



RAJASTHAN STATE LEGAL SERVICES AUTHORITY

CYBER CRIME AGAINST CHILDREN

&

AWARENESS

May, 2020

NISHEETH DIXIT

ADVOCATE



- **What is Cybercrime?**
- **Cyber Crime - “Combination of Crime and Computer Resource”.**
- What is Computer resource?
- Cyber crimes are committed while in the cyber space. They include crime like, cyber terrorism, intellectual property infringement, hacking, industrial espionage, on-line child exploitation, internet usage policy abuses ,illegal purchase of goods, sexual assault, internet fraud, software piracy, viruses, impersonation and many more.



Categories OF Cybercrimes :

- crimes where a computer is the target of the crime,
- crimes where a computer is a tool of the crime, and
- crimes where a computer is incidental to the commission of the crime.





TRUST, BUT VERIFY



- Depending upon the victim of cyber crime, it may be broadly classified under three heads:
 - (i) Against individuals;
 - (ii) Against Organizations; and
 - (iii) Against Society at large.



- **Internet crime using the Internet infrastructure-**
- Hacking
- Theft of information/passwords
- Theft of credit card numbers
- launch of malicious programs
- Espionage
- Spamming



Web based crimes-

- A-Website related crimes-
 - (i) Cheating and frauds
 - (ii) Insurance frauds
 - (iii) Gambling
 - (iv) Distribution of pornography
 - (v) Sale of pirated software
- **Crime through E-mail**
 - (i) Threats
 - (ii) Extortion
 - (lii) defamation
 - (iv) Launching of malicious software

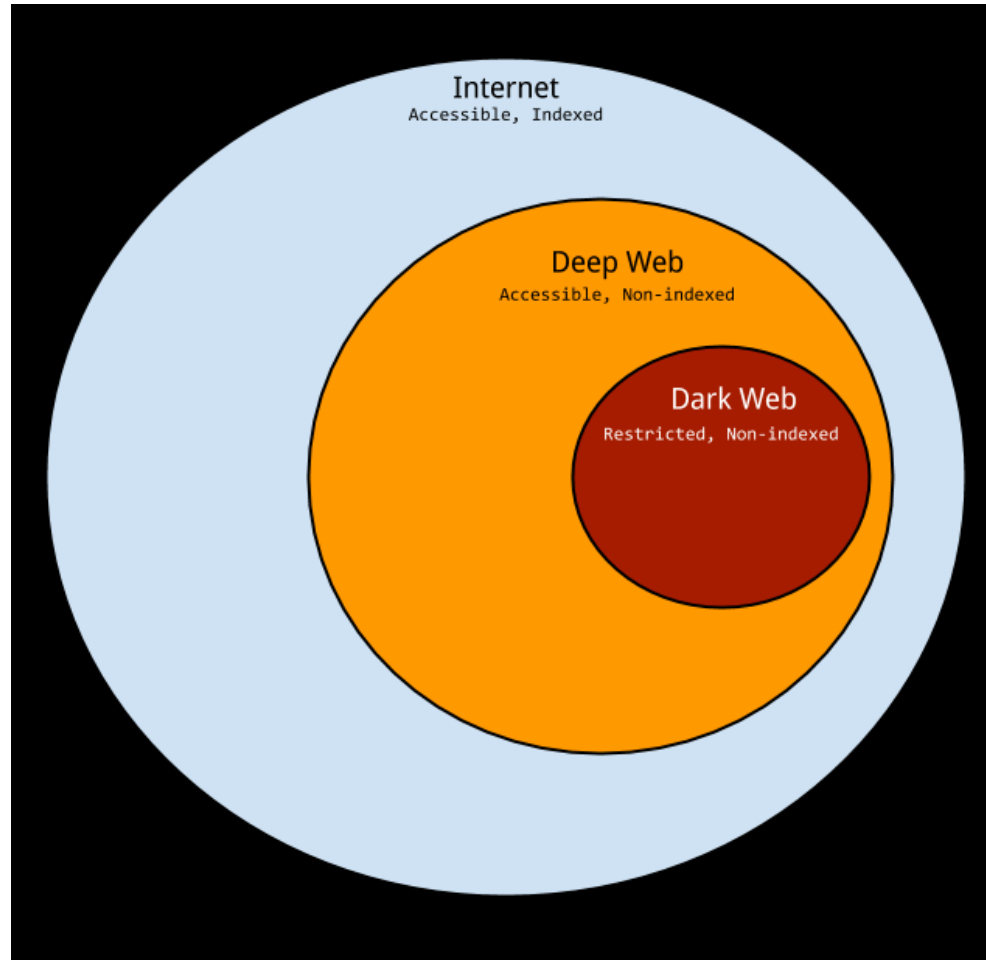


- **Use net related crimes-**
 - (i) Discussion on methods of hacking
 - (ii) Sale of stolen credit card numbers
 - (iii) Sale of stolen data
- **Internet relay chat crimes**
 - (i) Cyber stalking
 - (ii) Fraudsters use chat rooms for developing relations with unsuspecting victims
 - (iii) Criminals use it for meeting conspirators
 - (iv) Hackers use it for discussing their expertise of showing the techniques
 - (v) Pedophiles use chat rooms to allure small children



Reasons of Cyber Crime







- **Cyber Crime Statistics-India**

- As per the data maintained by National Crime Records Bureau (NCRB), India a total of 9622, 11592, 12,317, 21,796 and 27248 cyber crime cases were registered during the Penal Code and Special & Local Laws involving computer as years 2014, 2015, 2016, 2017 and 2018 respectively. This includes cases registered under the Information Technology (IT) Act, 2000.



CYBER CRIME DATA-NCRB

State	2016/2017/2018
Odisha	317/824/843
Andhra Pradesh	616/931/1207
Uttar Pradesh	2639/4971/6280
Rajasthan	941/1304/1104
Gujarat	362/458/702
West Bengal	478/568/335
Sikkim	1/1/1
Chhattisgarh	90/171/139
Maharashtra	2380/3604/3511
Total India	12317/21796/27248



CRIME AGAINST CHILDREN





Cyber Bullying





- **Cyber Bullying:**
- **Sending tormenting post, harassing messages, threatening contents** to a **minor to cause mental harassment and depressive or suicidal state of mind** to the recipient of such messages.
- Youths that have experienced cyberbullying have engaged in self-harm, such as cutting, attempted suicide, and committed suicide.
- Children who engage in cyber bullying utilize text messages, emails, websites, blogs, polls, social media posts, instant messages, and gaming and virtual reality sites, to humiliate, denigrate, harass, insult, spread false information, gossip or rumours, threaten, and/or isolate, exclude and marginalize other children.
- **Preventions:** Share those messages and posts with your Parents or teachers who are matured enough to understand the gravity of the matter and act accordingly. Do not keep on facing or enduring these troubles.



- **Roasting**
- Adults and children have willingly posted images and/or videos of themselves on social media and video sharing platforms, like Instagram, Twitter, YouTube, and Vine with the hashtag (#roastme), inviting others to post insults about them.
- In some instances, the goals of the "roast" is to bombard the victims with abusive online comments, images, videos, among other things, until the victims cannot take any more abuse and engage in the desired reaction (e.g., crying, self-harm, etc.) of those who roasted them.



- **Online Sexual Harassment**-Unwelcome sexual advances, request or demand for sexual favour, and other verbal or physical conduct of a sexual nature. “Sexual harassment” refers not only to sexual conduct with the explicit intention to violate the dignity of another person (i.e. purpose) but also to conduct of a sexual nature that a person experiences as offensive or intimidating.
- **Sexting**- Self-production and posting of intimate pictures, sexually explicit conversations, posting / sharing of intimate pictures.
- It is a type of "self-generated sexually explicit material" includes "consensual image taking and sharing, as well as consensual taking and non-consensual sharing of images (and sometimes even non-consensual taking and non-consensual sharing)". It is the most common type of self-generated sexually explicit material involving children



- **IDENTITY THEFT**

- This involves pretending to be someone else in order to steal money or get other benefits .The identity of another individual is impersonated in order to commit credit card fraud, create false profiles at networking sites and operate false e-mails. Identities.

- **WEBSITE DEFAACEMENT**

- This is usually carried out by the substitution of the homepage of a site by a system cracker that breaks into a web server and alters the hosted website creating one of its own. The hacker usually replaces the site matters with his own message or completely destroy the sites.



- **PHOTO EDITING APPS**

- **These apps that you use to beautify yourself are also known to retain your original copy of the photo you have uploaded and even the copy of the edited version is saved on their servers. You can only wonder what next would they do with the copy of your photos!**
- **Preventions:** Use reputed apps that you should be downloading from secured App stores. The fake photo editors may cause you harm and edit your lifestyle if used by them with criminal intent.



- **CLICK WRAP CONTRACTS**
- Parents-Children #
- **‘I accept’, ‘I agree’:** It is easy to accept the terms and **conditions** before downloading that app or software or game or e-book or music or video that you want it on your digital devices. But before that, understand at what cost are you giving permissions!
- **Preventions:** ‘Look before you Leap’ and so ‘Read before you Tread’ just before hitting on the ‘I accept’ or ‘I agree’ tab.



- **MOBILE RECHARGE SHOP**
- A Mobile Recharge Shop is a place where scamsters can gain access to your cellphone number because you have provided it to the recharge vendor.
- This number is then misused to call or text you and exploit your ignorance or even emotionally manipulate you.
- **KEYLOGGER**
- It is a malicious program that may be installed in the victim's computer for recording computer user keystrokes to steal passwords and other sensitive information. With Keylogger a scamster will be able to collect login details and other matter saved in the computer and have them mailed to a designated email address.



- **CYBER STALKING**
- Cyber stalking is the use of the Internet or other electronic means to stalk or harass another by misusing information uploaded on social networking sites.
- *Stalkerware*, a form of spyware, can run on a victim's computer, Smartphone or other Internet-enabled digital device and collect and relay all of the user's actions on these devices, from emails and text messages sent and received, to photographs taken and keystrokes). Some commercial software enables perpetrators who use this malware on smartphones to remotely switch on cameras and microphones, track the location of users and app usage, and intercept calls.
- **CALL SPOOFING**
- Call spoofing happens through apps that enable a person with criminal intent to change one's number and voice to impersonate another to defraud the receiver.



- **CAMERA HACKING**
- Camera hacking happens when photographs of a person are taken without consent, through malware that got downloaded with an attachment.
- Phones with no camera guard can be exploited for such criminal activities.
- **Live streaming of child sexual abuse**
- Live streaming of child sexual abuse involves the real-time broadcasting of child sexual abuse to viewers in remote locations

- **VOYEURISM**
- **Privacy breach is biggest concern with advent of pin hole cameras and latest spy cams that can be hidden and are not easily detectable. Could be hidden in shopping malls, changing rooms, washrooms, hospitals and diagnostic centers, and also in offices and washrooms located in private offices.**



- **PROFILE HACKING**
- Profile Hacking happens when your email or social networking site is accessed by a probable stalker who then compromises it.

- **PICTURE MORPHING**
- Morphing the face of a person to the body of another and publishing it to blackmail or otherwise intimidate the person is one of the ways by which people who upload photos on social networking sites can be exploited.



- **ONLINE GAMES**
- Girls who are vulnerable to loneliness, low self esteem and clinical depression can fall prey to dangerous online games that may become addictive and further harm them. Some like the notorious blue whale challenge even end in the victim ending her life. This is a personal as well as social challenge for the others around.
- **DATING WEBSITE**
- Females can be emotionally manipulated by smooth talkers on dating sites. Any private pictures or texts that they send across to probable dating companions on such sites are fair game for unscrupulous persons who can then blackmail them.



- **Cyber Defamation** -Using words or images or signals online to lower the reputation or prestige of the target.
- **Cyber Harassment** -Messaging abusive or other objectionable content to the target child or creating fake profiles in social media with the intention of targeting him or her.



- **Cyber Intimidation**-Communicating direct or implied threats through emails or messages in social media to inspire fear in the target child.
- **Cyber Grooming**-Preparing a child, significant adults and the environment for sexual abuse and exploitation or ideological manipulation. (The new Terminology Guidelines define grooming as "the process of establishing/building a relationship with a child either in person or through the use of the Internet or other digital technologies to facilitate either online or offline sexual contact with that person".)



- **Cyber Extremism-** Ideological indoctrination and recruitment, threats of extreme violence.
- **Social Exclusion-**Using online platforms to message the target child that he or she is not included with the peer group and its social activities.
- **Habit formation and online enticement to illegal behaviours-** Access to alcohol, cheating, plagiarism, gambling, drug trafficking, sexting and self-exposure.



- **SOCIAL TROLLING**
- Social Trolling is posting inflammatory messages or visuals about a person or organisation in an online community with the express purpose of causing humiliation or nuisance to the object of trolling.
- **CYBER TRAFFICKING**
- Cyber trafficking should essentially be understood as human trafficking that is committed with the help of computer networks.



CHILD PORNOGRAPHY

- Any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or representation of the sexual parts of a child, the dominant characteristics of which is depiction for a sexual purpose.”
- In recent years child pornography has increased due to the easy access of the internet, & easily available videos on the internet. Child pornography is the most heinous crime which occurs and has led to various other crimes such as sex tourism, sexual abuse of the child etc.



- **Child sexual abuse material(CASM)-** Sexually explicit representation of children. (The new Terminology Guidelines define this as material depicting acts of sexual abuse and/or focusing on the genitalia of the child.)



- *How do they Operate*
- Pedophiles use false identity to trap the children/teenagers.
- Pedophiles contact children/teens in various chat rooms which are used by children/teen to interact with other children/teen.
- Extract personal information from the child/teen by winning his confidence.
- Gets the e-mail address of the child/teen and starts making contacts on the victims e-mail address as well.
- Starts sending pornographic images/text to the victim including child pornographic images in order to help child/teen shed his inhibitions so that a feeling is created in the mind of the victim that what is being fed to him is normal and that everybody does it.
- At the end of it, the pedophile set up a meeting with the child/teen out of the house and then drag him into the net to further sexually assault him or to use him as a sex object.



- ***The role of internet in promoting child pornography***
- The Internet has escalated the problem of child pornography by increasing the amount of material available, the efficiency of its distribution, and the ease of its accessibility permits access to vast quantities of pornographic images from around the world makes pornography instantly available at any time or place allows pornography to be accessed (apparently) anonymously and privately facilitates direct communication and image sharing among users delivers pornography relatively inexpensively provides images that are of high digital quality, do not deteriorate, and can be conveniently stored provides for a variety of formats (pictures, videos, sound), as well as the potential for real-time and interactive experiences permits access to digital images that have been modified to create composite or virtual images (morphing)



- **THE IT ACT**

- To order the blocking of these sites, the DoT relied on Section 79(3)(b) of the IT Act. Section 79 lays down conditions under which ISPs or intermediaries are exempt from culpability for offensive content uploaded by a third party. It obligates the intermediaries to exercise “due diligence”, and to act on the orders of the court or the government and its agencies to qualify for immunity.
- Section 79(3) (b) states that intermediaries would not be entitled to exemption from liability if they failed to “expeditiously” remove or disable access to objectionable material “upon receiving actual knowledge, or on being notified by the government or its agency that any information... residing in or connected to a computer resource controlled by the intermediary” was being used to commit unlawful acts. In addition, under the Information Technology (Intermediary Guidelines) Rules, 2011, intermediaries must inform “users of computer resource not to host, display, upload, modify, publish, transmit, update or share any information that is... grossly harmful, harassing, blasphemous, defamatory, obscene, pornographic, pedophilic, libelous, invasive of another’s privacy, hateful, or racially, ethnically objectionable...”, etc., and “harm[s] minors in any way



- **S. 66C. Punishment for identity theft.**—Whoever, **fraudulently or dishonestly** make use of the **electronic signature, password or any other unique identification feature of any other person**, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.
- **Classification of offence**-Cognizable, Bailable, Triable by Magistrate of First Class.

Key Points - **fraudulently or dishonestly** make use of the **electronic signature, password or any other unique identification feature of any other person**



- **67. Punishment for publishing or transmitting obscene material in electronic form.-**
- Whoever **publishes or transmits or causes to be published or transmitted** in the **electronic form**, any material which is **lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons** who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished **on first conviction** with imprisonment of either description for a term which **may extend to three years and with fine which may extend to five lakh rupees** and in the event of a **second or subsequent conviction** with imprisonment of either description for a term which **may extend to five years and also with fine which may extend to ten lakh rupees**.
- **Classification of offence**-Cognizable, Bailable, Triable by Magistrate of First Class.
- Key Points- lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons , to read, see or hear the matter
- This section has been framed along the same lines of sec 292 IPC.
- Bazeer.com case



- **67-A. Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form.-**
- Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to **five years** and with fine which may extend to ten lakh rupees and in the event of **second or subsequent conviction** with imprisonment of either description for a term which may extend to **seven years** and also with fine which may extend to ten lakh rupees.
- **Classification of offence**-Cognizable, Non Bailable, Triable by Magistrate of First Class
- Key Points- publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct.



67-B. Punishment for publishing or transmitting of material depicting children in sexually explicit act etc - in electronic form

Whoever,-

- (a) Publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct; or
- (b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or



- (c) **Cultivates, entices or induces children** to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or
- (d) **Facilitates** abusing children online; or
- (e) **Records in any electronic form own abuse or that of others pertaining to sexually explicit act with children,**

shall be punished on first conviction with imprisonment of either description for a term which may extend to **five years** and with a fine which may extend to ten lakh rupees and in the event of **second or subsequent** conviction with imprisonment of either description for a term which may extend to **seven** years and also with fine which may extend to ten lakh rupees:



- Provided that the provisions of section 67, section 67-A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form-
- (i) The publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper writing, drawing, painting, representation or figure is in the interest of science, literature, art or learning or other objects of general concern; or
- (ii) Which is kept or used for bonafide heritage or religious purposes.
- **Explanation:** For the purposes of this section, "children" means a person who has not completed the age of 18 years.
- **Classification of offence**-Cognizable, Non Bailable, Triable by Magistrate of First Class
- Key Points- publishing or transmitting of material depicting children in sexually explicit act



POCSO

- **POCSO Act 2012** -The Protection of Children from Sexual Offences Act, 2012 came into force on 14 November 2012.
- **Section 13. Use of child for pornographic purposes.**
- Whoever, uses a child in any form of media (including programme or advertisement telecast by television channels or internet or any other electronic form or printed form, whether or not such programme or advertisement is intended for personal use or for distribution), for the purposes of sexual gratification, which includes--
 - (a) representation of the sexual organs of a child;
 - (b) usage of a child engaged in real or simulated sexual acts (with or without penetration);
 - (c) the indecent or obscene representation of a child,shall be guilty of the offence of using a child for pornographic purposes.
Explanation.--For the purposes of this section, the expression "use a child" shall include involving a child through any medium like print, electronic, computer or any other technology for preparation, production, offering, transmitting, publishing, facilitation and distribution of the pornographic material.

• .



- **14. Punishment for using child for pornographic purposes.**
- (1) Whoever uses a child or children for pornographic purposes shall be punished with imprisonment for a term which shall not be less than five years and shall also be liable to fine, and in the event of second or subsequent conviction with imprisonment for a term which shall not be less than seven years and also be liable to fine.
- (2) Whoever using a child or children for pornographic purposes under sub-section (1), commits an offence referred to in section 3 or section 5 or section 7 or section 9 by directly participating in such pornographic acts, shall be punished for the said offences also under section 4, section 6, section 8 and section 10, respectively, in addition to the punishment provided in sub-section (1).“



THE PROTECTION OF CHILDREN FROM SEXUAL OFFENCES (AMENDMENT) ACT, 2019

- "15. (1) Any person, who stores or possesses pornographic material in any form involving a child, but fails to delete or destroy or report the same to the designated authority, as may be prescribed, with an intention to share or transmit child pornography, shall be liable to fine not less than five thousand rupees, and in the event of second or subsequent offence, with fine which shall not be less than ten thousand rupees.
- (2) Any person, **who stores or possesses pornographic material in any form involving a child for transmitting or propagating or displaying or distributing** in any manner at any time **except for the purpose of reporting**, as may be prescribed, or for use as evidence in court, shall be punished with imprisonment of either description which may extend to three years, or with fine, or with both.
- (3) Any person, **who stores or possesses pornographic material in any form involving a child for commercial purpose** shall be punished on the first conviction with imprisonment of either description which shall not be less than three years which may extend to five years, or with fine, or with both, and in the event of second or subsequent conviction, with imprisonment of either description which shall not be less than five years which may extend to seven years and shall also be liable to fine.
- Abetment to commit any of the above offences (Section 16)



- **Section 20. Obligation of media, studio and photographic facilities to report cases.**
- Any personnel of the media or hotel or lodge or hospital or club or studio or photographic facilities, by whatever name called, irrespective of the number of persons employed therein, shall, on coming across any material or object which is sexually exploitative of the child (including pornographic, sexually-related or making obscene representation of a child or children) through the use of any medium, shall provide such information to the Special Juvenile Police Unit, or to the local police, as the case may be.



- **Section 21. Punishment for failure to report or record a case.**
- (1) Any person, who fails to report the commission of an offence under sub-section (1) of section 19 or section 20 or who fails to record such offence under sub-section (2) of section 19 shall be punished with imprisonment of either description which may extend to six months or with fine or with both.
- (2) Any person, being in-charge of any company or an institution (by whatever name called) who fails to report the commission of an offence under sub-section (1) of section 19 in respect of a subordinate under his control, shall be punished with imprisonment for a term which may extend to one year and with fine.
- (3) The provisions of sub-section (1) shall not apply to a child under this Act.



- **Report if you find content related to of Child Pornography (CP)/Child Sexual Abuse Material (CSAM) or sexually explicit material**
- Any content related to of Child Pornography (CP)/ Child Sexual Abuse Material (CSAM) or sexually explicit material such as Rape/ Gang Rape (CP/RGR) content should be report to the concerned social media website
- If anybody of your acquaintance shares Child Pornography (CP)/ Child Sexual Abuse Material (CSAM) or sexually explicit material with you, it is your duty as a responsible citizen to inform the concerned person that publication, collection and distribution of Child Pornography (CP)/ Child Sexual Abuse Material (CSAM) or sexually explicit material is illegal and he should refrain from doing such activities.
- You can also report it on National Cyber Crime Reporting Portal (www.cybercrime.gov.in)



Publishing material containing sexually explicit act on the internet (Sec67A)		Publishing material depicting children in a sexually explicit act (Sec67B)		Publication of obscene material in electronic form (67)	
Assam	208	Kerela	18	Assam	223
Chattisgarh	21	Chattisgarh	8	Chattisgarh	18
Odhisa	166	Odhisa	7	Odhisa	34
MAHA	39	MAHA	4	MAHA	40
AP	18	AP	2	AP	2
Raj	20	Raj	0	Raj	40
GUJ	26	GUJ	0	GUJ	32
UP	145	UP	21	UP	449
Total-India	1097	Total-India	82	Total-India	1334



Existing policies and Laws

- The **Information Technology Act, 2000**, which addresses aspects related to cyberspace, and the Information Technology (Amendment) Act, 2008 are the main pieces of legislation concerned with online activities and cover any communication device used to transmit any text, video, audio or image. The provisions of the National Cyber Security Policy, 2013 enable the development of a dynamic legal framework.
- The **National Policy for Children (NPC), 2013** does not refer directly to online risks. All policies related to education, ICT or cyber security are expected to incorporate the principles of the NPC and provide children with equal opportunities for learning and empowerment, while protecting them from harm.
- The **National Policy of ICT in Schools, 2012** is more explicit about regulating ICT to protect children from potential risks. It recognizes online risks and has provisions for regulating and monitoring Internet access. The promotion of ICT systems in schools and adult education is included in the National Education Policy.



- The **National Cyber Security Policy, 2013** addresses the **prevention, investigation and** prosecution of cybercrimes, including those against children. It calls for strengthening capacities of law enforcement agencies to investigate cybercrimes and gather data to enable prosecution.
- The **Indecent Representation of Women (Prohibition) Act, 1986** prohibits **indecent** representations of women and criminalizes the performance of obscene acts and songs but does not punish the audience or those who make the person perform such acts.
- The provisions of the Information Technology Act have been strengthened by the **Protection of Children from Sexual Offences Act, 2012** which deals **with** online offences against children, including child pornography and grooming. As the Information Technology Act does not have specific provisions for criminal intimidation, hate speech and defamatory content, the provisions of the Indian Penal Code apply in cases of online offences.



India's first hotline to report child pornography

- **The hotline will enable users to report child sexual abuse images and videos in a safe and anonymous environment.**
- The country's first-ever hotline to curb sexual abuse of children through the internet and to remove child pornographic content online is set to be unveiled next week.
- Aarambh Initiative, a network of organisations and individuals working on child protection in the country, has collaborated with UK-based Internet Watch Foundation (IWF), which is an industry watchdog and is the most successful hotline in the world at removing child pornography.
- The hotline in India will be hosted on aarambhindia.org and will enable users to report child sexual abuse images and videos in a safe and anonymous environment. While the hotline will initially be in English and Hindi, in the future it will also be available in as many as 22 regional languages.
- The purpose of the hotline is three fold – to block and ultimately remove offensive content, to trace the perpetrator and report him to the law enforcement agencies of his country, and to reach out to the child victim and rehabilitate him/her as and when required.
- The Union Ministry of Electronics and Information Technology directed al the ISPs to prevent the distribution and transmission of such content into India by adopting and implementing Watch Foundation Resources on or before July 2017.This initiative aims to curb online child sexual abuse material(CASM)



- **Partnership with National Center for Missing and Exploited Children (NCMEC)**
- FBI personnel assigned to the NCMEC review information that is provided to NCMEC's Cyber Tipline. The tip line receives reports of child sexual exploitation incidents via an online form. The NCMEC also maintains a 24-hour hotline at 1-800-THE-LOST and through its [website](#).
- FBI employees assigned to the NCMEC work to identify individuals suspected of any of the following: possession, manufacture and/or distribution of child sexual abuse material; online enticement of children for sexual acts; child sexual tourism; and/or other sexual exploitation of children. Once a potential suspect has been identified, investigators compile information and forward it to the appropriate FBI field office for investigation



- **Cases-#**
- The Delhi Police Cyber Crime Cell registered a case under section 67 of the IT Act, 2000. A student of the famous School , New Delhi was teased by all his classmates for having a pockmarked face. He created a website and posted explicit, sexual details were given about girls and teachers of the school. A case was registered under IT Act, 2000. The Police picked up the concerned student and kept him in Juvenile home. It was almost after one week that the juvenile board granted bail to the 16 year old student.



- A 13-year-old boy was targeted by one of his classmates who used a fake identity to create a Facebook account to send out offensive messages to other children in the school. The victim did not have a Facebook account but was admonished by teachers and other parents.
- A girl was forced out of a school WhatsApp group where her morphed obscene picture was shared. The embarrassment caused to the girl was immense, although the school mediated in identifying and disciplining the offender.



- **A shocking history of rape and blackmail in Hyderabad**
- The arrest of a college dropout in a blackmail and rape case in Bahadurpura in Hyderabad in March 2016 revealed shocking details of sexual exploitation, extortion and criminal intimidation of a teenage girl over a period of three years. The youth had shot some videos of intimate moments during a brief relationship with the victim's sister and used these to blackmail and rape the 17-year-old victim in 2012.
- A college senior of the victim also blackmailed her about the “sexual relationship” she had with the college dropout and sexually exploited her for three months until she became pregnant. The girl was forced to have an abortion by the second accused in February 2014.
- The first accused contacted the girl again on Facebook in September 2015 and resumed blackmailing her, claiming that he knew of her relationship with the second accused. He insisted that she should lodge a complaint against the second accused or else he would post her videos with the second accused on Facebook. He took her signatures on the complaint and also demanded Rs. 100,000. She paid Rs. 30,000 out of fear but also informed her parents who approached the police



- **Revenge pornography**
- In April 2015, a 21-year-old man was booked by the police in the village of Valsad (Gujarat) for allegedly spreading photographs of his teenage ex-girlfriend in compromising positions on popular social media sites. The accused was charged with sections of the Information Technology Act and the Protection of Children from Sexual Offences Act.



Child Pornography case

- Facts
- A complaint was received on email from Interpol against an IP address involved in sending child pornography images.
- Interpol was briefed by the Child Exploitation Online Protection Centre(CEoP)
- The email mentioned the uploading of child pornography images and receipt of payment using Internet account from Chennai.
- **Investigation**
- IP address revealed BSNL network. It led to the identification of a foreign national).
- His laptop was seized and examined forensically.
- It revealed hundreds of child pornography images. His bank account also showed payment details.
- A case was registered including section 67B of the IT Act.



- In Mumbai a Swiss couple gathered slum children and then forced them to appear for obscene photographs. They then uploaded these photographs to websites specially designed for pedophile. The Mumbai Police arrested the couple for child pornography.



- **Internet addiction: A reality or a myth?**
- In a recent case from India, two gaming-addicted brothers required a month of rehabilitation in the ward of the Ram Manohar Lohia Hospital in New Delhi. Several reports and articles in the media, which have been suggesting an increase in cases of Internet and gaming addiction, highlighted this case as an example of the perils of children spending excessive amounts of time on online gaming.



- **The “selfie” phenomenon**
- Self-portrait photographs or “selfies” to be posted on social media using mobile phones and, if resources permit, the selfie stick, have become popular. The increase in the number of cases of fatal accidents during selfie sessions are also a matter of concern.
- According to a report in the Washington Post, India suffered more selfie related deaths in 2015 than anywhere else in the world. Approximately half of the world’s 27 deaths linked to the pictures people took of themselves happened in India. Indeed, Mumbai police identified 15 sites around the city as “no selfie zones” after two people drowned in the Arabian Sea in January 2016, and announced plans to install warning signs and deploy lifeguards.



LEGAL REMEDIES

- cybercrime.gov.in
- Civil cases & Criminal Cases



ADVICE FOR PARENTS

- **The most important advice for parents is to have open and ongoing conversations about safe and appropriate online behavior.**
- **Other advice to consider:**
- Educate yourself about the websites, software, games, and apps that your child uses.
- Check their social media and gaming profiles and posts. Have conversations about what is appropriate to say or share.
- Explain to your kids that once images or comments are posted online they can be shared with anyone and never truly disappear.
- Make sure your kids use privacy settings to restrict access to their online profiles.
- Tell your children to be extremely wary when communicating with anyone online who they do not know in real life.



- Encourage kids to choose appropriate screen names and create strong passwords.
- Make it a rule with your kids that they can't arrange to meet up with someone they met online without your knowledge and supervision.
- Stress to your children that making any kind of [threat online](#)—even if they think it's a joke—is a crime.
- Tell your children not to Send obscene and inappropriate content – as it is a crime . If they receive such content they must report to parents immediately.
- Report any inappropriate contact between an adult and your child to law enforcement immediately. Notify the site they were using, too.



STAY SAFE, BROWSE SAFE

T H A N K S

RAJASTHAN STATE LEGAL SERVICES AUTHORITY

&

NISHEETH DIXIT

ADVOCATE

9829112511