



SETH ASSOCIATES



STAY SAFE ONLINE

ऑनलाइन सुरक्षा कवच



www.isea.gov.in

Women Rights Against Cyber Crime

By Dr Karnika Seth

AI Artwork by - Hasan Shahrukh

Handbook on women rights against cyber crime

Preface

With the advancement of information technology and rise in internet and mobile connectivity, internet has blurred the time and geographical divide. In India, in 2018, over 480 million internet users were across the country. This figure is projected to grow to over 660 million users by 2023. Internet's inherent feature of anonymity protects one's privacy but on the other hand, the cybercriminals misuse it to commit cyber crime, particularly against vulnerable sections of our society, including women and children.

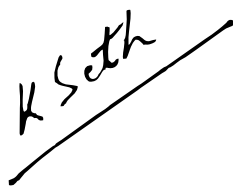
There is growing proliferation of cyber crime against women in the form of hacking, cyberstalking, video voyeurism, revenge pornography, sexting, sexual harassment, data theft, invasion of privacy, identity theft, sextortion, defamation, phishing and other computer related crimes. Traditional crimes which were committed offline in the past have shifted to online mode, often targeting gullible women and children. Cybercriminals garb fake identities or use dark web or proxy servers to hide their real identities and mask their IP addresses.

As per the NCRB Crime report, 2020, a total of 50,035 cyber crime were reported in 2020, up from 27,248 in 2018, an increase of 22,787 incidents of cyber crime within two years. Women and children are among the most vulnerable groups on the internet. According to the said report, a total of 10,405 incidents of cyber crime were reported against women in 2020, up from 6030 in 2018, with a glaring increase of 42%.

With the rapid increase in cyber crime against women, it is pertinent to empower women with cyberawareness on laws prevalent in India to combat cyber crime. This will not only be instrumental in preventing cyber crime, but will also increase reporting and more women seeking legal redressal of their rights.

This legal handbook is a concerted initiative in support of India's G 20 Presidency and 'Stay Safe Online' Campaign to empower women with the requisite knowledge of cyber laws to combat cyber crime. It is written in a simple Frequently Asked Question format for ease of understanding and reference. The Handbook can also be referred to by organisations working on women rights, Legal aid service authorities & literacy cells, teachers, parents, law enforcement agencies and other stakeholders involved in this process.

I am sincerely grateful to Hon'ble Justice Madan B.Lokur, Former Judge, Supreme Court of India for graciously writing the Foreword for this book. I also express my sincere gratitude to Lt Gen Rajesh Pant, National Cybersecurity Coordinator of India for writing a special Message for the book.



Dr. Karnika Seth

Advocate,

Supreme Court of India

Managing Partner, Seth Associates

New Delhi
Date: 23 February 2023

Justice Madan B. Lokur

Former Judge
Supreme Court of India

FOREWORD

In the recent past, there has been an increase in cyber crimes generally and an exponential increase in women-centric cyber crimes. Data provided by the National Crime Records Bureau suggests that the nature of women-centric cyber crimes includes publishing and transmitting sexually explicit material, extortion, blackmailing, morphing and fake profiles. This is worrying, to say the least. To make matters worse, cyber criminals are getting more sophisticated the use of technology and apprehending them and thereafter proving the guilt is becoming increasingly difficult.

Victims of such crimes are not particularly cyber literate and are unable to take any protective action, let alone any preventive action. What can they do in such a situation and what are their rights? Karnika has provided an answer to this question through her book on Women Rights against Cyber Crime. She is a renowned expert on cyber issues and is always in the forefront of women's rights and children's rights. It is therefore not surprising that she has devoted her time and expertise to deal with a subject that concerns not only individual victims but also society in general.

Karnika's book does not contain any jargon but has used simple language so as to reach computer illiterate persons. She has helpfully provided a glossary of terms which are heard from time to time whenever cyber crime is discussed. She discusses several kinds of cyber crimes and the rights of women. The discussion is not in the abstract but is with reference to the law and illustrative examples of various kinds of cyber crimes. The format used by Karnika is a simple question and answer format with a highly readable and simple explanation provided in respect of each type of cyber crime.

The effort put in by Karnika must be commended and encouraged. She has taken yet another step in the empowerment of women, a subject that is dear to her. Her book is ideal for use by every girl and woman, some of whom perhaps are unaware that they are victims of crime. She has lucidly treated a subject that most people are wary of discussing due to a lack of clear understanding on what constitutes a cyber crime. Karnika's discussion style would certainly appeal to everybody make it easier for them to deal with a variety of cyber crimes. The book is highly recommended for large circulation so that empowerment of women is possible in an area where few venture to tread.



Justice Madan B. Lokur

A-26, First Floor, Gulmohar Park
New Delhi - 110 049
E: madanlokur@outlook.com
M: +91 9868219007

Lt General (Dr) Rajesh Pant,
PVSM AVSM VSM (Retd)
National Cyber Security Coordinator &
Special Secretary to Government of India
Tel. : 011-23747965, 011-23451306
E-mail : ncsc@gov.in



सत्यमेव जयते

Government of India
National Security Council Secretariat
2nd Floor, Sardar Patel Bhavan,
Sansad Marg, New Delhi - 110001

MESSAGE

In the current technology driven world, Cybersecurity has become paramount for countering persistent cyber threats and preserving National Security. Cybersecurity is also the fulcrum for economic growth of any nation which cannot be achieved till its borders, enterprises and most importantly, citizens are cyber empowered! In the last few years, India has seen an unprecedented upsurge in Cyber-attacks, particularly on women, who being vulnerable, are often targeted by cybercriminals for harassment or illegal monetary gains. The Government of India has launched significant initiatives for bringing this much needed cyber awareness in India, inter alia, Digital India initiative, Information Security Education and Awareness (ISEA) of Ministry of Electronics and Information Technology (MeitY) and 'Cyber Jagrookta Diwas' of Ministry of Home Affairs (MHA), established to promote cyber awareness in the country.

I am delighted to write this Message for this remarkable hand book, '**Women rights against Cybercrime**' by Dr Karnika Seth, who is a veteran in the field of cyber laws and a practicing advocate in the Supreme Court of India and published by ISEA, Government of India on the special occasion of International Women's Day 2023! This handbook is a laudable initiative to empower women with knowledge to prevent and take a legal recourse against cybercrime.

Through this handbook, she supports Stay Safe Online Campaign by Ministry of Electronics and Information Technology during India's Presidency of G20 to sensitize women on their rights and legal remedies against cybercrime.

I wholeheartedly congratulate the author and the Information Security Education & Awareness project of the Ministry of Electronics & Information Technology, Government of India for publishing this excellent handbook to empower women of India with the required knowledge to effectively combat cybercrime!

'JAI HIND'

Place : New Delhi
Dated: 6th March, 2023.



(Rajesh Pant)

Message

Ch A S Murty,
Senior Director,
C-DAC, Hyderabad



As more and more aspects of our lives move online, cyber security is becoming increasingly important. In India, with a rapidly growing digital economy, cyber security is a crucial issue that needs to be addressed in order to ensure the safety and security of individuals, businesses, and the government. In recent years, cyber crime has become a growing concern for individuals, businesses, and governments around the world. While cyber crime affects people of all genders, women and children are often disproportionately impacted by this type of online crime. As such, a hand book that focuses specifically, on women and cyber crime is indeed a valuable resource for individuals, academics, and professionals alike.

This year during India's G20 Presidency, the Ministry of Electronics and Information Technology (MeitY), Government of India is taking up extended efforts to raises cyber security awareness among citizens. As part of this activity an awareness campaign called "Stay Safe Online" is in force and running successfully. For more details, please visit : <https://www.mygov.in/staysafeonline>

The women's handbook which is being released during this time of the year on 'Women's day' i.e, 08th March, 2023, provides necessary and useful information on cyber crime against women and legal provisions related to the same, and serves as good resource for raising cyber security awareness. The book elucidates in a Frequently asked Questions format, a range of topics related to women and cyber crime, including the types of cyber crime that disproportionately affect women, the psychological impact of cyber crime on women, combating cyber crime against women, including the Indian legal and regulatory landscape. This book is a significant contribution to strengthening cybersecurity and empowering women in India. It will serve as an important legal resource to raise awareness on the issue and empower individuals and organisations with the knowledge needed to protect themselves against cyber crime . It will also encourage reporting and legal recourse against cyber crime.

We sincerely acknowledge the efforts of Dr. Karnika Seth, Advocate, Supreme Court of India who has authored this handbook in collaboration with ISEA Project of Ministry of Electronics and Information Technology (MeitY) , Gol in support of India's G20 presidency and 'Stay Safe Online campaign'.

“Securing your digital world,
one page at a time. Happy reading!! “

Index

Glossary	7
Abbreviations	11
Introduction	12
Chapter 1	13
Introduction on cyber crime laws	
Chapter II	18
Women rights against cyber crime	
Trolling	19
Cyber bullying	21
Online sexual harassment	22
Violation of privacy	24
Voyeurism	25
Virtual rape	26
Cyber stalking	27
Sending obscene content over the internet	29
Cyber defamation	31
Morphing	32
Cyber pornography	34
Child grooming	37
Extortion	38
Identity theft	39
Cheating by personation	41
Data theft	42
Spamming	43
Bibliography	45

Glossary

Access

Getting entry into a computer system, computer network or any communication device such as a smart phone

Anti-virus

A program / software that protects a computer system from virus attacks so that the computer functions properly and protects data saved in a computer.

Attachments

a text, visual or audio video file that is sent along with an e-mail or a chat message.

Cognizable offence

Where police can register FIR, investigate complaint and arrest an accused without warrant from a court.

Bitcoin

A type of digital currency that uses blockchain technology or encryption and not controlled by a central distribution system.

Consent

Two or more persons are said to consent when they agree on the same thing in the same sense.

Computer Network

interconnection of one or more computers or computer systems or communication device through satellite, wireless, microwave, terrestrial line or other communication media

Communication Device

means cellphones, personal digital assistance, or other electronic device used to communicate, send or transmit any text, video, audio, or image.

Cyber

Relating to information technology / internet.

Cyber Bullying

Annoying a person, especially a child, by sending abusive, sexually colored or insulting messages to a child with the intention to intimidate. Such messages may be sent through social media or any other electronic means.

Cyber crime

Criminal act committed using computer as a means of causing harm to a person or one's computer device or computer resource such as data or database.

Cybersecurity

Protecting information, computer, computer network, communication device and information stored therein from unauthorized attacks, use, disclosure, disruption or damage

Glossary

Cyberstalking

Using computer or other communication devices or social media to monitor a person's online activities to cause inconvenience or harassment to a target person.

Data

It is a structured representation of facts, concepts or instructions that is suitable for use by a human or a computer or communication device.

Dark web

Internet that is hidden using masked IP addresses or proxy servers.

Dishonestly

Doing anything with the intention of causing wrongful gain to one person or wrongful loss to another person (Section 24, Indian Penal Code, 1860)

Defamation

Harming someone's reputation by words, written or oral, that are published online is cyber defamation.

E-mail

Method of exchanging messages using a computer or a mobile device.

Electronic Signature

Signature made in electronic form to distinguish one person from other. It may include a simple signature made on a touch screen, password, biometric fingerprint, iris or retina scan or any other form of unique identification.

Fraudulently

A person is said to do something fraudulently if he does that thing with an intent to defraud but not otherwise (Section 25, Indian Penal Code, 1860).

Grooming

Enticing a child by sweet talk into doing sexually explicit content over internet.

Hacking

Unauthorizedly gaining access into a computer system or a network to access, alter, copy, extract or destroy data, or introduce a virus, commit denial of service attack, disruption of services or facilitate such acts

Intermediary

Any person who on behalf of another sends, receives stores or transmits that record electronically such as internet service providers, online market places

Intimidation

Threatening someone of physical harm or harm to their property, with the intention to force them to do or not to do something which otherwise they would not do.

Glossary

Keylogger

Software which tracks the keys pressed by the user on a computer / communication device without his/her knowledge.

Malware

Software like spyware and virus, worms, trojans that infect or take control of a computer or mobile device.

Morphing

Superimposing one photo over another to create a completely new photo used for harassing someone or to commit extortion.

Online

State of being connected to a computer or a communication device which is connected to an internet network.

Phishing

A financial crime where a criminal sends a fake email or message to steal personal financial data or password(s) to cause unauthorized debits to one's bank account or e-wallets.

Privacy

State in which a person does not want to be observed or disturbed by anyone.

Revenge pornography

Publishing, transmitting or distributing sexually explicit pornographic clips or images of a person who has an estranged relationship with the offender

Service Provider

A company / organisation that provides its services over internet

Sexting

Sending sexually explicit content including images, photos, videos or other material in the form of a message using internet, computer, or communication device.

Sextortion

Act of putting a person in fear or threat to gain sexual favours

Simulated

Fake, imitating the real such as fake photos

Social Media

Social Media is an online service provider that allows third parties to share their ideas, opinions, and information on their platform through the internet

Glossary

Software

Set of data, instructions or programmes that allow the user to control a computer and perform specific functions or tasks on it

Spam

Unsolicited messages that cause annoyance or inconvenience to a recipient sent by an entity, person or as automated service

Spyware

Spyware is harmful software that collects information about a person or organisation and sends it to a third party in order to invade the privacy of a user or steal personally sensitive data to harm a user

Trolling

Sending offensive messages to someone, or posting offensive messages over the internet with the intention to annoy or insult that person. (Section 24, Indian Penal Code, 1860)

Virus

It is a malicious software which replicates itself and travels from one computer to another, causing harm to the data and software or a computer / communication device.

Woman

The word 'woman' means a female human being of any age (Section 10, Indian Penal Code, 1860)

Abbreviations

CD	Compact Disc
CSAM	Child Sexual Abuse Material
FIR	First Information Report
IPC	Indian Penal Code, 1860
IT	Information Technology
IT Act	Information Technology Act, 2000
POCSO Act	Protection of Children from Sexual Offences Act, 2012
JJ Act	Juvenile Justice (Care and Protection of children) Act, 2015
MMS	Multimedia Messaging Service
NCRB	National Crime Records Bureau
NCW	National Commission for Women
VOIP	Voice over Internet Protocol

Introduction

The advent of internet has proved to be a powerful means of publishing and dissemination of information, communication, entertainment and transacting business. The increased access to technology and ease of use also reduced the digital divide in urban and rural populace in India. However, inherent anonymity in cyberspace and lack of cyber awareness among general public led to steep rise in cyber crime in India. Cyber criminals often target vulnerable sections of the public, particularly women and children and senior citizens. According to National Crime Records Bureau, cyber crime against women has increased by 28% since 2019. Therefore, it is imperative to promote cyber safety awareness in general, and particularly, among women in India.

This book elucidates the different cyber crime against women in India, including invasion of privacy, video voyeurism, trolling, sexual harassment, sextortion, cyberdefamation, phishing, identity theft, data theft amongst other crimes. It informs readers in a simple 'Frequently Asked Questions' format about the best practices to prevent cyber crime and legal rights under Indian laws available to women who are target of a cyber crime. Besides equipping readers with key cyber safety tips, the book explains social engineering traps criminals use to defraud women to commit sextortion, QR code frauds or lure them into fake 'work from home' schemes. The book provides guidance on incident reporting, and necessary steps to seek legal recourse against cyber crime. The book explains the process to lodge a police complaint, right to seek compensation, blocking of fake accounts, objectionable content amongst other legal recourse available to women in cyber crime cases. It also encourages women to report cyber crime (which can even be reported anonymously) and explains the importance of preserving electronic evidence for investigation of the complaints.

The book refers to key provisions of the Information Technology Act, 2000 which are applicable to cyber crime. The Indian Penal Code (IPC), 1860, the Protection of Children from Sexual Offences (POCSO) Act, 2012, and Juvenile Justice (Care and Protection of Children) Act, 2015 are other relevant laws that are referred to in the book while explaining various cyber crime and key ingredients that amount to an offence under the said laws. The author has written the book in a simple & easily comprehensible manner and incorporated a glossary of cyber terms for the benefit of its readers.

In support of the India's G 20 Presidency and 'Stay Safe Online' campaign of the ISEA, Ministry of Electronics & Information Technology, Government of India, this book aims to empower women with cyber awareness. It focuses on imparting practical knowledge to effectively curb and combat cyber crime against women.

Chapter I

Introduction On Cyber crime Laws



Q What are cyber crime and which laws provide punishments for cyber crime?

A Any crime committed using computers, internet or information technology or a communication device such as mobile phone where either these are used as a medium to commit a crime or become a target of crime such as sexual harassment or hacking of data is known as Cyber crime.

The Information Technology Act, 2000 (hereinafter referred to as the "IT Act") contains special legal provisions that deal with various cyber crime such as violation of privacy, publication of sexually explicit content, amongst other computer related crimes. Indian Penal Code, 1860 also provides certain important provisions to protect women from cyber crime such as Section 354A prescribes sexual harassment committed online is a punishable offence with punishment of three years or fine or both. For cyber crime against girl child, Protection of Children from Sexual offences Act, 2012 is the special law that prescribes punishment upto five years of imprisonment for child pornography and upto three years for sexual harassment.

Q What is a 'Communication device' under IT Act, 2000?

A Section (1) (ha) of the IT Act, 2000 defines a communication device as cellphones, personal digital assistance or combination of both or any other device used to communicate or send any text, video, audio or images.

Q What are different kinds of cyber crime against women?

A There are various cyber crime targeting women such as cyberstalking, sextortion, revenge porn, trolling, sexting, data theft, amongst other crimes. Cases of cyberstalking and bullying of women have risen from 872 in 2020 from 739 in 2018. Conviction rate for publication or transmission of sexually explicit content is 47.1% while in case of cyberstalking and bullying it is at 27.6%. Cases targeting women with explicit content have doubled in past three years. According to NCRB report, 2020, U.P. (2, 2120) has highest number of cases involving sexually explicit content online followed by Assam (1,132). Cases of sexual explicit content rose 110% to 6308 from 3076 and these figures may not give real picture due to under reporting.

Q Where should a cyber crime be reported?

A If any woman becomes a victim or is being attacked by a cybercriminal online, it should be reported to nearest cyber crime cell or electronically on www.cybercrime.gov.in or on women helpline 1091, or 100, or 1930. Complaint can also be filed anonymously on www.cybercrime.gov.in. There is also a concept of zero FIR which means that if a woman is a target of any cyber crime when she is not in her domicile state, she can file FIR electronically on www.cybercrime.gov.in irrespective of where offence is committed from. For children, national helpline number is 1098. Most police stations have a cyber-cell in each district equipped to investigate cyber crime. A state wise list of cyber crime cells is accessible at <https://infosecawareness.in/cyber-crime-cells>. The National cyber crime reporting portal started in 2018, in 2021 received 600000 complaints including crimes against women out of which FIR was registered in 12776 cases.

Q Who is empowered to investigate cyber crime under IT Act, 2000 in a police station?

A A Police officer of rank inspector and above is authorized to investigate cyber crime complaints. Under Section 80 IT Act, 2000, police officer not below rank of inspector or other officer of Central or State Government authorized by Central Government may enter any public place and search and arrest without warrant any person found therein reasonably suspected of having committed or about to commit an offence under the Act.

Q Are there special courts under IT Act, 2000 to decide cyber crime cases?

A In India, the criminal courts that hear general criminal matters also decide cyber crime cases. For civil contravention, office of Adjudicating Authority is established by IT Act, 2000 to grant compensation for unauthorized access, alteration or damage to data and such cases under Section 43,43A of IT Act, 2000. At present, the appointed Secretary, Information Technology of every State is empowered to decide civil contravention cases. A Complainant needs to file a cyber crime complaint in nearest police station in case of cognizable offences and in non-cognizable offences, before nearest court of competent jurisdiction.

Q What is a cognisable offence?

A A cognizable offence is a criminal offence in which the police is empowered to register an FIR, investigate and arrest an accused without arrest warrant issued by a Court.

Q What is a non bailable offence?

A If a person is arrested for an offence which is non bailable, a Court in its own discretion can grant bail.

Q Are the offences under IT Act, 2000 compoundable?

A Under the IT Act, 2000, Section 77A provides that a Court will not compound (settle or compromise charges made) any offence where such offence affects socio economic conditions of the country or has been committed against a child below 18 years or a woman. In other cases, a Court of competent jurisdiction may compound offences other than offences for which punishment for life or imprisonment for a term exceeding three years has been provided. However, Court will not compound such offence where due to previous conviction such offender is liable to either enhanced punishment or punishment of a different kind.

Q Is there a special law dealing with cyber crime against children?

A Yes, POCSO Act, 2012 is a special law that prescribes legal provisions that prohibit child pornography (Child Sexual Abuse Material or CSAM) and sexual harassment of a child, including cyber crime.

Q What is abetment of an offence and whether it is punishable?

A Abetment of an offence means instigating a person (including by willful misrepresentation or concealment) to do that offence or engaging with others to commit the offence or intentionally facilitates in commission of offence. A person who abets an offence is punishable with punishment provided for that offence. This position is same under both IT Act, 2000 and POCSO Act.

Section 16 of POCSO Act describes meaning of abetment and Section 17 provides punishment therefor.

Likewise, under IT Act, 2000, same punishment for abetment is provided under Section 84B.

Q What is punishment for attempt to commit a cyber crime?

A Both under IT Act, 2000 (Section 84C) and under POCSO Act (Section 18) attempt to commit an offence is punishable with one half of longest term of punishment provided for that offence or fine or both. In POCSO cases, it may even extend to one half of imprisonment for life or fine or both.

Q Is there a provision for keeping identity of a girl child or woman undisclosed when she seeks legal recourse under POCSO or cyberlaw?

A Yes, proceedings in sensitive matters such as sexual harassment cases (such as Section 376 IPC) or under POCSO Act (Section 26) are held in camera, that is, in presence of parents or trusted persons and not in open court. Even norms of journalistic conduct stipulate that while reporting crimes against woman and children their identity and personal details ought not to be published. POCSO Act in Section 23 provides a child's name, address, photograph, family details, school, neighborhood or other details that disclose identity of the child shall not be disclosed. A Special Court trying a case may permit disclosure only if in the interest of the child. Violation of this duty attracts punishment of imprisonment of not less than 6 months but may extend to a year or with fine or both.

Q Is there any restriction in POCSO law on commenting or passing remarks on cyber crime against children?

A As per POCSO, Section 23 obligates one not to make any report or present comments on any child from any form of media or studio or photographic facilities without having complete authentic information that damages his reputation or infringes one's privacy.

Q Can a woman only file a criminal case under IT Act, 2000 or there are civil remedies too?

A A woman can file a civil case apart from criminal complaint under IT Act, 2000. A woman can file a civil action claiming compensation under Section 43 of IT Act, 2000 for any unauthorized access, copying, alteration, deletion of data from her computer system or communication device or introduction of a virus, disruption of a computer system, denial of access attack, amongst other acts mentioned in Section 43 of IT Act, 2000. An Adjudicating officer is empowered to decide such complaints and award compensation considering amount of unfair advantage as result of default, amount of loss caused to any person, repetitive nature of the default. Appeals from orders of Adjudicating Authority lie before the Telecom Disputes Settlement & Appellate Tribunal. A person aggrieved by the decision of the Appellate Tribunal can apply to the High court of concerned State within 60 days of the decision.

Q Are children also liable when they commit cyber crime?

A Yes, but in case of minors, Juvenile Justice Act, 2015 applies which provides procedural safeguards in case of children in conflict with law. Under JJ Act, special provisions have been made in respect of child offenders committing heinous offences in age group of 16-18 years. The Act mandates setting up of Juvenile Justice Boards and Child Welfare Committees in every district.

Q How can a woman get an objectionable post or message blocked from internet?

A A woman can seek removal of an objectionable post from internet by writing to the public grievance officer of the particular website whose details are published on the concerned website. Section 79 of IT Act, 2000 requires social media companies and other intermediaries to reply and take required action within 24 hours of receipt of actual complaint incase of obscene material and within 72 hrs in other cases. If notified by appropriate government or its authorized agency blocking directions may be given or through a court order blocking directions may be passed against intermediaries / websites.

Q Is there any free legal aid available to draft a complaint or file a legal case?

A Yes. A woman who has been target of cyber crime can avail free legal aid services by writing to NALSA office or its State legal Aid Services Authority.

Q Are screenshots of evidence or messages received on social media, videos or posts on websites accepted as evidence in a court of law?

A Yes, electronic evidence is accepted in a court of law if submitted as per procedure prescribed under Evidence Act, 1872, particularly Section 65A and 65B, which requires an affidavit to be filed by person producing the evidence. In order to investigate a crime, police may take mirror image of concerned device and send it for analysis to a central forensic analysis laboratory for forensic reporting.

Q How long will service providers retain transaction data on receipt of a complaint?

A An intermediary such as an online service provider/social media company is liable to retain relevant transaction data for atleast 180 days on receipt of a complaint. This is as per IT (Intermediaries Guidelines and Digital Media Ethics Code) Rules, 2021.

Q What online resources should a woman use as antivirus and antispyware?

A There are various free and paid versions of online safety as antivirus and antispyware such as by Norton, McAfee, Quick Heal Kaspersky amongst others. Software such as Zone Alarm even enable filtering of internet content unfit for viewing by children and helps monitor social media content and send an alert in real time when a suspicious post / message is sent to a child.

Q What are best practices for cyber safety?

A . Some important best practices for cyber safety are mentioned below-

1. Install latest configuration Wi-Fi
2. Keep strong passwords and use two factor authentication
3. Use password manager and change passwords periodically.
4. Never share content that is sexually explicit or obscene with anyone
5. Do not accept friend requests from strangers
6. Avoid posting inflammatory content/ hate speech / personal sensitive data
7. Block suspicious profiles / social media accounts
8. Beware of clicking links from untrustworthy sources
9. Report any suspicious or objectionable content to law enforcement authorities such as police
- 10.Keep screen shots of electronic evidence and don't delete content that needs to be reported
- 11.Type an address in URL, particularly while using net banking to safeguard yourself from phishing attacks and malicious links.
12. Read terms of use and privacy policy of websites / apps before you consent or give permissions / disclose personal data
- 13.Maintain regular backups of data
- 14.Update the operating system and software on your electronic devices.
- 15.Inform your bank incase you change your mobile number to receive alerts.
- 16.Don't leave your computer or mobile unattended.
- 17.Shop or pay online only on https websites and beware of fake advertisements or calls.



Chapter II

Women Rights Against Cyber crime

Trolling

What is trolling?

Trolling means posting messages or comments on the internet to harass, annoy or insult someone or invoke extreme emotional response or argument. Women often become targets of gender based online trolling for freely expressing their views and expressions on any sensitive subject. Such trolling may include verbal abuses and threats, including threats to hurt the woman physically or damage her reputation. Such trolls often cause mental and physical stress to the victim. A recent example is the reported Bullibai app incident wherein a cybercriminal uploaded pictures of several muslim women including journalists and activists on the app for purposes of auction to harass them.

What legal provisions protect women from trolling?

There is no provision using the term 'trolling' under Indian law. However, in law trolls may be prosecuted for criminal intimidation, insulting the modesty of a woman, and sexually harassing the woman online.

What is criminal intimidation?

Any act of a troll who threatens to cause injury to the person, property or reputation of a person, or any person in whom she is interested, amounts to criminal intimidation under Section 503 of the Indian Penal Code (IPC), 1860.

Elements of criminal intimidation are:

- Threatening a woman,
- To cause injury to her person, reputation, or property, or
- To cause injury to the person, reputation or property of anyone she is interested in,
- With the intent to
 - Cause alarm, or
 - Cause that person to do anything which he/she is not legally required to do, or
 - Cause that person to omit to do something which he/she is legally bound to do.

Cyberbullying is also a form of criminal intimidation as the intention is to put another person under threat.

1



What is the punishment for criminal intimidation?

The punishment for criminal intimidation is imprisonment that may extend up to 2 years, or fine or both.

If the intimidation is by an anonymous communication (by concealing one's location or identity using technical tools), the punishment includes an additional imprisonment term of 2 years. It is a non-cognizable and bailable offence.

What amounts to insulting the modesty of a woman?

As per Section 509 of the IPC, uttering any word, or making any sound or gesture, or exhibiting any object, with the intention that:

- such word or sound shall be heard by the woman, or
- such gesture or object shall be seen by the woman, or
- which intrudes upon her privacy.

Such act(s) amounts to insulting the modesty of a woman and includes a female child.

What is the punishment for insulting the modesty of a woman?

A person found guilty of insulting the modesty of a woman shall be punished with simple imprisonment for a term which may extend to 3 years and fine.



Harassment via e-mail?

Don't Panic
Save the Evidence & Report at
Cyber Crime Cell



2 Cyber Bullying

What is cyber bullying?

Bullying is harassing or threatening someone with unwanted and repeated written, verbal or physical behaviour. Bullying may involve hurling abusive, sexually tinted, derogatory remarks, or threatening or insulting a woman. When acts of bullying are committed through use of internet, it is called cyber bullying.

Women may become targets of gender based cyber bullying just after an emotional breakup, or cyber bullying may be used as a means of domestic violence. Different forms of cyber bullying include 'happy slapping' and 'rumour spreading' and 'trolling'.

Never retaliate to the provocative comments of the bully

Understand that others reaction is not your fault

Reach out for help, talk to your parents and friends

Save evidence and the screen shots for referring to the incident later

What is the law against cyber bullying?

There is no legal provision defining or using the word cyberbullying. However, Section 506 of IPC that punishes Criminal intimidation deals with and covers acts that amount to cyberbullying as its main aim is to threaten a target person.

What is Happy Slapping?

Happy Slapping is when the offender physically attacks the person targeted with the sole purpose of recording the assault and circulating so as to humiliate the targeted person.

Online Sexual Harassment

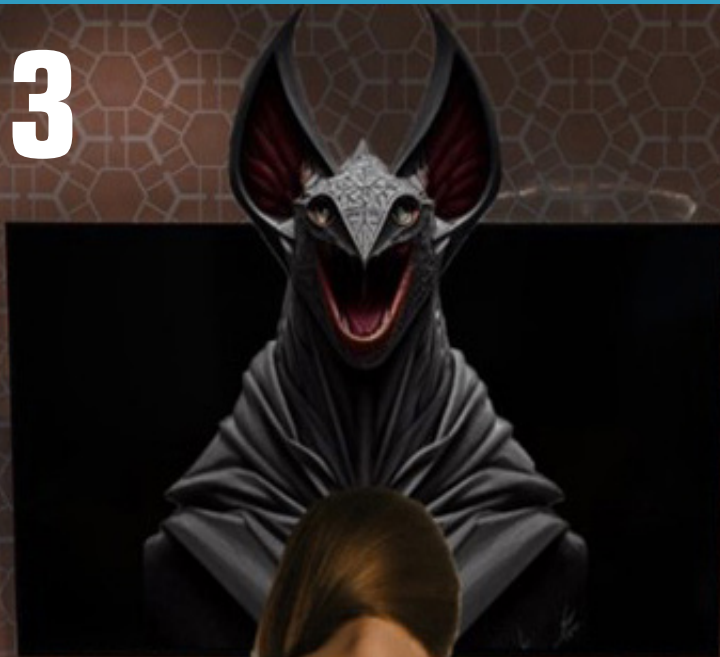
What amounts to sexual harassment of a woman?

Sec. 354A IPC defines sexual harassment of a woman as including any of the following acts committed by a man:

- physical contact and advances involving unwelcome and explicit sexual overtures; or
- a demand or request for sexual favours; or
- showing pornography against the will of a woman; or
- making sexual coloured remarks

If trolls targeting a woman include sexually coloured remarks, or demand or request sexual favours, it amounts to sexual harassment as provided above.

3



If you observe any objectionable or abusive content on social media, report on the social media help centre about it

Do not open attachments from people you do not know

Be aware that what you write and publish online has far reaching effect.

What is the punishment for sexual harassment?

The punishment for physical contact or advances, demanding or requesting sexual or making sexually coloured remarks is rigorous imprisonment that may extend upto 3 years, or fine or both. The punishment for making sexually coloured remarks is imprisonment upto one year, or fine or both.

What amounts to sexual harassment of a woman over the internet?

It has become very easy for a cybercriminal to garb a fake identity or create a fake social media account to contact a woman on social media. Often fake identities are intentionally created and used to contact women and young girls, with a criminal intent to sexually harass by sending offensive messages. If the purpose of these messages is to sexually harass the woman by demanding or requesting sexual favours, making sexually explicit remarks, showing the woman pornography against her will, or making sexually coloured remarks, the sender is guilty of sexually harassing the woman online, under section 354A IPC, as has been explained above.

What is the punishment for sexually harassing a woman online?

The punishment for demanding or requesting sexual favours or showing the woman pornography against her will is rigorous imprisonment that may extend upto 3 years, or fine or both.

The punishment for making sexually coloured remarks includes imprisonment upto one year, or fine or both.

Is there a special provision for minor victims of online sexual harassment?

In addition to sec. 354A of IPC, if the person targeted is a minor, that is below 18 years of age, the offender would also be liable under Sec. 11 and 12 of the Protection of Children from Sexual Offences (POCSO) Act, 2012.

What is sexual harassment of a child under the POCSO Act?

Under the POCSO Act, Section 11 provides following acts amount to online sexual harassment of a child: A person with sexual intent-

- uttering any word/ or making any sound or gesture or exhibiting any object with the intention that the act will be seen, or the sound would be heard by the child
- exposing any part of the body online with the intention that it is seen by the child.
- Forcing the child to exhibit his/her body online for viewing by the offender or any other person.
- Showing an object to a child for pornographic purposes
- Repeatedly watching or following the child through electronic, digital or other means
- Threatening to use in any form of media, either real or fabricated, any part of the body of the child, or the involvement of the child in a sexual act.
- Enticing the child for pornographic purposes.

What is the punishment for Sexual Harassment under the POCSO Act?

Under the POCSO Act a person held guilty for sexual harassment shall be punished with imprisonment, either rigorous or simple, which may extend to three years, and shall also be liable for fine.

Violation of 4 Privacy

What amounts to violation of privacy of a woman?

Under Section 66E of the Information Technology Act, 2000, capturing, publishing or transmitting online the images of the private parts of a woman, under circumstances which would violate her privacy, amounts to infringing her privacy.

What are the circumstances under which a woman's privacy may be violated?

Privacy of a woman may be violated in circumstances in which a woman can have a reasonable expectation that:

- She can disrobe in privacy, without an image of her private parts being captured; or
- Any part of her private area would not be visible to the public, regardless of whether that person is in a public or private place.

It is a cognizable but bailable offence and shall be punished with imprisonment for upto three years or fine not exceeding 2 lakh rupees or with both.

What are considered to be the private parts of a woman for violation of privacy?

Under the IT Act, the private parts of a woman include her naked or undergarment clad genitals, her pubic area, her buttocks or her breasts.

What is the punishment for violating the privacy of a woman?

Whoever intentionally violates the privacy of a woman shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.

Are there any other legal provisions protecting a woman's privacy?

Yes, Section 72 of IT Act protects a woman's data by providing punishment for breach of confidentiality and privacy. As per Section 72, any personal information of a woman obtained without her consent by a person and disclosed or made publicly available is an offence. Similar provision exists under Section 72A of IT Act, 2000 in respect of private service providers who access woman's record under a lawful contract such as a telephone company. It is a non-cognizable and bailable offence with imprisonment of upto 3 years or fine of 5 lac or both.

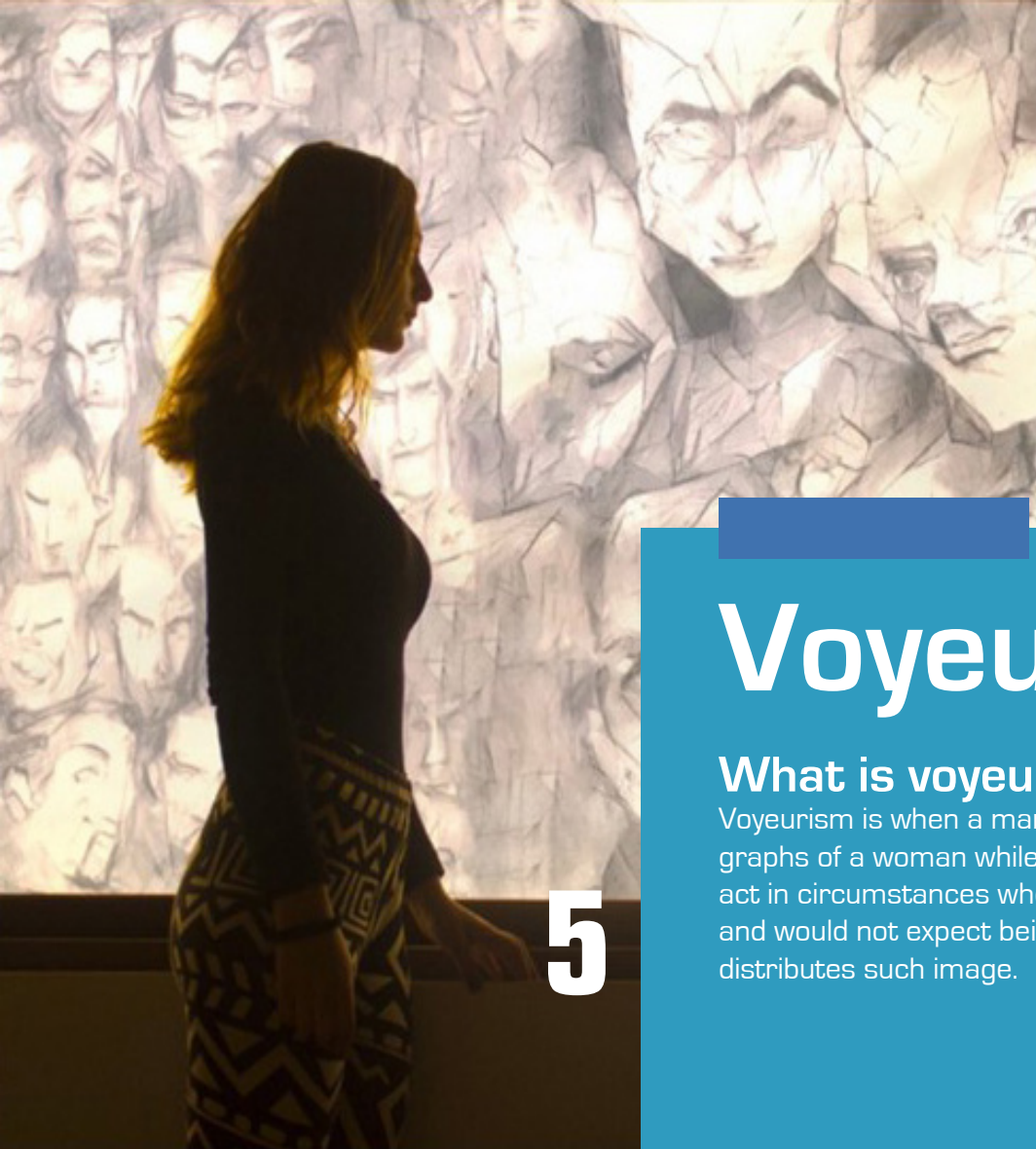
Know how to

 **Block**

 **Report**

 **Filter**

the content in
social media platforms



5

Voyeurism

What is voyeurism?

Voyeurism is when a man watches or takes photographs of a woman while she is engaged in a private act in circumstances where she would expect privacy and would not expect being observed by anyone or distributes such image.

What is the law against voyeurism?

Voyeurism is punishable under Section 354C IPC. According to the Section, the elements of voyeurism are:

- Man watches, captures or disseminates image of a woman
- while she is engaged in a private act,
- in private circumstances,
- where she would expect privacy, and
- not expect being watched by anyone.

In the Hyderabad voyeurism Case, the accused was in a relationship with a woman. After the woman declared the end of the relationship, he started blackmailing her with obscene videos he has, secretly taken of her and began circulating these videos on internet. The woman registered a complaint and he was charged under 354C IPC and relevant sections of the IT Act. [Retrieved from <http://www.ndtv.com/hyderabad-news/revenge-porn-case-in-hyderabad-video-mailed-to-woman-in-law-1427434>]

What is a private act under Section 354C IPC?

A private act is an act, in circumstances, which would reasonably be expected to provide privacy, and where the victim's genitals, posterior or breasts are exposed or covered only in underwear; or the victim is using a lavatory; or the victim is doing a sexual act that is not of a kind ordinarily done in public.

What if the woman had consented to capturing the image, but not to its dissemination?

If the woman had agreed to the capturing of the image, but not to the dissemination, but it is anyway disseminated to a third person, such dissemination shall amount to voyeurism under the section 354C IPC.

What is the punishment for voyeurism?

As per Section 354C IPC, in case of first conviction, the perpetrator shall be punished with imprisonment, of either description, for a term not less than three years, but which may extend to seven years, along with fine.

Copy/screenshot of alleged contents/profile

Screenshot copy of URL of alleged contents

Is voyeurism an offence under any other Section of cyberlaws?

Yes, apart from Section 354C IPC, Voyeurism is an offence under Section 66E of the IT Act, as has been explained hereinabove.

In one case, a MMS clip of two undergraduate students of a university was recorded by two other students of the University. This MMS was then circulated in the campus inside and outside the university. Some media reports stated that accused extorted moneys from the girl whose MMS was circulated. This not only amounts to Extortion but if these clips were recorded without the girl's consent, Violation of privacy under Section 66E IT Act, 2000 would also be applicable. [Retrieved from: <http://www.hindustantimes.com/delhi/mms-scandal-hits-jnu/story-W8GSA1qM7DKhS7ScAW2EDM.html>]

6 Virtual Rape

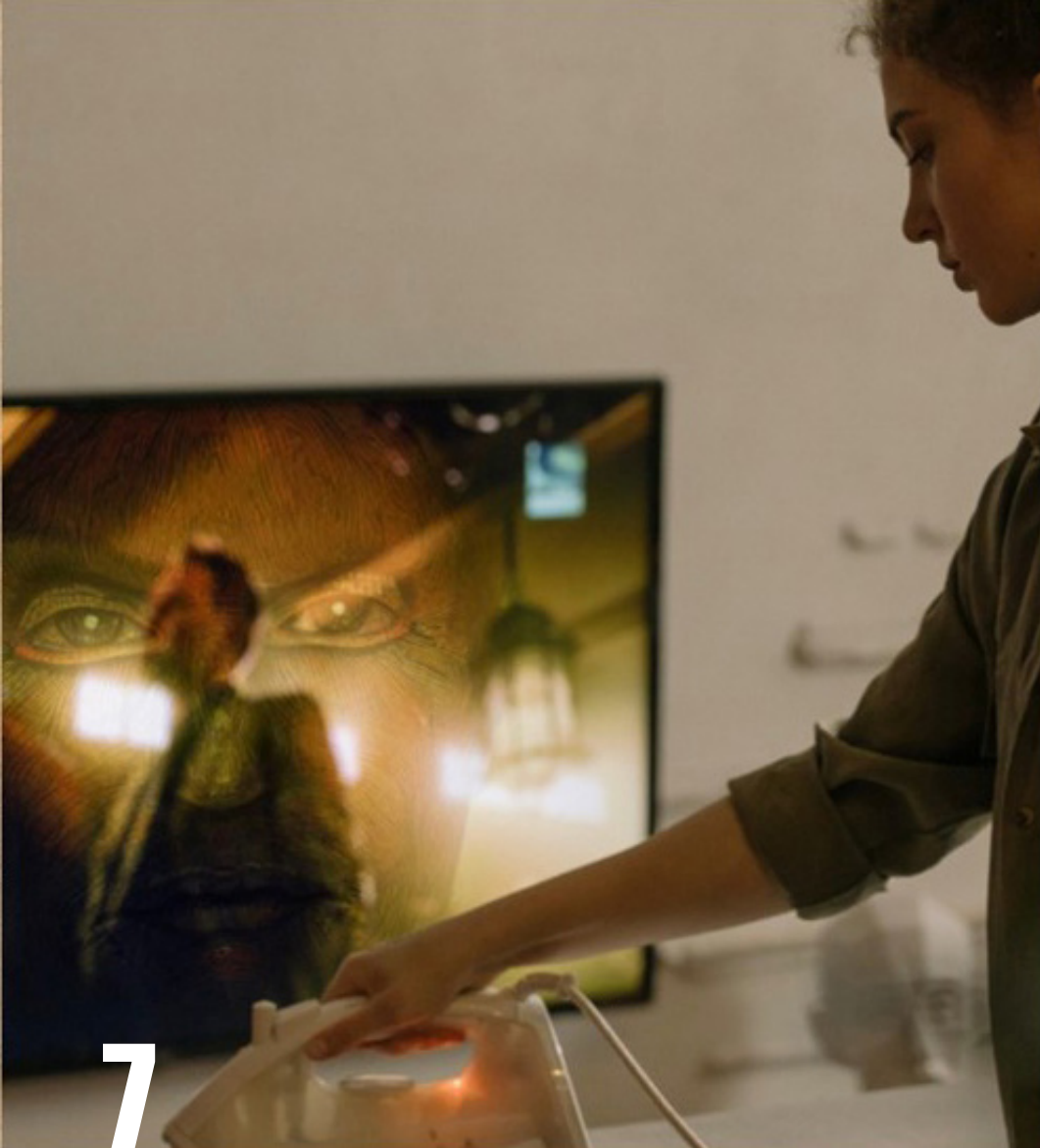
What is virtual rape?

Virtual rape occurs by sending rape threats to a woman online.

What is the law against virtual rape?

Virtual rape amounts to sexual harassment under Section 354A, IPC. If the purpose of virtual rape is to intimidate a woman, then the offender is also guilty of criminal intimidation under Section 506, IPC.

The offender may also be tried for insulting the modesty of a woman under Section 509, IPC.



Cyber Stalking

What is Cyber Stalking?

Stalking is following a woman, contacting her, or attempting to contact her, to make a personal interaction, even though the woman has made it clear that she is not interested in interacting with that person. When a perpetrator of crime uses internet, social media or IT enabled communication devices is called 'Cyber Stalking'

A new method of stalking a woman is by installing a malware called a key logger in the targeted woman's device remotely through infected links or attachments, which enables the stalker to see everything she types online.

Stalking puts the targeted woman under severe mental distress, and fear for her safety, and the safety of other people she may be interested in. In one case, Ritu Kohli, a 32 year old married woman was receiving a series of threats through emails from an unknown source that her morphed photos will be published on adult websites. The harassment included telephone calls for sexual favours. The Delhi Police traced the Internet Protocol (IP) address and the cyber stalker was arrested and charged under Section 509 of IPC for outraging the modesty of a woman.

What are the legal provisions to protect a woman from cyber stalking?

Section 354D(i), IPC deals with cyber stalking. The Section provides that when a man follows a woman, repeatedly contacts her, or attempts to contact her, to make personal interaction, even though she has made it clear that she does not want to interact with that person, is said to stalk the 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.

Are any acts exempted from the definition of stalking?

Under Sec. 354D, IPC the following acts would not amount to stalking, if the man proves that:

- He pursued the woman for the purpose of preventing or detecting crime, and he had been entrusted with such responsibility by the State.
- He had pursued the woman under any law, or to comply with any condition or requirement imposed by any person under any law.
- Such conduct was reasonable and justified in the particular circumstances.

What is the punishment for cyber stalking?

On first conviction, the person shall be punished with imprisonment of either description for a term which may extend to three years, and shall also be liable to pay fine.

On subsequent conviction, the stalker shall have to undergo imprisonment of either description for a term which may extend to five years, and shall also be liable to pay fine.

What if a stalker makes other sexual overtures?

If a stalker does any act, which has been mentioned hereinabove, which outrages the modesty of a woman, the stalker would also be liable under Section 509 IPC. If such person also makes sexually colored remarks, or uses words or gestures with sexual connotation, it would also amount to sexual harassment under Section 354A of IPC, 1860.

Does stalking also amount to violation of privacy?

If a stalker, while stalking the woman, captures the image of the private area of the woman, under circumstances violating her privacy, he would also be held liable for violating the privacy of the woman, under Section 66E of the IT Act.



8 Sending Obscene Content Over The Internet

Internet has made it very easy to communicate with unknown people. This feature is misused by cybercriminals who intentionally contact women by making unsolicited calls and text messages.

What are the legal provisions that punish acts of transmission of obscene content?

Section 67 of the IT Act, 2000 prohibits the publication or transmission of obscene content in electronic form.

What content can be considered to be obscene content?

Any content which is:

- lascivious or
- appeals to the prurient interest or
- tend to deprave and corrupt persons who are likely, to read, see or hear that material.

What is publication and transmission?

Publication includes the act of making obscene material available for electronic transfer or downloading to any other person, who is able to access and copy that material. In one case, *State of Tamil Nadu v. Suhas Katti*, [Criminal Case No. 4680 of 2004, Court of the Metropolitan Magistrate, Egmore], a woman complained to the police about a man who created a fake profile in complainant's name and was sending her obscene and defamatory messages in a Yahoo message group. The accused was found guilty of offences under section 469, 509 IPC and 67 of IT Act, 2000.

Transmission includes sending obscene photos or images to any person via email, messaging, WhatsApp or any other form of digital media.

What is the punishment for sending obscene content to a woman?

First conviction is punishable with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees.

On subsequent conviction, the person shall be punished with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

In State Cyber Cell v Yogesh Pandurang Prabhu, [C.C. NO. 3700686/PS/2009, ADDL. CMM, 37th court, Esplanade, Mumbai], the complainant received obscene messages from an unknown person on a social media platform. On investigation it was found that her colleague was sending messages from office premises and was charged under Section 509 IPC and 66E IT Act, 2000.

What is the punishment for sending sexually obscene content to a woman under Section 67A IT Act?

Under Section 67A IT Act, 2000, on first conviction, the person shall be punished with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees. In the event of second or subsequent conviction, with an imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

What if the material sent to the woman has sexual overtones?

Section 67A of the IT Act, 2000 prohibits the publishing or transmitting of material containing sexually explicit content. Therefore, if a man sends a woman sexually explicit content (showing sexually explicit act or conduct), he would also be held liable under section 67A of the IT Act.

What is sexting? Is it a punishable offence?

Sexting: It is a new term used for act of sending obscene and unsolicited texts, images or video to a woman which may contain semi-nude content or sexual act. This is also triable under section 67 and Section 67A of the IT Act, 2000.

Educate children on secured digital practices and dangers of befriending online strangers

Turn off your electronic devices and web cameras when you are not using them

Always be aware to use internet and online medium responsibly

9 Cyber Defamation

What is cyber defamation?

Cyber Defamation means causing harm to reputation of a person, by writing or speaking something about the person on the internet which is published or transmitted to another person.

What kind of imputation is said to harm the woman?

An imputation is said to harm a woman's reputation if, in the eyes of others, it lowers her moral or intellectual character, or lowers her credit, or causes others to believe that her body is in a loathsome state or is in a state that is generally considered to be disgraceful. .

What is the punishment for defaming someone?

The punishment for defaming someone is simple imprisonment for a term which may extend to two years, or with fine, or with both

Always save the screen shots of the online incidents as proof to support your claim or complaint with relevant evidence. Also make a note of the persons mobile number and other details of the suspect or culprit.

What is the law to protect a woman from cyber defamation?

Section 500 IPC, prohibits acts of defamation and includes cases where a woman is defamed in cyberspace. Section 499 IPC defines defamation as acts directed at harming the reputation of a person by words, either spoken or intended to be read, or by signs or by visible representations, making or publishing any false imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm the reputation of such person.

Morphing 10

What is Morphing?

Morphing means changing the contents of an image by combining two images, using a software. Morphing is used to create obscene pictures of women by superimposing their faces over other obscene pictures (which may be real or fake) using technical tools or software.



What are the legal provisions against Morphing?

There is no legal provision which directly prohibits morphing under IT Act, 2000. However, morphing may constitute forgery for purposes of defamation under Section 469 IPC punishable with imprisonment of upto 3 years and fine. A person morphing someone's image may also be tried for data theft from the targeted woman's computer under Section 66 read with Section 43 of IT Act, 2000, publishing or transmitting obscene material if he transmits/ publishes morphed image that is obscene [Section 67, 67A of IT Act, 2000].

What constitutes as forgery under the law?

Acts of morphing may constitute forgery under Section 463 Indian Penal Code. Under this section, forgery means:

- making false document or false electronic record
- with the intent to cause damage or injury to the public or a person

What is the punishment for forgery?

Whoever commits forgery shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both.

What if the image of a woman was stolen from her computer?

If the image has been stolen by unauthorizedly entering into the computer of the targeted woman, it amounts to data theft. As per Section 66 of the IT Act, if any person unauthorizedly, dishonestly or fraudulently accesses, downloads, copies or, alters, extracts any data, computer data-base or information, or destroys, deletes, damages such data he is liable to be tried for data theft.

What is the punishment for data theft under the IT Act, 2000?

A person held guilty of data theft shall be punished with imprisonment that may extend upto 3 years, or with fine which may extend upto 5 lakh rupees or with both.

Is it a cyber crime to receive a stolen computer device?

Yes, it is a crime to retain or receive a stolen computer resource if done dishonestly or with knowledge or reason to believe it is stolen. Punishment is three years of imprisonment or fine which may extend to one lakh or with both.

What if a man transmits a morphed obscene picture of the woman online, is it a cyber crime?

If the morphed picture of the woman is obscene and the man transmits or publishes it, he will be tried under Section 67 of the IT Act which prohibits the publication and transmission of obscene content on the internet.

If the morphed picture of the woman which has been published and transmitted over the internet is sexually explicit, the man shall be tried under Section 67A of the IT Act, which prohibits the publication of sexually explicit content over the internet.

Enable your security and privacy features on social media accounts

Never share your personal pictures online publicly

Use two factor authentication with strong passwords

Don't suffer in silence, know that you are not alone, reach out and seek help from trusted family and friends

What is the punishment under the Indecent Representation of Women (Prohibition) Act, 1986?

Any person who publishes obscene advertisements or books, pamphlets violates Section 3 and 4 of the Indecent Representation of Women (Prohibition) Act, 1986.

As per Section 6 of the said Act, on first conviction, a person held guilty shall be punishable with imprisonment of either description for a term which may extend to two years, and with fine which may extend two thousand rupees, and in the event of a second or subsequent conviction with imprisonment for a term of not less than six months but which may extend to five years and also with a fine not less than ten thousand rupees but which may extend to one lakh rupees.

Cyber Pornography

What is cyber pornography?

Cyber pornography is the publication and transmission of material containing people involved in sexually explicit content, over the internet using any form of media, video, picture, sound through computer, tablet, telephone or mobile. Such acts may be committed for personal consumption or for making commercial gains. In many cases, women are dishonestly recorded often without consent while they are engaged in sexual activities, by known or unknown persons and these images and videos are then circulated over the internet unauthorisedly. In one such case, DR. L Prakash v State, the accused who was a doctor was convicted for 7 years of imprisonment and fine of one lakh under IT Act, 2000 and IPC ,1860 for making through a hidden webcam and selling several obscene photos and videos of his women patients. In re: Prajwala letter dated 18.2.2015 the Supreme court of India dealt with the issue of blocking of several sexual harassment videos of women and child pornography that went viral on internet and passed various directions to intermediaries and the Government to take necessary action to combat the cyber crime.

11



What is the position of law in respect to cyber pornography?

The IT Act under Section 67, Section 67A and section 67B, prohibits publication and transmission of obscene content over the internet, Section 67B of IT Act, 2000 prohibits child sexually abusive material and child pornography. Recording and dissemination of Cyber pornography may also amount to infringement of privacy of a woman when done so without consent, which is prohibited under Section 66E, IT Act. If a man threatens to use sexually explicit content involving a woman, to pressurize or compel her to do something or not to do an act, it amounts to criminal intimidation under section 506, IPC. In *X v. Uol*, (2021 SCC Online Del 1788), Petitioner's photos taken from her social media and posted on pornographic websites without her knowledge or consent. The court directed Delhi Police/CyPAD to remove the objectionable content from all websites within 24 hrs and directed Search engines to make the content unsearchable within 24 hrs. The Court directed the Police to obtain information required for investigation from the websites within 72 hrs and observed that Petitioner may communicate to the investigating officer to remove the said or similar content from any other website as well.

What if a child is recorded, or fabricated, while engaged in a sexual activity?

In addition to the above provisions, there are special provisions for protection of children from cyber pornography under the IT Act, and the POCSO Act. Section 67B, IT Act, 2000: The Section punishes the following acts:

- Publication and transmission of any material in electronic form, which depicts children engaged in sexually explicit act or conduct;
- Creating, collecting, downloading, browsing, downloading, advertising, promoting, exchanging or distributing text or digital images depicting children in obscene or indecent or sexually explicit manner;
- Enticing and inducing children to engage in online relationships for sexually explicit purposes;
- Facilitating child abuse online;
- Recording sexually explicit acts involving children.

What is punishment for Child Pornography?

As per Section 67B of the IT Act, 2000, on first conviction, a person found guilty shall be punished 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.

Is Child Pornography a punishable offence under POCSO Act, 2012?

Section 13, POCSO Act: This Section specifically criminalises the using of a child on any form of media for sexual gratification. This is the case irrespective of fact whether it is for personal use or commercial exploitation. Such acts include- representation of sexual organs of a child, using a child in real /simulated sexual acts Indecent or obscene representation of a child.

To 'use a child' here means involving a child through any medium such as print, electronic, computer, or any other technology for preparing, producing, offering, transmitting, publishing, facilitation and distribution of pornographic material.

What is the punishment for committing child pornography?

The punishment for crime described under Section 13 is, on first conviction, imprisonment for a term which shall not be less than five years and fine, on subsequent convictions, imprisonment for a term which shall not be less than seven years and fine.

If the accused is himself involved in the pornographic act and using a child there are serious additional punishments provided under Section 14 of POCSO Act in addition to punishment provided for using a child for pornographic purposes in Section 13 of POCSO ACT.

Can child pornography and sexual harassment be attracted simultaneously?

Yes. Under Section 11(v), POCSO Act, if a person threatens to use the depiction of a child in a sexual act, whether real or fabricated, through electronic, film, digital or other mode in which any body part of the child is depicted, it amounts to sexual harassment of the child. If such person publishes or transmits such obscene content it amounts to child pornography.

Is child grooming a part of Sexual harassment under POCSO Act, 2012?

A. Yes, Under Section 11(vi), POCSO Act enticing a child for pornographic purposes also amounts to sexual harassment of the child.

Punishment: The punishment for sexually harassing a child under the POCSO Act is imprisonment of either description for a term which may extend to three years of imprisonment and fine.

Is storing or possessing child pornography also an offence?

Yes, under Section 15, POCSO Act. This section prohibits the storing or possessing of child pornography with intention of sharing or transmitting it.

The punishment for this offence is imprisonment upto 3 years, or fine or both.

The storing or possession of child pornography in any form for commercial purpose is a punishable offence. The punishment for this offence is imprisonment of minimum 3 years upto 5 years, or fine or both. On subsequent conviction, imprisonment of not less than 5 years extendable upto 7 years and fine or both.

Is it mandatory to report child pornography incidents?

It is mandatory to report child pornography or any instance of sexual harassment of a child likely to be committed or has already occurred under Section 19 of POCSO Act to local police/special juvenile police unit. Similar obligation is put on media, studio and photographic facilities to report cases. Non reporting of offence under Section 21 of POCSO Act attracts punishment of upto 6 months or fine or with both but the Section does not apply to non-reporting by a child. In case of an entity if an officer fails to report offence under POCSO, punishment is imprisonment upto one year and with fine.

It was recently reported by press 8 persons were arrested for distributing child pornography in South West Delhi. The police confiscated around 8 computers, memory card readers. 52 memory cards containing pornography from the accused. Cases under section 15 to the Protection of Children from Sexual Offences Act were registered against the arrested men. ('8 held for distributing child porn'. (2013, May 8) Hindustan Times, Retrieved from <https://in.news.yahoo.com/eight-held-distributing-child-porn-183000157.html>)

What is Revenge porn?

'Revenge porn' is publishing or distribution of sexually explicit images or videos of a girl / woman by her partner, or ex-partner, often after the girl and boy separate or have estranged relations. Revenge porn is punishable under Sections 67 and 67A, IT Act, 2000 for publication and transmission of obscene and sexually explicit content.

What is child grooming?

'Grooming' literally means preparing someone for a particular work. However, in cyberspace, child grooming means enticing and preparing children for doing sexually explicit acts on the internet.

12



Child Grooming

What is the law against child grooming?

In India, a person accused of child grooming may be tried for sexual harassment under Section 11, POCSO Act, and under Section 67B, IT Act.

Under Sec. 11(iv) POCSO Act, enticing a child for pornographic purposes amounts to sexual harassment. Certain gaming apps may contain malvertising that is, advertisements that lure children into cyber pornography.

What if the targeted woman commits suicide as a result of any of the abovementioned crimes?

If the targeted woman commits suicide, the cyber offender shall be liable for abetting the suicide under Section 306 IPC, and shall be punished with imprisonment of either description for a term which may extend to ten years, and shall also be liable to fine. For instance, there have been incidents of blue whale suicides where children are instigated to play a life threatening game and abets children to commit suicide

What is the punishment for child grooming?

A person found guilty under this section shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine.

Is child grooming also punishable under IT Act, 2000?

Yes, under Sec. 67B(c) IT Act, 2000. This Section includes the formation of a relationship with the child in order to entice her for doing sexually explicit acts on the internet.

What is the punishment for child grooming under IT Act, 2000?

A person found guilty for grooming under IT Act, 2000 is 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.



13

Extortion

What is extortion and sextortion?

Extortion is act of making wrongful gains by putting someone in fear of physical injury. Extortion is mainly related to making financial gains, however, if a woman is threatened to seek sexual favours, it also amounts to sextortion.

In case of sextortion, a man may be tried for sexual harassment (Section 354 IPC) and criminal intimidation (Section 506 IPC).

What is the law against extortion?

Extortion is prohibited under Sec 383 IPC. Under the Section, extortion is putting someone under fear of injury to make wrongful gains from that person, by compelling him to deliver money, property or other valuable security. A woman may be extorted by blackmailing her of distributing some sexually explicit content in which she is involved, or by morphing her images into obscene material.

Save the evidence and the screen shots for referring to the incident later

Never share any compromising images, posts, videos of yourself to anyone

What is the punishment for extortion?

Whoever commits extortion shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both. (384IPC)

Whoever, in order to the committing of extortion, puts any person in fear, or attempts to put any person in fear, of any injury, shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both. (385 IPC). Putting any person in fear of death or grievous hurt to commit extortion is punishable with imprisonment of upto 7 years and fine.

If extortion is for sexual favours, it amounts to sexual harassment. The accused is also punishable under Section 354A IPC, 1860 as has been provided above.

Identity Theft

What is identity theft?

Identity theft is committed when someone wrongfully uses another person's personal data or unique identification deceptively or fraudulently for illegal purposes such as economic gain or sexual abuse. Includes unauthorisedly using the unique identification of a person to commit fraud. There have been several cases where genuine pictures of women have been illegally used to create fake social media profiles amounting to identity theft. These fake profiles are made for illicit purposes such as harassment, defamation or posting objectionable content. Such fake accounts post obscene pictures of a woman for sextortion purposes, that is, to threaten them to gain sexual favours or as a revenge incase of estranged relationship with a man commonly known as Revenge porn.

14



What are the legal provisions for dealing with identity theft?

Section 66C of the IT Act prohibits Identity Theft. Under the IT Act, identity theft includes unauthorisedly using a woman's electronic signature, password, or other unique identification features, example her photograph, for dishonest or fraudulent purposes. It is a cognizable and a bailable offence punishable with imprisonment which may extend to three years and fine upto one lakh.

What is the punishment for Identity Theft?

A person held guilty of identity theft shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

What is phishing and how is it related to identity theft?

Phishing is a cyber crime wherein a cybercriminal garbs another person's identity to commit data theft for making illegal financial gains. For instance, a cybercriminal may send a fake email impersonating a bank seeking verification of debit card pin, which may be gullibly shared by a woman who then gets duped when cybercriminal siphons off her moneys using net banking. These days there are many cases of crypto frauds being reported wherein cybercriminal posts a link in any social media forum posing as genuine crypto advisors' group and dupes' people by asking them to click on a phishing link to invest in cryptocurrency.

Similarly, there are QR code scams wherein cybercriminal asks a targeted person to scan one's QR code to receive payment. When scanning is done, money is debited from payment wallet rather than being credited into targeted person's account which is also a social engineering fraud technique.

What is the intermediary liability in cases of identity theft?

Fake profiles can be immediately reported to the concerned service provider, such as Facebook or Myspace termed as an intermediary. An intermediary is a service provider that allows third parties to post content on their website and does not monitor such content nor controls sender or recipient of a message. Sec. 79 of the IT Act requires the intermediary to remove the fake profile within 72 hours from receipt of the written notice sent by a victim.

Moreover, the I.T. (Intermediaries Guidelines) Rules, 2021, mandatorily requires every intermediary to publish in its terms 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.

15

Cheating By Personation

What amounts to cheating by personation?

Cheating by personation is cheating someone by pretending to be someone else. There have been several cases of fake profiles on social media where women are cheated by impersonation, particularly on online dating and matrimonial websites.



What is the law against cheating by personation?

Section 416 IPC deals with cheating by personation. The Section defines cheating by personation as cheating someone by pretending to be some other person, or by knowingly substituting one person for another, or by representing himself or some other person as someone other than who he or that other person really is.

What is the punishment for cheating by personation?

The punishment for cheating by personation under the IPC is imprisonment of either description for a term which may extend to three years, or with fine, or with both.

Cheating by personation using a computer resource is punishable under Section 66D, IT Act, with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.



16

Data Theft

What is data theft? Is it a punishable offence under IT Act, 2000?

Dishonest or fraudulent and unauthorised access, downloading, alteration or deletion of data, disruption of a computer, computer system or network, denial of access attack, stealing, concealing source code, introduction of a virus into a data amount is a computer related offence under Section 66 of IT Act, 2000. It is a punishable offence with imprisonment of three years and fine upto 5 lakh or both.

Is a ransomware attack a form of data theft?

Yes. In a ransomware attack, a cybercriminal sends a malware through a link or attachment that causes the files in a computer system to get encrypted and locked and a woman is not able to decrypt or reopen the files in her system. It is a form of data theft and extortion as a cybercriminal generally asks for payment by bitcoins to decrypt the system and places a woman under threat of losing her data.

Do QR code scams on payment apps amount to data theft?

Yes, fraudsters target a victim by asking her to scan the QR code on a payment app to receive payment whereas on scanning senders QR Code money gets unauthorizedly debited from her account. This is punishable under Section 66 of IT Act, 2000 and cheating (Section 420 of IPC)

Is Phishing used to commit data theft?

Phishing is used as a means to commit data theft or for purposes of stealing financial information such as net banking pin of a woman and then siphoning off moneys from her bank account. Fraudsters post malware infected links or create fake accounts to target victims so that they gullibly disclose their personal financial information to make money illegally.



17

Spamming

What is spamming?

In cyberjargon, the term, Spamming denotes sending unsolicited messages persistently to someone to cause annoyance or inconvenience to the recipient. There have been several cases of women receiving obscene messages and mails from unknown sources to cause harassment. It may be directed at a woman or girl to intimidate her with offensive, disturbing or menacing content. It may contain malicious attachments which can infect the receiver's computer system or mobile and install virus, spyware, or keyloggers or other malware to infect her device. This could give the sender unauthorized access to the personal information of the target person, including her movements and daily activities.

What is the law for preventing spamming?

There is no law dealing directly with spamming, however, the sender may be prosecuted under different laws depending on the purpose for which the spam mail had been sent. Earlier, Section 66A of IT Act dealt with spamming as an offence which was struck down as unconstitutional in light of ambiguity in its wording as per *Shreya Singhal v UOI*, [2013]12 S.C.C. 73.

Data theft:

If the spam contains attachments which could give the sender unauthorized access to the content of the computer of the receiver, the sender is guilty of data theft under Sec. 66 of the IT Act.

Punishment: imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with bot

Stalking:

If the aim of the sender is to install a key logger or any other program so as to enable him to get access to the personal information of the receiver, including information about her movements and internet activities, the sender would be liable for stalking under Section 354D, IPC.

Sending obscene content:

If the spam mail contains obscene content, the sender would be guilty under Section 67, IT Act.

Sending sexually explicit content:

If the spam contains sexually explicit content, the sender would be liable under Sec 67A, IT Act.

Damaging Computer Source Code:

If the aim of the sender is to introduce virus into the computer system of the receiver so as to cause damage to the software of the computer, the sender would be liable for damaging the computer source code under Section 65 of the IT Act.

Punishment: imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.



Avoid opening links/attachments received from anonymous sources



Dr. Karnika Seth

About the Author

Dr. Karnika Seth is a renowned Cyber Lawyer & Expert and is the Founder of Seth Associates, a Law Firm in India. She practises law at the Supreme Court of India and the Delhi High Court and is advisor to many international organisations, corporate houses & IT Companies. She is the appointed Country Chair- India for Artificial Intelligence & Cybersecurity in G 100, a global group of women leaders leveraging technology to solve complex global challenges. She actively advocates women rights and founded Foundation for Institutional Reform and Education, an organisation promoting cyberawareness, particularly, among women and children. She has been officially consulted by the World bank on women laws in India and by the Indian Parliament and the Ministry of Information Technology on strengthening Cyber Law in India. On requisition of the E-Committee of the Supreme Court of India, she authored the e-filing User Manual for e-filing processes in District Courts and High Courts in India.

Dr. Seth has actively resolved many Cyber crime cases with the Indian Law Enforcement Agencies for over two decades. She is an Active Speaker on Cyber Law issues, both in Print and Electronic Media and actively supports cyber awareness initiatives, including of, ISEA, CDAC, Ministry of IT, Govt of India, National Commission for Women, NIPCCD, NCPCR, Chambers of Commerce, NASSCOM, FICCI, Assocham and international organisations, UNICEF, UNESCO, IJM & ICMEC. She also delivers Special lectures to Judicial Academics, Police Academies, Central Bureau of Investigation, Senior Government Officers, Industry Associations, Academia and Corporate entities. She is an acclaimed author who has written several books, e-books, legal toolkits and white papers on New and evolving technology issues. She has been consulted by IGNOU, UGC, National Law University, NCERT and other Institutions to draft Cyber law courses in India.

Dr. Seth is an empanelled Arbitrator at the WIPO Arbitration and Mediation Center, the Chartered Institute of Arbitrators, London, the National Internet Exchange of India and the Indian Council of Arbitration. She attained specialisation in Computer Science from Harvard University, holds a Doctorate in Cyber Law from NIU, and a Master's degree in Corporate and Commercial Laws from the King's College University of London.

Dr. Seth is the recipient of the Women Economic Forum's Exceptional Women of Excellence Award 2022, the Constitution Day Award 2022, the Platinum Excellence Amrit Award 2022, the Virangana Samman 2022, the Great Indian Women Award 2022 & the National Gaurav Award, 2017. She received the Digital Empowerment Award from BIF at the Digital India Conclave in 2015 and the Law Day Award from the Chief Justice of India in 2012.

Bibliography

Acts

- Indian Penal Code, 1860 (No. 45 of 1860)
- The Information Technology Act, 2000 (No. 21 of 2000)
- Protection of Children from Sexual Offences Act, 2012 (No. 32 of 2012)
- Juvenile Justice (Care and Protection of Children) Act, 2015

Books

- Arora, V., Women Laws (Universal Law Publishing, New Delhi)
- Being Safe Online (NCPCR, 2017)
- Cybersafety for everyone, Jaago Teens (BPB Publication, 2017)
- Information Technology Act, 2000, Bare Act (Universal Publishers, 2021)
- Information Security Awareness handbook, (Ministry of Communications and Information Technology, Government of India)
- Jaishankar, K. & Halder, D., Cyber crime Against Women in India (Sage, New Delhi, 2017)
- Justice M.R Mallick, Criminal Manual, Professional Book Publishers, 2016
- POCSO Act, 2012, Bare Act (Universal Publishers, 2021)
- Know about Laws for Women (National Legal Services Authority, New Delhi)
- Ramaswamy, B., Women and Law (Isha Books, New Delhi, 2013)
- Secure your Electronics, (Ministry of Communications and Information Technology, Government of India)
- Seth, K. Protection of Children on the Internet (Universal Law Publishing, New Delhi, 2015)
- Seth, K. Computers, Internet and New Technology Laws (Lexis Nexis, New Delhi, 2021)
- Seth, K. Cyber crime against Women (Amazon books, 2018)
- Seth, K. & I-probono, Legal toolkit-Child Victims of Cyber crime, (NCPCR, 2017)

DOs & DON'Ts to combat Online Threats

DOs



X DON'Ts



Use nick names instead of real names to create an account



Think carefully before posting pictures or videos of yourself



Play and chat only with known friends to avoid stranger danger



Be careful when someone offers you something for nothing, such as gifts and money.



Talk to a trusted adult, Never hesitate to seek help from your near ones



Save the evidence by taking screen shots and save messages



Block & Report ,Don't Ignore, Un-friend & Block immediately, if anyone make you feel uncomfortable



Respect other people's views, even if you don't agree with someone else's views doesn't mean you need to be rude

Don't retaliate, Know that .. Your response feeds the bully



Don't be a bully, Treat others in the same way you would like to be treated



Don't share your personal sensitive Information as it can be misused



Don't respond to provoking messages, or posts. Understand no response is powerful reply



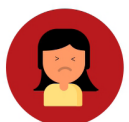
Don't give your password to anyone. Passwords are intended to protect your computer and your files.



Don't click unknown links sent through chats by unknown people with exciting offers



Don't get scared by threatening messages, Be Calm, Don't blame yourself, Be aware that it is not your fault.



Don't meet up with people you've met online., Some people on the internet lie about their identity



Supported by



National Cyber Crime Reporting Portal
<https://cybercrime.gov.in/>

National Cyber Security Helpline Number
1930