OUTLAWING CYBER CRIMES AGAINST WOMEN IN INDIA

Ms. Saumya Uma*

Abstract

The right to internet usage has now become a human right, as declared by the United Nations Human Rights Council in June 2016. But what are its ramifications in a society steeped in patriarchy, where violence, harassment and discrimination against women in the cyber world mirror that in the real world? While the Union Ministry of Women and Child Development has officially recognized the magnitude of cyber-crimes against women and the need for a concerted effort to address the same, this paper explores the ground realities - the existence and effectiveness of Indian laws in protecting women (and girls) and enabling a safe and congenial environment for them when they access the internet.

The paper identifies common forms of cyber-crimes against women, such as cyber stalking, cyber pornography, circulating images / video clips of women engaged in intimate acts, morphing, sending obscene / defamatory / annoying messages, online trolling / bullying / blackmailing / threat or intimidation, and email spoofing and impersonation. It discusses contents of each category of offences, analyses the applicable legal provisions and highlights reported cases and judgments by way of illustrations. The paper concludes that neither the IPC provisions nor the provisions of the IT Act fully reflect the ground realities of women's experiences, and that the first step towards providing legal remedies for women is to ensure that the online experience of harassment / threat / intimidation / violence caused to women is accurately translated into the written law through amendments to the two major statutes. It recommends further steps that need to be taken in order to address cyber-crimes against women in a holistic and effective manner.

If religion was the opium of the masses in the past, social media is the new opium as well as the tsunami of Indians today. The right to internet usage has now become a human right, as declared by

* Assistant Professor, Maharashtra National Law University (MNLU), Mumbai.

the United Nations Human Rights Council in June 2016.[1]But what are its ramifications in a society steeped in patriarchy, where violence, harassment and discrimination against women in the cyber world mirror that in the real world? In May 2016, the Union Minister for Women and Child Development, Ms. Maneka Gandhi, observed that the online abuse of women in India ought to be treated in the same manner as violence against women in the real world, and created a new forum for redressal, and further instructed the National Commission for Women to create a system for taking action against online abuse of women.[2]While official recognition of the magnitude of cyber-crimes against women and the need for a concerted effort to address the same is positive, this paper explores the ground realities-the existence and effectiveness of Indian laws in protecting women (and girls) and enabling a safe and congenial environment for them when they access the internet.

Introduction

The number of social network users in India has increased drastically from 181.7 million in 2015 to 216.5 million in 2016 to a projected 250.8 million in 2017.[3]It is expected that the same would increase to at least 336.7 million by 2020.[4] *Facebook*, *Twitter*, *Instagram*, *LinkedIn*, *YouTube*, *WhatsApp* and *SnapChat* are some of the more popular social networking sites in India.

While India's internet population may be exploding, there is a looming gender imbalance in social network users. This is visible in areas such as the number of internet users, the number of *Facebook* and *Twitter* users, digital literacy and political tweets. A study of internet users in India, conducted by the Boston Consulting Group and Retailers Association of India, states that approximately 29% of the users in India are women, while the remaining 71% are men.[5] The disproportionate access of the internet to men and women is a major contributor of this

---

1 'The Promotion, Protection and Enjoyment of Human Rights in the Internet', A/HRC/32/L.20, 27 June 2016.

2 *Online Trolling against Women to be Considered Violence: Maneka Gandhi*, DECCAN CHRONICLE, 18 May 2016.

3 *Number of Social Network Users in India from 2015 to 2021* (March 15, 2017, 11.04 AM), https://www.statista.com/statistics/278407/number-of-social-network-users-in-india/.

4 *Ibid*.

5 Boston Consulting Group & Retailers Association of India (2016), *Decoding Digital @ Retail: Winning the Omnichannel Consumer* (14 May, 2017, 5.30 AM),http://image-src.bcg.com/BCG_COM/Decoding-Digital-Retail-Feb-2016-India_tcm21-28732.pdf.

phenomenon. This phenomenon is closely linked to the increasing incidence of cyber-crimes against women. Women users are often seen as 'invading / trespassing' on the male space, particularly when they articulate their viewpoints on politically sensitive and volatile issues. A 2015 report by Observer Research Foundation indicates a significant under-representation of women in Twitter's political conversations in India, which mirrors a real world marginalization of women in political processes in India.[6]The report also highlighted that many women users, including prominent bloggers and activists, had deleted their account due to online abuse and harassment of women.[7]

Magnitude of cyber-crimes against women in India

Cyber-crimes use information technology and the internet as the primary means for commission of illegal activities, which are prohibited and punishable by criminal law of the land. While cyber-crimes may be committed against persons, property and the government, this paper focusses on cyber-crimes against women. The more common and frequently reported forms of cyber-crimes against women include cyber stalking, cyber pornography, circulating images / video clips of women engaged in intimate acts, morphing, sending obscene / defamatory / annoying messages, online trolling / bullying / blackmailing / threat or intimidation, and email spoofing and impersonation.

According to the official statistics provided by the National Crime Records Bureau, Government of India, 9622 cases of cyber-crimes were registered in 2014 and 5752 persons arrested. In 2015, 11,592 cases were registered – an increase of 20% in registration of cases from the previous year – and 8121 persons arrested.[8] The NCRB statistics provide no information on the profile of victims; hence no official statistics are available in India to inform us of the extent and forms of cyber-crimes against women.

The official statistics are complemented by a research was conducted in India in 2016 including analysis of media reports involving online harassment of high profile women, a survey of 500 social media users and interviews with ten of the respondents, combining quantitative and qualitative methods of

---

[6] Sydney Anderson, *India's Gender Digital Divide: Women and Politics in Twitter*, OBSERVER RESEARCH FOUNDATION ISSUE BRIEF, October 2015, Issue No. 108, (13 May, 2017, 11.00 PM), http://www.orfonline.org/wp-content/uploads/2015/12/ORFIssueBrief_108.pdf.

[7] *Ibid* at p. 6

[8] *Crime in India 2015*, Chapter 18 – Cyber Crimes, Ministry of Home Affairs, Government of India, p. 164.

research.[9] The key findings of this study pertaining to awareness and accessibility of the law included the following:[10]

- 30% of the respondents said they were not aware of laws to protect them from online harassment; and
- Only a third of respondents had reported harassment to law enforcement; among them, 38 percent characterized the response as "not at all helpful."

The legal framework

The internet has two unique characteristics. Firstly, it transcends physical / geographical barriers, and hence, the abuser may be acting from any part of the world. Secondly, the internet extends anonymity to the users. While this may be a comforting feature for many users, who can hide behind the curtain of anonymity even as they exercise their right to freedom of expression and opinion, it also affords anonymity to the abusers. Both the features pose formidable challenges in crime prevention, crime detection and implementation of the law.

Essentially, there are two major laws in India that address cyber-crimes against women to a large extent – The Indian Penal Code (IPC), 1860 (which has been amended several times including in 2013) and The Information Technology (IT) Act 2000, which underwent major amendments in 2008. The Indian Penal Code is a general criminal law of the land, which defines a large number of offences, and prescribes punishment for the same. It is important to note that these are intended primarily for addressing the commission of crimes in the physical / tangible / real world. Such IPC provisions are applicable to cyber-crimes against women by way of legislative amendments and judicial interpretations.

Unlike the IPC, the IT Act is a specific law dealing with many aspects of the use of information technology, including the commission of crimes. The primary objective of this Act is to create an enabling environment for the use of information technology. Through the experience in dealing with offences related to the misuse of information technology from 2000 to 2007, the 2008 amendment Act contained an inclusion of certain

---

[9] JapleenPasricha (2016), *Violence Online in India: Cybercrimes Against Women and Minorities on Social Media*, FEMINISM IN INDIA (13 May, 2017, 12.30 PM),https://feminisminindia.com/2016/11/15/cyber-violence-against-women-india-report/.

[10] *Ibid* at p.1.

offences / cyber-crimes. Both the laws complement and reinforce each other in addressing cyber-crimes against women.

Cyber stalking

Stalking is not necessarily sexual in nature, but nevertheless terrorizes, tortures, harasses and intimidates the victim. It is a blatant intrusion into an individual's privacy, where the stalker attempts to establish a relationship with the victim without her consent. Stalking could be perpetrated physically or through electronic means, in the form of cyber-stalking.

Cyber stalking is one of the most frequently reported cyber-crimes against women, which involves following stealthily and tracking a woman's online and offline movements and activities. This includes stealthily and without her knowledge, gathering information with regard to her interests, likes and dislikes, family members and friends, personal information, contact details, daily routine and so on through the internet. The information gathered may be used to commit other crimes, both online and offline, such as posting the woman's name and personal information on a dating service. A typical form of cyber stalking would be when a woman goes to watch film, and soon thereafter, she receives an email from a stranger, with the questions - "How was the movie? Did you enjoy it?"

S. 354D of the IPC, which defines and provides punishment for the offence of stalking, includes cyber stalking. Any man who follows a woman and contacts or attempts to contact her for personal interaction repeatedly despite a clear disinterest from such woman, would be accused of the offence of stalking. When he monitors the use of internet, email or any other form of electronic communication by the woman, after hacking/cracking her password/committing theft of her identity, such an act would amount to cyber stalking. This provision is also useful when the stalker frequently uses bulletin boards, enters chat rooms that woman frequents, constantly bombarding her with obscene messages and emails. A first conviction for stalking entails up to three years of imprisonment and fine, while a subsequent conviction would attract a punishment of up to five years of imprisonment and fine.

The first conviction in a cyber stalking case against a woman in Maharashtra took place in July 2015 in the case of *Yogesh Prabhu* v. *State of Maharashtra,* decided by theAdditional Chief

Metropolitan Magistrate M.R.Natu.[11] In 2009, the woman initially chatted with Yogesh Prabhu online. When he made a marriage proposal to her, she turned it down. Thereafter she stopped responding to his messages as she found his behaviour suspicious. She also removed him from her friends' list. However, Prabhu continued to keep an eye on her profile and her whereabouts, and stalk her through the internet. Some months later, she received mails from an unknown email account, containing obscene images and video clips.

She initially ignored them, but when the obscene mails did not stop, she lodged a police complaint, and the Cyber Crime Investigation Cell took over the investigation.Internet Protocol (IP) address of the computer was traced to a Vashi firm where Yogesh Prabhu worked. The cyber cell filed a 200 paged charge sheet in Sep 2009, after which trial began.During the trial, eight witnesses, including the aggrieved woman, Prabhu's colleagues, cyber experts and police officials were examined by the Public Prosecutor. The magistrate's court convicted Prabhu under S. 509 IPC (words, gestures or acts intended to insult the modesty of a woman) and S. 66E of the Information Technology Act, 2008 (punishment for violation of privacy). This was because the cyber stalking provision - S. 354D of the IPC - was enacted in 2013 and could not be applied retrospectively to a crime committed in 2009.

Cyber pornography

Cyber pornography is the act of using the cyber space to create, publish or disseminate pornographic materials. Traditionally, the law related to pornography has been addressed through S. 292 of the IPC, dealing with the offence of 'obscenity'. Any material is considered obscene if, taken as a whole, it is lascivious or appeals to the prurient interests or if its effect is to deprave and corrupt persons who use the same. The section makes selling, distributing, publicly exhibiting, putting into circulation, taking part in or receiving profit from any business related to use of obscene objects, advertising, offering or attempting to do any act which is an offence under this section as a punishable offence. Such an act is punishable with a term of up to five years imprisonment and up to a fine of Rs. 5000. Additionally, S. 354A of the IPC, inserted in 2013, dealing with sexual harassment, includes a man showing pornographic material to a woman against her will. These provisions are useful when pornographic

[11] Prasanto K Roy, 'Why online harassment goes unpunished in India', 17 July 2015 (13 May, 2017, 4.30 PM), http://www.bbc.com/news/world-asia-india-33532706.

images and videos are sent to a woman through *Whatsapp*, email or other means.

S. 67A of the IT Act provides a further legal recourse, as it prohibits publishing or transmitting or causing to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct, and treats such acts as punishable offences. The punishment under the IT Act provision is far more stringent – up to five years' imprisonment and a fine of up to Rupees ten lakhs for a first conviction, and up to seven years' imprisonment and a fine of up to Rupees ten lakhs for subsequent convictions.

The first ever conviction in India for cyber pornography, was in the case of *SuhasKatti* v. *State of Tamil Nadu*, decided by a Chennai court in 2004.[12] The woman, a divorcee, complained to the police about a man who was sending her obscene, defamatory and annoying messages in a Yahoo message group, after she turned down his proposal for a marriage. The accused opened a fake email account in the name of the woman, and forwarded emails received in that account. The victim also received phone calls by people who believed that she was soliciting for sex work.The police complaint was lodged in February 2004 and within a short span of sevenmonths from the filing of the First Information Report, the Chennai Cyber Crime Cell achieved a conviction. Katti was punished with two years' rigorous imprisonment and Rs. 500 fine under S. 469 IPC (forgery for the purpose of harming reputation), one year's simple imprisonment and Rs. 500 for offence under S. 509 IPC ((words, gestures or acts intended to insult the modesty of a woman) and two years' rigorous imprisonment and Rs. 4000 fine for offence under S. 67 of IT Act 2000(punishment for publishing or transmitting obscene material in electronic form).

Circulating images / video clips of women engaged in intimate acts

Acts of voyeurism, particularly directed at intimate acts of women, became visible in the context of contemporary developments in information technology that allows photographs and video graphs to be taken easily through the mobile phone, and disseminated widely through pornographic and social networking sites in the internet. These recordings are most often done and disseminated

[12] Order passed on 5 November 2004 in CC No. 4680 of 2004 by the Chief Metropolitan Magistrates Court, Egmore, Chennai (India).

without the knowledge or consent of the concerned women, either by strangers or by intimate partners.

The offence of voyeurism involves a violent invasion of the private space of a woman by a man. Similar to other sexual offences, voyeurism prevents women from having bodily autonomy and a sense of agency. S. 354C of the IPC defines the offence of voyeurism. Its salient features include:

- Watching or capturing the image of a woman or disseminating such image;
- The image is of a woman engaging in a private act in circumstances where she would not usually have the expectation of being observed by the perpetrator or others;
- Private act includes
  - the act of watching carried out in a place that would reasonably be expected to provide privacy to the womanand
  - where the victim's genitals, posterior or breasts are exposed or covered only in underwear; or
  - the victim is using a lavatory; or
  - the victim doing a sexual act that is not ordinarily done in public.

The offence of voyeurism in the IPC is punishable with 1-3 years of imprisonment and fine for the first conviction, and 3-7 years of imprisonment and fine for subsequent convictions. The IPC provision on voyeurism is complemented by S. 66E of the IT Act – which makes violation of privacy by capturing, publishing or transmitting the image of a private area of any person without his or her consent, a punishable offence.

The section provides an explanation to various terms used. For example, 'transmit' means to electronically send a visual image with the intent that it be viewed by a person or persons; 'capture', with respect to an image, means to videotape, photograph, film or record by any means; the term 'private area' refers to the naked or undergarment clad genitals, pubic area, buttocks or female breast; 'publishes' refers to reproduction in the printed or electronic form and making it available for public; 'under circumstances violating privacy' means circumstances in which a person can have a reasonable expectation that—

(i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or

(ii) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

One of the most well-known incidents of voyeurism was the Delhi Public School MMS incident of 2004, which involved the creation of a pornographic MMS of two students of Delhi Public School in a sexual act, and its illegal distribution as well as bid to auction on the website *eBay India* (then known as *Bazee.com*). The Chief Executive Officer of the website was thereafter prosecuted under various provisions of the Information Technology Act, as the IPC had not criminalized such acts.[13]

The circulation of video clips of rape and gang rape incidents on the internet would attract these provisions. It is important to note that there may be situations where the victim consents to the capturing of such an image, but does not consent to its dissemination to third persons. If the image is disseminated to such persons, the dissemination will be considered an offence under this section. For example, women have reported that they have sent images of themselves in skimpy clothes or in the nude to their intimate partners through WhatsApp or Instagram, based on the partner's request. In other situations, with the woman's consent, physical intimacy with the partner has been recorded. Subsequently, when the relationship turns bitter, the partner has attempted to take revenge or blackmail the woman by disseminating such images / video clips. Such acts would attract these legal provisions. They could also attract the provision of criminal breach of trust (S. 406 IPC), which involves dishonesty misappropriating or converting to his own use property that had been entrusted in him.

Morphing

Morphing involves editing the original picture by an unauthorized user - when an unauthorized user with fake identity downloads the victim's pictures and then uploads or reloads them after editing. It is a common phenomenon that women's pictures are downloaded from websites by fake users and again reposted/ uploaded on different websites by creating fake profiles after editing them.Very often, morphing involves attaching an image of the face of a woman, who is being targeted, with that of the naked or skimpily clad body of another through the use of image-editing software. Such morphed images are intended to tarnish the

[13] *Avnish Bajaj* v. *State*, judgment delivered by Justice S. Muralidhar of Delhi High Court on 29 May 2008 (India).

image of the victim woman and malign her character. Cyber-crimes against women involving morphed photographs are reportedly on the rise in India.[14] While celebrities are often an easy prey to this crime, an ordinary woman too is targeted by a man who may seek to take revenge on her for rejecting his proposal for an intimate relationship, or to blackmail her or to otherwise harass her/tarnish her image among her circle of family and friends for a real/perceived harm caused by her to the abuser.

Such an act could attract offences under S. 43 (which includes acts of unauthorized downloading/copying/extracting and destroying/altering data) and S. 66 of the IT Act (which spells out various computer-related offences). Additionally, the violator can be booked under various provisions of the IPC such as sexual harassment under S. 354A, public nuisance under S. 290, obscenity under S. 292A and S. 501 for defamation.

Sending Obscene / Defamatory / Annoying Messages

Posting a woman's photograph with phone number and other contact details on a pornographic site, stating she is a sex worker available for sexual services, is an often-reported cyber-crime against women. Apart from defaming and causing harassment to the woman, such acts also invade the privacy of the woman as her personal information such as contact details are posted in public domain. Sending obscene and annoying messages through WhatsApp, electronic mail, Instant Messenger and other such modes, are other forms of cyber-crimes against women.

A range of legal provisions may be applied to such crimes, including sexual harassment (S. 354A IPC), defamation (S. 499 IPC), assault or criminal force to woman with intent to outrage her modesty (S. 354 IPC) andword, gesture or act intended to insult the modesty of a woman (S. 509 IPC). Public morality, decency and modesty of women form the core elements of offences under S. 354 and S. 509 IPC, which are colonial and patriarchal notions linked to sexual assault of women.The application of these two provisions carries with them the potential pitfall of judicial determination of 'modesty' and whether the victim woman possesses 'modesty' which is being violated. Nevertheless, these are useful provisions to apply in contexts of cyber-crimes against women which do not fall within well-defined offences in the IPC and the IT Act.

---

[14] *Cyber Crimes Involving Morphed Photos Rising,*THE TIMES OF INDIA, June 29, 2015.

The offence of defamation under criminal law (S. 299 IPC), which involves harming the reputation of a person through words, signs or visible representations, may be particularly useful, and has the potential to be used when women are defamed as sex workers or are targeted using sexist / misogynist abuses / sexist slander that spoils their reputation in their online communitiesincluding at online chatrooms.

Online trolling / bullying / blackmailing / threat or intimidation

Bullying is defined as intimidation / aggressive behaviour through use of superior strength or dominant position; cyberbullying refers to the same act through the electronic medium. Cyber bullying is "wilful and repeated harm inflictedthrough the use of computers, cell phones or other electronic devices, bysending messages of an intimidating or threatening nature. Since the electronic medium lends the power and strength of anonymity and limitless reach across the world, even a person who may be bullied in real life becomes the bully online despite the lack of superior physical strength or dominant position in society. India reportedly ranks third after China and Singapore in cyber bullying.[15] The magnitude of cyber bullying of women in India is not known through it is frequently reported.

In *Saddam Hussain* v. *State of M.P.,* the accused had outraged the modesty of the victim, video recorded the same on his phone and used the same to blackmail her.[16] A criminal complaint was lodged under S. 354D IPC (stalking), S. 507 IPC (criminal intimidation by an anonymous communication) of the IPC and S. 66A of the IT Act (which has subsequently been struck down as unconstitutional in *Shreya Singhal* v. *Union of India*).[17] A petition was filed before the Madhya Pradesh High Court for quashing on the basis of a compromise arrived at between the woman and the accused. The High Court refused to quash the proceedings, stating that the offences were against the society at large and a personal compromise between the parties would not affect the continuation of the prosecution. This case indicates that courts treat cyber stalking and cyber bullying as very serious offences.

A related crime is online trolling, in which women are threatened with rape / gang rape / acid attack / other forms of grievous hurt

---

15 T.E. Raja Simhan,*India Ranks Third in Cyber Bullying*, BUSINESS LINE, June 26, 2012.

16 2016 SCC Online MP 1471 (India).

17 AIR 2015 SC 1523: (2013) 12 SCC 73 (India).

for voicing their opinion which may be against an opinion enjoying popular support. In an environment of decreasing respect for opinions that are different from one's own, trolling of women who dare to exercise their freedom of expression, particularly on political issues, is a common phenomenon. Although social media such as Facebook and Twitter have online complaints mechanisms for such crimes, these are not always effective.

Blackmailing through social network sites and information technology is often carried out by ex-husbands after divorce and ex-boyfriends. Blackmailing through cyberspace is often vindictive in nature, in contrast to blackmail in the physical world which often involves an illegal demand for money. Blackmail may be through threat of disseminating morphed photographs, threat to publish and disseminate images and video clips of the woman's intimate / private moments or actual circulation of such images and video clips through messaging services.

Trolling, bullying and blackmail are often addressed through the IPC provisions of criminal intimidation (S. 503 & 506 IPC) which involves threatening another with injury to person, reputation or property, and criminal intimidation by an anonymous communication (S. 507 IPC) where the harasser is unknown to the woman.

Email spoofing and impersonation

E-mail spoofing is a term used to describe fraudulent email activity in which the sender's address and other parts of the email header are altered to appear as though the email originated from a known or authorized source. By changing certain properties of the email, such as its header, from, Return-Path and Reply-To fields etc., hostile users can make the email appear to be from someone other than the actual sender.

Impersonation involves representing oneself to be a person one is not. The anonymity of users in the cyber space lends itself easily to impersonation of women. For example, in a reported case, Manish Kathuria impersonated a woman, RituKohli (a married woman) in an internet chat room in 2001, and used obscene language, disseminated her home phone number and invited phone calls.[18] She started receiving numerous phone calls at odd hours. He was arrested by the Delhi police, and charged with

[18] Prasanto K Roy, *Why online harassment goes unpunished in India*, 17 July 2015 (13 May, 2017, 4.30 PM), http://www.bbc.com/news/world-asia-india-33532706.

'outrage of modesty' (S. 354 IPC) & S. 509 – which had nothing to do with cyber-crimes he had committed – due to want of appropriate legal provisions. There was no progress in the case, and the frustrated woman reportedly moved out of India.

Email spoofing and impersonation could attract offences under cheating (S. 415 IPC) and cheating by personation (S. 416 IPC). 'Cheating by personation' entails cheating by pretending to be some other person, or representing himself to be a person that he is not. The law explains that the offence of cheating by personation is committed whether or not the individual who is personated is a real or imaginary person. S. 66D of the IT Act also provides for punishment for cheating by personation by using a communication device or a computer resource. It is an offence punishable with upto three years imprisonment and fine of up to Rupees one lakh under the IT Act.

Conclusion

Various forms of cyber-crimes are experienced by Indian women who use the internet in the contemporary context. Neither the IPC provisions nor the provisions of the IT Act fully reflect the ground realities of women's experiences. In many situations, such as morphing, email spoofing and trolling, IPC provisions are applied by extrapolation and interpretation for the want of more specific provisions of law. Although the IT Act contains a chapter on offences, including computer-related offences, the provisions deal mainly with economic and financial issues; there are no specific provisions on cyber-crimes against women even though they are rampant and are widely reported. The first step towards providing legal remedies for women is to ensure that the online experience of harassment / threat / intimidation / violence caused to women is accurately translated into the written law through amendments to the two major statutes.

Secondly, many women are unaware of their rights in law vis-à-vis cyber-crimes. Awareness-raising of women is an important agenda for the Indian government, as a method to prevent as well as punish such offences. Equally, awareness-raising of laws and perspective-building on cyber-crimes against women, among other stakeholders in the criminal justice system, particularly the police, Investigating Officers, public prosecutors and judges, is also an imperative.

Thirdly, developing confidence-building mechanisms with victims and potential victims is crucial, in order to encourage crime reporting. It is vital that personnel of the Cyber Crimes Cell

established by the police at the state level, are well-trained in the latest technological developments, including cyber forensics, in order that they may conduct speedy and efficient investigation into cyber crimes against women.

Additionally, grievance redressal mechanisms and institutions should be vitalized and popularized, with the ease of lodging complaints and minimizing delay in investigation and prosecution as major objectives.

It is important to acknowledge that law does not have the potential to provide all solutions to the issue of cyber-crimes against women in India. Women themselves should be trained to take preventive measures, such as caution in posting their and their loved ones' photographs and video clips online, caution in communicating with strangers online, and protecting passwords and other vital information which may compromise with the woman's security and privacy. Women internet users in India require an increased awareness of enhancing privacy settings in social networking sites as a preventive measure.

Cyber-crimes against women are a manifestation of the underlying patriarchy and misogyny that is prevalent in Indian society. Unless the root cause is addressed through long term, multi-pronged measures and sustained efforts, dealing with the manifestations through legal/social and political processes would provide only a temporary and superficial solution. Above all, political will is the fulcrum that would help address cyber-crimes against women in India in a holistic and effective manner.