

ISSN: 2582 - 2942



LEX FORTI

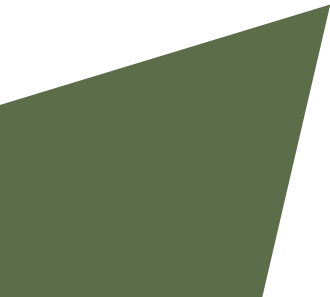
LEGAL JOURNAL

VOL- I ISSUE- V

JUNE 2020

DISCLAIMER

NO PART OF THIS PUBLICATION MAY BE REPRODUCED OR COPIED IN ANY FORM BY ANY MEANS WITHOUT PRIOR WRITTEN PERMISSION OF EDITOR-IN-CHIEF OF LEXFORTI LEGAL JOURNAL. THE EDITORIAL TEAM OF LEXFORTI LEGAL JOURNAL HOLDS THE COPYRIGHT TO ALL ARTICLES CONTRIBUTED TO THIS PUBLICATION. THE VIEWS EXPRESSED IN THIS PUBLICATION ARE PURELY PERSONAL OPINIONS OF THE AUTHORS AND DO NOT REFLECT THE VIEWS OF THE EDITORIAL TEAM OF LEXFORTI. THOUGH ALL EFFORTS ARE MADE TO ENSURE THE ACCURACY AND CORRECTNESS OF THE INFORMATION PUBLISHED, LEXFORTI SHALL NOT BE RESPONSIBLE FOR ANY ERRORS CAUSED DUE TO OVERSIGHT OTHERWISE.



ISSN: 2582 - 2942

EDITORIAL BOARD

EDITOR IN CHIEF

ROHIT PRADHAN

ADVOCATE PRIME DISPUTE

PHONE - +91-8757182705

EMAIL - LEX.FORTII@GMAIL.COM

EDITOR IN CHIEF

MS.SRIDHRUTI CHITRAPU

MEMBER || CHARTED INSTITUTE
OF ARBITRATORS

PHONE - +91-8500832102

EDITOR

NAGESHWAR RAO

PROFESSOR (BANKING LAW) EXP. 8+ YEARS; 11+ YEARS WORK EXP. AT ICFAI; 28+ YEARS WORK EXPERIENCE IN BANKING SECTOR; CONTENT WRITER FOR BUSINESS TIMES AND ECONOMIC TIMES; EDITED 50+ BOOKS ON MANAGEMENT, ECONOMICS AND BANKING;



EDITORIAL BOARD

EDITOR

DR. RAJANIKANTH M

ASSISTANT PROFESSOR (SYMBIOSIS
INTERNATIONAL UNIVERSITY) - MARKETING
MANAGEMENT

EDITOR

NILIMA PANDA

B.SC LLB., LLM (NLSIU) (SPECIALIZATION
BUSINESS LAW)

EDITOR

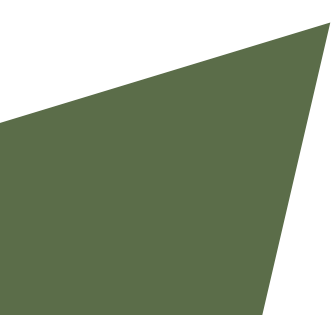
DR. PRIYANKA R. MOHOD

LLB., LLM (SPECIALIZATION CONSTITUTIONAL
AND ADMINISTRATIVE LAW)., NET (TWICE) AND
SET (MAH.)

EDITOR

MS.NANDITA REDDY

ADVOCATE PRIME DISPUTE



ABOUT US

LEXFORTI IS A FREE OPEN ACCESS PEER-REVIEWED JOURNAL, WHICH GIVES INSIGHT UPON BROAD AND DYNAMIC LEGAL ISSUES. THE VERY OBJECTIVE OF THE LEXFORTI IS TO PROVIDE OPEN AND FREE ACCESS TO KNOWLEDGE TO EVERYONE. LEXFORTI IS HIGHLY COMMITTED TO HELPING LAW STUDENTS TO GET THEIR RESEARCH ARTICLES PUBLISHED AND AN AVENUE TO THE ASPIRING STUDENTS, TEACHERS AND SCHOLARS TO MAKE A CONTRIBUTION IN THE LEGAL SPHERE. LEXFORTI REVOLVES AROUND THE FIRMAMENT OF LEGAL ISSUES; CONSISTING OF CORPORATE LAW, FAMILY LAW, CONTRACT LAW, TAXATION, ALTERNATIVE DISPUTE RESOLUTION, IP LAWS, CRIMINAL LAWS AND VARIOUS OTHER CIVIL ISSUES.

Cybercrimes and Women

Ajitesh Arya

ABSTRACT

The Paper, tries to understand the most common cybercrimes taking place against women and the reasons behind them. The paper sees if the current laws in place are capable of dealing with the crimes and what changes if any are to be brought at both substantial as well as procedural level. The Papers analyzes various reports and other works done in the field of cybercrimes to reach an answer. The Paper shows how despite the laws being in place there are many lacunas and a need of concretization and homogenization in favor of the victims.

Keywords: Cyber Crimes, Hacking, Stalking, Grooming, Pornography, IPC, IT Act, Voyeurism.

INTRODUCTION

The Advancement in technology and communication has facilitated the various activities of economies and nation-building. A man can now access a lot of things sitting in his office, he can get any information, buy or sell anything and do many other things with a few clicks, the development in information technology and communication has indeed reduced the gaps and shorten the distance. But everything good thing has a dark side as well. As the cyber world started taking shape we were introduced to the concept of cybercrime. The basic understanding of the cybercrime is a crime which involves a computer and internet system. The legislatures when realized the increasing dependence on the internet for the trade and commerce and the risk undertaken, they came up with the Information and the Technology Act, 2000 making India one of the few countries with a properly drafted IT act in place. However, the act being a 20 year old legislation, the legislators failed to contemplate a specific type of crimes against women. Though the recent most amendment of the year 2008 came with a few relieves but we definitely have to still traverse a long way. According to the recent most data of National Crime Records Bureau (NCRB) there was an increase of 42% in cybercrimes against women in the year 2018 since 2016 with the similar patterns throughout the union territories and the states as well.¹ Such findings are indeed problematic completely contravening the notion of woman as goddess.

In this paper, the researcher shall try to analyse the domain of Cybercrimes against women in the context of India, this analysis shall include the study of prominent heads of the crimes as reported with relevant provisions of statutes primarily the Indian Penal Code, 1862² and the Information and Technology Act, 2000³ along with the relevant case laws and reports. Though the study is specific to the context of India but similar trends have been observed in almost every part of the world even in European Union (EU) countries considered as the forerunners of data privacy and fiduciary liabilities. Debrati Halder has attributed this discrepancy to the overarching interest in economy instead of Human Rights. Similar approach was criticized for having been concretized into the preamble of the IT Act itself. The intent of the paper is to discuss the relevance of the legislations and the remedies for the underlying issues.

¹ Cyber Crimes Against Women (State/UT wise) 2018, NCRB, https://ncrb.gov.in/sites/default/files/crime_in_india_table_additional_table_chapter_reports/Table%209A.10.pdf (Last Accessed Apr. 21, 2020).

² Indian Penal Code, 1860, No. 45. Act of 1860.

³ Information and Technology Act, 2000, No. 21, Act of Parliament (INDIA).

METHODOLOGY

Owing to the recent developments and the lockdown the ground data could not be collected, thus as an alternative the reliance has been placed on the reports of various organizations such as NCRB, NCW etc. Additionally, many papers and books have been analyzed. Cyber Crimes Against Women in India by Debrati Halder being the primary.⁴ The paper, at the initial stage delves into the sociological and legal reasons to the increasing number of cases and underreporting of the cases. I shall also explain how there has been a circular relationship between the underreporting and occurrence of the crimes. The paper then analyzes the substantive aspects of law to deal with the cybercrimes in order to gauge their relevance and at the same time shall also analyze the procedural intricacies'. Before its culmination, the paper shall also try to look for the remedies given by various experts in the field.

REASONS FOR INCREASING CYBERCRIMES AGAINST WOMEN

Women have been prone to certain kinds of threats and crimes since the very beginning. Such was also recognized by Lord Macaulay during the drafting of the IPC, giving special protection to certain groups against certain crimes, Section 375, 509, 364 etc being some of the examples of the same. It is to be remembered that while I assert that women are prone to certain crimes it is nowhere intended to undermine that the other gender may also be targeted to similar sort of crimes.

There can be two major aspects attributed to the growing numbers of cybercrimes in India

1. Sociological reasons
2. Legal reasons

SOCIOLOGICAL REASONS

This head can be further divided into the following subheads.

SOCIAL POSITIONS AND GENDERED RELATIONSHIP

The social positions of the women is one of the leading reason for increasing rate of cybercrimes in India. Needless to say that women in Indian society- are considered as submissive whereas men are considered as the responsible member of the unit. These gendered constructs leads to lack of technological knowledge among girls as compared to the boys this is further aggravated by lack of proper training at school. Study by Choudhry and Basque highlights that despite the change in

⁴ Jaishankar & Halder, Cyber Crimes Against Women in India (1d ed, 2016).

familial considerations, girls feel more troubled in computer related issues whereas the other gender is less prone to privacy breach.⁵ Further differences can be attributed to the overall outlook of the internet shaped in patriarchal society.

Also, in the Indian society the idea of pureness of women and notions of attaching the pride of the family leads to the underreporting of such cases, where the fear of intrusiveness is constantly there, this motivates the perpetrator to breach the modesty with hardly any fear of legal consequences, the gravity of underreporting can be seen by the fact that the data of Cybercrimes as reported by (a Particular NGO) were thrice the NCRB data.⁶ Additionally there has been instances where the women are harassed due to property related issues in order to seek revenge from family due to this notional justice itself.⁷ If despite all this, a woman decides to report then the societal notions again come into play leading to secondary victimization of the women. As Halder and Jaishankar say-

“The victim shies away from the police in fear of defamation of her profile as well as her family’s name and often the victim is made to believe that she is the person who is responsible for the crime done to her by being trapped foolishly” (p. 58).⁸

This behaviour discourages further reporting and ostracization.

GLOBALIZATION AND DISASSOCIATION OF THE FAMILIES

As globalization opened up new opportunities, people started moving away from their families and nuclear families became the unit of family instead of the joint family. As Talcot Parson, from his empirical data has shown that this led to a cleavage in the foundational and emotional solidarity of the families and the individual started looking for the liquid love which is best found through social media. This opened up individuals to various scams and frauds. Domestication of women made them a softer target here.

⁵ Halder, S., & Choudhuri, S. (2011). Computer Self Efficacy and Computer Anxiety of Trainee Teachers: Issue of Concern. Proceedings of epiSTEME, 4, India. Retrieved on 7th September, 2013, from <http://episteme4.hbcse.tifr.res.in/proceedings/strand-ii/curriculum-and-pedagogical-studies-in-stme/halder-choudhuri-v2>.

⁶ DANNY OALMER, *CYBER CRIME: UNDER-REPORTING OF ATTACKS GIVES HACKERS A GREEN LIGHT, SAY POLICE*, ZDNET, [HTTPS://WWW.ZDNET.COM/ARTICLE/CYBER-CRIME-UNDER-REPORTING-OF-ATTACKS-GIVES-HACKERS-A-GREEN-LIGHT-SAY-POLICE/](https://www.zdnet.com/article/cyber-crime-under-reporting-of-attacks-gives-hackers-a-green-light-say-police/) (MAY 14, 2018, 08:51 PM)

⁷ Id.

⁸ *Supra* no.4

“To overcome depression and loneliness women, especially, home makers, tend to find a support outside their family circle. It is because of this reason that they tend to rely on strangers and make them their confidante” (Halder and Jaishanker 2011b)⁹

Furthermore, the ever emerging money-centric notions has led to an organized sectoral crime against women as content hosting websites started paying handsome amount to host pornographic content making households leading contributors. This led to problems like grooming, revenge porn etc as will be discussed later.

PERPETRATOR’S OUTLOOK

The internet allows the user to live in two words , due to anonymity it provides and live a life one cannot otherwise. This is one of the reason for internet addiction. As Griffiths put it-

“text-based virtual realities and take on other social personas and social identities as a way of making them feel good about themselves. In such cases, the medium of the internet may provide an alternative reality to the user and allow them godlike feelings of immersion and anonymity, feelings that may lead to an altered state of consciousness for the user” (Griffiths, 2010, p. 465)¹⁰

This anonymity and godlike feelings sometimes extend bounds shaping into criminal conduct. Additionally, one party being anonymous and staying behind the veil of personality does not negate that other person is also under the veil, and when this veil is removed shocking things are discovered leading to damaged ego promoting revenge and hate crimes.

LEGAL REASONS

Many commentators and the legal experts believe that the one of the prominent reason for the cybercrimes against women is resulting due to insufficient and non- homogenous laws throughout, this criticism is stemming from the preamble of the IT act itself which describes its intent as one preventing the commercial activities and not individual rights, secondly, due to lack of data protection acts and privacy rights like Europe.¹¹ There are many laws in our country to prevent the offences and abuses against women. There are provision under IPC, POCSO¹², Indecent Representation of Women (Prohibition) Act,¹³ Prevention of Sexual Harassment at Workplace

⁹ Halder, D., & Jaishankar, K. (2012). Cyber Crime and the Victimization of Women: Laws, Rights and Regulations (pp. 1-264).

¹⁰ Griffiths, M. D. (2010). Internet abuse and internet addiction in the workplace. Journal of Workplace Learning, 22(7), 463-472. doi: 10.1108/13665621011071127.

¹¹ Whitty, M. T. (2005). The Realness of Cyber cheating: Men’s and Women’s Representations of Unfaithful Internet Relationships. Social Science Computer Review, 23(1), 57-67. doi: 10.1177/0894439304271536.

¹² The Protection of Children from Sexual offences Act, No. 32 of 2012, Act of Parliament.

¹³ Indecent Representation of the Women (Prohibition) Act, No. 60 of 1986, Act of Parliament.

act,¹⁴ etc. The offences defined under these legislations, procedures are different and so are the punishments clearly lacking homogeneity which contributes to lacunae and chaos for the victims concerned.

In the next part of the paper, the researcher shall analyze some of the heads of cyber crimes against women in the light of different statutes, provisions and case laws. Having analyzed the issues of the substantial laws, the paper further analyzes the procedural inconsistencies and concerns.

CYBERCRIMES

The researchers and legislators often fall prey to consider the offences against women as that of sexual nature only which is not so true, the stats of NCRB data of show that women also fall prey to commercial types of crime in a large proportion. However, having understood this, in this paper, we shall only deal with the crimes specific to the women. In this part of the Paper, the researcher shall analyze commonly recognized cyber crimes by theorists and as per the NCRB recent reports, in the light of applicable and commonly applied laws.

CYBER STALKING

Cyber Stalking is one of the major offence threatening the perusal of the internet by the women, it amounts to almost 49% of the total crimes reported which is still very low.¹⁵ Cyber stalking can be understood as the repetitive approaches made by offender resulting in unpleasant feelings and intimidation to a women. "*Ritu Kohli case*"¹⁶ was the first case in India to deal with cyber stalking. In the particular case, the accused used the identity of the victim in order to chat with others and solicit them. The court convicted under s. 509 IPC, namely outraging the modesty of women. This case shows that there was no laws on cyber stalking and courts having wide discretion. The victim and the accused both at the mercy of the Court. Owing to this realization and failure of machinery in the Tragic Nirbhaya Rape case, IPC was amended to add section 354D to curb stalking it defines Stalking as-

"354D Any man who-

¹⁴ Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013, No. 14 of 2013, Act of Parliament. (INDIA)

¹⁵ Cybercrimes Against women (State/UT Wise), 2018, NCRB https://ncrb.gov.in/sites/default/files/crime_in_india_table_additional_table_chapter_reports/Table%209A.10.pdf

¹⁶ MUKUT, CYBER STALKING - A "VIRTUAL" CRIME WITH REAL CONSEQUENCES, WORLD PULSE [HTTPS://WWW.WORLDPULSE.COM/COMMUNITY/USERS/MUKUT/POSTS/22772](https://www.worldpulse.com/community/users/mukut/posts/22772) (LAST ACCESSED AT MAY 02, 2020).

1. *Follows a woman and contacts or attempts to contact such woman to foster personal interaction repeatedly despite a clear indications of disinterest by such woman; or*
2. *monitors the use by woman of internet, email or any other for of e-communication commits the offence of stalking*¹⁷

This amendment helped in delimiting the meaning of stalking and scope of the law as well. As the act of stalking would lead to persistent state of fear this can be read with section 506 UPC namely criminal intimidation and section 2(n) of the Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013 if happening at a professional level. Section 509 (Outraging Modesty of Women) IPC is also used.

There are mainly two points of contention against this law, one is the offence being bailable and therefore, the victim is at risk of re-occurrence of the offence, therefore, a civil remedy of restrain order is needed which is not there, secondly, the definition covers only male as perpetrator, there is rather a need of gender neutral definition as we have seen in case of Pooja Bedi, a woman harassing woman.¹⁸

IDENTITY THEFT AND AVATAR CREATION

This would be one of those offences which is the most underreported as both the victims as well as the reporting authorities feel it to be a very trivial issue. This is because the limited knowledge of the technology but this may lead to severe consequences. Despite the underreporting this still makes up for almost 9% of cyber crimes against women.

“A false image of the victim which is created by the perpetrator through technology with or without the image of the victim, circulating false or partially true information about the victim leading to creation of false identity of the victim’s personality among the right thinking members of society.” (Halder 2013, p97)¹⁹

The creation of the fake avatar can be done by either creating the fake profiles and morphing pictures of the victim (Morphing means editing merging the picture of victim with certain other picture mostly in compromising position) or by spreading the false information on web.

The former instance can be easily dealt with section 66C read as-

¹⁷ Indian Penal Code, 1860, Act no.45 of 1860.

¹⁸ Naziya Sayed, *Pooja Bedi Booked under POCSO act*, TOI <https://timesofindia.indiatimes.com/entertainment/hindi/bollywood/news/Pooja-Bedi-booked-under-POCSO-Act/articleshow/45570074.cms> (Dec 19, 2014, 09:11 am).

¹⁹ Halder D.(2013), Examining the Scope of Indecent Representation of Women (prohibition) Act, 1986 in light of cyber victimization of Women in India, NLSJ, 11,188-218.

“However, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine with may extend to rupees one lakh.”²⁰

Ritu Kohli’s case would be an apt case under this head. Additionally, other sections like 509 of IPC, 67A (Punishment for transmitting/Publishing sexually explicit content) 67B (Transmitting content child in Sexual position) of IT act etc. would also be applied depending upon the content posted/transmitted, Section 12 of POCSO (Use of child for pornography). Section 67A and 509 IPC is mostly used in cases of morphing. But it may also be applied with 66C as in-

Say if after impersonating A, B posts sexually explicit content and solicit others then section 509 IPC and 67A IT shall also be applicable. This example also shows that the crime though not motivated by sexual gratification but culminated in sexual harassment as well.

However, the latter case would be more problematic as that would be solely dependent upon the content posted additionally the discussion being on the public domain the speech is more likely to be protected under article 19 rights.²¹ As we have seen in cases of Sagarika Ghose and other journalists the reliefs were denied initially²² This uncertainty leads to gendered bullying and harassment at subtle levels of Public Discourse, debates etc.

VOYEURISM

Voyeurism involves clear violation of the privacy which is mostly motivated by sexual gratification and sometimes revenge. Voyeurism is generally understood as videographing/photographing an individual at a place where he has reasonable expectation of privacy and/or uploading that content where the person could not have reasonably anticipated the dissemination. Delhi High Court gave a landmark ruling in bringing this offence under section 66E of the IT Act. (Punishment for Privacy Breach). Which is gender neutral however, an amendment in the year 2013, amended the IPC to insert section 354C to deal with the Voyeurism giving a more streamlined understanding to the section, as “filming a woman where she expected to have privacy” or uploading clips filmed with her consent without her permission (dealt with provision 2). This widens scope of the but at the same time limiting the understanding of the perpetrator to males the problem that we have

²⁰ Information and Technology Act, 2000, No. 21, Act of Parliament (INDIA).

²¹ INDIA CONST. Art, 19.

²² Divya Arya, *Why are Women being Harassed at Social Media*, BBC India <https://www.bbc.com/news/world-asia-india-22378366> (May 08, 2015).

discussed in the previous sector as well. This problems shape from the legislators understanding as age-old understanding of rape where male ravaging sexuality of women but now there is a need to shift in that understanding as well as in the rape laws. The punishment is also quite small i.e. for one year which is not deterrent at all and that too bailable, resulting in probabilities of re-victimization by virtue of easily available anonymity over internet.²³ Despite the changes in law, the instances of voyeurism have not been curbed yet, there are instances of cameras found installed in girls hostel and changing rooms, lavatories etc.²⁴ this is mainly due to two reasons one being fragile laws and the other being uninformed and hesitant victims.

REVENGE PORNOGRAPHY

Revenge Pornography is the neighbor of voyeurism, the difference being the under the former the breach of privacy happens at the creation of the content whereas under the latter it takes place at the stage of dissemination. Cyber pornography amounts to almost 40% of total crimes against women, making it the second biggest concern.²⁵ In India dating opposite gendered, public displaying of affection etc are considered as taboo therefore people choose to indulge in the acts online. Teens sometimes indulge in sexual communication over internet and share sexually implicit/explicit content in order to impress other party or to evade screening etc. Theorist have termed this practice as sexting. This tendency is seen in adults as well. On the other hand the couples at times wish to capture their intimate moments with each other. Both of this leads to creation of the content which might appear harmless. The problem appears when there is a emotional separation and one of the party uses this to either blackmail or attack at the other party. This behavior is common among the teens but adults are not untouched either.

The landmark case that introduced us to the concept of revenge pornography is the case of “Delhi DPS School”²⁶ where the intimate video of two students was greatly shared. The boy was booked under sec 67 of IT act but got acquitted because of young age. In a more recent case the owner of bazee.com arrested for purchasing such clandestinely shot clippings.²⁷

²³ Jaishankar believes that anonymity is easily available over internet, one after getting bail may re-target their victim for revenge, as seen earlier as well. *Supra* no. 4.

²⁴ AMRITA MADHUKALYA, SMRITI IRANI BRINGS BACK FOCUS ON VOYEURISM PREVAILING IN OUR COUNTRY, DNA [HTTPS://WWW.DNAINDIA.COM/INDIA/REPORT-SMRITI-IRANI-BRINGS-BACK-FOCUS-ON-VOYEURISM-PREVAILING-IN-OUR-COUNTRY-2075010](https://www.dnaindia.com/india/report-smriti-irani-brings-back-focus-on-voyeurism-prevailing-in-our-country-2075010) (LAST ACCESSED MAY 1, 2020).

²⁵ *Supra* no. 15

²⁶ *DPS student suspended for sexually explicit MMS*, Hindustan Times <https://www.hindustantimes.com/india/dps-students-suspended-for-sexually-explicit-mms/story-E3SdDp96GgnPsyjRItNPdL.html> (Last accessed May 02, 2020).

²⁷ *Avnish Bajaj vs. State*, 2008 (105) DRJ 721,

The most common law used in order to curb this is section 67A or 67B coupled with the section 12 of POCSO act (use of children for pornographic purposes) if teen porn is involved. And 67B coupled with 509 IPC, 292 of IPC (public Display of obscenity) and Indecent Representation of Women (Prohibition) Act.

However, Jasihankar and Halder opposed the idea of section 67A due to their reservation of sub-clause a of the same section read as

“67A Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form.—Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees”²⁸

They believe that the women victims can be fallen prey to this section due to the term “Create” and “whoever” which is a very genuine question, on asking Mr. Avdhesh Maheshwari practicing advocate at Gwalior high court told us that police sometimes denies registering complain due to the said reason only. Here the police needs to be more empathetic instead of blaming the victims. Additionally the second explanation to section 354C IPC (Voyeurism) can come to their rescue which penalizes the dissemination of pornographic content created with consent of both the parties.

Apart from this, as we can see the dissemination of the revenge porn can fall as offence of hacking. Mr. Walls had described hacking as “*unilateral use of computer systems including networks with intention to breach security of either of the owner or owners.*”²⁹ We know that the network was not used with a purpose to disseminate the data to third parties. So as an alternative the section 43 sub-section a, b, c could be employed namely unauthorized use, alteration and delectation of computer and communication received thereby. It being said, the main advantage of this would be ease of getting compensation as civil remedy rather than cumbersome proceedings which proves to be a boon for the victim suffering from loss of respect, employment etc.

GROOMING

The traditional understanding of is to prepare or to make ready for some future prospects. But the advancement of the technology has given a new meaning to the term altogether. Grooming means

²⁸ Supra no. 18.

²⁹ Wall, David S., Cybercrime: The Transformation of Crime in the Information Age. POLITY, 2007. Available at SSRN: <https://ssrn.com/abstract=1066922>.

to motivate the victims to contribute to the victimization themselves. Groomers may use their victims to allure more victims and making into a system victimization. In cases like this, the victim usually meets their groomers online and through the continuous conversations the relationship of trust is built. The approach is somewhat similar to stalking the only difference being in the case of stalking the victim may feel repulsive whereas in the latter the victim feels sympathetic and coy. The general understanding is that the children only are susceptible to grooming as Wachs defined, “*cyber grooming is establishing trust based relationship between a minor and an adult using internet network to solicit the minor for sexual purposes. The component of the repetition, misuse of trust and relationship are important elements.*”³⁰ however this understanding can be attributed to adults new at internet, emotionally or financially vulnerable adults. The main concern regarding understanding of cyber grooming as a crime is that there has not been any direct legislations to protect adults. Also while reporting the roles of groomers are underwhelmed so much so there has not been prosecution about the victim-blaming.

Section 67B(c) IT act³¹ clearly there to protect the interest of the child from grooming, so does the section 12 of POCSO. But there are no direct provisions to protect the interests of the other. Remotely a case can be made under section 66D (cheating by impersonation) (if the courts extend impersonation to mean a creation of **farce personality and not false identity** to gain trust.) Grooming can be read into definition of cheating under section 415 IPC which include fraudulent deception to let someone deliver a property which he would not have otherwise. Here too property has to include pictures, videos etc. however, we cannot say with certainty what recourse will the courts take as this remains an untraveled route.

Having discussed the substantial issues it can be observed that major of the cyber crimes against the women in the present time can be dealt with the existing law but that depends on the interpretation given by the courts to the various provisions Also, as most of these cases are settled at level of sessions courts themselves, thus homogeneity and certainty is yet not expected. Before proceeding to the next section, it is important to point out that many theorist have understood cyber defamation as a separate head of the crimes which is not necessary as we can see almost all the crimes discussed above has elements of defamation and can be dealt with setion 500 IPC (punishment for Defamation) altogether. Reference to the case of The State of “*Tamil Nadu Vs*

³⁰ Wachs, S., Wolf, K. D., & Pan, C.-C. (2012). Cybergrooming: Risk factors, coping strategies and associations with cyberbullying. *Psicothema*, 24(4), 628–633.

³¹ 67B(c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees:

Suhas Katti".³² (also important for being the first case to be dealt with IT act). Additionally, there has been certain lacunae with the existing laws as pointed above, there is a need to update them to suit the present circumstances.

PROCEDURAL CONCERNS

Having discussed the concerns around the substantial law, we shall now focus on the procedural aspects. Although there are countless issues around procedures, we shall only be dealing with a few of them in this paper.

COMPLAIN MECHANISM

As we have seen in our previous section, how the different crimes are reportable under different legislations, for example IPC, IT or POCSO acts etc. The redressal mechanism provided under these acts are very different. For example Section 80 of the IT act provides that any cases under this act shall be dealt with the officer of inspector rank or above. Whereas section 154 of CrPC³³ provides that any case under IPC 354, 376 and 509 will be dealt and registered by the women officer only. At times it is hard to find out which authority to approach to and resultant delays in transfer of the complains. Though in some metros, the police HQ have a Cyber cell but in reality when someone goes to register complain there, they are asked to approach the police stations. Secondly, there are different recourses available say IT act in chapter IX talks of civil compensation, other do not in these cases while clubbing offences what punishment and compensation be given is not clear.

RIGHT TO BE FORGOTTEN

The right to be forgotten is recognized in the EU laws where the citizen can ask the data intermediary (usually the search engines) to delist certain search results. This law is not yet recognized in India. As Citron put it, "*often certain types of cybercrimes including online harassments such as cyber trolling, bullying, creation of fake avatar are not recognized, thereby ISP may be reluctant to take a call*"³⁴ as we know that data is mobile and transcends borders, getting the host to take them down may not be possible but the intermediaries can be asked to de-list that entry. In absence of the right to be forgotten the victim may not be heard by them. However, the IO may under section 69A IT Act may ask the intermediary to stop public displaying in a territory or the court through its order can

³² "Tamil Nadu v Suhas Katti (2004): Case related to the posting of obscene messages on the Internet". Retrieved 19 April, 2020.

³³ Criminal Procedure code, 1973, No. 2 of 1974, Act of Parliament. (INDIA)

³⁴ Citron, Danielle Keats. *Hate Crimes in Cyberspace*. Harvard University Press, 2014. Accessed May 3, 2020. www.jstor.org/stable/j.ctt7zsws7.

also recognize the right as it did in case of *Sri Vasunathan vs The Registrar*.³⁵ But this will lead to an cumbersome delay in cases where time is of essence

THE COLLECTION OF EVIDENCE

The evidence collected in cases of cyber crimes are usually delicate things like the computer systems, hard drives and discs etc. There is a tendency among the victims to destroy the evidences due to the embarrassing nature. They should be educated through the different e-safety tips etc. however that is a different story altogether. Assuming the victims preserve the evidence in a proper manner still a great deal of diligence is required from the IO. They need to recognize that the evidence they are dealing with has a different nature altogether from general criminal law evidences. Due to lack of technical knowledge however, there has been many instances reported of evidence being tempered, or chain of custody being lost. To curb this CBI came up with the general guidance on dealing with the computer evidence.³⁶ Out of all other handling guidelines, the major being the need to have the computer expert during the investigation. However, guidelines being guidelines, the cyber experts are scarcely available as told by and IO alone confiscate evidence sometimes leading to a great deal of loss.³⁷

CONCLUSION

As the paper has described the genesis of cyber crimes, substantive and procedural legal issues, the researcher would conclude the paper with some conclusions and possible legal remedies. Across legislation we have seen that there are many remedies and possible legal actions available to the victims, hence, it would not be right of many theorists to claim that laws are not there and underdeveloped. However, at the same time we need to recognize that some of the issues in the legal system specifically designed for the women are left unanswered making judicial interpretation an important thing there is a need to concretized them. There are greater problems at the procedural level due to both sociological reasons as gendered relationships and pride theories as well as legal reasons, at the legal level however, problems can be solved by homogenizing the laws into a single piece of legislation, preferably under the IT Act as the Chapter IX of the same provides for civil remedy of compensation to women suffered loss of reputation, job, marriage opportunities etc. This remedy would be helpful for the women not going for the criminal

³⁵ *Sri Vasunathan vs The Registrar*, [General Writ Petition № 62038 of 2016].

³⁶ *CBI upgrading Crime Manual to better tackle corruption and cyber crime*, The Hindu Bussiness Line (Sept. 12, 2019) <https://www.thehindubusinessline.com/news/national/cbi-upgrading-crime-manual-to-better-tackle-corruption-and-cyber-crime/article29397731.ece>.

³⁷ *Id.*

proceedings due to various societal reasons and save the time as well. If not possible then also the victim protection schemes of various states should be homogenized and concretized.

No legal revolution can be brought up in the absence of social change, there is a need of sensitization and training at three level peers namely for the students, guardians and the police. Children should be guided about the healthy use of the Internet and privacy measures to be taken while on the social media or elsewhere, they should also be told about not only their rights but also about the liabilities of the data fiduciaries, website hosts and intermediaries. The Guardians need to be educated about the ill-effects of stifling the cases and victim-blamming. Similarly the police etc should be educated about the safe procedures and behavioral aspect. Authorities like DLSA, NALSA etc can play key role here. There is a further need of the proper privacy legislations and right to be forgotten be brought up. It is high time now that the much debated Data protection Bill be passed. The Government need to realize a blanket ban on porn won't help as it is mostly accessible through VPNs there is a need of much stringent positive actions.

In the present time, where internet is transcending the gender boundaries in terms of accessibility there is a need to ensure that the consistent fear of privacy breach and crimes may not inhibit their enjoyment of technology. This will be another step in ensuring the equality enshrined in the Article 14 of the Indian Constitution.