DE JURE NEXUS LAW JOURNAL

Author:

Jagriti Rana

Amity University, Rajasthan

5th Year, BA LL.B. (Hons.)

CYBER CRIMES IN RESPECT OF WOMEN: THE LEGAL CHALLENGES AND SOLUTIONS

Introduction

Hundreds of years have come, and hundreds of years have gone yet the situation of ladies isn't probably going to change. As in our Indian culture ladies possesses a significant job, the Vedas celebrated ladies as the creator the person who gives life and venerated as "Devi". however, on the opposite side its all legendary. There is different violations against ladies possibly it is before the birth or after however women are continually being suppressed. As in the period of globalization and modernization the current patterns of wrongdoings are likewise expanding. Security of ladies has consistently been an issue, particularly in a nation like India where worm of crime percentage against ladies is expanding quickly. Prior, it was restricted to streets or at places from Home. Home was the most secure spot for a lady to shield herself from being deceived, yet not now. In present day times ladies are seen as sex objects, she is dealt with sub-par compared to men in different cultural circles and capacities, this has made a gigantic sexual orientation predisposition between the people where even the men believe that their off-base doings towards ladies can't be punished. Cybercrime and web tormenting work in comparative way where the individual who perpetrates a digital violations are not terrified of any power that can punish. The digital world in itself has a hazardous spot extraordinarily for ladies and anybody can cover up or even phony his character. This endowment of web is utilized by the criminally disapproved to perpetrate unjust acts. The universe of web today has become an equal type of life and living. Individuals are presently fit for doing things which were not believable a couple of years prior. The web is quick turning into a lifestyle for many individuals and furthermore a method of living as a result of developing reliance and dependence of humanity on these machines. Web has empowered the utilization of site correspondence, email and a great deal of whenever anyplace IT answers for the improvement of mankind. Web however offers incredible advantage to society, additionally present open doors for wrongdoing utilizing new and exceptionally complex innovative instruments. Today email and sites have become the favored methods for correspondence. Despite the fact that web is probably the quickest method of correspondence and has spread its circle, covering every single imaginable shade of humanity. Be that as it may, as the platitude goes, every great side has an awful side too. The equivalent is valid with the PC and web advancements as well.

The fast-innovative headways like the web obviously take steps to abandon the law. The open and unregulated nature of the web and the superfluity of geology implies that the web likewise gives worthless ground to criminal venture. The current criminal law is by all accounts unprepared to manage this up-degree in techniques and media of

carrying out wrongdoing. Digital wrongdoing has hence become a reality in India, hard to recognize, only from time to time revealed and even hard to demonstrate.

COVID-19 lockdown 'significant' increase in cybercrimes against women

- While people went in lockdown, many took to web to connect each other : web based systems administration goals including Facebook, Instagram, YouTube, TikTok, and progressed and web correspondence applications like WhatsApp, etc in a little while watched a flood of customer created substance which are at present colossally ate up by others. Not these customers made substance are truly for delight for all. There were a couple of substance which were are up 'til now being made unequivocally to target and bug women and youngsters. The essential stage that started getting substance for sex bullying, especially incitement to women was Zoom application which was being used by most of the educational establishments and workplaces for hanging on the web social events, classes, online courses, etc. In a couple of cases it was seen that Zoom social events were unauthorizedly gotten to by unwanted individuals who started posting troubling, unequivocally express comments, upset get-togethers with revealing private parts, showing masturbation, etc. In a little while Zoom masters went with a pubic introduction that computerized security and prosperity extents of the stage were not adequately ready to deal with such unexpected huge use. Who could truly be viewed as at risk for such unapproved get to by then? The web stage induced that organizers of the zoom social affairs and classes must make cautious strides. Nevertheless, would we say we were really arranged and careful and to make such reasonable strides? Probably no. The Zoom application mess up truly provoked four sorts online bad behaviors:

- Unapproved access to the social occasions
- Data assurance infringement
- Creation of unequivocally express substance
- Making movements, etc to hurt the quietude of women

While this is just a single kind of offense, web-based baiting of women didn't remain restricted to this so to speak. Given the path that during lockdown most by far of the accomplices of criminal value mechanical assembly including the police and courts and the web associations are working with obliged work and structure workplaces, offenders have put aside this push to uplift incitement. The correspondence applications like Whatsapp, Facebook dispatch, etc are at present flooding with web torturing. This is seen especially in the school and school social events. These stages have become picked stages for throwing unforgiving, irritating, startling comments towards associates, batchmates and moreover towards the teachers, especially female educators, accomplices and customers. I myself had been engaged by specific harassers and stalkers on Facebook dispatch and WhatsApp too. Beside this, various instances of online incitement which has raised to a most outrageous height during the Covid - 19 lockdown stage, that came as I would see it is creation of copying profiles by means of electronic systems administration media. We ought to at any rate esteem the way that emulate by using fascinating characters have been considered as an offense Under S.66C of the Information Technology Act, 2000(amended in 2008), which discusses discipline for information extortion and says "whoever, misleadingly or deceitfully use the electronic imprint, mystery key or some other stand-out distinctive verification segment of some other individual, will be repelled with confinement of either depiction for a term which may connect with three years and will moreover be liable to fine which may loosen up to rupees one lakh"

Understanding Cyber Crimes

Cybercrime is a term for any criminal behavior that utilizes a PC as its essential methods for commission. It is an offense that is carried out against people or gatherings of people with a criminal thought process to purposefully hurt the notoriety of the person in question or cause physical or mental mischief to the casualty straightforwardly or by implication, including genuine digital wrongdoings (cyber stalking , email spoofing etc)Women especially young

girls inexperienced in cyber world, who have been newly introduced to the internet and Cybercrimes and cyber bullying is of various types, some are

1. Cyber harassment : Stalkers are fortified by the namelessness the web offers. He might be on the opposite side of the earth, or a nearby neighbor or a close relative. The web reflects this present reality. That implies it additionally mirrors the reality and genuine individuals with genuine issues. Digital following for the most part happens with ladies, who are followed by men. There is no all-around acknowledged meaning of digital following. It includes following a person developments over the Internet by posting messages (once in a while undermining) on the announcement sheets frequented by the person in question, going into the talk rooms frequented by the person in question, continually shelling the casualty with messages and so on. As a rule, the stalker plans to cause passionate trouble and has no real reason to his interchanges. He doesn't have to leave his home to discover or disturb his objective, and has no dread of physical brutality since he accepts he can't be genuinely contacted in the internet. The batterers in this manner clandestinely place their objective under steady observation without her insight and utilize the data to compromise her or dishonor her by putting deception on the web.

An investigation led on 72 ladies by Megha Desai and K. Jaishankar named 'Digital Stalking - Victimization of Girl Students: An Empirical Study', expresses that 12.5% of the respondents had close connection with their digital stalker before the following began. As per the exploration, 62.5% of provocation began through messages and online visits. The examining office and clinicians both concur that following has gotten progressively wild with the appearance of unregulated web. In the ongoing NCRB 2016 insights, among all South Indian metros, Hyderabad had an incredible 74 situations when Bangalore faired with 45 and Chennai 10 creation Hyderabad the following capital of South India. Stalkers need a shroud of namelessness and what preferable spot to appreciate obscurity over the web? A larger part of the cases coming to front have some component of cyberstalking also, with attackers spilling pictures â€" some of the time even transformed ones â€" on the web, or hacking into records and utilizing different email IDs and IP delivers to do likewise. In spite of the fact that it might be increasingly wild, following virtual stalkers might be more straightforward than putting the genuine stalkers behind the bars. That is in such a case that the following is done by means of electronic methods, at that point following an IP address is sufficient to demonstrate the wrongdoing of the aggressor. Said as much, it turns into the obligation of the woman to hold up an objection as it is significant for police to start any activity. For housing a suo-moto case in following wrongdoings, proof assortment is dubious as it's impractical to place in such a great amount of labor to investigate each case with no tip off.

Tragically, both the people in question and here and there even the police hold up until things take a grave go to act and that is decisively what occurred on account of a 13-year-old young lady who disappeared from the Old City of Hyderabad in August 2017. She was being followed and pestered by a 22-year-old for more than a half year. In any case, just when she was snatched by him and taken to Gulbarga did her folks at long last document a police grumbling. 'In the event that I can utilize a blade to cut my hand, I can utilize it to cut your throat as well' the guilty party had advised her, related the young lady, after being rescued. There is no other method to battle this threat than by carrying these culprit to the book.

Ritu Kohli Case: Ritu Kohli case was India first instance of digital following revealed in Quite a while. The casualty whined to the police against the individual, who was utilizing her personality to talk over the web she further griped that the culprit was likewise parting with her location on the web and utilizing foul language. Her contact subtleties were additionally released prompting regular calls at odd hours. Thusly the IP address was followed and police researched the whole issue and eventually captured the guilty party, Manish Kathuria. The police had enlisted the case under Section 509 of the Indian Penal Code for insulting the humility of Ritu Kohli. In any case, Section 509 of the Indian Penal Code just alludes to word, motion or act proposed to affront unobtrusiveness of a lady and when same things are done on web, at that point there is no notice about it in the said area. None of the conditions referenced in the segment secured digital following along these lines, Ritu Kolhiâ€™s

case was an alarm to the Government, to make laws in regard to the previously mentioned wrongdoing and in regards to insurance of casualties under the equivalent.

Thus, Section 66A was included Information Technology Act, 2008 (ITAA 2008) and it recommends detainment for a term which may stretch out to three years and with finefor sending hostile messages through correspondence administration and so on.

Clarification: For the motivations behind this segment, terms electronic mailâ€? and â€œElectronic Mail Message implies a message or data made or sent or got on a PC, PC framework, PC asset or specialized gadget remembering connections for text, picture, sound, video and whatever other electronic record, which might be communicated with the message.

Moreover, the Indian Parliament made corrections to the Indian Penal Code, 1860 presenting digital following as a criminal offense. The Criminal Law (Amendment) Act 2013 included Section 354 D in IPC, 1860. It characterizes Stalking as a man who follows or contacts a lady, notwithstanding away from of lack of engagement to such contact by that lady or checking of utilization of web or electronic correspondence of a woman. A man or a lady submitting the offense of following would be subject for detainment as long as three years for the main offense, and will likewise be at risk to fine and for any resulting conviction would be at risk for detainment as long as five years and with fine.

2.Cyber stalking

Following is illicit. The individual could get dangerous. Stalking incorporates chasing after somebody or leaving messages on their telephone or on the web, and purposely attempting to cause them to feel terrified You should contact the police and get their recommendation. Spare any messages or messages to show the police if necessary. Stalking can likewise include dangers or sexual remarks. The stalker regularly attempts cause the individual they're following to feel threatened and scared. Stalking a sweetheart, beau or ex, or another person, is illegal in Victoria. Following somebody online is likewise illegal.

3.Defamation

The web and internet-based life are unquestionably an extraordinary thing for individuals and society when all is said in done, yet they are likewise interestingly viable favorable place for conceivably offensive statements. Defamation in India is viewed both as a misdeed and as a wrongdoing. It hurts the notoriety and eminence of an individual and makes the transgressor similarly at risk as hurting the body of the individual. The individual esteem of an individual is enviously protected by law. Like some other crime, slander likewise got a lift and crime percentage went up as the electron turned into the incredible mode of expansion of data climate sound or implicating.

Digital slander likewise called Cyber spreading can be comprehended as the deliberate encroachment of someone else's entitlement to his great name. Cyber Defamation happens with the assistance of PCs and/or the Internet. Women experience the ill effects of it as the Indian cultural structure is to such an extent that the unobtrusiveness, notoriety and social remaining of ladies are delicate. The web permits individuals to express their genuine thoughts too without any problem. The web is crammed with fascinating sites where somebody could deliberately or unintentionally leave a conceivably slanderous remark or post. Only a couple of these areas are: open remarks on sites; websites and remarks to blog postings; web based life like Facebook, Linkedin, and Twitter, and talk rooms or rundown workers and email containing slanderous data to the entirety of the person companions. While some sites screen posts for incendiary or illicit substance, the screening frameworks are not outfitted to look at each post for abusive substance, thus numerous disparaging postings end up on the web.

The IT Act doesn't explicitly talk of digital slander. In spite of the fact that it accommodates discipline to an individual who communicates or distributes or causes to be distributed or sent, any material which is vulgar in electronic structure, on first conviction with detainment of either depiction for a term which may reach out to five years and with fine which may stretch out to one lakh and in case of resulting conviction with detainment for a term which may stretch out to two years and with fine which may stretch out to ten lakh. Anyway this arrangement essentially appears to target controlling the expanding number of kid erotic entertainment cases and doesn't include different wrongdoings which could have been explicitly brought inside its ambit, for example, digital maligning, great that is a begging to be proven wrong subject.

Be that as it may, Section 499 of the Criminal Law (Amendment) Act, 2013 solely discusses criticism. It states whoever, by words either verbally expressed or expected to be perused, or by signs or by obvious portrayals, makes or distributes any ascription concerning any individual proposing to mischief, or knowing or having motivation to accept that such attribution will hurt, the notoriety of such individual, is said to criticize that individual. Here it is conceived that the meaning of publishing is sufficiently wide to take inside its ambit, proclamations made on the web.

S.499 IPC along with S.4 of IT Act offers acknowledgment to electronic records. In this manner S.499 of IPC read with S.4 of IT Act overcomes any barrier and gives help in circumstances in instances of digital maligning. Subsequently, slanderous material posted on the web utilizing messages or interpersonal interaction sites, it could draw the consideration of S. 499 of Indian Penal Code. The most significant inquiry of in the case of composing on the web adds up to distribution or not? To analyze this inquiry, it is basic to look at the unmistakable destinations where criticism may happen.

4.Morphing and cyber pornography

Morphing and cyber pornography is profoundly expanding it is finished by altering the first picture to abuse it. Culprits because of web access can in a couple of moments seconds download ladies' photos from online networking, WhatsApp or some different assets and transfer transformed photographs on different sites, for example, internet based life website, pornography locales or for enlisting themselves namelessly. Digital sex entertainment is another danger to ladies since this remembers distributing explicit materials for sex entertainment sites by utilizing PCs and web wherein ladies won't know about such indecent distribution of their own very picture.

Section 67 of the Information Technology Act makes publication, transmission and causing to be transmitted and published in electronic form any material containing sexually explicit act or conduct, punishable. This means viewing Cyber pornography is not illegal in India. Merely downloading, viewing and storing such content does not amount to an offence. However, publishing and transmitting cyber pornography via instant messaging, emails or any other mode of digital transmission is an offence. In my opinion online pornography should be completely banned as it is responsible for declining values and sexual permissiveness leading to sex crimes against women and children.

An attempt was made by the government in 2015 asking the telecom companies around the country to block public access to 857 porn sites, citing the need to protect public morality. Days later, the telecoms minister, Ravi Shankar Prasad, had to back down and the ban was lifted. Those against the ban argue that the government has no business to interfere in individual choice; considering eroticism is a personal choice, the people of the country should have a right to decide what to watch and what not and the state has no role in it and should not impose their morals on others. The IT Act does not provide specific wording for blocking of cyber pornography for public access and one has to include cyber pornography into the definition of pubic order to put check on cyber pornography, where Courts in India have already interpreted public order as maintenance of Law.

The cyber pornography is mainly defined under section 66 A E, 67, 67A and 67 B. All pornography related offences are bailable as per Section 77B of the Information Technology Act, 2000 the only exception being Section 67 A and 67B. This is the main reason why the offenders are committing pornography related offences and still have the audacity to repeat it, as they are entitled to bail as of right and not to mention the long trial period. These sections of the Act should be made non-bailable so as to strike fear into the minds of offenders, this will definitely reduce the crime rate to some extent.

5.E-mail spoofing

It alludes to an email that rises up out of one source however has been sent from another source. It can cause fiscal harm. Phishing: Phishing is the endeavor to increase touchy data, for example, username and secret phrase and plan to increase individual data.

6.Trolling

Trolls spreads strife on the Internet, criminal beginnings quarreling or upsetting casualty by posting provocative or off-subject messages in an online network, (for example, a newsgroup, discussion, visit room, or blog) with the expectation to incite casualties into a passionate, upsetting reaction). Trolls are proficient victimizers who, by making and utilizing counterfeit ids via web-based networking media, make a virus war air in the internet and are not even simple to follow. Digital Law Under the Information and Technology Act, 2000, stalkers and cybercriminals can be reserved under a few segments for breaking of protection:

Section 67 deals with publishing or transmitting obscene material in electronic form. The earlier section in ITA was later widened as per ITAA 2008 in which child pornography and retention of records by intermediaries were all included.

Section 66A: Sending offensive messages through communication service, causing annoyance etc., through an electronic communication or sending an email to mislead or deceive the recipient about the origin of such messages (commonly known as IP or email spoofing) are all covered here. Punishment for these acts is imprisonment up to three years or fine.

Section 66B: Dishonestly receiving stolen computer resource or communication device with punishment up to three years or one lakh rupees as fine or both. Section 66C: Electronic signature or other identity theft like using others' password or electronic signature etc.

Section 66D: Cheating by person on using computer resource or a communication device shall be punished with imprisonment of either description for a term which extends to three years and shall also be liable to fine which may extend to one lakh rupee.

Section 66E: Privacy violation – Publishing or transmitting private area of any person without his or her consent etc. Punishment is three years imprisonment or two lakh rupees fine or both.

Section 66F: Cyber terrorism – Intent to threaten the unity, integrity, security or sovereignty of the nation and denying access to any person authorized to access the computer resource or attempting to penetrate or access a computer resource without authorization.

Section 72: Punishment for breaching privacy and confidentiality.

Section 72A: Punishment for disclosing information during lawful contract.

Section 441 IPC: This section deals with criminal trespassing.

Section 354D: This section deals with stalking. It defines stalker as a man who follows a woman and tries to contact such woman, monitors every activity undertaken by the woman while using digital media.

Harassment Via Email The expansion of email as the favored strategy for correspondence has offered ascend to different issues of worry to the lawmakers and managers the same. By its very nature, email urges individuals to be completely forthright and open in the conversation and given the straightforwardness with which it is made and sent, individuals are usually not as cautious on the email as they would have been, in the event that they had submitted the substance of email precisely. Provocation through email, incorporates coercing, compromising and consistent sending of adoration letters in mysterious names or ordinary sending of humiliating sends. Email is equipped for playing out all the elements of a typical mail. The criminal law contains different segments that address wrongdoings of boisterous attack against and the provocation of ladies model Section 509(IPC), Section 354D of the criminal law (Amendment) Act 2013 relates to following, expressly including violations that include checking the electronic correspondence of a woman. The IT(Amendment) Act, 2008 have embedded Sections 66A; 67A to 67 C. Segment 67 An and B embed correctional arrangements in regard of offenses of distributing and sending of material containing explicitly unequivocal act and kid erotic entertainment in electronic structure individually. While Section 67 C manages the commitment of a delegate to save and hold such data as might be indicated for such span and in such way and organization as the Central government may recommend.

In 2001, a youngster in the eleventh Grade was indicted under area 509 for offering profane comments about female colleagues on a site called Amazing.com. It was not just an effective utilization of Section 509 to control online provocation, yet the first run through a minor had been reserved under the law.

There are, in this way, different arrangements that pre-exist the Internet which ladies can attract on to battle online maltreatment without engraving themselves in the risky talk of the foulness and profanity laws or off area 66A. Be that as it may, the inquiry remains: can a lady decide to utilize another law in lieu of 66A?

Despite the fact that S 67, recommends discipline for distributing or sending of material containing explicitly unequivocal act, and so forth., in electronic structure. In contrast,66A is a cognizable offense where the police choose whether or not a wrongdoing has been executed under it, instead of a judge a lady may contend for another law to be utilized when she goes to enlist a protest; in any case, given the doubt of and ominous encounters with the police the degree to which ladies will be willing and ready to make these contentions with progress is maybe flawed. At last, the choice is in the possession of law requirement, for whom the grounds on which somebody may dismiss Section 66A might be a subject that appears as outsider as pointless. For the most part the wrongdoing of badgering is controlled by broad laws and not by the arrangements of the IT Act.

Reason for Growth of cyber crimes

- The transcendental nature of the internet no boundaries, ever changing.
- Low equipment cost
- Numerous vulnerable targets - loneliness is a prime cause a many female students and staff live away from family and work for long hours over the computers. Thereby computers become their trusted pal.
- Easy concealment due to anonymity.
- Most of the cybercrimes remain unreported due to the hesitation and shyness of the victim and her fear of defamation of family's name.

What victim needs to do

- Use a full-service internet security suite.
- Use strong password.

- Keep your software updated.
- Do manage your social media.
- Talk to your children about the internet.
- Keep up to date on major security breaches.
- Take measures to help protect yourself against identity theft.

Legal Remedies to deal with cyber crimes

Indian penal code

Section 354 A - Physical contact and advances involving explicit sexual overtones, showing pornography and demanding sexual favours.

Section 354 D - Deals sexual harassment, stalking and includes harassment via electronic communication.

Section 509- word sound or gesture intended to insult the modesty of a women.

Section 499 - punishes as 'defamation' the publication by visible representations of an imputation concerning the women, when done with the intention to harm her reputation.

Information Technology Act

Section 67 - prohibits and punishes with imprisonment extending up to three years and fine for first conviction and to five years and fine upon second conviction, the publication, transmission and causing of transmission of obscene content.

Section 66 E Deals with violation of the privacy of a person. Under the section, capturing, publishing or transmitting the image of a private area of any person without her consent, under circumstances violating her privacy, is punishable with imprisonment which may extend to three years, and fine.

Purpose behind enacting IT Act

- To provide legal recognition ton e-commerce
- To facilitate e- governance
- To provide remedy to cyber crimes
- To provide legal recognition to digital evidence

Conclusion

India is considered as one of the very few countries to enact to IT Act 2000 to combat cybercrimes; There is no specific provision to protect security of women and children.14 However there are few provisions to cover some of the crimes against women in cyber space under IT Act. Cybercrimes are such types of crimes which can primarily be prevented along with other measures. Technological improvement may be helpful for detection, prevention and commission of such crimes. High standards for security and network reliability have to be required. Effective technological "locks" to prevent end users from copying and distributing copyrighted music in digital form. Special Statutes on cybercrime is required to be passed to deal with the new form of crimes and to protect digital data. It will include Intellectual Property crimes and crimes relating to human rights. The Government has to create a special branch of Cybercrimes and Intellectual property Crimes within its criminal infrastructure, so that the enforcement personnel may take quick action against the Cyber Criminals. All sorts of infrastructure facilities are required to be available to the investigating officers, especially in regard to mobility, connectivity, use of technology. With

expanding traffic in the virtual world, the odds of falling prey to digital wrongdoing pose a potential threat at the same time, more so on account of ladies who are frequently observed as easy prey. The classifications of online wrongdoings focusing on ladies have extended and the wave has neither disregarded India. A couple of all the newer age wrongdoings that merit a notice here are digital blazes, digital eve-prodding, and digital being a tease and cheating. Women in India all things considered avoid announcing matters, dreading potential negative media exposure, which may hopelessly affect their notorieties. The additional time ladies spend on the web, without being totally mindful of the traps of the web, the weaker they become. Ladies ought to be progressively aware of shield themselves from focused online assaults.