CYBER CRIMES AGAINST WOMEN

An Indian Law Perspective

Dr. Karnika Seth

COMBATING CYBERCRIMES AGAINST WOMEN

By

Dr. Karnika Seth

Cyber law Expert & Advocate, Supreme Court of India

LL.B (Faculty of Law, University of Delhi),

LL.M (Kings' college, University of London)

Ph.D. (Noida International University)

Visiting Faculty, National Judicial Academy, National Police Academy,

Central Bureau of Investigations and National Investigations Agency

Printed in India.

PREFACE

In India one cybercrime is reported to take place every ten minutes! According to the Indian Computer Emergency Response Team, (CERT-In), 27,482 cases of cybercrime were reported from January to June in 2017 itself. As cybercriminals misuse the anonymity of cyberspace to commit more cybercrimes, women and children typically are vulnerable targets owing to lack of cyber awareness in the country. This e-book is precisely written for the benefit and knowledge of all stakeholders including law enforcement, lawyers, legislators, researchers, academia, Not for Profit , International organisations who work for protecting women from cybercrimes. Apart from educating the readers on different kinds of cybercrimes and modus operandi of criminals online, it aims to explain the various Indian laws that come to the aid of a victim /potential victim , such as the IT Act,2000, Indian Penal Code, 1860, The Immoral Traffic Prevention Act,1956 and other extant Indian laws. The e-book explains the latest hybrid cybercrimes such as sexting, revenge porn, happy slapping , trolling, voyeurism, in easy and simplistic manner using examples, case studies and illustrations. The e-book briefly explains various cybercrimes against girl child aswell and relevant provisions of the POCSO Act,2012 and J.J Act,2015 which are special laws enacted to protect children in India. In the e-book's final chapter the Author guides the readers on legal remedies available under Indian law and steps required to claim legal redress in case a cybercrime incident occurs. I hope the e-book will achieve the objective of creating cyberawareness among all stakeholders working towards cybersafety & cybersafety for women in particular!

Dr. Karnika Seth

ABOUT THE AUTHOR

Dr. Karnika Seth is an internationally renowned Cyber law expert & is the Founder Partner at Seth Associates law firm in India. Dr.Seth is also the Chairperson of Lex Cyberia at Seth Associates, the World's first integrated cyber laws research, forensics and legal consulting centre. She is also the Founder of FIRE, Foundation for Institutional Reform & Education , a not for profit working towards spreading cyberawareness in India. Dr. Seth is one of World's leading authorities on cyber law & also known as a prolific Author & Educator on the subject. Her contribution to growth & development of cyber laws and spreading its awareness internationally and in India is widely acknowledged in the corporate world and by International organisations. She contributes to various Working Group Consultations and ICANN discussion forums aimed at designing policies for Next Generation Internet. She is part of Expert Panel of UNICEF working on children safety in the online world and actively associates with International Centre for Missing and Exploited Children (ICMEC) in its Think Tanks & cyber awareness activities in India. She is also associated with the International Telecommunication Union's initiatives and is a member of the Global Cyber Security Forum. Her expert views on cyber safety have been solicited by Indian Parliament and the Ministry of Information Technology, National Commission for the Protection of Child Rights for strengthening cyberlaws in India. She is empanelled as legal expert to advise National Internet Exchange of India and the Office of Comptroller of Certifying Authorities constituted under the IT Act, 2000. She is member of Advisory

Board of various educational institutions and was conferred title of *Honorary Professor* by Amity University in 2017.

Dr. Seth practices law at the Supreme Court of India and is principal legal advisor to many multinational groups and government entities. She has actively resolved complex Cybercrime cases in conjunction with the law enforcement authorities in India. She is also an Expert IT law Educator & Trainer to law enforcement authorities in India including the National Judicial and Police Academy, Central Bureau of Investigations and The National Investigation agency.

Dr. Seth writes extensively on key legal and cyber awareness issues for newspapers, journals and periodicals from time to time. Ms. Seth's book titled 'Computers, Internet and New Technology Laws' published by Lexis Nexis Butterworths elucidates the key developments in the field of Cyber laws across many important jurisdictions, India, United States and European nations.Dr. Seth was conferred the *Law Day Award* from the Chief Justice of India for authoring the comprehensive reference book in 2012. She received the *Digital Empowerment Award* for the year 2015 and the Law Day Award in 2015 for authoring the book, Protection of Children on Internet. In 2017, Dr. Seth was conferred the *National Gaurav Award* for exemplary contribution to the field of cyber laws in India. She regularly contributes her views on the subject in conferences, print & electronic media and television.

Table of Contents

CHAPTER 1

1 INTRODUCTION

In the digital age, the conventional crimes that were committed offline have shifted to the online world. Cyber criminals find internet as an easy medium to commit crimes as it gives them access to several vulnerable groups of people including women and children, and offers the anonymity and technical software to spoof /conceal their real identity online. India has witnessed drastic rise in cyber crimes in general and against women and children. The *NCRB crime in India Report,2015*, in its chapter 18 reports that 11592 of cyber crime cases were registered in 2015 under Information Technology Act,2000, related sections of the Indian Penal Code and offences under special and local laws and there was 20.5% increase from 2014. 8121 persons were arrested during 2015 showing in increase by 41.2% in the number of arrests in the year 2014. The Report reflects that 8045 cases were registered under the Information Technology Act indicating an increase of 11.7% from 2014. 81.6% cases pertained to

computer related cases and 10.1% pertained to publication or transmission of obscene content. 62.5% persons arrested belonged to the age group of 18 to 30 years and 30.8% between 30 to 45 years and 9% offenders were juvenile. An analysis of the motive of crime shows that 33.3% committed crimes for financial gain, 9.6% for fraud or illegal again and 5.2% for insult to the modesty of woman. 5.1% commit such crimes for sexual exploitation and 3.3% for damaging the reputation of woman. [1]

According to a Report prepared by UN, women between 18 to 22 years of age have higher vulnerability to becoming victims of cyber crime[2]. The said UN Report highlights 73% women are targeted online for exploitation and 61% of the cyber criminals are men. The Report identifies 11 broad categories of cyber crimes against women including hacking, impersonation, surveillance/tracking, harassment/ spamming, recruitment (traffic) and malicious distribution, revenge porn and sexting. However, there are other kinds of crimes also perpetrated against women apart from the mentioned crimes. Altogether, the ingredients which make or constitute these offences may slightly vary across legal jurisdiction. Certain basic factors will still remain common e.g. unauthorized access to one's email account or other secret data will certainly be referred to as hacking or a synonymous

[1] NCRB, Crime in India Report,2015

[2] Cyber Violence Against Women And Girls – A World Wide Wake Up Call, UN Broad Band Commission (Working Group Of Broad Band And Gender), 2015 Report.

term such as unauthorized access. Often while drafting laws legislators may club a few offences or sub-categories them under broad categories e.g. in India Section 66 of the I.T. Act,2000 deals with hacking includes within its ambit, any act which damages any computer system or network, data or data base residing in such system. In certain other countries such case may constitute a separate offence and may not be clubbed under hacking.

India is a signatory to the Convention on the Elimination of All Forms of Discrimination against women, an International Convention adopted by United Nations General Assembly. The States which ratified the Convention are required to enshrine into their domestic legislation and laws to protect women against the discrimination and establish Tribunals and Institutions to guarantee protection against discrimination. India has thus enacted various laws containing provisions that prohibit discrimination and crimes against women. Further, various amendments have been made in extant Indian legislations to protect women from growing cybercrimes such as sexual harassment & Cyberstalking. Apart from amendments in the IT Act,2000 and inclusion of deterrent provision against child pornography (Section 67B of IT Act,2000), Section 354A of IPC was introduced in 2013 against sexual harassment, Section 354D Of IPC against Cyberstalking and Section 354C of IPC for prohibiting voyeurism which are discussed in this e-book. For protecting children against cybercrimes, POCSO Act,2012 was introduced with deterrent punishments

for sexual harassment and child pornography, sexual assault which will be discussed briefly in this e-book.

For the Protection of women against sexual harassment at work place, following ruling in Vishaka's *case*[3] ,*the Protection of Sexual Harassment Act, 2013* was enacted that requires the employer to have policies and mechanisms in place of work to ensure safety of women employees, clients, customers and visitors from any form of sexual harassment. The scope of sexual harassment covered therein includes not only physical harassment but also harassment using phone, emails, messages, other forms of electronic contact. It also covers any events which are outside office such as meetings for official purposes. Any woman who has faced harassment can file a complaint within 90 days of the occurrence of the incidence to the Internal Complaints Committee set up by the Employer. It is required to maintain complete confidentiality of the matter and the ICC is required to submit its Report to the Management after enquiry within 10 days from completion of enquiry. The enquiry is required to be completed within 90 days. The term 'Sexual harassment' here includes unwelcome physical contact, showing pornography, and making sexually colored remarks against a woman colleague. It includes any unwelcome verbal or nonverbal contact of sexual nature, creating hostile work environment or asking for sexual favours. Section 2 sub-clause (n) defines sexual harassment as:

"(n) "sexual harassment" includes any one or more of the following

[3] 1997 (6) SCC 241

unwelcome acts or behavior (whether directly or by implication) namely: -

(i) physical contact and advances; or

(ii) a demand or request for sexual favours; or

(iii) making sexually coloured remarks; or

(iv) showing pornography; or

(v) any other unwelcome physical, verbal or non-verbal conduct of sexual nature;"

Section 3 of the said Act provides that no woman will be subjected to sexually harassment at any work place and mentions the circumstances wherein certain acts or behavior of sexual harassment will amount to sexual harassment such as express or implied promise of preferential treatment in her employment.

According to *Indecent Representation of Women (Prohibition) Act,1986*, Section 4 prohibits publication or sending by post of material containing indecent representation of women and Section 6 of the said Act prescribes the punishment for a term of two years and fine upto Rs.2000/- for the offence. However, the offence is bailable as per Section 8 of the Act. The section requires an amendment to include Electronic Media within its ambit. In 2012, an Amendment Bill was introduced in Parliament to amend the Indecent Representation of Women in Electronic Media titled 'The Indecent Representation of Women (Prohibition) Amendment Bill,2012, the bill seeks to widen the scope of the Act to cover new forms of communication such as Internet and other forms of Electronic Media, the same is yet to be passed. Similarly, *Immoral Traffic Prevention Act, 1956* prohibits

the act of seducing or soliciting for the purpose of prostitution with an imprisonment for a term which may extend upto 6 months or fine upto Rs.500/- or both. But it does not expressly mention that such solicitation will include Electronic Media. Such Amendments/Clarifications are need of the hour. The Section 228A of the IPC protects women victims' identity when reporting certain offences such as Rape offences under Sections 376, 376A, 376B, 376C,376D and 376E. Similar provision exists under Section 23 of the POCSO Act,2012.

A scheme for cyber crime prevention against woman and children has been proposed through the *Nirbhaya Fund.* The scheme will focus on crimes against woman including circulation of pornographic videos, online sexual abuse and harassment etc.4 The Indian Judiciary has also played its part in enforcing the law of the land and punishing the criminals for crimes against women which are discussed in subsequent chapter of this e-book.

The UN working group on discrimination against women and law made recommendations to combat crimes against women, interalia, increasing woman's cyber awareness and improving internet access and ensuring gender responsiveness of internet. According to the UN Report on cyber violence against woman and girls and a world wide wake up call, UN Broad Band Commission, (working group on Broad Band and Gender) suggested reforms, interalia, to develop system

[4] http://mha1.nic.in/par2013/par2016-pdfs/ls-030516/1421%20E.pd

to promote cooperation with Law Enforcement, making take down procedure more efficient, terminating the user account in case of misconduct and producing Transparency Reports to show how Law Enforcement's request was complied. It suggests use of Corporate Social Responsibility approach, encourage terms of use to be given on the website, disclose identity of a harasser as adopted in South Africa and Nova scotia and prescribe criminal liability for a company or individual if they fail to comply with court orders as adopted in South Africa. In India also a multi stakeholder approach needs to be adopted to combat rising cybercrimes against women. Combating cybercrimes needs greater cyber awareness, more reporting of crimes, law enforcement's cooperation and expeditious disposal of cases with cooperation from service provider in providing crucial evidence.

With this basic background it is pertinent to discuss the various kinds of cybercrimes against women and discuss the relevant provisions under extant Indian law which prescribe it as an offence.

CHAPTER 2

DIFFERENT CYBER CRIMES TARGETING WOMEN :

(i) Hate Speech:

In Social Media women actively express their views and opinions on various issues, political, religious or otherwise and become target of verbal abuse or criticism by certain group(s) of people. Citron mentioned this group attack as "Cyber Mob Attack"1. In India, the freedom of speech is a fundamental right guaranteed under the Constitution of India. However, the freedom of speech does not entitle anyone to use abusive language against another, whether it is offline or in online space. Section 66A of the Information Technology Act,2000, which now stands struck down by the Supreme Court in the *Shreya Singhal2* case, had prescribed punishment for sending offensive messages through communication service. The said provision was however struck down due to ambiguity in its words (such as 'grossly offensive

[1] Citron, 2009

[2] AIR 2015 SC 1523

or menacing character') which allowed its gross abuse or misuse.

The Section 66A of IT Act,2000 is as below-"*S. 66A. Punishment for sending offensive messages through communication service, etc. – Any person who sends, by means of a computer resource or a communication service, -*

(a) any information that is grossly offensive or has meaning character, or

(a) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device; or

(a) any electronic mail or electronic mail massage for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such massage,

shall be punishable with imprisonment for a term which may extend to three years and with fine."

Section 66A also covered sending of any information which the originator knew was false, but for the purpose of causing inconvenience, danger, obstructions, insult, injury, criminal intimidation, enmity, hatred, ill will persistently sends the same using computer. Such acts were punishable for a term which may extend upto 3 years and fine. Even though Section 66A of the IT Act,2000 has been struck down, Section 506 of the Indian Penal Code,1860 may apply to Hate Speech wherein the element of criminal intimidation has been used by the

offenders[3]. Criminal intimidation is punishable under Section 506 of Indian Penal Code,1860 with a term of imprisonment that may extend to 2 years or fine or both.

It is important to reproduce herein the provision Section 503 that defines criminal intimidation which is as follows:

"503. Criminal intimidation—Whoever threatens another with any injury to his person, reputation or property, or to the person or reputation of any one in whom that person is interested, with intent to cause alarm to that person, or to cause that person to do any act which he is not legally bound to do, or to omit to do any act which that person is legally entitled to do, as the means of avoiding the execution of such threat, commits criminal intimidation. Explanation. —A threat to injure the reputation of any deceased person in whom the person threatened is interested, is within this section. Illustration A, for the purpose of inducing B to desist from prosecuting a civil suit, threatens to burn B's house. A is guilty of criminal intimidation. "

In view of the above provisions, if a Hate Speech threatens the author of a comment/message (who may be a woman) to cause her physical injury or damage to her reputation or property, such person shall be guilty of criminal intimidation. If the criminal intimidation is by an anonymous communication such person is punishable with imprisonment with an additional term of 2 years.

Further, Section 509 of the Indian Penal Code may also apply in Hate Speech cases as words intended to insult the modesty of a woman which is punishable with imprisonment for a term upto 3 years and also fine.

---

[3] Karnika Seth, *Computers, Internet & New Technology Laws*,Lexis nexis 2nd Edition

"*509. Word, gesture or act intended to insult the modesty of a woman.– Whoever, intending to insult the modesty of any woman, utters any word, makes any sound or gesture, or exhibits any object, intending that such word or sound shall be heard, or that such gesture or object shall be seen, by such woman, or intrudes upon the ,*[4] *[shall be punished with simple imprisonment for a term which may extend to three years, and also with fine.]*

Classification of Offence. – The offence under this section is cognizable, bailable, compoundable with permission of the Court before which any prosecution of such offence is pending and triable by any Magistrate."

In case the words constituting Hate Speech involves sexual explicit remarks, Section 354A of the Indian Penal Code shall apply which prescribes punishment for a term upto 3 years of imprisonment or fine or both. In case sexually colored remarks, the term of punishment extends upto one year or fine or both.

(ii) Sexual harassment on social media:

Women may be contacted by other women or men for discussing any tropic of interest. It is often seen fake user IDs are created by men to grab a fake identity and pose as women or children or garb an identity to look younger or the older than the actual age. The motive behind such acts can be to carry out sexual harassment through writing such remarks, sexual favors or show pornography against the will of a woman. Such acts are punishable with an imprisonment which may be

[4] Substituted by the Criminal Law (Amendment) Act, 2013 (13 of 2013), S. 10, for "shall be punished with simple imprisonment for a term which may extend to one year, or with fine, or with both." (w.r.e.f. 3.2.2013).

extended upto 3 years or fine or both. The offence is cognizable, bailable and triable by any Magistrate.

Section 354A of Indian Penal Code is reproduced below for easy reference :-

"*354-A. Sexual harassment and punishment for sexual harassment.* –

(1) *man committing any of the following acts* –

(i) *physical contact and advances involving unwelcome and explicit sexual overtures; or*

(ii) *a demand or request for sexual favours; or*

(iii) *showing pornography against the will of a woman; or*

(iv) *making sexual coloured remarks, shall be guilty of the offence of sexual harassment.*

(2) *Any man who commits the offence specified in clause (i) or clause (ii) or clause (iii) of sub-section (1) shall be punished with rigorous imprisonment for a term which may extend to three years, or with fine, or with both.*

(3) *Any may who commits the offence specified in clause (iv) of sub-section (1) shall be punished with imprisonment of either description for a term which may extend to one year, or with fine, or with both.*

Classification of Offence. – The offence under this section is cognizable, bailable and triable by any Magistrate.

Sexual harassment of the nature of making sexually coloured remark, it is cognizable, bailable and triable by any Magistrate."

(iii) Voyeurism:

A person expects privacy in certain areas – washroom, changing areas in malls and in one's own bed room. However, it is shocking to see rampant privacy invasions

through use of hidden web cameras frequently reported in news reports[5].

Section 354C of the Indian Penal Code prohibits the act of voyeurism, that is, where someone watches or captures the images of a woman engaging in a private act where she would expect not being observed by the cyber criminal or publishes or transmits such images to a third person. The offence is punishable with a term of imprisonment not less than a year which may extend to 3 years and fine. On second conviction it is punishable with imprisonment for a term of not less than 3 years but which can extend to 7 years and also liable to fine. In cases where the victim agrees to capture the image but not to circulate such content, it will be an offence under this section. It is cognizable, bailable and triable by any Magistrate for his conviction. Second or subsequent conviction – it is cognizable, nonbailable and triable by any Magistrate.

The Information Technology Act,2000 also provides a provision to prohibit video voyeurism. Section 66E of the I.T. Act provides punishment for violation of privacy. In case any one captures or publishes or circulates the image of private parts of any person without his or her consent, it is punishable with imprisonment which extends to 3 years or fine not exceeding

[5] Police hunt man who placed hidden camera in Starbucks toilets after he accidentally filmed himself installing it, The Independent, http://www.independent.co.uk/news/uk/crime/starbucks-hidden-camera-voyeur-pervert-vauxhall-metropolitan-police-lambeth-london-a8068736.html

Rs.2.00 Lacs or both. Section 66E is reproduced hereunder for easy reference:

"S.66E. Punishment for violation of privacy. – Whosoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both."

(iv) Cyber Stalking:

A woman may be stalked in social forums, social media or even by installing a key logger which enables a criminal to see everything she types online. Before Section 66A was struck down, IT Act,2000 contained a specific provision prohibiting the cyber stalking. Section 66A(b) prohibited the act of sending an information which one knows is false but to cause annoyance, inconvenience or danger or to obstruct, intimidate a woman sends such information persistently through a computer or communication device such as mobile phone. This is a form of positive cyber stalking where the person who is stalked knows she is stalking.

Currently, Section 354D(i) of the Indian Penal Code prohibits stalking and states that any man who follows a woman and contacts or attempts to contact a woman to make a personal interaction repeatedly though a woman shows no interest is said to cyber stalk woman.

Section 354D(ii) of IPC describes passive form of cyber stalking wherein any man who monitors the

use by a woman of internet, email or any other form of electronic communication also commits offence of stalking. Such acts are punishable with imprisonment of a term which may extend to 3 years and also be liable to fine and punishable of second or subsequent conviction with imprisonment of a term which may extend to 5 years and also liable to fine.

The said section creates exceptions e.g. where stalking was committed to prevent or detect crime by the mandate of the State or pursued under any law or for compliance of law and in some circumstances where the contact was reasonable and justified. In the view of the Author, the last exception creates an ambiguity as it lays down no objective criteria to determine what is reasonable or justified. An act which may be reasonable to a person, may not be reasonable for another person e.g. a husband who suspects his wife to have an extra marital relationship may consider it justified or reasonable to stalk his wife online whereas it may amount to violation of privacy to his wife.

(v) Sending obscene content:

Sometimes women may receive unsolicited calls and obscene video or images which are obscene in nature from a stranger or a known person. Such acts are also punishable under the extant law in India. Section 67 of the Information Technology Act,2000 prohibits the act of publishing or transmitting any material which is obscene in nature and makes act punishable with imprisonment of upto 3 years and fine upto Rs.5.00 Lacs

and in the event of second conviction with imprisonment for a term which may extend upto 5 years and fine upto Rs.10.00 Lacs.

Section 67A of the Information Technology Act provides punishment for publishing or transmitting material containing sexually explicit content and makes it punishable with imprisonment for a term upto 5 years and fine upto Rs.10.00 Lacs.

(vi) Cyber Defamation:

Incase any person is defamed online/offline, that, is one's reputation is injured by words spoken or written which is published or transmitted to another person, it is a punishable offence. Victim can seek civil remedy of claiming damages and in criminal remedy seek punishment for offender.

Section 500 of the Indian Penal Code provides punishment for defamation with simple imprisonment for a term upto 2 years or fine or both. It is non-cognizable, bailable and compoundable with the permission of the court and triable by a Magistrate of First Class.

Defamation is defined in Section 499 of the Indian Penal Code and covers words spoken or written which makes or publishes any imputation concerning a person to bring him harm or knowing that it will cause such harm to the reputation of such person. Often women are defamed online by imputing her morally weak character or placing similar allegation to lower her dignity. Explanation 4 to Section 499 is particularly helpful in

explaining the kind of imputation that will attract the offence of defamation. According to explanation 4 an imputation is said to harm the reputation of a person if directly or indirectly in the estimation of latter's moral or any intellectual character of the person or latter's credibility of that person or causes someone to belief that the body of that Person is in disgraceful state. Section 499 of IPC is reproduced below for easy reference-

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

The Section lists few exceptions wherein acts will not constitute defamation such as when reporting of true facts which are for public good, public conduct of public servants, merits of case decided in court, imputation made in good faith by a person to protect his own interest etc.

(vii) Morphing: -

The term 'Morphing' means to use photograph of a person from the personal pictures posted by the person on internet or clicked by a person and changing the contents using some part of the picture using Software. Software that allow morphing could be misused to create obscene pictures of women where certain parts of the pictures are juxtaposed by using another picture. Such acts may constitute fabrication under Indian Penal

Code. Under Section 192 of the Indian Penal Code (Hereinafter referred to as 'IPC') which prohibits making of an electronic record which is false for the purpose of use in evidence. In case such picture is stolen by a person prior to morphing it may amount to hacking and after morphing if it is transmitted it may also amount to publishing or circulating obscene images violating Sections 67 and 67A of the Information Technology Act,2000. Section 463 of IPC defines 'forgery' and Section 469 of the IPC defines 'forgery for the purpose of harming reputation' and Section 470 of IPC defines 'forged document or electronic record'. The offence of forgery is punishable with imprisonment for a term upto to 2 years or fine or both. Forgery is non-cognizable, bailable, non-compoundable and triable by a Magistrate of First Class. Section 469 of IPC prescribes a punishment upto 3 years and fine for forgery for the purpose of harming reputation.

(viii) Identity theft:

A number of cases have been reported where fake profiles of women have been created on social media using their genuine pictures illegally used from the internet. This constitutes the offence of 'identity theft' which is punishable under Section 66C of the Information Technology Act (Hereinafter referred to as 'IT Act'). Any person who fraudulently or dishonestly makes use of the electronic signature, pass word or other unique identification feature e.g. photograph of a person

without his consent is punishable with imprisonment for a term upto 3 years and fine upto 1.00 Lac.

Complaints about Fake profiles can be immediately reported to the service provider such as Facebook or My Space who also have a 'report abuse button' and a legal department to take necessary action to block or take down such fake profiles.6 Section 79 of the IT Act,2000 requires an intermediary such as Facebook to remove such fake profiles from his service when actual notice is given to it. The necessary action must be taken within 36 hours from the receipt of actual written notice sent by the complainant. The I.T. (Intermediaries Guidelines) Rules, 2011 require an intermediary to remove such unlawful content within 36 hours.

According to the said guidelines, every intermediary is required to publish in its term and conditions warnings to users not to host, display or transmit or upload any data which is impersonating another person or contains any virus or is harmful in nature or that violates any law in force in India.

(ix) Spamming:

The erstwhile Section 66A of the I.T. Act prohibited the offence of spamming which means sending any unsolicited messages to a person to cause annoyance, inconvenience or to mislead the recipient about the origin of the message. Such acts were punishable with upto 3 years imprisonment and fine. However, after

[6] Karnika Seth, *Computers, Internet & New Technology Laws*, Lexis nexis, 2nd edition

such provision was struck down in the *Shreya Singhal versus Union of India* by the Supreme Court of India, there is no specific provision to deal with spamming in India.

(x) Cheating by impersonation:

In many cases specially on matrimonial sites fake profiles of men are posted where women may be cheated due to impersonation. A man who is married may portray to be unmarried and cheat a woman whom he promised to marry. In such cases, Section 66D of IT Act,2000 prescribes punishment for cheating by personation using a computer resource with imprisonment for a term which may extend upto 3 years and liable to fine upto Rs.1.00 Lac.

(xi) Virtual rape:

In many cases cyber victimization of a woman could occur where offender posts vulgar messages threatening to rape her and encourage other members to comment on his post. This would attract punishment for offence under Section 354A of the IPC and under provisions of the Section 4 of the Indecent Representation of Women (Prohibition) Act, 1986. Section 4 of the Indecent Representation of Women (Prohibition) Act,1986 prescribes punishment of upto 2 years, fine or both for publishing, sending any message containing indecent representation of women.

(xii) Cyber bullying:

When a harasser intimidates a woman online she is said to be cyber bullied. Though men are also cyber bullied,

women typically are targeted for example, just after an emotional break up or as domestic violence or as modus operandi of by an offender. This is punishable also as criminal intimidation under Section 506 of the IPC prescribing punishment of imprisonment upto 2 years or fine or both.

(xiii) Revenge porn:

In many cases, when a relationship between a man and woman gets estranged, the ex-friend or the ex-husband may post or publish pictures or video which are personal in nature and unauthorisedly circulate it to the targeted woman and her close friends. This is known as sending of revenge porn. There is no express provision using this term under the I.T. Act but it has provisions that can apply in this context. Sections 67 and 67A of the I.T. Act discussed hereinbefore and Section 354C of the IPC may apply. Even in case where the woman consents to the capture of images but not to their dissemination to third party, such dissemination is considered as offence punishable with imprisonment for a term not less than one year but may extend to 3 years.

(xiv) Domestic violence through verbal abuse:

In many cases where a man or a woman are experiencing relationship difficulties, one may vent out anger against the other on social media. Depending on the content of the message, if it contains sexual abuse, it may constitute sexual harassment under

Section 354A of the IPC or act to outrage modesty of a woman under Section 509 of IPC.

(xv) Extortion:

Cybercriminals may employ phishing technique to make unlawful financial gains or send phishing emails posing as if the mail has been sent by a genuine bank. Such mails are fake and sent with a view to unauthorisedly extract the personal sensitive information about one's Credit Card or net-banking details. A phisher could then rob one of monies and may even install viruses and steal data such as personal pictures and later extort the victim to get monies or sexual favours. This is known as sextortion. Extortion is an offence under the IPC under Sections 383 and 384 punishable with imprisonment upto 3 years or fine or both. The offence is cognizable, non-bailable, non-compoundable and triable by any Magistrate. If any person puts another in fear of injury, such person is liable to be punished for an imprisonment for a term upto 2 years and fine or both as per Section 385 of IPC. On the other hand if the extortion is for gaining sexual favours, it will fall under Section 354A of IPC punishable with imprisonment for term of one year, fine or both.

(xvi) Breach of Data:

Where personal sensitive data of a woman is stolen by a person fraudulently or dishonestly it will fall under Section 66 of the I.T. Act r/w Section 43 of the I.T.

Act, 2000 punishable with term of imprisonment of upto three years, fine or both. However, if such data is taken by a person who is authorized by the I.T. Act to collect such information and he without the consent of the person discloses such information, such act is punishable with imprisonment for a term which may extend to 2 years or with fine which may extend to Rs.1.00 Lac or both.

Section 72A of the I.T. Act puts similar obligation on private service provider such as phone companies. Anyone who without the consent of such person whose personal information they collect under a lawful contract, discloses it to a third person in breach of the contract knowing it will lead to a wrongful loss is liable to be punished with imprisonment upto 3 years or fine upto Rs.5.00 Lacs or both. In Matrimonial Litigations often spouses may file electronic evidence such as logs of a telephone number of their spouse obtained from the service provider to show infidelity as the volume of calls to a particular number may serve as evidence to substantiate the allegation. However, in case such logs are illegally given out by intermediaries, it breaches Section 72A of the I.T. Act making the intermediaries such as telephone companies liable.

CHAPTER 3

CYBER CRIMES AGAINST GIRL CHILD

In this e-book focus is not only on laws prohibiting cybercrimes against women who are 18 years of age and above, but also covers those women who are below 18 years of age. For protection of girl children on internet ,detailed book written by the Author,' Protection of Children on Internet' may be referred to as there are special acts in India that prohibit crimes against children such as the Protection of Children against Sexual Offence Act,2012 and the Juvenile Justice Act, 2015 which are discussed in greater detail therein. Though the scope of this book is limited, nevertheless, a brief discussion on laws protecting children from cybercrimes is dealt with in this chapter.

According to a recent survey conducted by Tata Consultancy Service 7 out of 10 children shop online, 76% children use Face Book. 9 out of 10 children have a mobile phone[1]. Another survey by Assocham reveals that nearly 60% of

[1] Tata (2014) TCS Gen Y 2013-'14

Indian teenagers view 125 messages in a day.[2] Recent studies have led to findings that Internet addiction is on the rise among children who show increase in signs of depression and anxiety.[3] Among the several threats to children online, the most common are sexual exploitation, child pornography and cyber bullying. According to a survey conducted by the Ministry of Women and Child Development in 2005, 53% of the children in India were reported to have been sexually abused.[4]

There are specific laws in India to protect children on the Internet such as law prohibiting child pornography and sexual harassment.

(i) Child Pornography-

Section 67B of the IT Act,2000 expressly prohibits child pornography. If any person publishes or transmits material depicting children in sexual explicit acts in electronic form or creates images text, calls, seeks, down loads, advertises, promotes or distributes contents that depict children in obscene manner, such person is punishable with imprisonment for a term which may extend upto 5 years and fine upto Rs.10.00 Lacs.

---

[2] "WhatsApp keeping Indian teenagers up at Mid Night", Times of India, 20th July,2014

[3] Goel D. Subramanium, A. Kamath, a study of prevalence of Internet addiction and its associate with Psychopathology in Indian Adolescents, Indian J Psychiatry, 2013 April and June,'55(2) page 140-143

[4] Ministry of Women and Child Development, Government of India (2007), a study of child abuse, India 2007 available at http://wcd.nic.in/childabuse.pdf

(ii) Child Grooming-

In case of child grooming activities, i.e. where a person entices a child into online relationship with one or more children for sexual explicit act or facilitates abusing children online or recording own abuse or that of others relating to sexual explicit acts with children such acts are punishable with imprisonment for a term upto 5 years and fine upto Rs.10.00 Lacs. In the event of second conviction, it is punishable with imprisonment for a term upto 7 years and fine upto Rs.10.00 Lacs.

(iii) Cyberbullying-

According to Global youth online behavior survey conducted by Microsoft 53% children between the age 8 and 17 in India were found to be the victims of cyber bullying.5 Most of these cyber bullying cases arise out of social media encounters covering 60% of these cases, whereas, mobile phones and online chatrooms comprised of the second and third category totaling 40% of such cases. Some commonly known forms of cyber bullying are *happy slapping* i.e. where a mobile or camera is used to record an incident where a child is being bullied and then circulated the same on social media. *Trolling* is another form of cyber bullying where abusing and hurtful submissions are made online on social media.[6] *Rumor spreading* is a form of cyberbullying

[5] Microsoft Safety and Security Centre, http://www.microsoft.com.security/resources/research.aspx

[6] Karnika Seth, *Protection of Children on the Internet*,Universal Publishers, 2015

where gossip is spread through email, pictures or other means. Girl child is most susceptible to receiving such threats online.

(iv) Photo Morphing-

Photo morphing is yet another crime targeting children particularly girl children where harmless pictures of girl children are morphed into obscene pictures and circulated online. In one such reported incident, a girl of 17 years committed suicide as her morphed picture was uploaded on Facebook along with her phone number and she had started receiving obscene calls and faced harassment.[7]

(v) Sexting-

Sexting is sending of sexually explicit messages through mobile phones. Sexting is also quite common as cyber criminals entice children to create their own selfies having obscene content and mail them instantly.[8]

(vi) Cyberstalking-

Cyber stalking is yet another rampant problem where a cyber criminal closely follows or stalks a child's activity online causing the child harassment or inconvenience. In one such case a 14 years old girl from Mumbai committed suicide due to cyber stalking wherein a boy had been posting her obscene pictures on her Face book account.[9]

---

[7] Girl kills over Face Book harassment (26th June,2014, Times of India)

[8] Sexting linked to risky sexual behavior among kids, July 8,2014, Times of India

[9] Gupta, S. (2013), November 20) Mumbai – allegedly stalked on Face Book by a friend, 14 years old commits suicide NDTV)

(vii) Other cybercrimes-

Among other rising crimes against children are online gambling enticing children into drugs, financial frauds targeting children through fake messages known as Phishing and injecting malware in mails, electronic files for breaching the privacy of children[10]. Children often watch DVDs or listen music and use the pirated versions could contain malware infecting the device used by them.[11] Identity theft and hacking into online accounts is yet another rampant problem as fake profiles of children are easily created on Social Networks by imposters and cybercriminals.[12]

Laws combating cyber crimes against children

India is a signatory to the *Convention on the Rights of the child,1990 (CRC)* and Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography. India has also ratified the Universal Declaration of Human Rights and its Covenants, the UN Convention against Transnational organized crimes and the Protocol to Prevent, Suppress and Punish Trafficking in Women And Children, SAARC Convention on Prevention and Combating Trafficking in

[10] Karnika Seth, Protection of Children on the Internet,Universal Publishers, 2015

[11] Microsoft and Truth Lab. (2014). Pirated and counterfeits of Software. Emerging risks and threats to Public Safety and National Security, a Forensic Analytical Report

[12] Seth, K. Speech (2012), October 5 at DPS School, Noida on Social Network sites vis-à-vis freedom of speech, presentation by Seth, K. (2010) learning with Social Media, Legal and Regulatory issues, AUME, 2010, Delhi.

Women And Children For Prostitution and Convention on Regional Arrangement For Promotion Of Child Welfare In South Asia And The Convention On Elimination Of All Forms Of Discriminations Against Women. To implement its mandate the National Commission for Protection of Child Rights was set up to examine the complaints of violation of child rights in India. There are two special Acts for protection of children in India relevant to the subject under discussion.

(i) Juvenile Justice (Care & Protection of children) Act,2015

The J.J Act,2015 implements provision of the Convention on the Rights Of The Child which India ratified in 1992. The JJ Act was enacted in 1986 amended in 2000 and the present Act is of 2015. The Second chapter of Act describes

general principles of care and protection of children, Principle of presumption of innocence, dignity and self worth, safety right to privacy and confidentiality, natural justice amongst other principles. The Third chapter of the Act provides for establishment of Juvenile Justice Board to decide juvenile justice related cases. It provides for setting up Observation Homes and Special Homes for children in conflict with the law. It provides provisions for adopting child friendly procedures for adjudication of cases, recording of testimony and evidence of children in conflict with law. For children who are victims of crime, it provides for special care and protection measures, rehabilitation measures apart from

protecting the identity of child. It also prescribes setting up of child welfare committees for welfare of children. The new J.J Act,2015 provides that juveniles between 16 to 18 years committing heinous offences can be tried as adults. This development was made after the Delhi (Nirbhaya) gang rape case.

(ii) POCSO Act,2012

To protect children from sexual abuse the POCSO Act,2012 has been enacted. Child Pornography is banned under Protection of Children from Sexual Offences Act,2012 which contains provisions against sexual assaults, sexual harassment and child pornography. Section 13 of the POCSO Act provides that whoever uses a child in any form of image for the purposes of sexual gratification which includes representing the sexual organs of a child, using a child in any real or simulated sexual acts, indecent or obscene representation of child, such person will be guilty of the offence of child pornography. Section 14 provides punishment for child pornography which would extend upto 5 years and fine on first conviction and in case of subsequent conviction imprisonment for a term upto 7 years and fine. Sections 13 and 14 are reproduced hereinbelow for easy reference: -

"Section 13. Use of Child for Pornographic Purposes. – *Whoever, uses a child in any form of media (including programme or advertisement telecast by television channels (whether or not such programme or advertisement is intended for personal use or for distribution),*

for the purposes of sexual gratification, which includes –

(a) *representation of the sexual organs of a child;*

(b) *usage of a child engaged in real or simulated sexual acts (with or without penetration);*

(c) *the indecent or obscene representation of a child, shall be guilty of the offence of using a child for pornographic purposes.*

Explanation:- For the purposes of this section, the expression "use a child" shall include involving a child through any medium like print, electronic, computer or any other technology for preparation, production, offering, transmitting, publishing, facilitation and distribution of the pornographic material."

Section 14 provides that the punishment for child pornography shall be imprisonment which can extend upto five years and with an imprisonment of a term which may extend upto seven years and also be liable to fine.

"Section 14. Punishment for using child for Pornographic purpose. – *(1) Whoever, uses a child or children for pornographic purposes shall be punished with imprisonment of either description which may extend to five years and shall also be liable to fine 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 be liable to fine.*

(2) If the person using the child for pornographic purpose commits an offence referred to in section 3, by directly participating in pornographic acts, he shall be punished with imprisonment of either description for a term which shall not be less than ten years but which may extend to imprisonment for life, and shall also be liable to fine.

(3) If the person using the child for pornographic purpose commits an offence referred to in section 5, by directly participating in pornographic acts, he shall be punished with rigorous imprisonment of description for a term which shall not be less than ten years but which may extend to imprisonment for life, and shall also be liable to fine.

(4) If the person using the child for pornographic purpose commits an offence referred to in section 7, by directly participating in pornographic acts, he shall be punished with imprisonment of either description for a term which shall not be less than six years but which may extend to extend to eight years, and shall also be liable to fine.

(5) If the person using the child for pornographic purpose commits an offence referred to in section 9, by directly participating in pornographic acts, he shall be punished with imprisonment of either description for a term which shall not be less than eight years but which may extend to extend to ten years, and shall also be liable to fine."

Section 15 of the POCSO Act prohibits storage of pornographic material involving a child with imprisonment upto 3 years or fine or both. The POCSO Act in Section 11 covers the several crimes targeting children online (and also offline) under the umbrella offence of sexual harassment such as child grooming, cyber stalking or other forms of child abuse including threats to use any obscene content involving a child in a sexual act. Section 12 makes sexual harassment a punishable offence with imprisonment for a term upto 3 years and fine. Section 20 of the POCSO Act puts an obligation

on Media, Hotels, Hospitals or Clubs to report any material containing child pornography by contacting the police[13]. Such proactive provision is not found in the IT Act,2000 as on date of writing. A person who fails to report the matter shall be punishable with an imprisonment for a term of six months or a fine or both. The POCSO Act provides for establishment of Special Codes in each District to try the offence under the Act. The National Commission for Protection of Child Rights or the State Commission for Protection of Child Rights in addition to the function assigned to them under the commission for Protection of Child Rights Act, 2005 monitors the implementation the POCSO Act[14]. The National Commission for Women has also been set up as statutory body in January 1992 under the National Commission for Women Act, 1990 to review the Constitutional and legal safeguards for women; recommend remedial legislative measures, facilitate redressal of grievances and advise the Government on all policy matters affecting women.

There is greater need to set up fast track courts and special tribunals established under POCSO Act to combat rising cybercrimes against children. Many States are still under process of establishing such tribunals. Government also needs to intensify its focus on to this area particularly in light of blue whale suicide incidents in the country to create national

[13] NCPCR, FIRE,i-probono, *Child Victims of Cybercrime legal Toolkit*, 2017

[14] K. Seth, "Overview of Laws against online child sex abuse in India, U.K, U.S", 2(1) *International*
Journal of Research 75 (2015) available at http://internationaljournalofresearch.org

policies that aim to prevent and combat such cybercrimes targeting children.

(iii) IT Act,2000: -

While the sections discussed earlier apply equally to girl children such as Sections 66E for invasion of privacy15 and 67A of IT Act,2000 for prohibiting circulation or publishing of sexually explicit content, Section 67B of IT Act,2000 particularly deals with the offence of child pornography and prohibits the same as well as the child grooming. The said Section is reproduced hereinbelow for reference:

"67B. Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form. – Whoever –

(a) *publishes or transmits or caused to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct; or*

(b) *creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or*

(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*

(d) *facilitates abusing children online; or*

---

[15] Karnika Seth "Inadequacy of laws Protecting children against Online Sexual abuse in India", 12(1)
Indian Journal of Human Rights & the Law 43-59 (2015).

(e) *record in any electronic form own abuse or that of others pertaining to sexually explicit act with children, shall be punished on first conviction with imprisonment of either description for a term which may extent 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 extent to seven years and also with fine which may extend to ten lakh rupees; Provided that provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting representation or figure in electronic form –*

(i) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting representation or figure is in the interest of science, literature, art or learning or other objects of general concern; or

(ii) which is kept or used for bona fide heritage or religious purposes."

In Kamesh Vaswani v UOI[16]*,* the Supreme court dealt with a PIL seeking directions from the court to block all child pornographic websites in india. The court formed a high level committee to suggest ways to curb and block child pornography on internet.

(iv) The Immoral Traffic Prevention Act,1956

The Immoral Traffic Prevention Act,1956 defines prostitution and sexual exploitation and abuse of persons for commercial reasons. The Act prohibits sale, procuring or exploiting any person for prostitution. The punishment is stricter if crimes are committed against the children

[16] 2014(6) SCC 705

below 16 years of age[17]. Section 5 of the Act states that if a person procures or induces a child for prostitution minimum term of 7 years of imprisonment is provided which can extend to life imprisonment.

(v) Indian Penal Code,1860

Under Indian Penal Code,1860(Hereinafter referred to as 'IPC') Section 292 of IPC prohibits sale, publication, distribution of obscene pictures which is punishable with a term upto 2 years and fine upto Rs.2000/- on first conviction. Section 293 of IPC prohibits sale, publication, circulation of obscene objects to persons below 20 years of age with a term of imprisonment upto 3 years and fine upto 2000/- on first conviction.

[17] NCPCR, FIRE,i-probono, *Child Victims of Cybercrime legal Toolkit*, 2017

Chapter 4

Case Studies on cybercrimes against women on India

According to the National Crime Record Bureau Report,2015 the number of cases publishing obscene information under Information Technology Act, 2000 rose from 97 cases in 2007 to 1203 cases in 2013. In 2014, 758 crimes were reported in which 491 people were arrested.[1] According to a recent survey commissioned by Norton, it was found that 8 out of 10 people in India have experienced online harassment wherein 41% of women became victim of Sexual harassment online.[2] The Indian Computer Emergency Response Team (CERT) reports that 27482 cases of cyber crime were reported from January to June,2017 in India which means in every 10 minutes there was a cyber attack in India.[3] Further, analysis of the data between 2013 and 2016

[1] National Crime Records Bureau Report, 2015

[2] Yuthika Bhargava, "8 out of 10 Indian have faced online harassment", The Hindu, 5th October,2017

[3] "One crime in every 10 minutes in the first six months of 2017, Live mint, 22nd July, 2017."

shows malware attacks accounted for 17.2% of crimes and India had witnessed 1.71 lacs cases of cyber crimes in the past three and a half years. The CERT was of the view that the number is likely to cross 50,000 by December 2017.

A common cyber crime targeting women is cyber stalking, which though affects both men and women, women are particularly targeted (specifically between 16 to 35 years of age).[4] According to a Report prepared by Centre for Cyber Victim Counselling, 80% victims had no knowledge that cyber stalking, cyber bullying and sending threatening messages is a punishable offence[5]. Hardly 8.3% of women reported such acts to the police. According to another study, a survey indicated that for every 500 cyber crime incidents, only 50 are reported to police, out of which only one is actually registered.[6] However, few cases have been reported and after prosecution, convictions have been made in some cases.

Case studies:

(i) ***State of Tamil Nadu versus Dr. L. Prakash***[7] **-**

In this Case, Dr. Prakash was convicted for committing Sexual harassment of women and posting their obscene

[4] Aggarwal and Kaushik "Cyber crimes against women" GJRM Vol.4 June,2014

[5] Debarati Halder (Centre for Cyber Victim Counselling (CCVC), India) and K. Jaishankar (Manonmaniam Sundaranar University, India), Cyber Crime and the Victimization of Women: Laws, Rights and Regulations,2011

[6] "For victims of cyber stalking, justice is elusive", Live mint, 22nd July,2016"

[7] 2002(7) SCC 759

pictures and videos on internet. Dr. Prakash was arrested in December,2001 and was booked under various sections of the Indecent Representations of the Women Act and the Indian Penal Code and was sentenced to life imprisonment.

(ii) ***Aarti Tiwari versus State of Chandigarh***[8] -

In this case also obscene video and photographs were taken at the clinic by the accused of their patients and the accused were tried under Section 509 of Indian Penal Code (Hereinafter referred to as 'IPC'), Sections 4 and 6 of Indecent Representations of the Women (Prohibition) Act ,1986 and Sections 66E, 67 and 72 of Information Technology Act,2000;

(iii) ***Avnish Bajaj versus State***[9] -

In this case an obscene MMS video was posted for sale on the website: www.bazee.com although the website had the required filter to detect such material, it failed to detect obscenity and published the same. Although notice was sent to the service provider, yet the clip was not taken down expeditiously and the Managing Director of the website was arrested for committing cyber crime of publishing obscene information online. An FIR was registered under Section 292 IPC, Section 67 of the I.T. Act, 2000 r/w Section 85 of IT Act, 2000. The MMS in question involved a video clip that was shot using a mobile phone wherein two children of a School

[8] MANU/CG/0285/2014
[9] MANU/DE/0851/2008

were seen to be in an obscene position. In a petition for quashing of charges filed by the accused, charges were dropped under Section 292, but not under Section 67 of the I.T. Act r/w Section 85 of the I.T. Act which contains provision for deemed liability of the director for acts of a company. However, in *Aneeta Hada* case charges under Section 67 of the I.T. Act were quashed as the company was not made a complainant in the case and only the Managing Director had been arraigned in *Aneeta Hada's* case;[10]

(iv) ***State versus Jawant Kumar Das***[11] **-**

One person named Jawant Kumar Das was arrested in 2012 for uploading remarks against a journalist's wife on an obscene website. He defamed the woman in order to take revenge on her husband who exposed his illegal money lending business in Print Media. The court held him guilty of posting the obscene material and convicted him of the charges framed against him.

(v) ***Yogesh Prabhu versus State***[12] **-**

In this case a senior executive of a private company was convicted for the offence of cyber stalking and sentenced to four months' imprisonment. The accused cyber stalked his colleague working in a Cargo Handling Farm and sent her pornographic images and videos.[13]

---

[10] *Aneeta Hada versus God Father Travels and Tours Pvt. Ltd.* – 2012 (5) SCC 661

[11] Manu /TN/0676/2002

[12] In the court of Additional Chief Metropolitan Magistrate, Mumbai, CC No. 3700686/PS/2009

[13] "Cyber Case Conviction in Maharashtra", Times of India, 3rd July, 2015

(vi) ***Ritu Kohli case*** –

This case pertains to cyber stalking as a woman named Ritu Kohli complained of receiving number of mails from an unknown source. The cyber stalker posted her phone number on various websites inviting people to chat with her. The IP address of the sender was tracked down and was found to be a Cyber Café. The cyber stalker Manish Kathuria got arrested by the Delhi Police and was booked under Section 509 of the IPC for outraging the modesty of a woman and under I.T. Act,2000.[14]

(vii) ***Neha Ghai case*** –

In another case of cyber stalking a 20 years old woman, Neha Ghai was shocked after receiving objectionable calls and messages on her mobile and vulgar emails. She lodged a police complaint against the accused for cyber stalking and the investigation took place by tracking the IP address of the system which the accused used to commit the offence.[15]

(viii) ***Salem case*** –

A 21 years old lady in Tamil Nadu's Salem District lodged a complaint against the accused for morphing her pictures and converting it into an obscene image and posting it on Face book. The woman told her parents about the man she suspected behind this act. She rejected his proposal for marriage. In a malafide

[14] Aggarwal and Kaushik "Cyber Crime against women" GJRM Vol.4, June,2014

[15] Aggarwal and Kaushik "Cyber Crime against women" GJRM Vol.4, June,2014

and revengeful manner he morphed her picture and uploaded it on Facebook. After the complaint was filed, another morphed image was tagged to her Face Book ID with her name and her father's phone number on it. On the same day, the woman committed suicide. In her Suicide Note she persistently stated that she had not sent any such picture to any one. Such cases are very unfortunate. Instead of combating crime with full faith and support in the victim and her actions, the fear of social stigma puts undue pressure on victim which compels them to commit such acts such as suicide.

(ix) ***MMS case - of an Adibasi girl in Birbhum***.

A 16 year old tribal girl who worked as a daily waged laborer was punished by the Local Panchayat for falling in love with a nontribal boy from a nearby village in June,2010, when she was stripped publicly and made to walk in the village and was sexually harassed, photographed by the villagers which was circulated in the village. Shockingly no case was registered against her attackers and reportedly the community leaders were the perpetrators of the crimes. However, the girl lodged the police complaint against 6 main accused who were arrested. She was housed in a government welfare home for her protection and is now continuing her education.[16]

Other important cases-

The judiciary has taken serious action incases involving targeted cyber attacks against women. One such case,

16 UNICEF, "Child Online Protection in India Report,2016

suo moto writ petition (In re: Prajwala letter dated 18th February,2015 Writ Petition (Crl.) No. 3 of 2015) dealt with videos of sexual violence distributed online. The Supreme Court passed an Order on 20th March, 2015 directing Google to track uploaders of said videos. Later on 5th December,2016 notices were issued to Microsoft and Face Book as well[17].

In *State of Maharashtra versus Dr. Praful B. Desai*, [18] the court held that for recording of a statement of a sexually abused victim, due precaution must be adopted and adequate provisions made to record statements through videoconferencing.

The court rightly held as follows:

"....Evidence can be both oral and documentary and electronic records can be produced as evidence. This means that evidence, even in criminal matters, can also be by way of electronic records. This would include video- conferencing. 13. One needs to set out the approach which a Court must adopt in deciding such questions. It must be remembered that the first duty of the Court is to do justice. As has been held by this Court in the case of Sri Krishna Gobe versus State of Maharashtra [(1973) 4 SCC 23] Courts must endeavour to find the truth. It has been held that there would be failure of justice not only by an unjust conviction but also by acquittal of the guilty for unjustified failure to produce available evidence. Of course, the rights of the Accused have to be kept in mind and safeguarded, but they should not be over emphasized to the extent of forgetting that the victims also have rights."

Sexual abuse of a girl child and sextourism is wide spread and is one of the worst forms of violence and discrimination suffered by women.

17 http://judis.nic.in/temp32015632032015p.txt)
18 2003(4)SCC 601

In the Landmark Judgment of *Vishakha versus State of Rajasthan*, the Hon'ble Supreme Court prescribed guidelines to protect women against sexual harassment.[19] In *Vishakha's* case – a Complaint Mechanism was prescribed to look into the complaints filed by women employees at their work place and the Complaints Committee was directed to be formed by every employer.

In *Shanker Kishan Rao Khade v State of Maharashtra*[20], *the* court dealt with issue of non reporting of cases of rape of minor girls and neglect of witnesses in lodging FIR. The Apex court held that it is duty of every citizen of India to report a case of sexual abuse against a minor. Non reporting of such crime is serious crime punishable under Section 21 of POCSO Act,2012.

19 1997 (6) SCC 241
20 (2013) 5 SCC 546

Chapter 5

Legal remedies to protect women against the cyber crime

In order to combat rising cybercrimes against women in India, greater cyber awareness is required and conscious proactive reporting of such incidents to law enforcement. There are special laws in India to prohibit different cybercrimes, and special courts set up to decide cases, particularly under POCSO Act,2012. However, to combat cybercrimes cyber training of police officers and members of Judiciary and the lawyer fraternity is the need of the hour.

There are special hotlines for reporting cybercrimes against women in India, such as 1091/1090 and free legal aid is also available by contacting the concerned State's Legal Services Authority office. National Commission for Women also offers immediate assistance to women seeking legal redress in India. In case where a woman becomes victims of cybercrime, it is important to preserve all the evidence found against the perpetrators of the crime including snapshots of the

objectionable post if any and the lodge police complaint in the nearest police station. In non-cognizable cases, a complaint may be filed before the Magistrate in the nearest court having jurisdiction. In such cases it is advisable to seek the professional help of the Cyber Law Experts for necessary guidance and legal support. Any computer/electronic data should not be tampered or deleted.If possible record any attacks of cybercrime by video/audio clips /CCtv/ and snapshots. You may also get a forensic analysis of a device through a forensic lab incase you suspect any spyware/malware on your mobile /laptop. One can seek logs of a telephone/mobile if you are getting calls from different phone numbers/ or a criminal is stalking a person. The Service providers handover logs to the authorized owner of a mobile phone. Mobile operators and telephone companies usually store such logs atleast for a period of one year. It is useful to substantiate your complaint with the help of such supporting proof/evidence.

In civil remedy, a woman may ask for compensation or damages for defamation or other crimes where compensation is payable as per law such as data theft Cases under Section 43 r/w Section 66 of the I.T. Act,2000 or approaching the nearest civil court having jurisdiction for blocking/injunction orders to block an objectionable page/post or seek other restraint orders.

One must inform the Internet Service Provider in case any objectionable video or fake post is found on any Social Media about the victim or if the email account has been compromised

and in similar other situations. The Internet Service Providers are mandated by law to appoint a Public Grievance Officer to resolve such issues and are required to respond within 36 hours of receiving actual notice of a written and signed complaint by the aggrieved party as per Section 79 of IT Act,2000 & rules framed thereunder.In such cases, they are mandated to preserve the evidence for further investigation of the complaint.

I hope readers found this concise e-book a useful read! If you have any queries, please mail me at karnika@sethassociates.com