PECA. The licence of ISPs requires them to comply with the orders and directives of the PTA. Failure to comply with directives can result in revocation of the licence. However, ISPs are immune from liability from individual citizens, such as women pressing claims of online harassment.
37. Social media companies based in foreign jurisdictions are not subject to Pakistani laws and are not accountable to citizens who use their services. Most of these companies have their own "community guidelines" and have wide discretion in accepting court orders from other jurisdictions, such as Pakistan. Pakistan does not have a Mutual Legal Assistance Treaty (MLAT) with the US or any European country—which is where these social media companies are often situated—which makes data sharing and content removal extremely difficult.

---

[29] "Section 38. Limitation of liability of service providers: (1) No service provider shall be subject to any civil or criminal liability, unless it is established that the service provider had specific actual knowledge and willful intent to proactively and positively participate, and not merely through omission or failure to act, and thereby facilitated, aided or abetted the use by any person of any information system, service, application, online platform or telecommunication system maintained, controlled or managed by the service provider in connection with a contravention of this Act or rules made thereunder or any other law for the time being in force:
Provided that the burden to prove that a service provider had specific actual knowledge, and wilful intent to proactively and positively participate in any act that gave rise to any civil or criminal liability shall be upon the person alleging such facts and no interim or final orders, or directions shall be issued with respect to a service provider by any investigation agency or Court unless such facts have so been proved and determined:
Provided further that such allegation and its proof shall clearly identify with specificity the content, material or other aspect with respect to which civil or criminal liability is claimed including but not limited to unique identifiers such as the Account Identification (Account ID), Uniform Resource Locator (URL), Top Level Domain (TLD), Internet Protocol Addresses (IP Addresses), or other unique identifier and clearly state the statutory provision and basis of the claim.
(2) No service provider shall under any circumstance be liable under this Act, rules made thereunder or any other law for maintaining and making available the provision of their service in good faith.
(3) No service provider shall be subject to any civil or criminal liability as a result of informing a subscriber, user or end-users affected by any claim, notice or exercise of any power under this Act, rules made thereunder or any other law".

E. Legal Jurisprudence

38. There are very few reported judgments interpreting the law regarding online harassment. Case law and jurisprudence are a very important component of implementing the law and providing relief to victims of online harassment—a bad precedent can discourage other women from reporting and result in injustice in individual cases.
39. One of the few reported judgments involving online harassment is *Muhammad Munir v. the State, PLD 2017 Pesh 10*. The defendant created a fake Facebook profile in the name of the complainant and uploaded her picture without her consent. The judgment concerns bail proceedings, however section 36 of the ETO and its application are reasoned judgment.
40. In another bail-related judgment, *Yasir Lateef v. the State, 2016 PCrLJ 1916*, the defendant had hacked into the complainant's Facebook account and uploaded her personal pictures online without her consent. The court condemned the actions in the harshest possible terms: "obnoxious and filthy in nature". The court acknowledged the reputational harm by pointing out the fact that she had been "disgraced in the eyes of general public and her family".
41. The Baluchistan High Court in *Mustafa Ali v. the State, 2014 PCrLJ 1464*, dealt with a case where a fake profile was made of a female complainant. The profile was used to send obscene and threatening messages, while using her pictures without her consent. The judgment deals primarily with the technicalities of bail and does not discuss the crime itself. Again, given the fact that there is little analysis in these judgments, there not room for much substantive comment.
42. In *Waqas Ahmed Siddiqui v. the State, 2012 YLR 320*, the court held that it could not decide prima facie whether section 36 of the ETO applied to the facts of the case, and thus bail was granted and the question was left to the trial (no reported judgment of the trial could be found). The facts involved a former husband uploading objectionable pictures of the complainant without her consent and disseminating those pictures among her friends and family. The defendant also threatened to upload an objectionable video online. The court was conflicted whether the language of the ETO, which dealt with "damage to information system" applied to this particular set of facts. It does not come as a surprise that there was confusion whether a complex case of online harassment such as this would fall under the purview of the law that was designed to deal with transactions and admissibility of electronic evidence.

F. Conclusion

43. While legislative developments have taken place to address online violence against women, it remains to be seen whether these developments correspond with effective and gender-sensitive implementation at an institutional level. The issues identified throughout this report are based on real experiences of women and aim to provide an insight into the problems that occur when a woman experiences online violence and tries to address it using the various mechanisms at her disposal.