Cyber Crime Investigations Against Women & Children

A guide for law enforcement agencies

Published by

RESPONSIBLE NETISM™

NAMES OF CONTRIBUTORS:

Shri. Brijesh Singh IPS – ADG Maharashtra Police

Adv. Vaishali Bhagwat

Adv. Dhrumi Gada

Team Responsible Netism

Published By:
Responsible Netism
C -Wing Office No 6, Belleza of Shanti Sadan, 90 Feet Rd, Mulund East, Maharashtra 400081

Designing By:
Orangetip Designs

Printed by:
Prashuma Art Printers

Disclaimer

Every effort has been made to avoid errors or omissions in this guide, errors may creep in, any mistake, error, or discrepancy noted may be brought to our notice on responsiblenetism@gmail.com which shall be edited in the next edition. It is notified that, the publisher will not be held responsible for any damages or loss of action to anyone, of any kind in the manner therefrom. It is suggested that, to avoid any doubt, the reader should cross check all the facts, law and contents of the publication with original government publication or notification. This Handbook offers only a guideline and should not be constructed as professional or legal advice.

INTRODUCTION

About Responsible Netism:

Responsible Netism is a social purpose organization, committed to the cause of women and child online protection and safety since 2012. The initiative invests in protecting internet safety rights of netizens through capacity building, so as to inculcate values of cyber hygiene. We advocate for the cause of cyber wellness to minimize damage caused to victims of cyber-attacks, to ensure mental well-being in cyber space. Responsible Netism conducts research on user trends to substantiate our interventions and imparts training and education about responsible online behaviour. We run a Pan-India helpline that provides free legal guidance, technical assistance and psychological support to the victims of online distress. We have been instrumental in setting up India's first holistic Cyber Wellness Centre in Goa in 2022. Having successfully educated over 1.5 million netizens since inception, we aspire to make India cyber safe for children youth and adults.

Rationale:

Rise in usage of technology has surged vulnerabilities in cyber space like never before. Threats of cyber space hold neither economic, social, geographic boundaries nor barriers. Cyber violence has penetrated into semi urban, rural and tribal segments across the country mainly because of the lack of understanding about online safety protocols. Children, women and the geriatric population are the most common victims and are highly vulnerable to cyber-attacks. Since the awareness about online safety is significantly low, it impacts the ratio of reporting of cyber-crimes. With netizens being fearful of reporting cyber-crimes to the local law enforcement agencies due to lack of an appropriate response from them causing delays, there is a dire need to build stronger, user-friendly mechanisms to report online distress by the local law enforcement agencies. In order to ease the process for the law enforcers across the state and the country, the need for a handy guide on reporting of cyber-crimes that brings in clarity on the sections of laws applicable to register the complaint was sensed.

Responsible Netism, on its 10 year work anniversary, decided to take on the initiative to support the law enforcement agencies by creating a handbook, a ready reckoner called **Cyber-Crime Investigations Against Women & Children - A Guide for Law Enforcement Agencies.** The book was launched on November 12, 2022 by the **Hon. Chief Minister of Maharashtra, Shri. Eknath Ji Shinde, the Deputy Chief**

Minister, Hon. Shri. Devendra Ji Fadnavis, the Hon. Minister for Women and Child, Shri. Mangal Prabhat Lodha Ji, along with other respected dignitaries amidst stalwarts and domain experts from the field of education, information technology, mental health and the law enforcement.

We strongly believe, cyber-crimes need to be combatted collectively and this guide would prove to be a one-stop resource for the law enforcers to address cases related to cybercrimes, effectively. This guide would enable faster reporting of complaints, strengthen reporting mechanisms, would help in escalating the ratio of conviction and allow netizens to build trust in the system and provide appropriate and timely relief to victims of cyber-attacks.

Team Responsible Netism

ACKNOWLEDGEMENTS:

This guide would not have been possible without the proactive support from the following people who have been our pillars of strength and safe sounding boards.

We wish to thank Adv. Dhrumi Gada for the timely compilation of this guide with patience and grit.

We extend sincere thanks to Adv. Vaishali Bhagwat for sharing her time, expertise, opinions and her valuable inputs to make this guide user friendly and relevant.

Shri. Brijesh Singh for being one strong pillar of support and adding ground level expertise from the law enforcement perspective which would prove to be extremely hands on and practical.

Thank you Dr. Auradha Sovani for re-instilling our faith in this compiling this guide and for your guidance.

Appreciation and gratefulness towards our designers, team Orange Tips and our printers, team Prashuma Arts for their relentless support and their patience to deal with last minute edits.

A big thank you to the law enforcers who would use this as a guide to help victims of online distress.

In gratitude to the most important of them all, children and women for whose protection this guide was compiled with the hope and faith that they would be safeguarded from the damage caused due to cyber violence and be able to seek the right and timely support when in distress.

And finally, to everybody at team Responsible Netism for proof reading and verifying the content time and over again tirelessly, for being the best critics and the best support and for standing by, through thick and thin always.

PREFACE
- Adv. Vaishali Bhagwat

The purpose of this handbook is to serve as a ready and a quick reference for the most common types cyber-crimes that are reported in India. The handbook covers the applicable law, reporting procedures and a basic guideline for investigation of cyber-crimes along with handling and preservation of digital evidence.

The law that addresses cyber-crimes is India is primarily the Information Technology Act 2000 and the Indian Penal Code. However, there are other legislations as well that define crimes against women and children and intellectual property crimes which will also be discussed in this handbook. The legislations have described the cyber-crimes in a certain way that may not always coincide with the names used for the cyber-crimes in common parlance. For example, there is no legal provisions that includes the word 'sextortion'. However, there are provisions that deal with sexual harassment and extortion and those are the provisions that need to be referred to when a case of sextortion is reported.

Reporting and redressal mechanisms have been defined in law as well as there are several initiatives taken by the Ministry of Home Affairs to facilitate easy and timely reporting of cases. This handbook makes an attempt to compile all the latest available reporting channels.

Gathering of evidence from the crime scene which is mainly digital in nature poses some unique challenges. Certain evidence is also available with third parties and it is important to compel the third parties to disclose such relevant evidence which is in their exclusive custody for the purpose of investigation. The Indian Evidence Act and the information Technology Act along with the rules notified thereunder have laid down guidelines for the purpose of collection of digital evidence and its presentation before a court of law. A brief summary of the procedures are included in this handbook, so that it will serve as a starting point for further detailed reading and understanding of the techniques of collection of digital evidence

Every topic in the handbook will contain a brief description and nature of the cyber- crime, common modus operandi, applicable law, process of investigation, collection of evidence, preservation of evidence and reporting and case laws.

Adv. Vaishali Bhagwat

Vaishali Bhagwat is a practicing civil and cyber lawyer with 24 years of experience in litigation and advisory practice. She specializes in Cyber Law, her work focuses on law relating to violence against women and children. Vaishali is an advisor to several companies and is on the advisory board of several chambers of commerce, Maharashtra State Commission for Women, Maharashtra Cyber (Police) for Legal Reforms and Board of Studies for Symbiosis Centre for Distance Learning, Symbiosis Skills University and the Suryadatta Institute on Cyber Security. Her work has been recognized by NASSCOM, Data Security Council Award in 2016 and by Rotary International at the International Convention at Soeul. She won that state award at the hands of the Governor of Maharashtra for Vocational Excellence and Women Empowerment. Vaishali is a TCS Chevening Scholar of the British High Commission on “Cyber Policy and Cyber Defense” from Cranfield University UK.

INDEX

TYPES OF CRIMES

A. HACKING

Description of the crime

Hacking in a broader sense can be used to refer to situations where the perpetrator gains unauthorized access various electronic devices such as computers, mobiles or social media profiles and other online accouunts. The reasons behind such attacks could be varied:

- **Data theft**: Data is a deadly and valuable weapon in today's world, some hacks are carried out to collect personal data like bank account details, emails etc.
- **Destruction**: Herein the hackers target websites to destruct the database and cause damage.
- **Financial and monetary gains**: The financial cost of this crime is immense. Corporations have lost millions of dollars over the years by falling prey to this crime.
- **State sponsored hacking**: This is a form of cyberwarfare carried out to steal the national intelligence related information of other countries or destabilise or create confusion in another country.
- **Corporate espionage**: One company employs hackers to steal their competitors details to get an edge in the market.
- **Tarnishing reputation**: On multiple occasions hackers access social media platforms of their victims and send out objectionable content to their contacts to defame them.

Computer and network hacking is similar to that of someone trespassing or entering your home without your permission. Instead of home, the place broken into is your computer or network. **Section 43, Section 66 of the Information Technology Act 2000 cover the civil and criminal offenses of data theft and hacking respectively.**

Modus operandi of the criminal in this crime - Hackers deploy different techniques to meet their goals:

- **Ransomware**: After accessing your systems and files the attacker encrypts your data preventing you from accessing your data and asks for ransom to unlock it.
- **Denial of Service (DoS**): The attacker sends targets a service or a website and tries to overwhelm it by sending huge amount of traffic from multiple sources. Thus, rendering the service or network unavailable to the legitimate users. These attacks are carried out

using botnets, a DDoS Tool is used to create an army of source computers.

- **Virus**: A type of malware that attaches to another program, replicates itself and corrupts the system and the files on the computer. The attacker can then deploy a virus into your computer in many ways. One such way includes sending out an email to the victim with a malicious attachment, the victim accidently opens the files, not understanding the contents of it and hence downloading the virus in the system.
- **Phishing**: It is a type of social engineering where the attacker sends trick messages to people designed to bait them into giving sensitive information away.
- **Cookie theft**: Cookies on websites contain information about the users. These cookies are hacked and decrypted to get details about the user.

Investigation procedure to be followed

Step 1: Identification

Once it has been realised that hacking has taken place, the investigation officer (IO) should identify how the victim was able to figure out about the hacking attack. For example; it could be through someone who has received incriminating or obscene texts or demand for money from the victim's mail I'd, or a certain intrusion into the system by an outsider physically or virtually or by any unknown / unidentified downloads that have taken place, or even identifying if it was a link that resulted in the attack.

Step 2: Initial Investigation – Damage Survey

An initial investigation should be carried out to determine the impact of the attack, to identify all systems and services that have been affected. Further investigation can help discover if there were bugs in the website, if the source of the attack was an email or if there was a password leak.

Step 3: Record the details: A detailed log of the following information should be taken:

- Affected systems
- Compromised accounts
- Disrupted services
- Data and network affected by the incident

- Amount and type of damage done to the systems

Step 4: Immediate Actions to limit more damage

In order to prevent the spread of the attack the IO should take preventive measures. For example, in cases of phishing incident, after mapping the damage and potential damage the users should be informed to not click on any unwarranted links in their emails, reset passwords for all their accounts.

Step 5: Further Investigation

After ensuring that the hacking can cause no further damage, further investigation should be taken up to procure the source of evidence.

Step 6: Sharing the evidence with a well-trained forensics team

After the evidence has been filed by the police, the evidence should be shared with the forensics team for the analysts and forensic experts to preserve the data and prepare a report.

Step 5: Data extraction, analysis and report preparation

The next stage includes the extraction of data and analysis. The data extraction should be conducted using proper cables and software and should be further analysed. A detailed report should be prepared based on the results.

Example of certain judgements / case laws or real scenarios

Case Law 1: Kumar v. Whiteley - Facts of the case

The accused had gained unauthorized access to the Joint Academic Network (JANET) by logging into the BSNL broadband Internet connection as if he was the authorized genuine user. He deleted, added files and changed the passwords denying access to the legitimate users. The investigations revealed that the subscribers had incurred a loss of Rs 38,248 due to Kumar's act.

Judgement -

The accused was held liable under Section 420 IPC (cheating) and Section 66 of the IT Act (Computer related Offense) and was sentenced to one year of rigorous imprisonment and a fine of INR 5,000.

B. ONLINE FAKE ACCOUNTS / IMPERSONATION

Description of the crime

The commission of crimes through fake accounts has many facets and implications. These types of crimes include or are involved with identity theft through fake emails or social media accounts, harassment, sextortion, cyberbullying, financial frauds, phishing, child pornography or child sexually abusive material, etc. Though the term 'cybercrime' has not been defined in any statute, the National Cybercrime Reporting Portal of Ministry of home affairs defines it as "any unlawful act where a computer or a communication device or a computer network is used to commit or facilitate the commission of a crime". This is a separate category of crimes where the electronic resource is used to commit the crimes. Hence, investigation of such crimes requires a certain set of skills which include the knowledge of modus operandi of the cyber criminals.

Modus Operandi of the criminals in this crime

Most commonly reported and seen crimes that are associated with fake accounts are people making threats, bullying, harassing, stalking others on social media. First the fake accounts are made on the social media platforms or emails in the name of victim. Messages are then sent to the other people from the fake ID. Morphed images and defamatory material about the victim is posted on the account or sent through email. The nature of account is dependent on the intention of the criminal. If the intention is to harass the victim, a fake id in the name of victim may be made. If the intention is to defraud or induce the victim into doing something, then the fake id is made in any other name. If the intention is to commit a financial fraud, an mail id identical to the reputed portal/website/e-commerce website is made or a fake social media Id is made identical to the person in friends list. Cyber hacking is done by luring the victim into clicking on malware link in order to get access to the data, camera, microphone, etc. on the victim's phone. This access to camera, microphone and data can then be used for various crimes such as bullying, sextortion, harassment and pornography by using fake social media or email accounts. Children are more susceptible to these crimes. The basic idea behind creating a fake Id is to hide behind the electronic curtain.

With the increase in the online transactions, financial frauds have also increased. These crimes are committed through the fake Email

accounts or under the garb of fake identities. A group of people forming bogus call centre send fake emails such as 'your account is under attack. Do this now to prevent damage!' to the users which have seemed to be sent by reputed sites such as e-commerce, social media platforms, banks, etc. Once the user clicks on the link sent, the criminals get the access to the user's gadget. The emails are sent to the users regarding computer repairing services, anti-virus, offers, etc. Once contacted by the user, the tele-callers convince the user to take their paid services and make the payment through certain apps, gift cards and bank accounts in various other countries. The gift cards are redeemed through the telegram channels and money from bank accounts is converted through bitcoins. A demand of money as a loan is made through the profile identical to the person from the user's friends list on social media such as Facebook and Instagram. Duplicate profiles of many important personalities such as Commissioner of Municipal corporation, doctors, reporters, etc. have been made to make such demands.

Investigation Procedure to be followed

a. **Application of law -** When fake accounts is committed, the criminal is booked under s. 66D of Information Technology Act, 2000 along with s. 416 of Indian penal Code, 1860. The accused can be booked under local or any other special law. Then with respect to the nature of crime, the sections of IPC and IT Act will be attracted such as s. 354A of IPC for harassment of a woman, s. 354D of IPC for stalking, ss. 67,67A & 67B of IT Act, 2000 for the crimes related to publishing obscene material or explicit material showing involvement of child in sexual act.
b. **Pre investigation assessment -** Depending upon the nature of incident, investigating officer (IO) collect and preserve necessary information and evidence from the victim or complainant to understand the full scope of the incident. It helps the IO to draw a plan of action.
c. IO should ensure that all the details of the incident are captured in the complaint as well.
d. A legal request is made to the social media platform /email company by the IO. The information regarding internet service provider/s (ISP) of the culprit is obtained from them.
e. The ISPs have the IP address of the culprit. These crimes maybe committed from different IP addresses as well as different devices. The right information has to be obtained such as IP address and

IMEI numbers for the time and date of the crime. The permission of a magistrate has to be obtained to get the IP address from ISPs.

f. **Preliminary review of the scene -** From the above information, IO should then investigate the location of the incident and do the preliminary review of the scene of offence – whether a cyber-café, home, company space, etc.

g. **Evaluation of scene of offence -** IO identifies the scene of offence, secures it, take notes of individuals present and their roles. If the systems of computers or networks are on, IO should keep them on. If they are off, they should be kept off for the technical assistant to handle it, identify and collect the evidence. All the possible evidence should be collected. IO should make sure that all the perishable evidence should be identified and taken note of. Investigation of the physical space should be done. Passwords, bank account details, etc if found should be collected and preserved.

h. Preliminary interviews of the persons present at the scene of offence should be done. It helps identifying and seizure of potential evidence. A list of questions should be organised for the purpose of interviews. These interviews depend on the nature of crime.

i. **Technical assessment -** Type of connection obtained from the IP address, number of computers, system details, details of removable data storage, details of the network peripherals, CCTV clippings, etc. should be identified and collected for the purpose of further investigation.

j. **Standard operating procedure –** Standard operating procedure laid down by the Data Security Council Of India (DSCI) for the collection of evidence and investigation has to be followed. Standard Operating Procedure deals with Panchanama, interviews, forensic collection of digital media, forensic duplication, packaging and labelling of evidence, legal procedure to be followed post seizure of evidence, transportation of evidence, gathering information from external agencies, etc.

Example of certain judgements / case laws or real scenarios

a. State of Tamil Nadu v. Suhaskatti - CC No. 4680 of 2004:

The accused was the victim's family friend and wanted to marry her but she married another man which resulted in a divorce. After her divorce, the accused influenced her again and on her unwillingness to marry him, he took the course of harassment through the Internet. He opened a false e-mail account in the victim's name and posted obscene, defamatory, and annoying

information about the victim. Chargesheet was filed under Section 67 of the IT Act and Section 469 and 509 of the Indian Penal Code, 1860 against the accused. The accused was convicted under Section 469 and 509 of the Indian Penal Code, 1860 and Section 67 of the IT Act by Additional Chief Metropolitan Magistrate. He was punished with a Rigorous Imprisonment of 2 years along with a fine of Rs. 500 under Section 469 of the IPC, Simple Imprisonment of 1 year along with a fine of Rs. 500 under Section 509 of the IPC, and Rigorous Imprisonment of 2 years along with a fine of Rs. 4,000 under Section 67 of the IT Act.

b. Vishal Rajput v. State of Himachal Pradesh - Cri. M.P. .(M) No. 1170 of 2021

In February 2021, though victim turned down the marriage proposal of accused, however, chatting continued between them. At accused's insistence, the victim sent her nude photographs to instant messenger through WhatsApp. Petitioner got frustrated when his marriage proposal was rejected for the second time by the victim. He thereafter created a fake Facebook account of the victim and uploaded her nude photographs in that fake account.

c. Vishal v. State of Madhya Pradesh - MCRC No. 21888/2021

Complainant's daughter went to Alen coaching Indore in the year 2018 for preparation of PMT examination. The accused also studied with the victim. During said period, the accused clicked some objectionable photo graphs of the victim girl. After completing her course, in the month of November the victim came back to her house, thereafter, the accused sent the said photos to the mobile phone of complainant through whatsapp, due to which the complainant made a complaint to accused's father. Accused's father deleted the photos from the accused's mobile phone. After 4-5 days, applicant threatened the complainant that if he made appear his daughter in PMT examination, he will upload the said photographs on ID and defame her. On 29.08.2019 at about 6 am, applicant created a fake ID on Facebook only to upload the objectionable photos of complainant's daughter. Thereafter, complainant lodged the complaint against the applicant.

C. CYBER BULLYING

Description of the crime

Cyberbullying or online bullying is committed with the help of various communication technologies such as cell phones, internet to threaten, harass, insult, troll or intimidate someone with the help of instant messaging, e-mail, chat rooms or other social media platforms like Instagram, Twitter and Facebook. Almost all the people on social media are exposed to this crime and can become a victim to it without even realising. It can result in the victim committing suicide or taking other extreme measures, hence, should be given due consideration.

Provisions pertaining to cyber bullying:

- **Sec 304**: provisions of culpable homicide become applicable in situation where the victim dies.
- **Sec 306**: Abetment of suicide in cases where cyberbullying leads to someone committing suicide.
- **Sec 307**: Attempt to murder where the cyberbullying leads to murder.
- **Sec 323 to 326**: Causing hurt and grievous hurt and their respective punishments, this can become applicable in situations where cyberstalking turns into stalking which further takes the form of perpetrator harassing and causing hurt to the victim.
- **509 500** – 503
- **Sec 506**: Punishment for criminal intimidation
- **Sec 66C of IT Act**: Identity Theft
- **Sec 66D of IT Act**: Cheating by impersonation by using the computer resource
- **Sec 66E of IT Act**: Violation of privacy
- **Sec 67B of IT Act**: Punishment for publishing or transmitting of material depicting children in any sexually explicit act, etc. in electronic form
- **Sec 72 of the IT Act**: Breach of confidentiality and privacy

Modus operandi of the criminal in this crime

It is important for the authorities to understand that cyberbullying can take various forms with perpetrators operating in the following ways:

- **Harassment**: A person can harass someone by constantly sending them threatening or dangerous messages. These messages are sent with the intent to harm someone physically or their reputation.
- **Outing/Doxing**: It is an act of revealing sensitive or private information about someone for causing humiliation to that person on internet. The sensitive information shared publicly can include pictures, documents, messages etc. Evidently, the consent of the victim is absent in such situation leading resulting in severe embarrassment to them.
- **Trickery**: As the name suggests, the bully tries to befriend the victim, gains their confidence and then takes advantage of the victim by disclosing their private information publicly or to someone specifically.
- **Cyberstalking**: This particular crime can take dangerous forms. It can further take the form of stalking and prove to be fatal. During cyberstalking the stalker uses different means to stalk individuals or groups. Women and children in India are especially vulnerable to cyberstalking.
- **Fraping**: Here the social media platforms of the victims are used to post inappropriate content with their name. This can severely harm the reputation of the victim if not contained timely.
- **Masquerading**: A fake profile or a dedicated profile on social media platforms is created just to bully people online by the perpetrator.
- **Dissing**: The aim of the bully here is to tarnish the reputation of their victim by sending out insensitive and cruel information about them either through personal texts or public posts.
- **Trolling**: While it is difficult to understand what kind of trolling qualifies as cyberbullying. This form of cyberbullying is still omnipresent on all social media platforms these days wherein the bully posts indecent remarks about their victim on social media.
- **Flaming**: The bully directly sends out insults or vulgar text messages to their victim directly or they post bad remarks about their victims directly.

Investigation procedure to be followed

A. Process of investigation - Due to the varied nature of crimes that come under the purview of cyberbullying, the investigation takes shape depending on the type of cyberbullying. But the broad outline for approaching investigation should include:

Step 1: Identifying and acquiring sources of evidence

- Obtain a detailed description of the incident as well as the time of occurrence of incident from the complainant. Based on the complaint filed by the victim, the concerned authorities should try and identify the sources of evidence which may prove the victim's claims such as phone, computer etc. The sources should then be acquired to get a hold of the evidence.
- Ask the complainant if he or she knows who is sending the harassing messages. If he/she knows the suspect then IO may ask for information about the suspect: name, age, address, telephone number, vehicle information, and relationship to victim.

Step 2: Acquiring and handling different kinds of evidence - Ascertain when and how the harassment began. Find out if it has happened only via the Internet (e-mail messages, chat rooms, mailing lists, instant messages, Web site) or through telephone calls, cell phone calls or texts, postal letters as well

Situation 1: The victim should be asked to save the objectionable messages or take a screenshot of the abusive content in case of texts, chat boxes etc. on Facebook, WhatsApp etc. Noting the URL of the objectionable content and taking the screenshots is also important. Both, soft copy and the hard copy of the content should be maintained properly and kept in proper place.

Situation 2: The authorities can also reach out to the respective social networking sites under the section 91 of Cr. P.C which mention about the summon to produce documents to get details such as the IP address of the uploader which helps identifying the uploader of the objectionable content; the date and timestamp on which the content in question was uploaded; and any other details that the social media sites can provide to the police like the mobile number, e-mail I'd etc.

Step 3: Blocking objectionable content - In case the content is objectionable for example, it has pornographic images, or nudes of kids and women etc. that reveal their identities should be blocked after downloading them for evidentiary purposes by issuing a court notice to that effect.

Step 4: Sharing the evidence with a well-trained forensics team

After the evidence has been filed by the police, the evidence should be shared with the forensics team for analysts and forensic experts to preserve the data and prepare a report. Due care should be taken to

ensure that the evidence is not modified or deleted. For this, evidence sources must be isolated from the network so that no new data is received that can change or damage the evidence.

Step 5: Data extraction, analysis and report preparation

The next stage includes the extraction of data and analysis. The data extraction should be conducted using proper cables and software and should be further analysed. A detailed report should be prepared based on the results.

Step 6: Jurisdiction outside India - If the jurisdiction falls outside of India, MLAT process can be initiated.

Step 7: If the suspect has been identified, then their devices should be taken into custody for further investigation.

B. Preservation of evidence

Secure any physical evidence available and start the chain of custody to protect the evidence from getting tampered. The evidence should be recorded in both paper printouts and electronic files or on an electronic media such as a disk or CD/DVD-ROM. Ask the complainant, if he or she has any material evidence. Items to request include:

• Web page images • Chat room messages • Instant messages • E-mail messages & e-mail headers • Social network messages/wall posts • Mailing list messages • Message Board messages • Phone conversation recordings • Text Messages

1. **Packaging**
   Anti-static bag should be used to store the electronic media evidence seized, especially when electrostatic discharge can cause damage to the media. This should be covered in a layer of bubble wrap to prevent physical damage and scratches. Finally, loads of tape should be used to seal the packet.
2. **Labelling**
   Proper labelling of evidence is a crucial step for easy identification of the evidence even in future cases. All the details should be carefully mentioned on a tag for the packet of evidence and these details should also be recorded in relevant diaries like daily diary and case diary to maintain a proper schedule of evidences for different cases.

3. **Transportation**
   The evidence should be protected from physical damage and drastic temperature changes. A skilled person capable of taking care of such sensitive evidence should carry these packets for transportation.

Additional guidelines for the Police

- Keeping in mind that the source of evidence in cybercrime related cases are smartphones, computers etc, they should be stored properly to ensure their upkeep.
- The current state of the device should not be tampered with to prevent loss of volatile data.
- People without proper forensic training should not handle such evidences.

Example of certain judgements / case laws or real scenarios

Suhas Katti v. State of Tamil Nadu

Facts of the case - This is a landmark judgment in the history of cybercrime jurisprudence in India as it was the first case in India where the accused was convicted under the Information Technology Act, 2000 (I.T. Act) for posting of obscene messages on the internet. The accused was interested in marrying the victim but she declined his proposal and decided to marry someone else instead. After she got divorced the accused started contacting her again but the victim rejected his advances again. As a result of this, he started harassing her online by sharing her number and posting obscene messages on various groups with the intention of humiliating her. She started receiving embarrassing and obscene messages from people and was being harassed online. Hence, she decided to file a complaint in February 2004.

Judgement - The accused was sentenced to rigorous imprisonment for 2 years under Section 469 of IPC and had to pay a fine of Rs.500; two years' imprisonment and a fine of Rs 4,000 under section 67 of IT Act 2000; one-year simple imprisonment and a fine of Rs 500 fine under Section 509 of IPC. All sentences were to run concurrently.

State (cyber cell) v Yogesh Pandurang Prabhu (2009)

Facts of the case
reasons, she decided to unfriend him. As an aftermath of this incident, the accused had created a fake email ID to send offensive emails to the

reasons, she decided to unfriend him. As an aftermath of this incident, the accused had created a fake email ID to send offensive emails to the victim. On 03-03-2009, the reporter opened her email account only to find vulgar comments about her. Additionally, the victim was also receiving random calls from stranger as the accused had also made a fake I'd in her name.

Judgement

The court found the accused guilty under Section 509 of IPC,1860 and also Section 66E of IT Act, 2000 vide Section 248(2) of Criminal Procedure Code and he was punished with simple imprisonment for 1 month and a fine of Rs 5,000 in addition to being punished with simple imprisonment for 3 months and a fine of Rs 10,000 in default to suffer simple imprisonment for 2 months. And both the sentences ran concurrently.

D. JOB FRAUDS

Description of the crime

Job fraud is a sophisticated deception technique in which job seekers are offered bogus job possibilities. This form of fraud is typically committed using online services such as phony websites or unwanted e-mails purporting to be from well-known companies or brands. It has become difficult to tell whether a job offer is genuine or fraudulent. The fast advancement of ICT i.e., information and communication technology has radically altered the job seeking process be it for remote jobs, full-time jobs, or any freelance work. Nowadays, we begin all of our job searches online, which allows fraudsters to dupe us into falling for scams. Online job search causes us to hand over all of our personal information to job portals that may be scammers in disguise.

The Reserve Bank of India (RBI) warned citizens not to fall victim to job scams on March 21, 2022. The RBI has highlighted how online job fraud is committed, as well as the measures that the average person should take while applying for any job opportunity, whether in India or abroad. As employment fraud falls within the area of cybercrime, the laws for it are covered by the Information Technology Act of 2000 along with provisions of Indian Penal Code, 1860. The following are some sections pertaining to this crime:

Information Technology Act, 2000

- **Section 66D** - Punishment for cheating by personation by using
- computer resource
- **Section 74** Publication for fraudulent purpose

Indian Penal Code, 1860

- **Section 415 -** Cheating
- **Section 416 -** Cheating by personation
- **Section 420 -** Cheating and dishonestly inducing delivery of property

Modus operandi of the criminal in this crime

A job fraud is a crime wherein a criminal targets job seekers online, and in the guise of acting as a recruiter or employer, tricks the victim into

paying money for a job. A criminal might target any person registered with a job finding portal online and call them claiming to be from a recruiter and telling them that their profile had been shortlisted for a job. The victim would then be made to take an online test after making a payment to the offender (recruiter). This is a very standard modus operandi of job fraud these days. When the victim does not clear the test, they make ask for a refund. Here, the recruiter acting as a thorough professional asks for card details to refund the amount back and thereby, hacking the victim's bank account to withdraw money.

If one pays or agrees and accepts their part-time job offer, the fraudsters then continuously calls them and start threatening by saying that there are criminal cases registered against the company which offered the job and also against the victim and demand money from them to clear the case which has been registered against him. Believing the version of the fraudster, the person pays the amount mentioned by the fraudster.

Work from home scams- Work-from-home scams are when deceitful people create fake job postings to benefit themselves. They may use these as a means to steal your personal information or financial assets. As work from home jobs become more popular, scammers are starting to target this market with seemingly lucrative job offers. They may pose as a company or reputable person to get you to trust them.

Steps of Modus operandi - For most scammers, online job portals are a popular haunt to find prey. Here's how they proceed:

1. Applicant profiles accessed from job recruitment sites.
2. Mass mails sent to potential candidates.
3. Fraudsters pose as job consultants, set up fake websites, temporary 'offices'.
4. Candidates are asked to deposit registration fees via wallet or bank transfers.
5. Online or telephonic interviews are conducted.
6. Fake appointment letters are offered but in reality, this job is never offered.

OR

Modus Operandi for Work from Home Job scams

1. The scammers send phishing messages on WhatsApp, SMS, email and fake websites seeking candidates for DTP jobs
2. Victims open these links, fill the form or call on the number;
3. They are asked to do an interview after which they receive a communication of acceptance via email, Whatsapp etc.
4. Victims are then asked to submit their address, Pan Card or Aadhaar Card
5. Victims are then asked to sign online PDF forms which have 'penalty clause' for errors in its Terms and Conditions.
6. The employees then send a Portal for submission of work.
7. Sometimes these employees also ask for a Security Deposit before work starts
8. In the first few days, they do not identify any errors but then start identifying mistakes and consolidate errors and produce a bill.
9. The last step is when the perpetrators start harassing the victim which results in victim up paying.

Victim profile - These are the type of people who are most likely to fall prey to job scams:

1. Mostly from tier 2 or tier 3 cities
2. Graduate from lesser-known colleges or institutes
3. Poor interpersonal communication skills
4. 0-5 year of work experience
5. In their early to mid-20s

Investigation procedure to be followed

1. **Receive and responding to a complaint**
   After receiving complaint from a source or various sources the job scams or recruitment scams, a proper investigation team should be established specializing to look into such cybercrimes. They should be assigned defined responsibilities for carrying out the investigation successfully.

2. **Interviewing the Victim and conducting a preliminary assessment**
   The interview of the victim should be planned carefully to find a way to extract all the relevant information on their case with respect to identifying all portals where their resume or application was made, which job platforms did they visit frequently, how did the scammer contact, what details did they take, etc.

The team so established should carry out discussions to streamline their investigation process, gather necessary information on the case and understand the starting point. The purpose of these discussions should be to:

- Understand the context of the situation
- Establish the availability of evidence

3. **Preserve and collect evidence**
   Requisite steps should be taken to probe the online recruitment fraud by preserving any electronic evidence or any other evidence available. The following evidence should be collected:

- The number from which the link for the interview and job was shared with the victim.
- The number from where the call was made to the victim for selection for the job.
- The website used by the victim to reach out to the bogus employers.
- Saving up texts, mails etc. that serve as a proof for communication between the victim and the perpetrator.
- Any UPI link or bank account details that were given to the victim for the initial advance payment or security deposit for securing the job.

4. **Analyse financial and electronic records**
   The financial records, electronic records and transactional activities on the victim's bank account should be analysed properly. Forensics experts should also be involved for vetting the evidence properly. This will help determine the extent of potential liabilities or losses that might exist.

5. **Take down of fake sites or fake profiles**
   Also, such fake sites or portals where jobs are being offered should be sent a notice, and take down shall be carried out. Or if there is any profile of an employer on legitimate sites which is fake, then the same should be reported to the support / grievance team of these legitimate sites.

6. **Taking steps to prevent continuity of the scam**, mitigate losses and help in the recovery of losses to the victims.

Example of certain judgements / case laws or real scenarios

Case 1: In July, 2022 Faridabad police arrested five men for allegedly duping 335 people. They promised jobs in a private airline to these

victims and lured them with good packages. The perpetrators collected data from job seekers from different websites and posed as senior officials of a private airline. Conducted fake online interviews. They asked the victims to deposit fees for medical assessment, registration, and other joining formalities, along with a refundable security amount. The news of the fraud surfaced when one of the victims reached out to the police to file a complaint. He was duped of ₹6.80 lakh after he applied for a job through a website. ₹3.97 lakh were recovered.

Case 2: An international gang duped 300 Indian nationals by offering them jobs in Thailand. They are now trapped in Myanmar's Myawaddy area where the gang has held them captive and is forcing them to do cybercrime activities. Some Tamil men sent out an SOS video requesting Union and Tamil Nadu government to help them.

E. DATING APP / MATRIMONIAL SCAMS

Description of the crime

Dating App Frauds also known as Romance Scams or as Catfishing are carried out when the criminal adopts a fake online identity to scam their victim, blackmail them and extort money or other sexual favours.

Section 66-D of the Information Technology Act, 2000 provides for punishment for cheating by personation by using a computer resource. Section 415, 416, 417, 419 and 420 of the Indian Penal Code deal with cheating and cheating by personation.

Modus operandi of the criminal in this crime

The criminal adopts a fake online identity to gain a victim trust. The scammer tries to use the fake romantic relationship aspect to steal from the victim or manipulate the victim. They use fake images to create profiles and try to get attention. Stolen photographs of attractive people are often used to lure the victim. The scammer creates such profiles with the intention of gaining the trust of the victim as soon as possible and establishing a relationship. Sometimes these scammers propose marriage or make plans to meet in person, which never materializes.

1. Blackmail

a) Some romance scammers capitalise on the obscure fetish their victim might have and make the victim pay for making travel arrangements for the meeting.
b) Some scammers somehow get their victims to perform sexual acts on webcam which gets recorded and is later used to extort money from them.

2. Posing as someone from a reputed institution or from a reputed job and target their victims

Some scammers pretend to be army personnel, a doctor with an international organisation and ask people to pay for a plane ticket or other travel expenses, for surgery or other medical expenses, money for paying off gambling debts, visa or other official travel documents. Some scammers pretend to be lonely or have a sad back story or talk about how they are trying to help and support the members of the community and need financial assistance for that.

3. Pro-daters

These scammers actually meet their victims but it is all a ruse to build deeper relationship and manipulate the victim into spending more money in a short span of time. The entire date is a set-up wherein more than one people are involved to fool the victim.

4. Customs Scam

The scammer gains the trust of the victim they have met through online dating apps, matrimonial websites or other websites. After proclaiming their fake love for the victim, they propose for marriage or show interest in meeting the parents of the victim to take permission for marriage. On the date of such bogus travel the victim gets a call from fake customs officials informing him or her about the amount of gold and money the person is carrying with them and how they cannot allow for it to pass through unless some amount is paid as tax.

Investigation Procedure to be followed

1. **Registering the complaint -** The Investigating Officer (IO) needs to register the complaint encapsulating all the possible details such as:

- The platform on which the victim first spoke to the perpetrator to lure the victim in the trap
- The profile details of the perpetrator
- The messages that hint towards a fake romantic relationship between the two (in case the perpetrator has proposed to the victim for marriage or has spoken about meeting him/her)
- Messages that reflect the extortion intent of the perpetrator (in case he/she has asked the victim to send money for different purposes etc.)
- If the victim has met the perpetrator or not and if so, has the details regarding the place of their meeting
- In case any money has been transferred from the victim's account to the perpetrator
- If Bank Account details have been shared by the victim

2. **Blocking the account**
   If the victim has shared the bank account details and personal financial information along with it, a cheque which is yet to be deposited, if a wire transfer has been initiated, any transaction in digital currency such as cryptocurrency. Relevant steps should be taken to immediately block such accounts, stop transactions etc. to prevent further transactions and deduction of money.

3. **Getting third party information from service providers -** Police officials can seek third party information from service providers:

a. **Social Networking website company**: Registration, access details of the fake profile created by the accused, other details such as name, date of birth, IP address, email IDs given by the accused while creating the fake profile.
b. **Email Service Provider**: Access details of the subject email ID which has been used to circulate the objectionable morphed pictures content.
c. **Internet Service Provider**: After obtaining details of the IP address, name etc. the IO should get the physical address of the IP address from which the fake profile for scamming the victim has been created.

Information can also be collected from such dating app nodal officers or matrimonial website support team for further information on the profile or any other additional information they may have regarding the profile created or any information that was given by the accused while creating this profile.

4. **Starting preliminary investigation**
Once the complaint is received by the concerned officer, it is imperative for him to execute a pre-investigation assessment into the matter. Based on the information shared, the officer initiates an investigation to ascertain the intensity of the romance scam and the legal provisions applicable to the case in hand. Further, the officer examines the digital evidence provided by the victim such as texts from the scammer and may also collect additional evidence required for investigation.

5. **Sending the reports to the magistrate**
A police report needs to be sent to the magistrate under Section 157 of the CrPC. This is done to keep the magistrate updated about the status of the investigation. Additionally, a 'final report' is also sent to him at the end of the investigation under section 173.

6. **Investigation order by Magistrate**
The Magistrate has the power to direct or hold a preliminary inquiry under Section 159 after receiving a report under Section 157. The Magistrate can also order for a police investigation.

F. CYBER STALKING

Description of the crime

Cyber stalking is a crime in which the perpetrator uses internet resource to harasses the victim. Platforms such as e-mail or instant messaging (IM), or other social media platforms are used to deliberately stalk (follow) someone and either harass them or bully them online. Some of these online harassment and stalking cases become physical as well wherein after keeping a track of the online movements of the victim, the perpetrator starts following them offline. This online cyberstalking can often translate into the person cyberstalking the victim in the real by showing up either at their workplace or house etc.

What does cyberstalking include?

- Defamatory accusations against the victim
- Making sexual comments about the victim or publishing things with the intent of defaming the person

Indian Penal Code, 1860

- Section 354D of IPC
- Section 292 of IPC
- Section 507 of IPC
- Section 509 of IPC

Information Technology Act, 2000

- Section 67 of the IT Act
- Section 67A of the IT Act
- Section 67B of the IT Act
- Section 66E of IT Act, 2000 and Section 354C of IPC

Modus operandi of the criminal in this crime - Cyberstalking can take dangerous forms and prove to be fatal. During cyberstalking the stalker uses different means to stalk individuals or groups. Women and children in India are especially vulnerable to cyberstalking. Types of cyber stalking:

1. **Webcam Hijacking**: In this, the stalker tricks the victim into downloading a malware infected file through email, messages etc., this provides them with the access to your webcam.

7. **Probing of property or any place important in investigation**
The police has the power to search any place or property that holds any interest in the case under Section 165 of CrPC. Though for searching the property a search warrant needs to be issued by the Magistrate. Proper reasons need to be given by the police officials for getting the warrant. A report needs to be shared with the Magistrate after the completion of the search. The laptop device, mobile or any such electronic evidence through which the crime has been perpetrated can be seized and sent to the forensic laboratory for further evidence collection. The police is required to issue a "challan" or "charge sheet" after the completion of the investigation. It should contain all the details regarding the investigation.

Example of certain judgements / case laws or real scenarios

Cases:

1. In May, 2022 Cyberabad Cybercrime police booked a complaint wherein a dating app was used by a woman to extort two lakh rupees from a data engineer. The two met on AISLE dating app wherein the woman asked the man to strip and she recorded him while he was taking off his clothes, later started threatening him to release his video and demanded Rs 2.4 lakh.

2. In November 2021, a 27-year-old man got duped for approximately Rs 65 lakh. He came across the mobile number of a dating company, he called the number and after speaking to a woman named Shweta, who encouraged him to join a dating app, he decided to do the needful. He was then asked to pay a refundable amount of Rs 18,000 and was introduced to a girl. But he continued to receive calls from Shweta who kept asking him to deposit certain sums of amounts. He made many transactions up to Rs 65 lakhs over a span of few days and when finally realised he was being scammed, he refused to pay, one of the employees of the company threatened to frame him under a rape charge.

2. **Observing location check-ins on social media**: Once the victim puts up check-ins on social media, it is used by the stalker to follow the victim.
3. **Visiting virtually via Google Maps Street View**: With the advancement of technology, it is now easier for the stalkers to find the area and neighbourhood of the victim with the help of street view. Once they figure out the details of where the victim lives etc., it gives them much easier physical access to victim.

Investigation procedure to be followed - The broad outline for approaching investigation pertaining to cyberstalking includes:

1. **Registering the FIR**
   The first and the foremost step would be proper registration of the FIR with comprehensive and nuanced details. In cases where the victim is a woman, a lady police officer should register the FIR encapsulating details such as:

- How did they realise that they were being stalked?
- Do they have any textual or image proof to back up the stalking claim?
- Do they know the person who is stalking them?
- If yes, is the person from their neighbourhood, someone from work, someone who has had romantic interest in the victim etc.?
- Has the stalking been just online or offline as well?
- Did the victim share the check-ins on social media?

2. **Starting the preliminary investigation**
   The IO should prepare an investigation team to look into the leads by the victim. It is the duty of the police authorities to ensure that the victim does not come in contact with the stalker.

3. **Identifying and acquiring sources of evidence**

- Based on the complaint filed by the victim, the concerned authorities should try and identify the sources of evidence and then get a hold of the evidence.
- For example, if the victim thinks or the police officials have the reason to believe that the victim was being webcam stalked, they should immediately send the device with the webcam for forensic examination.
- If in case there have been calls received by the victim from the stalker, all the details with respect to IMEI details, subscriber

details, address of residence, the tower locations shall be mapped.

- If the same has happened over social media, then the officials should try mapping the digital footprint of the same and get more information from the nodal officers and grievance cell of that social media platform. Open-Source Intelligence techniques can also be performed by the LEAs or forensic officials to map out the probability of the location of the stalker.

4. **Bringing in the suspect for questioning**
   If the stalker is identified, the police should bring in the suspect for comprehensive questioning, to collaborate facts etc. and acquire other relevant sources of evidence.

5. **Sharing the evidence with a well-trained forensics team**
   After the evidence has been filed by the police, the evidence should be shared with the forensics team for the analysts and forensic experts to preserve the data and prepare a report. Due care should be taken to ensure that the evidence is not modified or deleted. For this, evidence sources must be isolated from the network so that no new data is received that can change or damage the evidence.

6. **Data extraction, analysis and report preparation**
   The next stage includes the extraction of data and analysis. The data extraction should be conducted using proper cables and software and should be further analysed. A detailed report should be prepared based on the results and the same shall be submitted in the court.

Examples of certain judgements / case laws or real scenarios

Case law: Manish Kathuria v Ritu Kohli

This is the first case of cyber stalking to be reported in India. The accused was using the name and identity of the complainant to send obscene and obnoxious messages to people. Additionally, he shared the contact details of the complainant. It is when she started receiving texts from strangers, she realized something was wrong and further went on to complain with the police. The accused was booked under sec 509 of IPC for outraging the modesty of women.

Recent cases:

1. In the year 2020, Divya Sharma noticed that almost 200 pictures of her on Instagram were liked by a stranger. Initially she did not consider it to be dangerous. But soon this man started writing indecent comments on her profile. Additionally, she started receiving DMs from this person. He repeatedly asked her to go on dates with him but she decided to ignore the texts. Divya then finally lodged a complaint with the cyber police and necessary steps were taken such as suspension of the account made by the stalker used for posting obscene comments and threats.

2. The case of Raina Raonta is a classic example of how cyberstalking can result in physical stalking in no time. In this case a man had sent 30,000 texts to her on Facebook messenger and they did not even know of each other before this. The stalker started bothering her parents by calling on the phone and then stalked her sister. Raina finally lodged a complaint against him and during the investigation the police acquired his laptop only to find that he had her picture as the screensaver.

G. Morphing

Description of the crime

Morphing is a technique through which the one image can be faded into another by using various software and tools. This technique is being increasingly used by criminals to morph pictures of young children and women in obscene pictures and videos and using these to blackmail them. These images and videos are also misused for creating fake profiles on social media platforms and these profiles can be operated by perpetrators to scam other people, relative of the person whose pictures they have morphed further tarnishing the reputation of the victim. There are cases wherein these altered images and videos are also being used for sexting sex chats, pornographic content, nude pictures etc.

Applicable Laws: Section 465, 469 of IPC (Forgery, Forgery for purposes of harming reputation) and Section 67 of IT Act (publication or transmission of obscene material in electronic form).

Modus operandi of the criminal in this crime

Digital manipulation techniques are on the rise, and are being used for harming the reputation for revenge or blackmailing people for money, sexual favours etc. People committing the crime of morphing operate one of the following ways:

Case 1: The perpetrator downloads the victims' pictures or is able to acquire their pictures from various sources and then uses these to morph false images in certain compromising positions to blackmail the victim or get other favours.

Case 2: The perpetrator makes video calls on social media platforms and as soon as the victim picks up the call, the mobile screen records and the criminal edits the videos and shows the victim in obscene positions. This is then used by them to call the victims asking for money.

Investigation procedure to be followed: - An outline of the process of investigation that should be followed is mentioned below:

1. **Blocking objectionable content**
   In case the content is objectionable for example, it has pornographic images, or nudes of kids and women etc. that reveal their identities should be blocked after downloading them for evidentiary purposes by issuing a court notice to that effect.

2. **Getting details from the victim**
   This step lays the foundation for a streamlined investigation. The IO should ask the victim details such as the places where the pictures and videos were uploaded; if pictures have been shared with someone; if the picture used to create the new morphed image can be identified.

3. **Advising victim to not delete her social media profiles**
   Many a times victims delete their social media platforms out of fear, guilt, shame and embarrassment. The IO needs to specifically advice victims to not delete the profiles as they can be an important piece of evidence.

4. **Getting third party information from service providers**
   In cases of content being posted on any social media accounts or websites with morphed pictures featuring the victim in compromising position the police officials can seek third party information from the service providers.

   a) Social Networking website company: Registration, Access details of the fake profile created by the accused, other details such as name, date of birth, IP address, email IDs given by the accused while creating the fake profile.
   b) Email Service Provider: Access details of the subject email ID which has been used to circulate the objectionable morphed pictures content.
   c) Internet Service Provider: After obtaining details of the IP address, name etc. the IO should get the physical address of the IP address from which the morphed pictures and videos have been uploaded. The IP can also reach out to the email service provider to obtain various information of the accused.

5. **Collecting evidence from accused and scene of offence**
   Once the preliminary investigation helps in procuring IP address from the internet service providers, the police officials can then proceed to search the premises under CrPC provisions. The identified computers, mobiles etc. should be seized. Points to be kept in mind during the search and seizure of the evidence:

- The authorities should not take the help of the accused to switch on the phone, computer or log into the system or social media platforms etc. as this can result in accused trying to delete the evidence or tamper with it.

6. **Correct timestamps**
   Most of the service providers are international companies with time stamps in GMT, PT etc., hence the time stamps of the evidence collected should be converted into Indian Standard Time (IST).

7. **Sharing the evidence with a well-trained forensics team**
   After the evidence has been filed by the police, the evidence should be shared with the forensics team for the analysts and forensic experts to preserve the data and prepare a report. Due care should be taken to ensure that the evidence is not modified or deleted. For this, evidence sources must be isolated from the network so that no new data is received that can change or damage the evidence.

8. **Using software**
   Certain software can be used to determine whether the image has been morphed or not. Not just that, but thoroughly checking the evidence source procured for such morphed images or videos or tools used for morphed pictures can prove to be helpful.

9. **Data extraction, analysis and report preparation**
   The next stage includes the extraction of data and analysis. The data extraction should be conducted using proper cables and software and should be further analysed. A detailed report should be prepared based on the results.

H. SEXTORTION

Description of the crime

The term “sextortion” is a combination of two words namely “sex” and “extortion”. In this crime, the perpetrator threatens to reveal the person and sensitive information of the victim if the sexual offers proposed by them are not fulfilled. Sexual offers, corruption and blackmailing are all humiliating ingredients that make up for this crime. Sextortion is committed through various mediums such as social media, phishing schemes through emails, sextortion through hacked webcams, through account hacking etc. in which the victim is threatened to share sexual photographs or information in order to extort money or sexual pleasure. It can take two forms - accused asking for money or other favours for not leaking sexual sensitive information of the victim or the accused asking for sexual favours in exchange for a benefit that the offender has the authority to withhold or give.

The Laws governing sextortion in India and the relevant sections are as follows:

- The Protection of Women from Domestic Violence Act, 2005
- The Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013
- Section 108(1)(i)(a)
- Section 292
- Section 354
- Section 354A
- Section 354B
- Section 354C
- Section 354D
- Section 406
- Section 499
- Section 500
- Section 506
- Section 509
- The Protection of Children from Sexual Offences Act, 2012
- Section 66E
- Section 67
- Section 67A
- Section 67B of the Information Technology Act
- Section 72 of the Information Technology Act

1. Sending the reports to the magistrate

Various reports are sent to the magistrate throughout the investigation process. The purpose of this is to make him aware of the status of the investigation. Under Section 157 of CrPC, it is mentioned that a “police report” needs to be sent to the magistrate to inform him of the reasons on whose basis the suspicion, of a crime having been committed, is founded. Thus, it informs the Magistrate that the particular case is being investigated by the police. The Magistrate cannot stop the investigation process once it has been started, hence this sending of the police report is merely a formality. Apart from this report, a ‘final report’ is also sent to him at the end of the investigation under section 173.

2. The order to investigate by the magistrate

Section 159 of the CrPC empowers the Magistrate to direct investigation or to hold a preliminary inquiry, into a case upon receiving the report sent in accordance with Section 157. He has the authority to order the police to start the investigation.

3. Identification & Attendance of the Witnesses

After investigating the crime and finding all the necessary pieces of evidence, suspects, and witnesses, the police officer has the authority to call any person who appears to be acquainted with the facts and circumstances of the case, to be present for interrogation. Any person having first-hand knowledge of the crime can be a witness and they are obliged to state correct and true facts relating to the matter because their statements matter a lot in the case. The power to identify and address the witnesses is enshrined under section 160 of CrPC.

4. Examination of Witnesses by Police

Section 161 of the CrPC empowers the police to interrogate the witnesses. The witnesses play a crucial role in the investigation process. They are required to answer each and every question asked by the police during the interrogation. However, they are not bound to answer such questions the answers to which have a tendency to expose him to a criminal charge, or to a penalty, or forfeiture. In such cases, the person may refuse to answer the question. Ethically, the person should state the real and the correct facts pertaining to the case. The statements made during the examination may be reduced to writing by the police officer, however, it is not a compulsory provision, and thus it's upon the investing officer to decide.

Modus operandi of the criminal in this crime

The crime is a psychological coercion wherein the person committing the crime has power over its victim in two ways – first they possess sensitive information of the victim or there is an inherent power imbalance between the offender and the victim. In the cases pertaining to latter situation, the accused is generally a person who has been entrusted with power, such as judges, government officials, teachers, elders, doctors, and employers. These individuals seek to coerce sexual favours in exchange for anything within their power to grant or withhold, such as government officials requesting sexual favours in exchange for permits or licences, interviewers requesting sexual favours in exchange for a job, or teachers requesting sexual favours in exchange for grades.

People committing these crimes usually operate in the following ways: Case 1: When the victim and accused are unknown:

1. The victim might receive a video call from an unknown number.

2. Though this video conference the perpetrator captures the image of the victim which is further morphed to create objectionable content used for blackmailing the victim.

Case 2: When the victim and the accused are known to each other:

In this scenario, the trust between the parties leads to one of them sharing intimate pictures and videos with another which is then used to blackmail the victim.

Investigation procedure to be followed

Section 157 of the CrPC provides us with the preliminary inquiry method. According to this, after receiving the information about the crime, the officer in charge of the police station is empowered to investigate the case and to send the report of the same to the Magistrate, who would then take cognizance of the case. The Police need to go to the crime scene to collect evidence and arrest the suspect if needed. They can also deny investigating on the ground that the case involves some non-cognizable offences, which cannot be investigated without the order of the Magistrate. If the investigating officer does not find any reasonable grounds to investigate, then he is not bound to investigate, and he can inform the reasons for the same to the magistrate.

5. Recording of Statements or Confession by Magistrate

Section 164 empowers the Magistrate to record the statements or the confessions made by any person during the whole investigating process, or before the commencement of the inquiry or trial. For the purpose of this section, it is immaterial whether such a Magistrate has jurisdiction in the case or not. The Magistrate is required to inform the person that he is not bound to make the confession, and the same can be used against him in court. If someone is not wanting to make the confession then the magistrate cannot force him to do so. The confession needs to be purely voluntary.

6. Acceptability of Evidence

The confession recorded under Section 164 can be used as evidence against the person who has made the confession. It is upon the court to measure all the factors pertaining to the evidence and then consider it. The confession should be presented before the court in its entirety to decide whether it is useful or not.

7. Probing of Property or any Place important in Investigation

The power to search any place or property is given to the police under Section 165 of CrPC. A police officer conducting the investigation or a subordinate officer under his order can search any place or property, which holds any interest in the case. For searching a place, the police are required to have a search warrant issued by the Magistrate. If the place or the property to be searched is located outside the territory of India, then the Magistrate can write a letter asking for permission to search that place from the authority of that area.

The police officers are required to give a proper reason, in writing, for the search along with the materials that they are searching for. After the completion of the search, they are supposed to send the report of the same to the Magistrate, so that he can inform the same to the owner of the property.

By the end of the investigation, the police are required to present a “challan” or “charge sheet” to the court which contains all the necessary information regarding the investigation. After this, the suspected persons are charged with the crime, and then the trial begins. This provision is mentioned under Section 173 of CrPC which mandates the police officers to produce a charge sheet having all this essential material of the investigation, before the court.

Additional guidelines for the police: Safe reporting system for victims

- The police personnel should be trained to give adequate support to the victims
- Keeping in mind the stigma attached to such issues getting victims to report such crimes is a difficult task. To improve the statistics on the number of reporting's there must be a formal and confidential system to receive and register complaints further ensuring that the incidents are investigated with utmost confidentiality.

Example of certain judgements / case laws or real scenarios

State of West Bengal v Animesh Boxi, C.R.M. No. 11806 of 2017, GR/1587/2017.

Facts of the case:

Animesh Boxi, the accused had asked for various intimate pictures of the woman he was in a relationship with. After getting his hands on these pictures and videos he started blackmailing her into spending time with him. A few days later, the victim's brother discovered the nude pictures and videos on a porn site with the video giving away the victim's identity. Boxi was charged under sections 354A (Sexual Harassment), 354C (Voyeurism), 354D (Stalking) and 509 (Criminal Intimidation) of the Indian Penal Code, 1860 ("IPC") and sections 66C (Identity theft), 66E (Violation of privacy) and 67/67A (Transmitting obscene material online) of the Information Technology Act 2000 ("IT Act").

This case is of historic significance as it is the first conviction in a 'revenge porn' case in India. The court sentenced him to 5 years' imprisonment along with a fine of Rs. 9,000.

I. Sexually abusive crimes against children

[Child Pornography, Online Child Grooming, CSAM, Sextortion, online child trafficking (labour)]

Description of the crimes:

Over the years, the growth of Internet users has been massive with billions of people daily accessing internet services worldwide. It is a space of infinite connectivity and information but comes with comes with its own risks and vulnerabilities. With the internet becoming a standard part of our daily life, especially among children and youth, it is vital to have effective rules and regulations in place to ensure the users' safety.

Various sexually abusive crimes against children in today's online world, as described below:

1. **Child Pornography -** It is a visual depiction of sexual activities involving a child. Any simulated or real image, video, or film of a child engaging in sexually explicit activities including sexual intercourse, masturbation, or demonstration of a child's genitals will come under the ambit of child pornography. The term child pornography has been clearly defined under Section 2 (da) of the POCSO Act, 2012.
2. **Child Sexual Abuse Material (CSAM) -** Many experts have now alternatively started using the term CSAM in place of child pornography to highlight the fact that the sexual images/videos are nothing but 'the sexual exploitation and abuse of children.' Under CSAM, the consent of a child holds no importance since it is believed that a minor has not attained the mental acuity to make informed decisions.
3. **Online Sextortion -** It is a serious crime wherein a person threatens to share private or sensitive information with the intent to extort money or sexual favours from the other person (a child in this case). Children often fall prey to such crimes and are blackmailed to perform sexual favours against their consent. The perpetrator could threaten to leak sensitive information or harm the child and their close ones.
4. **Online Child Trafficking -** A heinous crime that involves illegal transportation and selling of children away from home for the purpose of exploitation, forced labour, physical and sexual abuse. These children are then forced to work as slaves in hazardous industries, made to beg on roads, or forcefully thrown into the world

of prostitution. Criminals these days have come up with innovative ideas to lure children online into child trafficking by using fake identities and offering children job opportunities in far-off cities with lucrative salaries.

5. **Online Child Grooming -** It is an act of befriending a minor online and gaining their trust with an ulterior motive of sexually abusing the child. The groomers nefariously choose a target, become acquainted with the target (child) online, gain their trust and lure them in to gain sexual favours.

These various legislations have been enacted to ensure the safety of children against online crimes:

1. **The Protection of Children from Sexual Offences (POCSO) Act, 2012**
   It is a comprehensive law to safeguard children against sexual harassment and assaults. It includes provisions particularly formulated to deal with online offenses against children.

2. **Sections 11 and 12 - Deal with the definition of sexual harassment and its punishment which may extend to three years along with a fine.**

a. Section 13 - Any person who uses a child in any form of media for "sexual gratification" shall be guilty of "using a child for pornographic purposes".
b. Section 14 - Deals with the punishment for child pornography u/s 13
c. Section 15 - Prescribes punishment for storing or possessing pornographic material in any form involving a child
d. Section 20 - makes it mandatory for any personnel of the media, hotel, lodge, hospital, etc. to provide information to the authority on coming across any sexually exploitative material involving a child
e. Section 23 - Lays down the procedure to be followed by the media while reporting news related to children

3. **Information Technology (IT) Act, 2008 -** This law deals with cybercrimes against children and adults.

a. Section 66E - Punishes any person who publishes or transmits images of the private area of any person
b. Sections 67B - Punishment for publishing, transmitting, or browsing any material that depicts a child in a sexually explicit act, etc. in electronic form

4. **Indian Penal Code (IPC), 1860 -**

a. Section 293 – There is no direct provision dealing with child pornography in IPC but the code's section 293's ambit is wide enough to cover child pornography
b. Sections 370 - This section pertains to the buying or selling of any person as a slave

Modus operandi of the criminals in this crime - The modus operandi of criminals for crimes against children on online spaces has been outlined below:

1. **Child pornography**

Children are often recorded without their permission by the criminals during sexual activities or in compromising positions and these pictures and videos are the uploaded online. Additionally, some criminals make use of the poor background of some children thus forcing them into the pornographic industry.

2. **Online Sextortion**

a. The perpetrator usually befriends children on social media networks and lures them into sharing their nude pictures etc.
b. The child might receive a video call from an unknown number. When the victim pics up the call the perpetrator captures the image of the victim which is further morphed to create objectionable content used for blackmailing the child.

3. **Online Child Trafficking**

a. Kidnapping/Abduction: Kids in most countries are kidnapped or abducted and trafficked for different purposes.
b. In some countries, the parents of the victims from rural areas give their consent to traffic their kids or sell their kids for money. And the criminals make use of such vulnerabilities and traffic children.

Investigation procedure to be followed

1. **Pre- Investigation Assessment**

After receiving the complaint, it is imperative for the Investigating Officer (IO) to conduct a pre-investigation assessment. Depending on the nature of crime reported, the IO will collect relevant details from the victim/complainant to understand the nature and intensity of the crime in hand. Such assessment helps the IO to decide the

further line of action and the make decisions accordingly in the interest of the victim. The police officials should:

a. gather important facts (who, what, where, when, how)
b. conduct a preliminary assessment of the risk to the child involved
c. determine the priority of response
d. consider reaching out to relevant agencies

2. Protective Custody

The police officials need to figure out if there is a need to put the victim in protective custody by considering the following:

a) If there is a need for medical care
b) If the child is in imminent danger of continued abuse
c) If the situation is such that it can pose severe threat to child's health and softy
d) If there are no parents or guardian to take care of the child
e) history of prior offenses or allegations of child abuse

3. Shelter Homes

The police authorities should keep a list of shelter homes and points of contacts ready in such cases as kids in need of shelter and care can be sent to such homes until further steps are taken.

4. Identification and documentation of evidence

Digital evidence comes in different forms and types. It is important for the IO to identify all such evidence related to the case and secure them without causing any loss and destruction to it. The evidence is broadly collected in two ways:

a. From the victim/complainant

b. From other stakeholders under section 91 of CrPC such as Internet Service Providers or Social Media Companies. The IO can furnish details of the suspects including their IP address, MAC ID, user activity from time to time, personal details shared with the online portal etc.

If incase there is a tipline report that is received by the police then the investigation starts from this step itself. The access to one lakh-plus Tipline reports prepared by America's National Center for Missing and Exploited Children (NCMEC) has helped check the growing number of cases of child pornography and child sexual abuse across the country.

any help from outside India, CBI Interpol Division is approached and the provisions of Mutual Legal Assistance Treaties are applied. (MLAT processes mentioned below)

10. **Final Report Preparation -** A final report should be prepared with detailed information on the following aspects:
    a. Details shared by the victim(s)
    b. All evidence identified and collected
    c. Statements from victim, witness and suspect
    d. case progress details

Additional Guidelines to be kept in mind

1. Police officials should wear plain clothes while dealing with children who have been victims of any of the above-mentioned crimes.
2. The police officer should take care of the food requirement and other basic amenities of the child as long as the child is in their charge.
3. The police officials should be in constant touch with the Child Welfare Committee(s) and NGOs working with children that are capable of helping kids and provide necessary support in terms of shelter, food, protection and care in addition to providing legal and emotional help.
4. Special care should be taken to ensure that the identity of the victim of abuse and the report of suspected child abuse is kept confidential.
5. Identities of users engaging in cryptocurrency transactions to buy child pornography online can be traced with proper coordination between Ministry of Electronics and IT and Ministry of Home Affairs. Online payment portals and credit cards should not be allowed to process payments for pornographic website.
6. Notices should be issued to all social media platforms to mandate them to recognise and remove Child Sexual Abuse Material. Gateway Internet Service Providers (ISP's) must bear a significant liability to detect and block CSAM websites. Intermediaries shall also be responsible to report to the designated authority, IP addresses/identities of all those searching/accessing child porn/CSAM keywords.

Example of certain judgements / case laws or real scenarios

When a citizen gives a tip about a crime to law enforcement agencies through a dedicated number or website, it automatically gets converted into a report for action making it as 'Tipline report.' The NCMEC, which is the United States' centralized reporting system for online exploitation of children, has been sharing these tipline reports with India following an agreement it signed with the National Crime Records Bureau (NCRB) three years ago. These tiplines come to NCRB if the complaint is related to India. NCRB then forwards it to the respective State and UT police jurisdictions and from there further it is forwarded to individual police jurisdictions.

5. **Taking down and blocking objectionable content**

The nodal officers who will handle child pornography/rape and gangrape content complaints have been asked to save all the evidence received from complainants in the system, and immediately issue notice (s) to content hosting providers (CHPs) and internet service providers (ISPs) for taking down the identified sexual abuse videos/photos or blocking the links/content. After securing the required evidence and obtaining necessary court permission, notices and takedowns should be served to digital portals to delete child sexual abuse material in order to avoid further access and transmission of the objectionable content.

6. **Proper packing, labelling and transportation of evidence**

The digital evidence recovered should be properly packaged to avoid contamination or destruction, labelled appropriately to avoid further confusion and transported cautiously to avoid any damage and scratches.

7. **Evaluation of evidence**

After the search and seizure of digital evidences is done, the IO obtains the necessary permission of the competent court to send such evidences for forensic analysis and expert opinions. A detailed report is then shared with the IO post examination of the evidences by the forensic scientists and experts.

8. **Interrogation and arrest of the suspect**

The suspect(s) should then be interviewed/interrogated followed by a consideration on whether they should be arrested or not.

9. **Investigation Abroad**

Section 166A of CrPC provides for issuing letters to the competent authority outside India to request examination of any person related to the cybercrime case in hand. Further, if the investigation requires

P.G. Sam Infant Jones v. State, 2021 SCC Online Mad 2241

Facts of the case

The Madras High Court in this case determined whether child pornography is an offence or not. The petitioner here had browsed, downloaded, and transmitted child pornographic material by using his Airtel sim through his e-mail and Facebook Account.

Court Observation

The Hon'ble High Court noted that privately while watching pornography is not considered to be a crime. But, under Section 67-B of the Information Technology Act, 2000, every act relating to child pornography is punishable, therefore even watching child pornography is illegal.

Judgement

The order was that petitioner be released on bail in the event of arrest by the respondent police on execution of personal bonds for a sum of Rs. 5,000/- (Rupees Five Thousand only) with two sureties each for a like sum to the satisfaction of the respondent police. Additional condition was that the petitioner shall appear before the learned Sessions Court/Special Court for trial of cases under POCSO Act, Madurai, and execute fresh personal bonds for a sum of Rs. 5,000/- (Rupees Five Thousand only) with two sureties each for a like sum to the satisfaction of the Sessions Court/Special Court within a period of one month, from the date of resumption of regular work in subordinate Courts.

Sr. No	Service	Can CSAM be reported?
1.	Facebook Messenger	Messages in a secret conversation can be reported if they violate Facebook's Community Standards. Content related to bullying, sexual violence, or sexual exploitation constitutes a violation of the said policy
2.	WhatsApp	WhatsApp Terms of Service mentions illegal and obscene conduct; however, it does not specify child pornography or CSAM. A contact or group can be reported in its entirety, and a particular piece of content cannot be selected.

Sr. No	Service	Can CSAM be reported?
3.	Viber	Viber prohibits content that seeks to exploit or harm children by exposing them to inappropriate content.
4.	iMessage	Apple does not have any specific reporting feature for CSAM, though it does have a feature for reporting junk and spam
5.	Telegram	Yes, child abuse is one of the categories under which content on a channel can be reported. However, there is no reporting feature to report individual user accounts.
6.	Twitter	Report a Twitter account distributing or promoting child sexual exploitation, through their child sexual exploitation form by providing the username and links and links to all relevant Tweets.
7.	Instagram	CSAM can be reported using the built-in reporting options in the app.
8.	Snapchat	To report harassment, bullying, or any other safety concern press and hold the offensive story or a snap someone sent you and tap 'Report Snap' or 'Report' respectively. For more details on the process for reporting a safety concern on Snapchat visit the site: https://snap.com/en-US/safety/safety-reporting

J. Sexually abusive crimes against women

Description of the crimes:

Over the years, women across the globe have been subjected to various crimes. Violence and crime against women still remain to be one of the most widespread human rights violations in the world. With the growth in technology and a significant increase in the number of internet users, cases of cyber-crimes have also shot up.

1. **Pornography -** It is one of the most common forms of crime against women, pornography essentially involves morphing a woman's picture, thereby creating a simulated and sexually explicit image of a woman for illicit purpose. Or it is the circulation and depiction of women in sexual situations by the perpetrators.
2. **Cybersex Trafficking -** It is a form of modern slavery wherein the offender sexually abuses or exploits the victim, and broadcast such act via live streaming, webcams or other electronic devices. It is different from other sex crimes in the sense that the victim is brought to "cyber dens" having a pre-installed camera for the purpose of broadcasting the coerced sex tapes of women.
3. **Revenge Porn -** It is an act of sharing or transmitting the sexually explicit images or videos of a woman via electronic form without their knowledge or consent. The offender is usually a former partner of the victim who have had shared an intimate relationship with the victim, engages in such an act to harass, embarrass or take revenge from the victim.
4. **Indecent Representation -** Section 2(c) of the Indecent Representation Act, 1986 clearly defines the indecent representation of women as an act of depicting a woman's figure or body that results in corrupting the public morality of a woman.
5. **Sextortion -** A heinous act of extorting money or sexual favours from a woman by threatening to leak sensitive information on the web. It is a type of online abuse of women, wherein the perpetrator approaches a woman online via direct messaging apps, and manipulates her into sharing her intimate images or videos.
6. **Online Trafficking -** The internet has transformed the ways of human trafficking with perpetrators now making use of online platforms to target the vulnerable community i.e. women and children. Trafficking is a global issue which involves illegal buying, selling and abusing of humans in exchange of money. Victims are sent to far-off places and then physically and sexually exploited.

A list of few provisions that safeguards the interest of women against such crimes include:

1. **Indian Penal Code (IPC), 1860 -** Until the 2013 Criminal Amendment Act, there were no special provisions dealing with the cybercrime against women. Section 354A to Section 354D were added in 2013 to safeguards women's right in cyberspace.

a. **Sections 354A -** This provision clearly states that any man who demands sexual favours from a women or shows pornography against her will, shall be liable to punishment which may extend up to 3 years' imprisonment along with fine.

b. **Section 354C-** Deals with the definition of voyeurism and its punishment which may extend up to 3 years along with fine for first conviction and up to 7 years for subsequent convictions. Voyeurism is an act of watching, capturing or distributing images of a woman engaged in private act against her will or knowledge.

c. **Section 354D -** Deals with online stalking of a woman

d. **Sections 503, 506 and 507 -** These sections deal with the definition and punishment for criminal intimidation, i.e. an act of threating to cause an injury to person's reputation or property. Section 507 includes the possibility of criminal intimidation through anonymous communication. Mostly anonymous communication is done via online devices.

e. **Sections 500 to 502**: Deals with the provisions of defamation either orally or via written communication. Section 501 deals with printing defamatory content which would tarnish the image of the other person

2. **Information Technology (IT) Act, 2000 -** This law includes several provisions dealing with cybercrimes against individuals.

a. **Section 66C -** Identifies online identity theft as a punishable offence with imprisonment up to 3 years along with a fine of maximum one lakh rupees. Identity theft as defined in the section is making use of electronic signature, password, etc. with a dishonest or fraudulent intention

b. **Section 66D-** Deals with provision of cheating by personation using an electronic device

c. **Section 66E-** Prescribes punishment for capturing, publishing or transmitting images of a private area of a person including female breast, without her consent

d. **Section 67A-** Prescribes punishment for publishing or transmitting sexually explicit content in electronic form

3. **The Indecent Representation of Women (Prohibition) Act, 1986 -** It is a concise act enacted with an aim to prohibit the indecent representation of women in any manner or form. In order to expand the scope of existing law, an Indecent Representation Bill was passed in 2012 to include information and communication technology. This bill was later withdrawn in July 2021.

Modus operandi of the criminal in this crime

1. **Pornography:**
   a. **Case 1**: The perpetrator downloads the victims' pictures or is able to acquire their pictures from various sources and then uses these to morph false images in certain compromising positions to blackmail the victim or get other favours.
   b. **Case 2:** The perpetrator makes video calls on social media platforms and as soon as the victim picks up the call, the mobile screen records and the criminal edits the videos and shows the victim in obscene positions. This is then used by them to call the victims asking for money.
   c. **Case 3**: The perpetrator has already recorded the victim and he/she ends up sharing the videos and images of the victim online without their consent.
2. **Cybersex Trafficking:** In this cybercrime the perpetrators usually create 'cybersex dens' which are equipped with webcams and good internet services. Victims are transported to such places, are forced to either listen to the consumers of the consumers or traffickers. It is a form of sexual slavery wherein they force these victims to perform sexual acts on themselves or other people, they are sometimes even raped by the traffickers. The victims are usually women or children who are poor and fall prey to such cybercrimes.
3. **Online Trafficking**
   a. **Kidnapping/Abduction**: Women, especially younger women are kidnapped or abducted and trafficked with the idea of forcing them into sexual slavery.
   b. **Buying and selling of women**: This is a very common practice in the rural part of the country wherein women are sold and bought for petty amounts. The parents of such women suffer severe economic crisis and the perpetrators utilize that to their advantage and buy women to sell them off for sexual slavery, bonded labor etc.

a minor, relevant provisions of POCSO Act are invoked during investigation.

4. Investigation Process

a. Once the complaint is received by the concerned officer, it is imperative for him to execute a pre-investigation assessment into the matter. Based on the information shared, the officer initiates an investigation to ascertain the nature and form of cybercrime, the severity of the crime committed against the women, extent of bodily invasion and harm inflicted and the legal provisions applicable to the case in hand.

b. Further, the officer examines the digital evidence provided by the victim and may also collect additional evidence required for investigation. Typically two ways to collect evidence -

I. **From the victim or complainant** - In case of sextortion or cyber bullying, the victim must provide screenshots of the objectionable chats or emails received from the accused that can be held as evidence before the competent court.

II. **From Service Providers or other stakeholders**: The investigating officer may call for details of the accused from third parties, as and when required. This includes server information or information of the traffickers accused of uploading objectionable content on web, personal details of the accused shared with the social media companies etc.

An investigation process also starts here if a complaint is received by the police officials handling the CCPWC [Cyber Crime Prevention against Women & Children] portal, which is established in every state in a nodal cyber police station. Central government has launched Cyber Crime Prevention against Women & Children (CCPWC) portal to strengthen women safety. The portal cybercrime.gov.in will receive complaints from the citizens on objectionable online content related to online Child Pornography (CP) / Child Sexual Abuse Material (CSAM) or sexually explicit content such as Rape / Gang Rape (CP / RGR) content. CCPWC portal will facilitate victims / complainants to report cyber-crime complaints online in either anonymous mode or 'report & track' mode.

From these nodal cyber police stations in every state, the complaint is then forwarded to the respective police station in the state jurisdiction for immediate action.

5. **Labelling and Documentation of Evidence:** After receiving all the evidence, the investigating officer must categories such

4. **Indecent Representation:** The victims are often portrayed indecently, their form or body or any part is represented in an indecent way, or seems derogatory to, or denigrating to women, or is likely to deprave, corrupt or injure the public morality or morals through advertisements, publications, writings, paintings, figures.

a. **Sextortion**: People committing these crimes usually operate in the following ways:
Case 1: When the victim and accused are unknown, the victim might receive a video call from an unknown number. Though this video conference the perpetrator captures the image of the victim which is further morphed to create objectionable content used for blackmailing.
Case 2: When the victim and the accused are known to each other, the trust between the parties leads to one of them sharing intimate pictures and videos with another which is then used to blackmail the victim.

b. **Revenge Porn:**
Case 1: The perpetrator records the women without her consent and shares her videos and pictures online without her permission.
Case 2: The perpetrator obtains the pictures and videos through legitimate means but shares them online without the consent of the women.

Investigation procedure to be followed

1. **Recording Information -** According to the first proviso to sub-Section 1 of Section 154 inserted by the amendment act of 2013 and subsequently amended by the amendment act of 2018 first information report in the cases of rape and sexual offences needs to be registered by a woman Police officer or any woman officer.
2. **Recording of statement -** The statement should be recorded by a woman officer and FIR should be issued immediately followed by further investigation.

3. **In case the victim is a member of SC/ST community, minor etc. -** If the victim is a member of SC/ST community, appropriate Sections of SC & ST (POA) Act (Scheduled Castes and Scheduled Tribes (Prevention of Atrocities) Act, 1989) should be applied during the investigation. Similarly, if victim is

evidence and secure them without causing any damage to it. Different evidence requires different level of care, and therefore, the officer must keep all the precautionary measures in mind while handling the evidence.

6. **Forensic Analysis and expert opinions:** Once the evidence are collected and segregated based on the circumstances of the case, the officer-in-charge must send the evidence for forensic analysis. The experts and scientists after carefully examining the evidence, prepares a comprehensive report that lays down the foundation of the case.
7. Meanwhile, the officer, based on his discretion or on orders received from the competent court, must ensure that objectionable content is taken down from the internet after the complaint has been received.
8. Further, in case of cross-border crimes, the provisions of Mutual Legal Assistance Treaties are applied.

Example of certain judgements / case laws or real scenarios

1. X v. Union of India, (2021) 2 HCC (Del) 16

It is a 2021 judgement given by the Hon'ble Delhi High Court bench dealing with the guidelines to remove objectionable images of a woman from the internet.

In this case, the petitioner asserted that her images were picked up from her social media accounts without her consent or knowledge and later shared on an explicit site. The petitioner further asserted that though the images were unobjectionable but the mere fact that such images were shared without her consent on a pornographic site leads to an offence under the IT Act.

Judgement: While hearing the facts of the case, it was noted that despite court's order, the images were not taken down from the internet and were further re-posted on other websites. Therefore, the court directed the police to disable access to all the URLs provided by the petitioner that contains the objectionable images and further, laid guidelines for the search engines such as Google, Bing etc. "to around the world de-record and de-reference" the distasteful content in question.

2. Avinash Bajaj v. State (NCT) of Delhi

In this case, the petitioner was the CEO and Managing Director of Bazee.com, a company facilitating the sale of property and thereby, earning commission. He was incriminated for broadcasting sexually explicit content on his website which is a criminal offence under Section 67 of the IT Act, 2000 and Section 292 of IPC, 1860. Though the obscene video shared on the site was taken down within few days, it was already purchased by a number of buyers and the company software failed to track down the offender who made the listing. The petitioner asserted, it was a case of direct buying and selling between the parties and he could not be made a party to it, hence allegations against him stand void.

Judgement: After hearing the facts and circumstances the case, the court held that the company was essentially an agent in the entire process and an integral part of the transaction made between the buyer and seller. It generated revenue in the form of commission and therefore, shall be held as a principle accused in the case. The court further held that prima-facie, the petitioner - Mr. Bajaj individually cannot be held guilty in the present case but shall be made liable in the capacity of him being a Managing Partner/CEO of the company.

I. INVESTIGATION GUIDELINES -
Shri. Brijesh Singh IPS

While law enforcement aims to maintain peace and order in society, a lot of effort goes into achieving the same.
Maintaining evidence integrity is one such challenge that law enforcement agencies have to deal with while investigating. Especially dealing with electronic evidence in cybercrime cases can be tedious as we need to consider time stamps and hashes. Even the slightest unintentional handling of the fragile evidence can render it unacceptable, for example even if one of the officers tries to log into a system in good faith to retrieve a picture or a video, if not done properly can compromise the value of the evidence. The best way to tackle this issue would be to train the personnel to be deployed at the site and push for strict adherence to the guidelines.

There has been a lot of discussion on the low conviction rates in India, but one must understand that conviction depends upon a lot of aspects - proper recording of the FIR, thorough investigation, search and seizure, and submission of a charge sheet, (a chronicle of all the material facts about the accused). All this requires professional investigation and there are several layers to the process in case an expert testimony is involved, regarding the admissibility of the evidence and much more. However, before taking this work to the court, senior police officers should ensure that investigation is supervised properly.
Japan has a conviction rate of approximately 99%. This is because they have a separate prosecution wing which does not allow them to charge sheet if the evidence is not up to the mark. Something similar can also be implemented in India wherein the filing of the charge sheet should be backed up with sufficient evidence so that it can stand the scrutiny of law.

Then, of course, the presentation of the evidence during trial is of utmost importance, and here comes the role of the prosecution. The prosecution should, to the best of their ability present the evidence in a comprehensible and convincing manner that is appreciated by the court. Lacunas here are the issues regarding quality of investigation and quality of prosecution. I think that in these kinds of technical matters, the judiciary should also be trained to understand how to appreciate scientific and technical evidence.

One more facet which is vital and is a game-changer is the cross-examination and standing for cross-examination. While policemen know how to collect evidence and produce it in a court of law, at times the case falls weak because of their inability to stand a cross-examination. A skillful cross-examination can destroy the best-collected witness by creating doubt in the minds of the court.

If the cross-examination fails and the evidence becomes doubtful, the case becomes weak like a house of cards. The standard of proof that we follow in criminal proceedings has been defined very well in the code of criminal procedure for the prosecution side. However, if the other party has to just create a small doubt, and if they are successful, then this whole edifice of evidence collapses. At all times getting fool-proof evidence that is presented appropriately and appreciated by the court and not assailed by a well-paid smart lawyer, becomes difficult and hence, one should look at acquittal cases with concern.

In fact, the police manual gives a very detailed procedure of scrutinizing all the acquittal cases. Supervisory officers would be failing in their duties if they do not supervise acquitted cases and find out what went wrong in the case, how could it have been corrected, and see to it that it does not happen again. This exercise, if followed by policemen, will go a long way in making sure conviction cases go smoothly.

Then there are challenges with the investigation as well such as anonymity, encryption, and the difficulty of getting data through MLATs. Getting data even from intermediaries can also be cumbersome and difficult. If you talk to officers everywhere: they would say that the response to the 91 CrPC notice is very scant even the responses to the newer notices under the IT act 79 (3)(b) of the Information Technology Act, 2000, read with Rule 3 are not appropriate. Indeed, it is also the responsibility of stakeholders and intermediaries to see that the platforms are not misused and they cannot go scot-free claiming themselves as just mere conduits because of their negligence. Thus, the responsibility should be put fair and square on the shoulders of these platforms and it should be made sure that they do not become breeding grounds of abuse and crime. We are all living in a globe of anonymity due to digitization and the internet. It is a grey space that allows people to commit crimes and then disappear. This kind of programmed lawlessness will just affect the fabric of society.

I believe even the 'big tech has a duty to care'. Especially towards the vulnerable sections of society such as children, senior citizens, and people who stand in a disadvantaged position. With increasing crimes against women and children the stakeholders and the big tech cannot turn a blind eye. They should make diligent efforts towards developing policies that protect the ones in need. Undoubtedly, company policies cannot be bigger than the sovereignty of a country.

Only through the adherence to the stringent provision and collective responsible efforts can we ameliorate this situation.

Shri. Brijesh Singh IPS

Additional Director General Maharashtra Police

Brijesh Singh headed Maharashtra Cyber, a unit looking after Cybersecurity of Government of Maharashtra. He led the implementation of MH Cyber Project, CERT MH and Predictive Policing units. He also implemented the unique project of Automated Multi-Modal Biometric Identification System (AMBIS), which was the first initiative in India, where IRIS, Face recognition, Finger and Palm prints were used for identification of criminals. Previously, he has implemented huge and successful projects like Crime and Criminal Tracking Network & System (CCTNS) project, other IT schemes for Policing. Presently he is also heading the CCTNS Task force developing big data solutions and analytics on crime data. He has penned and published the thriller "Quantum Siege" for Penguin books and “Dangerous Minds of India” which are very popular.

II. MLAT PROCESS OF REPORTING CASES OF CROSS BORDER JURISDICTION

MLATs and LETTERS ROGATORY

Mutual Legal Assistance Treaties (MLATs) and Letters Rogatory (letters of request/LR) are two tools through which law enforcement agencies can seek assistance from foreign law enforcement agencies and courts during criminal investigations.

S.105 of the Code of Criminal Procedure (CrPC) empowers the Indian government to enter into reciprocal arrangements with foreign governments to provide assistance for service of summons, warrants and judicial processes abroad.
To date, the Indian government has entered into MLATs with 39 countries. MLATs are diplomatic, mostly bilateral agreements entered into between states to exchange evidence and to serve summons during criminal investigations and prosecutions.

Letters Rogatory or letters of requests are issued by courts as per Section 166A of the Code of Criminal Procedure (CrPC) and are traditionally considered to have a broader reach as they can be enforced in the absence of a treaty, during criminal, civil and administrative proceedings and are available to private parties

Requests for user data that originate from an Indian investigative agency, either through MLATs or LRs are routed through the central authorities of the requesting and requested states. The central authorities designated for this purpose are Ministry of Home Affairs (MHA) in India and the Office of International Affairs (OIA) under the Department of Justice in U.S. With a view to streamline evidence gathering, the MHA issued guidelines for LEAs on serving summons/notices/judicial processes on persons residing abroad through MLATs and LRs. The only distinction being that LRs need to be issued by a court while MLAT requests can be made directly by LEAs.

Through Mutual Legal Assistance mechanism countries cooperate with each other to share data and information that can help in prevention, investigation of a crime. Hence, countries enter into Mutual Legal Assistance Treaties (MLATs) to facilitate international cooperation regarding cross border data sharing. These treaties are bilateral in nature.

After signing the MLAT, a Central Authority is designated by the parties for receiving and making requests regarding the criminal law matters. For example, the Ministry of Home Affairs or any such person designated by the Ministry of Home Affairs operates as the nodal authority or the Central Authority for India. For civil and commercial matters, the Ministry of Law & Justice takes the lead.

MLAT Procedure

In case an investigative agency wants to get evidence from outside, it needs to follow the below mentioned steps:

1. The agency must obtain valid summons, warrant, or other judicial process: Section 105 of CrPC outlines the extra-territorial application of summons, warrants or judicial processes issued in India in a manner laid by the Central Government. The Indian Government can enter into reciprocal arrangements with foreign governments under this section.
2. A covering letter from the Registrar accompanies these summons and are together submitted to the MHA.
3. If the relevant treaty has a provision that allows direct communication between the central authorities, then MHA can send the request directly to the central authority. If not, then the request goes through the diplomatic mission of India in that country.
4. The rest of the process is dependent on the laws of the relevant country.
5. Once the results of the requests are received, the same are communicated by the central authority in the requested state to the investigating agency through the same chain used for initiating the request.
6. The contents of the covering letter must encapsulate the facts of the case and the details of the offence committed. The details should be mentioned in a fashion that makes it easier to understand what evidence the investigating agency is looking for.
7. In cases where the request is made to the countries that do not have English as their official language, a certified translation of the letter must also be provided.
8. The narration of the facts must be framed with an understanding of the domestic legal process of the requested state.

The MLAT does not have a dual criminality requirement, instead requiring the subject of investigation to be a crime only in the requesting country. However, the law of the requested state is applicable in so far as the execution of the request is concerned. Courts in the requested state are expected to follow their domestic law while executing requests

under a MLAT and can deny the requests only if it is specifically prohibited under their law

Key statute pertaining to the extra-territorial jurisdiction with respect to cybercrimes: Information Technology Act, 2000

a. Section 1(2): The Act "shall extend to the whole of India and, save as otherwise provided in this Act, it applies also to any offence or contravention hereunder committed outside India by any person."
b. Section 75(1): "The provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality"
c. Section 75 (2): "Further this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India"

III. AN OVERVIEW OF JUVENILE JUSTICE ACT

The Juvenile Justice (Care and Protection of Children) Act, 2015 is an act which strengthens and amends the law relating to children who are alleged to be in conflict with the law and children who are in need of care and protection by meeting their basic needs through adequate care, protection, development, treatment along with social reintegration by adopting and implementing a child-friendly approach in disposal of cases in the finest interest of children and for their rehabilitation.

SALIENT FEATURES OF JUVENILE JUSTICE ACT, 2015

DIFFERENCE BETWEEN CHILDREN IN NEED OF CARE AND PROTECTION AND CHILDREN IN CONFLICT OF LAW.

The Juvenile Justice Act, 2015 deals with children in need of care and protection and children in conflict of law. “Children in conflict with the law and juvenile offenders” refer to children being alleged for committing a crime or who has been suspected of committing a crime. "Child in need of care and protection" refers to any child who is homeless or resides with someone who is not his guardian and has threatened, abused, or harassed the child or forced him to work as child labour. Additional categories like victims of armed conflict, civil commotion, or natural calamity are introduced under the term "child in need of care and protection". Under this act; segregation is made between children in need of care and protection and juveniles in conflict with the law.

Some categories, like a child found begging, children reside in brothels, and uncontrollable children are excluded from the act. Under this act, segregation is made between children in need of care and protection and juveniles in conflict with the law.

SEGREGATION OF CHILDREN IN CONFLICT OF LAW

Under the said act, children in conflict of law are distinguished into two classes

Class-1:

I. In case of petty and serious offences, children who are below 18 years of age

II. in case of heinous offences, children who are below 16 years of age

Class 1 may be tried by juvenile justice board constituted by state government under the said act.
Class 2 In case of heinous crime, children who have completed 16 years of age but are below 18.

Act gives permission to treat Class 2 children in conflict of law as adult. They must be kept in the safety place until the age of 21 and thereafter may be sent to an adult jail to complete remainder of sentence.

TYPES OF OFFENCES - Act categorised the offences committed by a juvenile in three types:

1. Petty Offences - It includes the offences which are punishable under Indian Penal Code or any other law with imprisonment upto three years.
2. Serious Offences - It includes the offences which are punishable under Indian Penal Code or any other law with imprisonment for the period between three to seven years.
3. Heinous Offences - It includes the offences which are punishable under Indian Penal Code or any other law with imprisonment for seven year and more.

RESTORATION OF CHILD

Act is focuses on restoration of child. Restoration of child means restore them to their parents, adopted parents and foster parents.

INTRODUCTION OF JUVENILE POLICE UNIT AND CHILD-FRIENDLY POLICE OFFICER

Act establishes the juvenile police unit and also made mandatory to appoint at least one police as a child-friendly police in each station. The Act further deals with the constitution and functioning of the Juvenile Justice Board, the Child Welfare Committee and Institutional Care and discusses its roles and responsibilities in detail.

PUNISHMENT FOR OFFENCES COMMITTED AGAINST CHILD

The act enumerates the new offences committed against a child and its punishment such as -

1. Sale and procurement of children for any purpose including illegal adoption, corporal punishment in child care institutions: imprisonment of five years.
2. Use of child by militant groups:
3. Offences against disabled children and,
4. Kidnapping and abduction of children.

The Juvenile Justice Act, 2015 is a comprehensive act that covers aspects related to children and juveniles.

Please note: In cases of cyber-crimes, the Juvenile Justice act is invoked when the offender is a minor. This chapter on JJ act is added into this guide for this limited purpose only.

IV. CODE OF CONDUCT FOR LEAs

A. FIR

1. The provisions of Sec 154 Cr.P.C should be followed while recording an FIR.
2. In cases of cybercrimes such as sextortion, cyberstalking etc. where the victim is a woman, the FIR should be recorded by a woman police officer or any woman officer.
3. FIR forms the foundation of an investigation; hence all the details should be documented properly with utmost care.
4. A copy of such information as recorded should be provided to the victim or the informant free of cost.
5. The authorities should try not to delay the registration of and FIR, but in case of a delay they should record the reason.
6. If the victim is not comfortable with English or Hindi, for the convenience of the victim the FIR should be recorded in the regional language.
7. Compulsory registration of FIR in case of cognizable offence under subsection (1) of section 154 of the Code of Criminal Procedure, 1973 (CrPC). The law also enables the police to register FIR or a "Zero FIR" (in case the crime is committed outside the jurisdiction of police station) in the event of receipt of information on commission of a cognizable offence, which includes cases of sexual assault on women.

B. Treatment of victim

1. The victim of such crime should be treated with honour and sensitivity.
2. Understand that the victim or the family are in shock, fear, anger and in trauma, therefore listen to their emotion and not react.
3. Give them realistic inputs estimation and not build on false hopes
4. Victim may be unwilling to take the discussion forward due to fear, guilt, ridicule or consequences, hence the comments from the law enforcers need to refrain from making any derogatory comments, remarks that are moralistic, hurtful or insulting.
5. Need to build confidence of the victim and gain trust in the system and understand that such situations happen due to our neediness, hence the need for implementing the learning from such experiences
6. In case of complainants being parents of minors, they need to be explained that the victim needs parental support, hence not giving

up on the victim is critical.

7. Parental counselling and victim counselling can be referred to the Responsible Netism centre
8. The officers talking and interacting with the victim should avoid any questions that are indecent or might trigger the victim leading to further victimization.
9. The identity of the victim should be protected and should not be revealed to the media, especially in cases where the victim is a minor.
10. While interacting with the media, speculations and declarations made without evidence could not just tamper the case but jeopardise the safety of the victim.

Where the victim is temporarily or permanently, mentally or physically disabled

If the person against whom an offence is alleged to have been committed or attempted, is temporarily or permanently, mentally or physically, disabled, such information shall be recorded, at the residence of the person seeking to report such offence or at a convenient place of such person's choice, in the presence of an interpreter or a special educator, as the case may be. The recording of such information shall be video graphed.

If victim is of different linguistic background - In this case the FIR/statement must be recorded. An interpreter for the victim with different linguistic background may be provided, during investigation, for recording of statement / FIR.

If victim is a minor -

1. Parents must be present, their consent is required while recording the statement of the victim or the FIR. In the absence of a parent, guardian a representative of NGO or Child Welfare committee should be present.
2. As per Section-24(2), POCSO Act I.O. shall wear plain clothes during interview/investigation.
3. It is the duty of the police officers to ensure that the victim does not come in contact with the accused in any manner in accordance with Section- 24(3) 36, POCSO Act r/w Section-273, Cr.P.C.)
4. A child cannot be detained in the police station at night as per the mandate of Section-24(4), POCSO Act
5. If the victim is a victim of incest in addition to being a minor, such child should be taken away from the custody of the suspected

investigating officer should get the victim medically examined within 24 hours from the time of receiving the information relating to the commission of such offence.

2. Where the victim is a woman, she should be examined by lady doctors or at least under their supervision.
3. The medical report should then be forwarded to the Magistrate by the I.O.
4. A Rape victim above 18 years of age can be examined only after obtaining her written consent and, if victim is below 18 years of age (as per the mandate of Section-27, POCSO Act) or temporarily / permanently mentally disabled, she can be examined only after a written consent from her parents / guardians. In certain case such consent may be obtained through electronic medium.

G. Proof of age

In cases under POCSO Act the age of the victim is an important factor hence certain documents/procedure shall be relied upon (Section-34, POCSO Act read along with Juvenile Justice (Care and Protection of Children) Act, 2000.):

1. A date of birth certificate from the school, or matriculation or equivalent certificate from the concerned examination Board, if available; and in the absence thereof,
2. Birth certificate given by a corporation or a municipal authority or a Panchayat,
3. And only in the absence of 1 and 2 above, age shall be determined by an ossification test or any other medically proven and improved age determination test

H. Collection of evidence

1. All kinds of evidence should be safeguarded and collected properly for analysis. Mobiles, laptops, screenshot of chats, websites, videos etc all form an important part of the investigation process related to cyber rimes.

I. Preservation of evidence

- **Packaging**

  Anti-static bag should be used to store the electronic media evidence seized, especially when electrostatic discharge can cause damage to the media. This should be covered in a layer of bubble wrap to prevent physical damage and scratches. Finally, loads of tape should be used to seal the packet.

accused and should be taken to a child protection shelter and a report notifying the Child Welfare Officer should be sent within 24 hours

6. The victim should be given a place to stay in a shelter home in case the child does not have a place.

C. Investigation - Investigating Officer

1. In cases where the victim is a woman, efforts should be made to have a woman officer head the investigation.
2. Even while making the investigation team, it should be ensured that at least one of the officers in the team is a woman.

D. Recording of statement of victim under section 161 Cr.P.C.

1. The victims mental and emotional state should be observed carefully while talking
2. The incident should be recorded in detail in the language of the victim.
3. The IO should visit the home of the victim in plain clothes and ensure that they are sensitive about the condition of the victim while trying to get information from them. The victim should not be called to the police station.
4. Under POCSO Act, parents/guardians of the victim must be present all the time of recording of statements.
5. In cases where the victim is not from the country, the IO after taking due permission from immediate superior officer examine such witness through video conferencing and other electronic means. This is only in cases where the IO feels that the examination of witness is pertinent to the investigation proves and such witness cannot be examined without an amount of delay, expense or inconvenience which, under the circumstances of case, would be unreasonable.

E. Videography of statement

If the person making the statement is temporarily or permanently, mentally or physically disabled, or the victim is of different linguistic background, the statement made by a person with the assistance of an interpreter or a special educator, may be video graphed.

F. Medical examination of victim

1. In cases where the victim has been raped as an outcome of any of the cybercrimes or example, cybersex trafficking the

- **Labelling**
  Proper labelling of evidence is a crucial step for easy identification of the evidence even in future cases. All the details should be carefully mentioned on a tag for the packet of evidence and these details should also be recorded in relevant diaries like daily diary and case diary to maintain a proper schedule of evidences for different cases.
- **Transportation**
  The evidence should be protected from physical damage and drastic temperature changes. And a skilled person capable of taking care of such sensitive evidence should carry these packets for transportation.

J. Proof of electronic evidence

Electronic evidence would need to be proven as under Sec. 65-B of the Indian Evidence Act.

K. Scientific and chemical examination of exhibits

1. Evidence collected should be preserved properly and sent for analysis with the forensics team,
2. DNA analysis should be done in cases where required.
3. Chain of custody of exhibits should be adhered to.

L. Arrest - The authorities should make an effort to arrest the suspect promptly. Investigation of the suspect should be carried out carefully.

M. Witness Protection - It is the duty of the police officials to ensure that the victim, her family, etc. are not threatened and are safe.

N. Submission of Charge sheet

1. All offences against women shall be promptly investigated and charge sheets should be filed in the court of law within sixty days as per section 173 Cr.P.C.
2. At no point of time, the quality of investigation should be compromised. Orders for chargesheet should be issued after due scrutiny to ensure that the investigation and subsequent prosecution does not suffer from any lacuna or omission.
3. The I.O./SHO shall ensure that all material documents such as medical examination reports, FSL reports, Test Identification, relevant daily diary are included with the charge sheet
4. An advance copy of the charge sheet should be supplied to the

prosecutor.

5. A copy of the chargesheet should be supplied to the victim or informant, without any cost.

O. Rehabilitation of the Victim

1. Some of these victims need rehabilitation especially women and children who have bene victim of online sex trafficking and other such serious offenses. Therefore, it is the duty of the police authorities to fnid the right shelter home for such victims.
2. The victims should be provided with counselling to help them cope with the emotional and physical trauma.

V. MEASURES TAKEN BY THE GOVERNMENT FOR THE LEAs

To ensure safety and security of women and young children on online platforms the Ministry of Women and Child Development in collaboration with Ministry of Home Affairs (MHA), Ministry of Electronics and Information Technology (MEITY) and Ministry of Education are taking measures to strengthen the mechanism to deal with cybercrimes. Some of the initiatives taken by the Central Government include:

1. Tweaking school curriculum

Ministry of Education has been requested to issue necessary directions to Central Board of Secondary Education (CBSE) for incorporating pertinent information in the school curriculum of children to educate them about cyber safety.

2. Section 67B of the Information Technology (IT) Act

Section 67B of the Information Technology (IT) Act, 2000 provides stringent punishment for publishing, transmitting or viewing Child sexual abuse material online.

3. Section 66D of the IT Act, 2000

The Information Technology (IT) Act, 2000 also has a provision to deal with fake calls and messages made through internet as medium. Section 66D of the IT Act, 2000 provides for punishment of imprisonment up to three years and fine for cheating by personation.

4. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules

a)The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 puts the onus of the safety on social media platforms for its users. In accordance with these rules, the intermediaries have been directed to adopt a robust grievance redressal mechanism including time-bound disposal of grievances.

b)The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 also require Significant Social Media Intermediary (SSMI) to endeavour to deploy technology-based measures to proactively identify child sexual abuse material

5. Duty of intermediaries

a)The Intermediaries are required to convey certain terms and conditions to its users to not host, display, upload, modify, publish, transmit, update or share any information that is harmful, defamatory, obscene, invasive of another person's privacy, harm minors in any way or are otherwise unlawful.

a) Intermediaries are also expected to remove any information violative of any law in India as and when brought to their knowledge either through a court order or through a notice by an appropriate government or its authorised agency.

6.Indian Cyber Crime Coordination Centre (I4C)

a) Indian Cyber Crime Coordination Centre (I4C) has been established by the Government under the aegis of Ministry of Home Affairs. This Centre helps to provide for a framework and ecosystem for LEAs to deal with the cybercrimes in a comprehensive and coordinated manner.

a)NCRB has established a National Cybercrime Training Centre (NCTC) under Indian Cyber Crime Coordination Centre (I4C). A Massive Open Online courses (MOOC) platform, namely CyTrain has also been developed to provide professional e-learning courses for all cybercrime investigation to all LEAs, prosecutors, judges and other stake holders. To access free online training courses the stakeholders can to register on CyTrain Portal **http://cytrain.ncrb.gov.in** to complete them at their own pace and get an e-Certificate after successful completion of the course.

7. Cyber Crime Prevention against Women and Children (CCPWC)

'Cyber Crime Prevention against Women and Children (CCPWC)' has been implemented under the Nirbhaya Fund. This project is being used as a platform to spread awareness about cybercrimes, issuance of alerts/ advisories, capacity building/ training of law enforcement personnel/ prosecutors/ judicial officers, improving cyber forensic facilities etc.

8. www.cybercrime.gov.in

A National Cyber Crime Reporting Portal **www.cybercrime.gov.in** has been launched to enable public to report incidents of cybercrimes, with a special focus on cyber-crimes against women and children

9. Helpline number

A toll free number 1930 (earlier 155260) has been operationalized. This number provides assistance in lodging online cyber complaints. Incidents reported on the National Cyber Crime Reporting Portal are routed automatically to the respective States based on information furnished by the applicant in the incident report for further handling.

10. Training on cybercrime awareness and investigations

More than 19,600 LEA personnel, judicial officers and prosecutors have been provided training on cybercrime awareness, investigation, forensics etc. under Cyber Crime Prevention against Women and Children Scheme. Special curriculum has been prepared for LEA personnel, prosecutors and judicial officers to educate them on ways

of better handling an investigation.

11. **Twitter handle @cyberDost**
    MHA has taken various steps to spread awareness on cybercrime such as dissemination of messages on cybercrime through Twitter handle @cyberDost, radio campaign, publishing of Handbook for Adolescents / Students.
12. **Deploying effective security policies**
    On 18.08.2017, several guidelines were issued by the Central Board of Secondary Education (CBSE) to the schools on the safe and secure use of Internet. This circular directs schools to install effective firewalls, filtering and monitoring software mechanisms in all the computers and deploy effective security policies.
13. **Awareness material available online**
    Information Security Education & Awareness (ISEA) is a program being run by MEITY to create awareness among users highlighting the importance of digital safety while using Internet **https://www.infosecawareness.in** has all the relevant awareness material.
14. **Blocking access to child pornography webpages**
    An order has been issued by the Government to concerned Internet Service Providers (ISPs) asking them to implement Internet Watch Foundation (IWF), UK or Project Arachnid, Canada list of CSAM websites/ webpages on a dynamic basis and block access to such child pornography webpages/ websites.
15. **Spreading awareness**
    All Internet Service Providers (ISPs) have been requested to make proper arrangements to spread awareness among their subscribers about the use of parental control filters in the end-user machines through messages of email, invoices, SMS, website, etc.
16. **Tipline report**
    An MoU is signed between the NCRB, India and National Center for Missing and Exploited Children (NCMEC), USA regarding receiving of Tipline report on online child pornography and child sexual exploitation contents from NCMEC. The Tip lines, as received from NCMEC, are being shared with States/UTs online through Nation Cybercrime Reporting Portal for taking further action.

VI. HOW AND WHERE TO REPORT A CRIME?

The Ministry of Home Affairs, Government of India has developed a Cybercrime reporting portal under National Mission for the safety of women. The aim of the portal is to make the complaint process easier and convenient for the victims and complainants.

What kinds of complaints can be registered through this portal?

Complaints related to:

- Online Child Pornography (CP)
- Child Sexual Abuse Material (CSAM)
- Sexually explicit content such as Rape/Gang Rape (CP/RGR)

Reporting Other Cybercrimes: Through this option complaints regarding cybercrimes such as mobile crimes, online and social media crimes, online financial frauds, ransomware, hacking, cryptocurrency crimes and online cyber trafficking can also be registered.

Who will deal with these complaints?

Based on the information provided by the complainants the respective police authorities of States/ UTs will deal with such complaints.

Anonymous Reporting

as per the direction of Hon'ble Supreme Court under the matter of Suo Motu Writ Petition no.3/2015, the portal also has an option for anonymous reporting of CP/RGR content.

How to report a cybercrime?

For online reporting of cybercrime, visit the Cybercrime reporting portal: **www.cybercrime.gov.in**

The two options for filing a complaint on www.cybercrime.gov.in are:

a) Report Crime related to Women/ Child and
b) Report Other Cybercrimes.

In cases of "Reporting crimes related to Women/Child", two ways of registering your complaint:

1. **Report Anonymously:** Complaint's regarding online Child Pornography / Rape or Gang Rape (CP/RGR) content can be

registered anonymously. The person filing the compliant does not have to provide any personal information. But information related to the complaint should be accurate and complete to facilitate further necessary action.

2. Report and Track: Under this option, fields marked with a red asterisk (*) are mandatory. The police need accurate and complete information related to the complaint in order to take further actions. Therefore, one should provide required information such as your name, phone number, email address, details of the complaint and necessary information supporting the complaint.

In case of other cybercrimes:

- Choose the “Report Other Cybercrimes” section.
- Register yourself using your name and valid Indian mobile number
- You will receive a One Time Password (OTP) on your mobile number.
- The OTP remains valid for 30 minutes only.
- Once you successfully register your mobile number on the portal, you will be able to report the complaint by selecting appropriate category and sub- category.

The fields marked with a red asterisk (*) under this section are mandatory. These details are required by the police authorities to take further actions therefore, should be complete and accurate.

Evidence needed to support the complaint

It is important to keep any evidence you may have related to your complaint. Evidence may include:

- Credit card receipt
- Bank statement
- Envelope (if received a letter or item through mail or courier)
- Brochure/Pamphlet
- Online money transfer receipt
- Copy of email
- URL of webpage
- Chat transcripts
- Suspect mobile number screenshot
- Videos
- Images

List of other reporting portals

1. If you receive any fraudulent sms, e-mails, phone calls asking for banking or sensitive personal information, please report immediately to Maharashtra Cyber's portal **www.reportphishing.in**
2. To register a cybercrime online, report it on the website: **https://cybercrime.gov.in**
3. To block your mobile IMEI number in case your mobile is stolen or lost and is at the risk of losing data, photos and confidential data from the phone, then immediately, please report it to **www.ceir.gov.in** To see your 15 digit IMEI number dial *#06# and save it with you
4. Toll Free Helpline Number 1930 for cybercrime complaints for women and children
5. The Ministry of Women and Child Development has launched a distinct helpline complaint **mwed@gov.in** to report cyber bullying, online harassment, and cyber defamation, particularly against women and children.
6. For registering complaints against malicious and pornographic texts, visit:
   https://web.umang.gov.in/landing/department/cybercrime - reporting - portal.html
7. Local police help can be availed by dialling 100 and for women and children its 103 in Maharashtra. National Women helpline number is 181.
8. For reporting a complaint on online Child Pornography (CP)/ Child Sexual Abuse Material (CSAM) or sexually explicit content such as Rape/Gang Rape (CP/RGR) content either anonymously (ie. without revealing your identity) or by revealing your identity.
   Report on: **https://cybercrime.gov.in**
9. To report Cyber Financial Fraud, call 1930 (Earlier 155260). The service is available 24*7

Source Courtesy:

1. DSCI Cybercrime investigation manual: Data Security Council of India
2. Protection of Children from Sexual Offences Act, 2012
3. Indian Penal Code, 1860
4. The Code of Criminal Procedure, 1973
5. Information Technology Act, 2000
6. SCC
7. Manupatra
8. Crimes Against Women: Investigation Techniques (Ms. Shikha Goel and Dr. Vasanth Kumar Gonu)
9. Investigative workflow Manual On Cyber Harassment Cases by Bureau of Police Research & Development
10. Standard operating procedure for collection of digital evidences and cyber investigation techniques by S.K. Dubey & H.S. Papola
11. Standard Operating Procedure (SOP) for Investigation and Prosecution of Rape against Women by BPR&D
12. Pib.gov.in
13. Kerala Police: Standard Operating Procedure (Digital Evidence Related to Crimes Against Women and Children)

This guide has been Compiled by:

Adv. Dhrumi Gada

Adv. Dhrumi Gada, has been the Chief Ministers Fellow inducted in the 2019 batch, and has worked with the Maharashtra Cyber department. She is currently pursuing her PhD from Symbiosis law School in data protection laws. She is a double gold medalist in her LLM from Mumbai University and an LLB from Government Law College. She worked with India Child Protection Fund on curbing online child sexual abuse in the State of Maharashtra in collaboration with Maharashtra Cyber and the International Centre for Missing and Exploited Children (ICMEC). She assisted in the Operation Blackface and was a major contributor in the awareness drives for the CyberSafe women's campaign. She is a registered resource person with the Ministry of Human Resources and Development." She has also worked with KPMG as a forensic investigator and has been visiting faculty lecturer at Government Law College, Mumbai, MIT Law college Pune, Pravin Gandhi College of Law, Mumbai and Advani Law College, Bandra and has been associated with Responsible Netism as an honorary Consultant.

NOTES

Cyber Wellness Helpline

7353 10 7353

www.responsiblenetism.org

RESPONSIBLE™
NETISM