Kathmandu School of Law Review (KSLR),
Volume 7, Issue 1, 2019, pp. 85-99
https://doi.org/10.46985/10.46985/kslr.v7i1.1202

Cyber Violence against Women and Girls in Nepal

Poonam Kaphle[*]

Abstract

Violence against women and girls in the virtual space is the emerging concern in the global context. With the growth in use of technologies and the internet, cyberspace has been an equally vulnerable area for violence targeted against women and girls as that of public space. With the rise in numbers of existing forms of violence, conceptual clarification on the dynamics of cyber based violence is a major need of time. Moreover, it has been an issue of immediate concern to assess the current situation of Nepal for the identification of policy and legal remedies. The present study attempts to identify the pattern and forms of cyber based violence against women and girls in Nepal through the study of registered cases in Cyber Crime Unit of Nepal Police and also, reflect on the nature of cases adjudicated by the Kathmandu District Court. In the absence of a clear legal framework and technical knowhow of cyber based crimes, law enforcement authorities have been constantly facing challenges to critically intervene the process and secure safe spaces for women and girls in use of technology. The study concludes that a coherent approach from all concerned stakeholders is required in defining a clear legal and policy framework to ensure use of information and technology as a tool of gender empowerment, thus addressing the crimes committed through cyberspace.

1. Introduction

Recent years have seen an important shift in the pattern of crime commission in our society and global world. The concept of cyberspace and internet has unlocked numerous opportunities for the people in the online world to connect with each other and develop technology; however, it has equally generated a growing concern in the parallel universe of social media to induce cybercrimes. There is not any rigid or distinctive definition of cybercrime which is said to be the first challenge of dealing with it.[1] European legal framework on cybercrime states that cybercrimes are of different types ranging from offences where information systems are targets of crime and where the computers are used as instruments for the commission of crime.[2] Broadly, cybercrimes have been defined as offences which relate to any illegal behavior

[*] Poonam Kaphle is a Legal Officer at the Ministry of Education, Science and Technology. She is Assistant Professor at Kathmandu School of Law. She can be reached at poonamkaphle@gmail.com.

[1] Francesco Calderoni, 'The European legal framework on cybercrime: striving for an effective implementation', *Crime Law Soc Change*, 2010 available at https://doi.org/10.1007/s10611-010-9261-6, accessed on 22 September 2018.

[2] Ibid.

committed by means of, or in relation to, a computer system or network which typically cluster around categories such as i) offences against the confidentiality, integrity and availability of computer data and systems; ii) computer-related offences; iii) content-related offences; iv) offences related to infringements of copyright and related rights.[3] According to Wall, cybercrime illustrates a range of harmful activities and behaviors which broadly includes four categories:

- **Cyber-trespass:** It is the crossing of cyber boundaries into spaces of other people's computer systems, where rights of ownership or title have already been established, and causing damage, e.g. hacking and virus distribution.

  Cyber-deceptions and thefts: It includes different types of acquisitive harm that can take place within cyberspace. At one level are the more traditional patterns of theft, such as the fraudulent use of credit cards and (cyber) cash, but there is also a current concern regarding the increasing potential for the raiding of online bank accounts as e-banking becomes more popular.

- **Cyber-pornography:** It means the breaching of laws on obscenity and decency.

- **Cyber-violence:** It denotes the violent impact of the cyber activities of others upon individual, social or political grouping. Whilst such activities do not have to have a direct manifestation, the victim nevertheless feels the violence of the act and can bear long-term psychological scars as a consequence. The activities referred here range from cyber-stalking and hate-speech to tech-talk[4]

A report based on the studies carried out in 10 countries, United Nations (the, "**UN**") estimates that 95% of aggressive behavior, harassment, abusive language and denigrating images in online spaces are aimed at women and come from partners or former male partners.[5] Issues of abuse and violence against women and girls ("**VAWG**") existed before the internet, of course, but the new medium has made such attacks easier and more frequent.

Cyber VAWG, often synonymously used as technology related VAWG, exists on a continuum with physical violence, and both problems are byproducts of a society that is inherently unequal for women.[6] What make technology related VAWG distinct are the medium and the mode by which the violence is committed i.e. through virtual and digital spaces, through cyberspace, through Information and Communications Technology ("**ICT**"). It is the distinct characteristic of technology related VAWG that

---

3 United Nations, 'Cybercrime', *United Nations Office on Drugs and Crime*, available at https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html, accessed on 22 September 2018.

4 Majid Yar, 'Cybercrime and Society', May 22 2013, Google Books, p. 10 available at https://books.google.com.np/books?hl=en&lr=&id=Ye4QAAAAQBAJ&oi=fnd&pg=PP2&ots=cQyjyYU3pC&sig=T6R_sTQ4NNI9lkzTYyNRjVeUyWs&redir_esc=y#v=onepage&q&f=false, accessed on 22 September 2018.

5 Association for Progressive Communications, 'How Technology is Being Used to Perpetrate Violence Against Women-And to Fight it', Association for Progressive Communications, available at https://www.apc.org/sites/default/files/How%20Technology%20is%20Being%20Used%20to%20Perpetrate%20Violence%20Against%20Women%20%E2%80%93%20And%20to%20Fight%20it_1.pdf, accessed on 24 April 2018.

6 UN Women, 'Urgent action needed to combat online violence against women and girls, says new UN report', 12 October 2015, UN WOMEN, available at https://www.unwomen.org/en/news/stories/2015/9/cyber-violence-report-press-release, accessed on 24 April, 2018.

sets it apart from other forms of VAWG. The manner of its commission through virtual and digital spaces has made technology related VAWG an emerging phenomenon. Technology, in recent times, has had the potential to facilitate the prosecution of crimes in cases by generating digital evidences. Yet, at the same time, with the growing threat of cyberspace based crimes, the victimization of women within a sphere that is increasingly important and ungoverned makes it cause for concern.

Cyber violence is just as damaging to women as physical violence is, according to a new UN report entitled '*Combating Online Violence Against Women & Girls: A Worldwide Wake-Up Call*' released by the United Nations Broadband Commission which also warns women are growing even more vulnerable to cyber violence as more and more regions gain internet access.[7] The UN defines violence against women as 'any act of gender-based violence that results in, or is likely to result in, physical, sexual or psychological harm or suffering to women, including threats of such acts'.[8] The report notes that cyber violence is an extension of that definition including acts like trolling, hacking, spamming, and harassment. Further, the report also argues that 'cyber touch is recognized as equally as harmful as physical touch', suggesting that online harassment might be just as lethal as domestic violence or sexual abuse.

This paper seeks to explore the concept and situation of cyber violence especially targeted against women and girls as one of the categories of cybercrime in context of Nepal. The increasing manifestation of the violence against women and girls in the digital world in Nepal, thus, requires a serious study on its nature and forms of violence trending as well as in identification of policy and legal remedies, gaps and challenges for successful prosecution of these cases. Moreover, given the nature of the crimes committed in cyberspace, they are ungoverned and difficult to frame strategies in lack of gender disaggregated data on prevalence of cybercrime against individuals.

In this milieu, the article aims at setting out incredibly important issues to locate the new forms of internet mediated violence specially targeted against women and girls. Further, the article attempts to reflect the trends of violence that women and girls are facing in online world, legal and policy framework addressing the cyber violence against women and girls, issues and concerns related therewith. Further, to the paper will shed light on the existing challenges for the law enforcement authorities in securing prosecution of cases of violence against women and girls in cyberspace. The article has been prepared in consultation with the police personnel handling the cases and complaints of cybercrimes in Metropolitan Police Office and Metropolitan Crime Division, Kathmandu, Central Bureau of Investigation, Crime Investigation Department of Nepal Police Headquarter and district government attorneys of Kathmandu District Court.

---

7 Charlotte Alter, 'U.N. Says Cyber Violence Is Equivalent to Physical Violence Against Women', TIME (September 2015) available at https://time.com/4049106/un-cyber-violence-physical-violence/, accessed on 24 April 2018.

8 UN Women, 'Urgent action needed to combat online violence against women and girls, says new UN report', 12 October 2015, UN WOMEN, available at https://www.unwomen.org/en/news/stories/2015/9/cyber-violence-report-press-release, accessed on 24 April, 2018.

2. Dynamics of Violence against Women and Girls in Cyberspace

Globally, acts of cybercrime show a broad distribution across financial-driven acts, and computer-content related acts, as well as acts against the confidentiality, integrity and accessibility of computer systems. There are various forms of cyber VAWG, including, but not limited to, cyber stalking, non-consensual pornography (or 'revenge porn'), gender-based slurs and harassment, 'slut-shaming', unsolicited pornography, 'sextortion', rape and death threats, 'doxing', and electronically enabled trafficking. Cyber violence is not a separate phenomenon to 'real world' violence, as it often follows the same patterns as offline violence.[9] Cyber VAWG includes hate speech (publishing a blasphemous libel), hacking (intercepting private communications), identity theft, online stalking (criminal harassment) and uttering threats. It can entail convincing a target to end their lives (instigating/encouraging suicide or advocating genocide).[10] The internet is also a space for other forms of violence against girls and women including trafficking and sex trade. Not only does commercialized sex on the internet drive the demand for the sex industry overall, it also allows traffickers to use the legal aspects of commercial sex on the internet as a cover for illegal activities. Some of the main uses of the internet by traffickers include advertising sex, soliciting victims on social media, exchanging money through online money transfer services and organizing many of the logistical operations involved in transporting victims.[11]

According to the VAW learning network, there are six broad categories that encompass forms of cyber VAWG.[12]

a. **Hacking**: It is the use of technology to gain illegal or unauthorized access to systems or resources for the purpose of acquiring personal information, altering or modifying information, or slandering and denigrating the victim and/or VAWG organizations. e.g., violation of passwords and controlling computer functions, such as freezing the computer or logging off the user.

b. **Impersonation**: It is the use of technology to assume the identity of the victim or someone else in order to access private information, embarrass or shame the victim, contact the victim, or create fraudulent identity documents; e.g., sending offensive emails from victim's email account; calling victim from unknown number to avoid call being blocked.

c. **Surveillance/Tracking**: It is the use of technology to stalk and monitor a victim's activities and behaviors either in real-time or historically; eg, GPS tracking

9 European Institute for Gender Equality, 'Cyber violence against women and girls', 23 June 2017, European Institute for Gender Equality, available at https://eige.europa.eu/publications/cyber-violence-against-women-and-girls, accessed on 7 April 2018.

10 UN Broadband Commission for Digital Development Working Group on Broadband and Gender, 'Cyber Violence against Women and Girls', 2015, UN Broadband Commission for Digital Development Working Group on Broadband and Gender, available at https://en.unesco.org/sites/default/files/genderreport2015final.pdf, accessed on 7 April 2018.

11 Ibid.

12 Centre for Research & Education on Violence against Women & Children, 'Understanding Technology-Related Violence Against Women: Types of Violence and Women's Experiences', 2013, Centre for Research & Education on Violence against Women & Children, available at http://www.vawlearningnetwork.ca/our-work/briefs/briefpdfs/LB-06.pdf, accessed on 9 April 2018.

via mobile phone; tracking keystrokes to recreate victim/survivor's activities on computer.

d. **Harassment/Spamming**: It is the use of technology to continuously contact, annoy, threaten, and/or scare the victim. This is ongoing behaviour and not one isolated incident; e.g., persistent mobile calls/ texts; filling up voicemail with messages so no one else can leave a message.

e. **Recruitment**: It is the use of technology to lure potential victims into violent situations; e.g., fraudulent postings and advertisements (dating sites; employment opportunities); traffickers using chat rooms, message boards, and websites to communicate/advertise.

f. **Malicious Distribution**: It is the use of technology to manipulate and distribute defamatory and illegal materials related to the victim and/or VAWG organizations; e.g., threatening to or leaking intimate photos/video; using technology as a propaganda tool to promote violence against women.

g. **Hate Speech**: It denotes such speech which attacks a person, or a group being based on certain attributes such as gender, race, religion, ethnicity, class, ideology, sexual orientation and similar others. These hate speeches are shared through online platforms documented in videos creating a large number of audiences. In absence of a generous balance between hate speech and freedom of expression, social harmony and individual freedom, dignity are always at stake. Contrarily, hate speech is used to offend individuals and attract momentary publicity.

In addition, the proliferation of online violence means cyber VAWG now has its own set of terminology; 'revenge porn' consists of an individual posting either intimate photographs or intimate videos of another individual online with the aim of publicly shaming and humiliating that person, and even inflicting real damage on the target's 'real-world' life.

Five distinctive characteristics that distinguish cyber VAWG[13] includes the aspects of:

- Anonymity: abusive person can remain unknown to victim/ survivor
- Action at a Distance: abuse can be done without physical contact and from anywhere
- Automation: abusive actions using technologies require less time and effort
- Accessibility: the variety and affordability of many technologies make them readily accessible to perpetrators

3. Propagation and Perpetuity: texts and images multiply and exist for a long time or indefinitely Current Experiences of Cyber Violence against Women and Girls in Nepal

[13] Association for Progressive Communications, 'Voices from digital spaces: Technology related violence against women', December 2011, Association for Progressive Communications, available at https://www.genderit.org/sites/default/files/apcwnsp_mdg3advocacypaper_full_2011_en_0_0.pdf, accessed on 9 April 2018.

Digital spaces are crucial areas for women to participate in given their importance for work, politics and social engagement, which means, it is imperative for women to advocate for the right to communicate, including on the internet, to create gender-just online spaces.[14] Nepal has not been immune to increased cybercrime either. The expansion of mobile phone service has helped to shoot up internet users nowadays. Introduced by a private sector in 1996 in Nepal, the internet has been gradually encompassing people from diverse professions.

Similarly, the rate of reporting complaints of crime in cyberspace through social media is alarming these days as revealed by the statistics of concerned authorities. As many as 560 cases of cybercrime have been registered in the first six months of the 2017/2018 fiscal year. There were a total of 830 complaints related to cybercrime in last fiscal year as stated by the Metropolitan Crime Division in Teku.[15] Of the total cybercrime related complaints registered, cases have been lodged against 11 such incidents.[16]According to Metropolitan Police Crime Division, 221 complaints regarding crimes on social media sites have been filed in the fiscal year 2015/16. However, this number has increased to 769 complaints in the fiscal year 2016/17. According to Kathmandu District Court, total 50 cases have been filed in fiscal year 2015/16 out of which 19 cases of harassment of women were reported. Similarly, total 27 cases have been filed in fiscal year 2016/17 out of which 14 cases of harassment were reported.[17]

Statistics from the Metropolitan Police Crime Division ("**MPCD**"), Kathmandu also paints a similar picture. According to the MPCD, there has been an escalation in the cases registered at the MPCD of women troubled through social media. There were 91 cases filed in FY 2013-14, 221 in 2014-15 and a giant leap of 769 cases in the fiscal year 201516. Nepal Police defines cybercrime as harassment through social networking sites, email threats, illegal data access, ATM breaches, server hacks, obscene websites, copyright and phishing (an attempt to obtain sensitive information such as user names, passwords, money by disguising as a trustworthy entity in an electronic communication).[18] Legal experts find it worrisome that not all women who have been victimized seek legal remedy. An official working in Nepali judicial service said "At times we have to deal with critical cases which cannot be disclosed. Cybercrimes, especially the cases of harassment against women, are the most sensitive cases where the victim does not want to disclose identity even to the lawyers and keep away from the court procedures".[19]

---

14 Women's Rights Programme, 'The impacts of ICTs on women's public and political life', January 2013, Association for Progressive Communications, available at https://www.apc.org/sites/default/files/WG%20final%20paper_word.pdf , accessed on 7 April, 2018.

15 Rastriya Samachar Samiti, '560 cases of cybercrime registered in six months', The Himalayan Times (February 2017) available at https://thehimalayantimes.com/nepal/560-cases-cybercrime-registered/, accessed on 7 April 2018.

16 Ibid.

17 Bikalpa Dhakal, 'Situation of Cybercrimes in Nepal', ICT FRAME available at https://ictframe.com/situation-of-cybercrimes-in-nepal-bikalpa-dhakal/, accessed on 8 April 2018.

18 Samipa Khanal, 'Cyber crimes of harassing women on rise', THE KATHMANDU POST (April 2017) available at http://kathmandupost.ekantipur.com/news/2017-04-07/cyber-crimes-of-harassing-women-on-rise.html, accessed on 7 April 2018.

19 Ibid.

Analysing 45 cases of cybercrimes, filed within 8 months of period from July 2017 to Feb 2018[2020], targeted against women and girls, under investigation of the Central Bureau of Statistics, social media such as Facebook and Messenger have been used as a medium in 95.56% of cases. Among them 45% cyber crimes committed were aimed at character defamation of women and girls by posting fake information regarding their character, demoralizing their confidence to participate in any of their public life whereas in 55% of the cases, women and girls were harassed by posting obscene videos and photos, texting indecent messages with image manipulation and sharing the same to wider range of online audiences especially to their family members. This included the tendency of forceful recording of indecent videos and images and thereby threatening to distribute it to the family and relatives. In 96% to 97% of cases of such nature, the acts committed were of non-consensual nature while in 3% to 4% of such cases, consents were obtained either with threat, due pressure or with fraudulent allurement of marriage. Above 90% cases of these natures, cyber-crime and abuse of profile in online media has been observed as a ploy used by partners to mentally harass women and girls, which has been witnessed both as a process and outcome in an abusive relationship. Thus, in 90% of cases, the victim knew the harasser who was either an ex-partner, friend, relative or online acquaintance who posed the threat by disclosing the personal videos made consensually. In some cases, the specific intention was only to cause fear and apprehension for some supposed humiliation. Driven by the intention of mental harassment and undermining the position of women, the majority of women in relationships are being victimized of abusive behaviours through cyber stalking whereby their profiles are being regularly stalked and misused by their partner.

Similarly, a research conducted by a team of police personnel from Nepal Police and government attorneys on 30 cases filed at Kathmandu District Court as an offence under Electronic Transaction Act 2063 B.S. showed that.

- Suspects were convicted in 53% cases and in 47% cases, suspects were acquitted due to hostile witness, hostile victims and inability of the victim to submit relevant evidence against the perpetrators of cybercrime to establish the offence.
- One of the cases was interpreted as an offence committed under the Public (Crime and Punishment) Act, 2027.
- 90% of the crimes committed in cyberspace were targeted against women and girls.
- Facebook was used as a social media to commit cybercrime in 60% cases, while in 40% crimes were committed through mobile messages and emails.
- 90% cases filed in Kathmandu District Court were filed on charge of posting indecent videos, obscene images, threatening messages and posts with fake details in social media against women and girls.
- In 65% of cases, either victim or accused belonged to Kathmandu valley whereas in 35% cases, the victim or accused belonged to regions out of Kathmandu valley.

[20] Central Bureau of Statistics for July 2017-February 2018.

In 25% cases, the victim did not appear before the Court to submit their statement at the Court, while in 10% cases; the victims were hostile during the hearing. Thus, the studies on cases of cybercrimes under observation of court as well as investigations made by the law enforcement authorities showed that the technology-related violence documented use of social media, particularly Facebook as the common platform used by abusers. One of the common categories of technology mediated violence experienced by women and girls in Nepal included the creation of fake profiles in social media like Facebook and thereby sharing inappropriate content, fake information, indecent manipulated photos and videos. In addition, undignified, demeaning and threatening messages were posted to women and girls through social media for the purpose of revenge, harassment, character defamation and blackmailing. Also, in some cases, such offences were committed for the extortion of money. Sharing of the indecent photos to the family members, relatives and friends of the victims through hacking of profiles or home addresses of the women and girls in social media formed the usual category of the online violence. Furthermore, gender based hate speech (targeted against women and girls), hacking of online profile, impersonation, stalking and malicious distribution of the photos and information were cybercrimes occurring repetitively against women and girls experienced in Nepal as noted by one of police personal handling the complaints of Cybercrime at Metropolitan Crime Division Kathmandu.

1. Policy and Legal Context

The Constitution of Nepal embodies the provisions of fundamental human rights in its Part 3 which forms the major basis for ensuring right of access to justice to women and seek remedies of violence against women. Article 38 (3) of the Constitution spells out the rights of women where no woman shall be subjected to physical, mental, sexual, psychological or other form of violence or exploitation on grounds of religion, social, cultural tradition, practice or on any other grounds. Such acts are punishable by law, and the victim has the right to obtain compensation in accordance with law. Article 28, relating to the right to privacy, asserts on the privacy of any person, his or her residence, property, document, data, correspondence and matters relating to his or her character shallot be, except in accordance with law, inviolable. Similarly, rights relating to freedom of opinion and expression, in Article 17 (2) (a) in its proviso provides that nothing shall be deemed to prevent the making of an Act to impose reasonable restriction on any act which may be contrary to public decency or morality. Further, Article 19(1) of the Constitution also has its relevance with the cyber violence as it provides right to communication stating that no publication and broadcasting or dissemination or printing of any news item, editorial, feature article or other reading, audio and audio-visual material through any means whatsoever including electronic publication, broadcasting and printing shall be censored. However, the proviso clause does provide for reasonable restriction on any act which may be contrary to public decency and morality.

The only relevant law for computer related offences is the Electronic Transactions Act 2063 BS. ("**ETA**") and Electronic Transaction Rules 2064 BS. in Nepal. The ETA, as stated in its preamble, is framed for authentication and regularization of the

recognition, validity, integrity and reliability of generation, production, processing, storage, and communication and transmission system of electronic records by making the transactions to be carried out by means of electronic data exchange or by any other means of electronic communications, reliable and secured.[21] In addition, the Act aims to address and control the acts of unauthorized use of electronic records or of making alteration in such records through the illegal manner.[22]

The ETA has limited its areas of concern and addresses only issues relating to computer related crimes, electronic records, digital signatures, digital certificates, their uses and standards to be met by the government. Analysing the contents of the ETA, it seems as though the ETA had been produced as a legal tool to address more of the crimes related with information and communication technology rather than cybercrimes targeted against individuals such as women and girls. The provision of Section 47 of ETA thus seems to visualize and confine itself in computer related crimes such as publication of illegal material, regulation of transactions made through electronic media and internet, issues of public morality, spreading hate or jealousy intended to jeopardize the harmonious relationship among people of various castes and communities. It is therefore, in lack of specific provisions, any of the offences reported by women relating to their experiences in cyberspace were repeatedly interpreted and dealt under Section 47 which formed the core provision for punishing the offence of publication of illegal materials in electronic form. Thus, whatever the acts are committed against women and girls in online platforms and social media like Facebook, Messenger, Whatsapp etc., all of them are being vaguely defined as 'computer related crimes' under Section 47 of ETA 2063. The provision though, was confined to the fact, that if any person publishes or displays any material in the electronic media including computer, internet which are prohibited to publish or display by the prevailing law or which may be contrary to the public morality or decent behaviour or any types of materials which may spread hate or jealousy against anyone, it was also used to take account of any nature of cases of violence against women in cyber space irrespective of their *modus operandi* and gravity.

Analysing the element of *actus reus* as articulated in Sec 47 of ETA 2063, the acts of 'hate', 'jealousy', 'unnecessary trouble', 'act contrary to public morality and decent behaviour' constitute computer related crimes which are vague, ambiguous, imprecise and subject to open interpretation. The provision therefore fails to internalize the whole new levels of cybercrimes and their severity occurring against women and girls in social media. Due to lack of separate comprehensive cyber laws, attorneys are under legal compulsion to prosecute every kind of such offenses under Sec 47 of ETA relating it with computer crimes. In many cases, it is the police investigation report that guides the government attorneys for prosecution of cases. Inadequacy of the knowledge on conceptual and technical aspect of cyber laws, its content and objectives, there is a little room for both the investigating and prosecuting authorities to critically intervene the procedure so as to establish the offence, punish culprits as per the intensity of the harm caused and to secure justice for the victims.

[21] Electronic Transaction Act, 2008 (Bidhutiya Karobaar Ain, 2063), preamble 1st recital.

[22] Ibid, preamble 2nd recital.

It was only after a recent amendment introduced by '*An Act to amend some Nepal Acts for maintaining gender equality and ending of gender-based violence, 2072 BS*.', the tendency of violence against women in online spaces were recognized to some extent by the Act. However, the amendment does not seem appealing to address the trending issues of violence against women in cyberspaces. It is because the amendment in its literal interpretation seems to fail in recognition of the various dynamics and seriousness of cybercrimes occurring and impacting lives of women and girls. It only states that '*the act of harassing and causing unnecessary trouble against women, or act of defamation or insult of women*' shall be punishable with a fine not exceeding one hundred thousand rupees or with imprisonment not exceeding five years or with both.

In some cases, Sec 2(c1)[23] of Some Public (Crime and Punishment) Act, 2027 BS (1970 AD.) are referred to prosecute cases in which obscene materials are published, however, the provision in this Act is silent on what constitutes the intensity of an act to make it obscene. Additionally, it is not clear as to which nature of acts should be prosecuted under this Act and how it should be different than publishing an indecent obscene video in social media. This is due to the lack of a separate detailed law on cybercrime against individuals.

Similarly, Sec 76 of the ETA asserts on the right of compensation to be recovered from the offender by any person if any loss or damage has been caused by the reason of offences committed under the ETA. However, due to the lack of recognition of all categories of violence against women occurring in cyberspaces in the Act, it seems quite impossible for women victims to produce a reasonable claim for the loss they have suffered mentally and economically in many cases. In addition, due to the nature of anonymity of perpetrators in cybercrimes against women and girls, the situation of access to justice in crimes of such nature seems to be much more complicated and far away from reality.

Moreover, in absence of establishment of the Information Technology Tribunal as envisioned in Sec 60 by the ETA 2063, a procedural barrier for access to legal remedies has been created in prosecution and suit of cybercrimes occurring against women and girls. The Kathmandu District Court has been looking into cybercrime cases as per the Clause 60(5) of the Act which states that any of the District Courts could be authorized to start the initial proceedings and settle the cybercrime-related cases until the IT Tribunal was formed.[24] The decision made by Nepal Government on 2064/12/25 to refer cases of electronic transaction to Kathmandu District Court as the judicial authority has even narrowed the scope of prosecution of cybercrimes against women and girls.

In comparison to the laws enacted, the National Information and Communication Technology Policy, 2015 AD. attempts to uphold the women's right approach and gives

[23] It reads: "To print or publish any obscene materials by using obscene language or by any word or picture which denotes obscene meaning; or to exhibit or sell or distribute such obscene publication in public place other than the purpose of public health or health science;"

[24] National, 'Supreme Court directive to form cyber crime tribunal', (June 2015) available at https://kathmandupost.com/national/2015/06/03/supreme-court-directive-to-form-cyber-crime-tribunal, accessed on 3 July 2015.

the impression of being gender sensitive in its provisions as it foresees the necessity of framing specific measures to promote the use of ICT to change gender norms, prevent gender-based violence as well as report incidents of gender- based violence. Similarly, the policy of 2015 also emphasizes on taking steps to secure full and comprehensive implementation of Electronic Transaction Act with required amendments in the legal and regulatory framework to allow for effective investigation and prosecution of cyber related crimes.[25]

Commitments have also been observed from the Ministry *of Women, Children and Social Welfare as, their Annual Progress Report 2072/73 BS*. states that now a Gender Violence Elimination Fund established by the Government of Nepal for the remedy, consultation, legal remedy and re-establishment of women made victims of violence. The government has also formed the Gender *Violence Elimination Fund (Operation) Regulation, 2067 BS*. for the mobilization of the amount in the fund. However, the question whether this mechanism has internalized the technology-based violence against women within its working mandate is still an unrequited issue.

To refer to international standards, General Recommendation No. 35 of Convention on the Elimination of all forms of Discrimination Against Women ("**CEDAW**") on Violence against Women in its paragraph 20 has laid down an obligation on the part of States in recognition of the contemporary forms of gender based violence against women occurring in the internet and digital spaces.[26]This has equally been forwarded as a serious matter of concern by a report of the Secretary General in an '*In-depth study on all forms of violence against women*' in 61st session of the UN General Assembly.[27] It states:

> 'Forms and manifestations of violence against women vary depending on the specific social, economic, cultural and politic al context. Some forms of violence may grow in importance while others diminish as societies undergo demographic changes, economic restructuring and social and cultural shifts. For example, new technologies may generate new forms of violence, such as Internet or mobile telephone stalking. Consequently, no list of forms of violence against women can be exhaustive. States must acknowledge the evolving nature of violence against women and respond to new forms as they are recognized.'

In 2013, the outcome document for the Commission on the Status of Women's 57th session, for the first time, included the issue of technology and violence, calling for

25 National Information and Communication Technology Policy, 2015 AD.

26 Paragraph 20 of the General Recommendation No. 35 states: 'Gender-based violence against women occurs in all spaces and spheres of human interaction, whether public or private. These include the family, the community, the public spaces, the workplace, leisure, politics, sport, health services, educational settings and their redefinition through technology-mediated environments, such as contemporary forms of violence occurring in the Internet and digital spaces. In all these settings, gender-based violence against women can result from acts or omissions of State or non-State actors, acting territorially or extraterritorially, including extraterritorial military action of States.'

27 Report of the Secretary-General, 'In-depth study of all forms of violence against women', United Nations, available at http://www.un.org/womenwatch/daw/vaw/violenceagainstwomenstudydoc.pdf, accessed on 28 July 2018.

states to:

> 'Support the development and use of ICT and social media as a resource for the empowerment of women and girls, including access to information on the prevention of and response to violence against women and girls; and develop mechanisms to combat the use of ICT and social media to perpetrate violence against women and girls, including the criminal misuse of ICT for sexual harassment, sexual exploitation, child pornography and trafficking in women and girls, and emerging forms of violence such as cyber stalking, cyber bullying and privacy violations that compromise women's and girls' safety'.[28]

Earlier this year the *UN Working Group on Discrimination against Women in Law and Public Life* also highlighted technology and violence against women in their first thematic report. The report recommends that States should support women's equal participation in political and public life through ICTs, including by: increasing women's digital literacy, particularly among marginalized women; ensuring gender-responsiveness in the promotion and protection of human rights on the Internet; improving women's access to the global governance of ICTs.[29]

2. Issues and Concerns

The number of individuals using the scientific equipment and technology in their daily life has been constantly increasing. A data revealed by the recent Management Information system ("**MIS**") report from Nepal Telecom Authority ("**NTA**") states that internet penetration rate is nearly 63% as of Kartik 2074 is in Nepal which is a large number considering Nepal being an underdeveloped country.[30]If we compare this figure with the literacy rate of Nepal according to the CBS report, 2011, it is just 3% more i.e. 66%. Availability of smart phones at an affordable rate these days and the availability of network in the rural areas can also be considered as one of the major reasons for the high percentage of internet penetration in Nepal.[31]The increased acquaintances with internet, computer and smart gadgets among youths in one hand has connected them closer to global trends, exposure to social media and online platforms, however it has equally increased the risk of abusing the same to drive them towards cybercrimes. In this scenario, the risk of committing crime using these technologies is therefore unavoidable and is in need of immediate concern.

---

28 'Agreed conclusions on the elimination and prevention of all forms of violence against women and girls', United Nations, available at http://www.un.org/womenwatch/daw/csw/csw57/CSW57_Agreed_Conclusions_(CSW_report_excerpt).pdf, accessed on 30 July 2018.

29 Human Rights Council, 'Report of the Working Group on the issue of discrimination against women in law and in practice', 19 April 2013, Human Rights Council, available at https://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.50_EN.pdf, accessed on 9 April 2018.

30 MIS Report (Oct 2017-Nov 2017), Nepal Telecommunication Authority, Year XIV, Issue: 108, vol.156, p. 4.

31 Bidushee Koirala, 'According to NTA, the internet penetration in Nepal has reached 63%', 5 February 2018, Gadgetbyte Nepal, available at https://www.gadgetbytenepal.com/internet-penetration-nepal/, accessed on 28 July 2018.

Increment of new forms of violence against women and girls emerging in cyber space, though having a different *modus operandi*, its inherent roots lies on the concept of gender inequality prevailing in our society. As an emerging form of VAW it is a significant barrier to women's and girls' ability to take advantage of the opportunities that ICTs provide for the full realization of women's human rights and development.[32]It is observed that women's opportunity to exploit the potential of ICTs is conditioned by many factors in our society and is related to gender-based discrimination and power relations. Gender based cultural attitude of our society is one among them. Most importantly, the fact of technology mediated harassment and cyber violence is a lesser known issue and women and girls are being the most vulnerable groups due to the inadequacy of digital literacy.

The nature of the cybercrime in itself is a unique criminal act. Criminals committing crime against women and girls in cyberspace have opportunities to use numerous techniques of electronic media, internet and networks enabling them to go anonymous and destroy digital evidence. Unlike traditional crimes, perpetrators of cybercrimes commit crime in the virtual space of the online world and tackling such acts is largely a matter of resource and capacity. Thus, it is obvious that human resources involved in investigation and prosecution should be armed with the latest technological advancement made so far in the online world so as to locate these virtual natures of crimes and criminals. As stated by Police Personnel of Metropolitan Police range and Metropolitan Crime Division, investigating authorities in Nepal lack updated technological infrastructures to assist in tracing the illegal transactions and abuse of social media to harm the dignity of an individual.

The manifestation of cyber violence against women and girls is also a relatively new phenomenon whereby a vacuum created in the legal regime has disabled law enforcement authorities to react deeply into this matter. Equally complex for law enforcement authorities is the vagueness of the legal provision, inadequate policy framework, lack of technical knowhow among the investigation authorities and insufficient resources to locate digital evidence. Further, the inadequacies of available national legal framework, lack of knowledge of cybercrime offences specially targeted against women and girls, issues regarding jurisdiction, access to complaint mechanism and admissibility of electronic evidences are some critical areas of discussion that need a coherent approach in responding to the increasing nature of cybercrimes.

Moreover, narrowed perceptions among people regarding violence against women often tend to equate every such act with the physical violence because of which virtual violence is not given much concern. Contrary to the fact, the enduring harm suffered by women in cybercrime exceeds in its impact much more than physical violence resulting in psychological stress, mental violence and in some cases violation of economic rights too. Analysing the rapid development made in the communication and information technology, it seems that it is easier to detect the criminal act and intent. However, this is equally true that use of complicated technological methods make it difficult for the investigation authorities, in their limited capacities and resources, to access the actual

[32] Jan Moolman, 'Violence against women online', 2013, Global Information Society Watch, p. 38 available at https://www.giswatch.org/sites/default/files/gisw13_chapters.pdf, accessed on 28 July 2018.

perpetrators and electronic evidence against them.

Another pressing issue is that we can hardly rely on the statistics of reported cybercrimes against women and girls to access and presume the gravity of the scenario. Because in many cases, these incidents do not reach the mainstream crime investigation process due to the legal and procedural difficulty, socio-cultural background in addition with the psychological status of victim, fear and anxiety associated with character defamation among women and girls. Recorded statistics of crimes of cyber violence against women and girls thus simply project the associated level of many factors such as access of victim to legal remedies, availability of the mechanism, specialized capacity of the investigating unit, background of the victim and the severity of the issue rather than actual underlying crime rates. Thus, in majority cases, women and girls lose their confidence in participating in public life as a result of confrontations with the psychological and emotional harm due to the damaged reputation, character defamation and loss produced by cybercrimes.

3. Ways Forward

Cybercrimes are those natures of crimes that have dissolved the concept of border and territory in its commission. Violence against women and girls in online spaces is gradually increasing. However the legal and policy regime to address it does not seem to penetrate deep enough on the gravity and changing dynamics of the cybercrimes specially targeted against women and girls in Nepal. Reliance on existing means of the criminal justice system does not deliver the sensible response to ensure justice to the victims of cyber violence. It is therefore a matter of immense necessity to discourse on the changing dynamics of technology-initiated gender based violence. Moreover, the government has envisioned ensuring access to internet to all the citizens by 2020 as per the Information and Communication Technology Policy 2072[33] If this plan is achieved, the situation of cybercrime against women and girls might get more aggravated if not any immediate efforts are initiated to address the existing legal and procedural vacuum.

Creation of a safe online environment should be prioritized from the beginning for prevention through programs relating to awareness on growing issues of online violence. Realizing the darker side of the online world and its power to track the information, monitor, defame as well as create prejudices, it should be clearly explained to all user groups and the aspect of digital literacy should be emphasized. Strategies to respond to these natures of crimes should be framed through joint collaboration between the States developing a mutual legal assistance treaty. Law enforcement authorities, prosecutors, judiciary and concerned stakeholders are required to draft long-term and sustainable evidence-based policy as well as anticipate opportunities of international cooperation for the comprehensive technical support and assistance required for the investigation and combating of cybercrime. Integration of strategies to prevent cybercrimes is thus a matter of holistic effort to be contributed by all relevant stakeholders including lay people from their own respective position. Similarly, creating

[33] National Information and Communication Technology Policy, 2015 AD., no. 10.5.

awareness and training programs on all components of cybercrimes to all concerned actors and audiences is another important step to conquer the demand of the time. ICT policies and laws should be framed to indoctrinate the concept of equality and dignity assuring women's rights approach and securing their safe space in the virtual world of the internet. Moreover, policies should be framed in such a way whereby ICT can be used as a tool for gender empowerment as well as for achievement of human rights standards. Providing necessary resources, powers and measures for effective investigation to law enforcement authorities is also a matter of equal importance.