



# The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2024

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

---

## GLOBAL PERSPECTIVES ON CYBER SEXTORTION: EXAMINING MULTIFACETED CRIME LEGISLATION IN INDIA AND BEYOND\*

~ *Kavish Mehra , Student , Khalsa College of Law*

*"Data is the pollution problem of the Information age and privacy is the environmental challenge."*

### INTRODUCTION

In the present era "technology and digital platforms are increasingly becoming integral parts of everyday lives and vital societal functions, particularly in the wake of the COVID-19 pandemic." These platforms are also increasingly used to spread misogyny, radical messaging and hate speech and have left states, organizations and individuals vulnerable to cyber-attacks. "Cyber-crime is defined as "a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offence (cyber pornography, hate crimes)." Cybercrimes can go unnoticed, undetected and unreported due to its anonymity. The word cyber is generally misunderstood as "the word only and wholly concerned with the web and internet; however, it also includes other communication networks and electronic networking devices e.g. cellular networks and devices, telephones and many other e-devices." The sine qua non for cybercrime is that there should be an involvement at any stage, of the virtual cyber medium i.e. the computer. The menace of cyber-crime has spread its tentacles throughout the world posing a major threat to nations, governments and general public. But women across the world are at risk of gender specific crimes in the sphere of cyber world. Cyber sextortion is part of a larger continuum of image-based sexual offending in which images are used for harm. Despite the serious nature of this crime, there exists

---

\* *Kavish Mehra , Student , Khalsa College of Law*

a dearth of empirical knowledge of sextortion.<sup>1</sup> Sextortion is a sort of internet blackmail in which offenders use graphic or compromising content to compel others into offering money, sexual favours, or other concessions. This information is usually gained by hacking, social engineering, or tricking people into providing sensitive information. As the prospect of discovery grows increasingly credible and tougher to rebut, the stakes for victims rise. The methodology and motivations that drive cyber sextortion are similar to other interpersonal crimes such as intimate partner violence (Bates, 2017), cybercrime (“Record Numbers of UK Men Fall Victim to Sextortion Gangs,” 2018), and child exploitation (Acar, 2016).<sup>2</sup> The most important element of sextortion is that images are used to threaten victims and force their compliance. It is the power and control that an offender yields over another individual to possibly harm that is central to this crime. The uncertainty of whether images will be distributed, whether they are in fact distributed, creates fear and desperation for the victim. It is in this sense that cyber sextortion is unique.

Cyber Sextortion is not a narrow term it is a wider term which includes various others sexual offences under it. It act as a multifarious. Since social media has become a daily destination for a majority of people, the wrongdoers are using these platforms as a weapon to commit the crime. A set of fear is created of making the intimidating picture public, under this danger of leaking sexually suggestive material, victims are made to do certain things at the perpetrators desire, hence it becomes imperative to take certain steps to curb this extensively growing crime. The greatest requirement is the proper education, along with a specific legislation covering this crime, then only such damaging attacks could be deterred or, at the very least lessened. Technology and digital platforms have become an essential part of daily life and have been increasingly used to spread misogyny, radical messaging, and hate speech. Cyber-crime is a crime that involves the use of a computer as an object of the crime or as a tool to commit an offense. Cyber-crimes can go unnoticed and unreported due to anonymity. Cyber-crime is not only limited to the internet but also includes other electronic devices. Women are at risk of gender-specific crimes in the cyber world.

---

<sup>1</sup> Sextortion: An emerging crime into the gray area of law, Legal Service India - Law, Lawyers and Legal Resources, <https://www.legalserviceindia.com/legal/article-6707-sextortion-an-emerging-crime-into-the-gray-area-of-law.html> (last visited Jun 1, 2024).

<sup>2</sup> Publisher, Waging War on the sextortion epidemic TechNewsWorld (2023), <https://www.technewsworld.com/story/waging-war-on-the-sextortion-epidemic-177981.html> (last visited Jun 1, 2024).

## **SEXTORTION AS A MULTIFARIOUS CRIME:-**

Cyberspace is a new realm created by information technology that provides various opportunities for accessing data in text, audio or video format. It has widened the scope of human activity and level of comfort in availing services such as banking, travel, government amenities, educational activities, and social networking. However, the growth of information technology has also led to the growth of a new type of crime called cybercrime. As cyberspace is a borderless world, this new format for committing a crime is a global concern that has its impact from anywhere to everywhere in the world. Sexual extortion is a horrific and dehumanising assault that feeds on the humiliation of victims. Sextortion is similar to online blackmails in that the blackmailer demands the victim to participate in sexual activities, such as posing for naked images or masturbating in front of a camera, or demanding a large sum of money.

The most popular method of sextortion is through social media. Through online conversation and/or SMS, sextortionists form tight relations with their potential victims. Once confidence has been established, they encourage their victims to provide nude photos or videos. They then use those photographs as a kind of blackmail to force their victims to generate additional film to their perverted standards.<sup>3</sup> Obscene refers to indecent words, thoughts, books, pictures, etc., especially sexually explicit conduct that is disgusting and offensive. Pornography is an act of describing or showing sexual acts to cause sexual excitement, through images, films, or video clips, etc.<sup>4</sup> Sextortion is not a single crime but includes various different sexual Offences under its ambient. we can say that sextortion is a multifarious crime. Crimes like Cyber Stalking, Revenge Porn , sexting, Pornography, Cyber Obscenity, etc are inter related with the term cyber sextortion.

## **INTERLINKAGE OF CYBER SEXTORTION WITH OTHER SEXUAL OFFENCES:-**

If we look the term sextortion it is not a new term early there were different cyber sexual offences which we can say now can be merge or read under a single wide term that is cyber sextortion.

---

<sup>3</sup> Sextortion: An emerging crime into the gray area of law, Legal Service India - Law, Lawyers and Legal Resources, <https://www.legalserviceindia.com/legal/article-6707-sextortion-an-emerging-crime-into-the-gray-area-of-law.html> (last visited Jun 1, 2024).

<sup>4</sup> Publisher, Waging War on the sextortion epidemic TechNewsWorld (2023), <https://www.technewsworld.com/story/waging-war-on-the-sextortion-epidemic-177981.html> (last visited Jun 1, 2024).

Sextortion combines both sexual favour and corruption components. The former involves an explicit or implicit request for any type of unwelcome sexual action, while the latter occurs when the person demanding the sexual favour holds a position of power that is abused. The fundamental concept is quid pro quo, in which a sexual favour is demanded or accepted in exchange for a benefit that the offender has the authority to withhold or give. Because of the power imbalance between the offender and the victim, the perpetrator can use psychological coercion similar to that used in monetary corruption. Sextortion involves blackmail, in which the victim is threatened to share sexual photographs or information to extort money or sexual pleasure. Let us detail various sexual offences as under the single term cyber sextortion.

➤ **REVENGE PORN A INTRINSIC OF CYBER SEXTORTION:-**

With the advent of technology a series of new crimes has been added out of which revenge porn is one crime which is spreading very fast. It is rightly said “Data is like a toothpaste once it is out can never be put back.” Revenge porn is a form of image-based sexual abuse that involves sharing personal or intimate images and videos without the consent of the person in the media. It is not consensual and can be used as a form of blackmail or to harm the other person. This form of non-consensual pornography includes sharing material online or offline like uploading and sharing on the internet, adult websites, social media, sharing through email, etc. It is often used as a tool for vengeance, and men frequently use it to punish women. This is because of the patriarchal society we live in, which has led men to punish women for being in relationships, being sexually active, leaving them, or even for denying sex while in a relationship. Though this tool for vengeance is gender-neutral, it is women who are mostly targeted. It's important to remember that such acts are never justified and that people who indulge in such acts lack empathy for others.<sup>5</sup>Technology plays an important role in facilitating revenge porn. Revenge porn is a gross misuse of technological advancements, and it's challenging to regulate the deep web and the borderless nature of the internet.

**REVENGE PORN AND ITS GLOBAL SCENARIO**

Revenge porn gained international media attention when Hunter Moore launched the website Is Anyone Up in 2010. The site featured user-submitted pornography, including identifying

---

<sup>5</sup> Wikipedia contributors. “Revenge Porn.” Wikipedia, July 2023, en.m.wikipedia.org/wiki/Revenge\_porn.

information such as the subjects' names, employers, addresses, and links to social networking profiles. Activist Charlotte Laws was one of the first people to speak out against Moore and one of the first people to publicly support revenge porn victims. She became known around the world as the "Erin Brockovich of revenge porn" and was one of the first activists to meet with legislators in an effort to get laws passed against revenge porn. In February 2015, Reddit announced a change to its privacy policy to ban the posting of sexually explicit content without the consent of those depicted. In March 2015, Twitter followed suit with new rules to address the posting of unauthorized content and specifically revenge porn. In June 2015, Google announced it would remove links to revenge porn on request. Microsoft followed suit in July. Both have placed forms online for victims to complete. Together, the two organizations account for nearly 90% of the internet search market in the U.S. The term "revenge porn" is controversial because not all visual depictions of nudity or sexual activity are pornographic, and those who share images without permission may be motivated by profit, notoriety, entertainment, or other goals besides revenge.<sup>6</sup>

A survey conducted by BBC England showed that almost 30 percent of people involved in revenge porn activities were under 19 years of age, the average age of the victim was around 25 years, and Facebook was the social media platform that was majorly used. Cyber & Law Foundation (an NGO situated in India) released a survey, which showed that 27 percent of people aged 13 to 45 had experienced revenge porn at least once in their lifetime.<sup>7</sup> A study shows that almost 50 percent of the victims of revenge pornography experience day-to-day cyberstalking, and 85-90 percent of the people who were targeted by the culprits suffered from mental and emotional breakdowns for a long period of time.

Laws banning revenge porn have been slow to emerge due to a lack of understanding about the gravity of the problem, free speech concerns, belief that existing law provides adequate protection, a lack of care historically for women's issues, and misunderstandings of First Amendment doctrine. The American Civil Liberties Union and the Electronic Frontier Foundation have drawn attention to the implications for free speech if legislation is too broad.

---

<sup>6</sup>Jaiswal, Nishtha. "Bodies Online: Image-Based Sexual Abuse or 'Revenge Porn' in India." *Feminism in India*, Jan. 2022, [feminisminindia.com/2020/07/17/bodies-online-image-based-sexual-abuse-revenge-porn-india](https://feminisminindia.com/2020/07/17/bodies-online-image-based-sexual-abuse-revenge-porn-india).

<sup>7</sup> Verma, Ayush. "What to Do if You Are a Victim of Revenge Porn - iPleaders." *iPleaders*, 1 June 2022, [blog.iplayers.in/victim-revenge-porn](https://blog.iplayers.in/victim-revenge-porn).

There is a concern that revenge porn laws may not be constitutional according to the **Miller v. California**<sup>8</sup> decision if the porn does not categorically appeal to the prurient interest, if it is not, in itself, patently offensive, or if it has Different legislation has been enacted by different countries. The Philippines became the first country in 2009 to penalize non-consensual pornography, with punishments ranging up to 7 years of imprisonment. Israel also criminalized revenge pornography, with punishments of up to 5 years of imprisonment. Japan, England, and Germany have also criminalized revenge pornography. In Australia, there are no specific laws related to revenge pornography, but there are general laws related to online harassment that cover the acts of revenge pornography. The scenario in the USA is also unique. The District of Columbia and almost 27 states have laws to ban non-consensual pornography, but the remaining states have a general set of rules to check the menace of revenge pornography.<sup>9</sup>

#### ➤ REVENGE PORN AND ITS POSITION IN INDIA

India's first-ever case of revenge porn was **State of West Bengal v. Animesh Boxi**,<sup>10</sup> a 2018 case where the accused was punished with five years of imprisonment and a fine of Rs.9000 for publishing and sharing private images and clips of his ex-partner without her consent as revenge porn after she ended the relationship with him. The victim was pressured to share her intimate and sexually explicit images with him on the pretext of marriage and was later blackmailed into uploading the previous pictures to leverage more such pictures from her. The accused even used her phone without permission to get more such pictures. In another instance, an engineer and a law student were arrested by Bangalore Police for running a blackmail racket. The two of them used to download images from social media sites and upload them on porn websites and engaged in blackmailing.

Another recent instance of revenge porn was in the case of **Subhranshu Rout v. The State of Odisha**, where the offender and the victim were a couple in a relationship. The perpetrator went to the victim's home, assaulted her, and recorded the incident on his cell phone. He later threatened and blackmailed the victim to not disclose the incident to anyone else he would release the photos

---

<sup>8</sup> 413 U.S. 15 (1973)

<sup>9</sup> Banerji, Oishika. "The Growing Menace of Revenge Porn : A Major Need for Explicitly Related IT Laws - iPleaders." iPleaders, 30 Aug. 2021, [blog.ipleaders.in/growing-menace-revenge-porn-major-need-explicitly-related-laws](http://blog.ipleaders.in/growing-menace-revenge-porn-major-need-explicitly-related-laws)

<sup>10</sup> C.R.M No .11806 OF 2017

and videos to the public. When the victim told her parents about the incident, the perpetrator uploaded all of the photos on Facebook. The Court refused to grant bail to the perpetrator and observed that allowing such objectionable photos and videos to remain on social media without her consent is a direct affront on a woman's modesty and right to privacy. The Hon'ble Court also emphasized the significance of the 'Right to be Forgotten' in the context of the right to privacy. With the rising cases of revenge porn, it has been highlighted that trained professionals in the police force are needed to handle such cases and the collection, reception, storage, analysis, and production of electronic evidence.<sup>11</sup>

In conclusion, revenge porn is a heinous crime that violates an individual's right to privacy and dignity. It is a serious issue that needs to be addressed by society and the law.

### **CYBER OBSCENITY ANOTHER FACET OF CYBER SEXTORTION**

Obscenity is defined as any act or utterance that strongly offends the prevalent morality of the time. The Oxford Dictionary defines obscenity as an extremely offensive word or expression, while the Macmillan Dictionary defines it as "offensive in a sexual way" and "so unfair or immoral that one feels angry."<sup>12</sup>To determine whether a work is obscene, factors such as "prurient interest," "patently offensive" and "contemporary community standards" are considered. However, the standards and factors for obscenity vary depending on the norms and values of the state, town or city. The notion of obscenity is related to morality and decency, which varies from person to person. With the rise of information technology, people are becoming more focused on their freedom and less on their duty to maintain moral standards and decency in society. Cyber obscenity is a global threat to internet users, as there are no territorial limits that distinguish the commission of crime between countries.

### **CYBER OBSCENITY AND INTERNATIONAL PROSPECTIVE:-**

The first World Congress was held in Stockholm in August 1996 to address the issue of commercial sexual exploitation of children. The United Nations Congress took special initiatives to prevent cybercrimes, and the United Nations Economic and Social Council (UNESCO) adopted uniform preventive and controlling measures to curb online sexual abuse, child pornography, and

---

<sup>11</sup> BLAPL No.4592 of 2020

<sup>12</sup> Cyber Obscenity and Victimization of Women in India - iPleaders." iPleaders, 10 May 2017, [blog.ipleaders.in/cyber-obscenity](http://blog.ipleaders.in/cyber-obscenity).

pedophilia. In October 2000, the EU and the USA prepared the first draft of the International Treaty on Cyber Crimes, inviting international cooperation to curb the fast growth of cybercrimes worldwide. In **Regina v. Hicklin**<sup>13</sup> the word "obscene" was defined as any matter that could deprave or corrupt those whose minds are open to immoral influence and into whose hands a publication of this sort may fall. This led to the establishment of the Hicklin test, which is a legal test for obscenity. In the US, the Supreme Court set out the Miller Standard for obscenity test, which states that material is obscene if:

- a) The average person, applying contemporary standards, finds that the material as a whole appeals to the prurient interest
- b) The material depicts or describes sexual conduct in a patently offensive manner specifically defined by applicable state law
- c) The material, taken as a whole, lacks serious literary, artistic, political, or scientific value.

The Court reasoned that people in different states vary in their tastes and attitudes, and this diversity is not to be strangled. Consequently, widely varied standards from state to state may ensue.<sup>14</sup>

### ➤ **CYBER OBSCENITY- INDIAN OUTLOOK**

The Indian Penal Code (IPC) deals with obscene acts and songs in public places. Section 292 of the IPC defines obscenity as any material that is lascivious or appeals to prurient interest and tends to deprave and corrupt those who read, see or hear it. However, this section is not applicable to works done in public interest such as in cases of science, literature or religious purposes. Section 293 of the IPC bans the selling of obscene objects to young persons and prescribes punishments for the same. Punishment for publishing of obscene material in electronic form is given under Sec 67 of IT Act. Other laws like the Indecent Representation of Women Prohibition Act, 1986, Cable Television Networks Regulation Act, 1995, Cinematograph Act, 1952, and Young Persons Harmful Publication Act, 1956 also prohibit obscene acts and publications.

---

<sup>13</sup> 11 Cox C.C 19(1986)

<sup>14</sup> Growing Indecencies or Obscenity in Cyber World and Legal Regime in India.  
[www.legalserviceindia.com/legal/article-1593-growing-indecencies-or-obscenity-in-cyber-world-and-legal-regime-in-india.html](http://www.legalserviceindia.com/legal/article-1593-growing-indecencies-or-obscenity-in-cyber-world-and-legal-regime-in-india.html).

In the case of **Avnish Bajaj v. State (NCT of Delhi)**<sup>15</sup>. Since the Internet is global and dynamic in nature, we have Section 75 of the IT Act taking care of the issues related to electronic transmission of obscene material from other jurisdictions as well.<sup>16</sup>

➤ **CYBERPORNOGRAPHY AN ANOTHER KIND OF CYBER SEXTORTION:-**

The issue of cyber pornography has become a global problem, leading the government to ban 827 websites that possess pornographic content. Despite the ban, many people, especially youngsters, are still addicted to cyberporn and are using various means such as VPN, DNS Server Change, or downloading Opera Mini with inbuilt VPN activation to access it. The term pornography comes from two Greek roots, meaning "writing about" or "description of" and "prostitute," "harlot," or "female captive." In legal terms, pornography is defined as "obscenity," which includes any sexually explicit videos, pictures, or movies that are considered indecent by the public. Live exhibitions like sex shows and striptease are not considered pornography. 30% of Internet content is porn. One can get abundant access to pornographic content on the dark web. Dark web even contains the child pornographic contents. It is worthy to note that only 10% of the total content is available on the surface web, the rest of the content is available on the dark work and the deep web. In the year 2005, there were more than 2 billion searches for porn. Almost 20% of the mobile phone searches are for porn. 28,258 users watch porn every second. 90% of boys and 60% of girls watch porn by the time they turn 18.<sup>17</sup>

➤ **CHILD PORNOGRAPHY-A HEINOUS CRIME**

While the term "pornography" itself is already associated with negative connotations, adding the prefix "child" to it increases the severity of the term exponentially. The combination of "child" and "sexual activity" sounds inherently sinister, and displaying it to people who watch it to arouse their sexual desires only makes it worse. As a result, such actions lead to the exploitation, trafficking, and violence towards children, making child pornography a particularly heinous crime.

---

<sup>15</sup> 116(2005) DLT427

<sup>16</sup> Naik, Yeshwant. "Cyber Obscenity and Victimisation of Women in India - iPleaders." iPleaders, 10 May 2017, [blog.ipleaders.in/cyber-obscenity](http://blog.ipleaders.in/cyber-obscenity).

<sup>17</sup> Ramanuj. "Cyber Pornography Law in India- the Grey Law Decoded - iPleaders." iPleaders, 20 Sept. 2019, [blog.ipleaders.in/cyber-pornography-law-india](http://blog.ipleaders.in/cyber-pornography-law-india).

In India, child pornography is defined under the Protection of Children from Sexual Offences Act, 2012 (POCSO). According to section 2(da) of the act, child pornography is any visual display of overt sexual activity that involves a child, including images, videos, or computer-generated pictures that cannot be easily differentiated from real children. This includes any images that depict a child engaging in sexual activities, whether created, adapted, or modified.

The POCSO Act defines a "child" as any person who has not yet reached the age of eighteen years, according to section 2(d).

On an international level, the Optional Protocol on the sale of children, child prostitution, and child pornography (OPSC) addresses the issue of child pornography. Article 2 of the OPSC defines child pornography as the depiction of a child involved in either real or simulated explicit sexual conduct, as well as the revealing of sexual body parts of a child, mainly for sexual motives.<sup>18</sup>

The sharing of child pornography has seen a rapid increase worldwide. In 1998, the total reported cases of child sexual abuse imagery were over three thousand. However, in just a decade, the number of cases rose to more than one lakh. This number crossed one million for the first time in the year 2014. Later in 2018, the number of cases that were reported increased to 18.4 million, which was found to be more than one-third of the total cases ever reported. In 2020, 21.7 million cases were reported, representing a 28% increase over 2019. These horrific statistics clearly indicate the high demand for child pornography.<sup>19</sup>

The reasons for the high demand for child pornography vary across different age groups. Adolescent viewers, aged between 18 to 21 years, who have sexual dysfunction, find it difficult to maintain erections and achieve orgasms, and hence, are the primary viewers. In contrast, many children or adolescents watch it simply to fulfill their curiosities or fantasies. The demand for child pornography would be ineffective if there was no means to fulfill it in the first place. This is where the internet comes in, which has become the nucleus of sharing such materials, making them more popular. The advancement of digital technology and the expansion of the internet have contributed significantly to the rise of the child pornography market. The videos are easily available,

---

<sup>18</sup> Srivastava, D. K. Cybercrime in India Challenges and Solutions. 2021, [hdl.handle.net/10603/448897](https://hdl.handle.net/10603/448897).

<sup>19</sup> Pornography as Cyber Crime. [www.legalserviceindia.com/legal/article-914-pornography-as-cyber-crime.html](http://www.legalserviceindia.com/legal/article-914-pornography-as-cyber-crime.html).

affordable, and they conceal the identity of the viewer, thus increasing the number of people watching the same.<sup>20</sup>

### ➤ LEGISLATIVE MEASURES ACROSS GLOBAL

The Optional Protocol to the (U.N.) Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, the Council of Europe's Convention on Cybercrime, and the Council of Europe's Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse are effective tools in combating the sexual exploitation and abuse of children. They contain specific definitions of offenses and provisions requiring punishment for criminalized behavior, allowing for the more effective prosecution of perpetrators. The European Union also adopted a Directive on combating the sexual abuse and sexual exploitation of children and child pornography, which provides explicit guidelines for criminal legislation regarding sexual abuse and exploitation of children. India is a signatory to many international instruments and declarations about the rights of children to protection, security, and dignity and is fully committed to implementing all provisions of the UNCRC.

### LEGISLATION IN INDIA

Under Protection of Children from Sexual Offences Act, 2012 (POCSO)

The POCSO Act makes the act of using a child for pornographic purposes punishable. Now what all acts constitute to be usage of a child for pornographic purposes have been explained in **section 13** of the Act. According to the said section, any person who uses a child for the purpose of sexual gratification through any kind of media either printed or electronic, no matter whether it was aimed for distribution or just personal use is said to have used the child for pornographic purposes. It includes the display of a child's sexual organs, indecent representation of a child, and engaging a child in true or simulated sexual activity where penetration is not a mandatory condition.

**Section 14** of the POCSO Act punishes any person committing an offence u/s 13 with an imprisonment for at least 5 years and fine. And if the person is convicted for the same offence again, then he would be punishable with imprisonment for a minimum of 7 years and fine. It further

---

<sup>20</sup> Growing Indecencies or Obscenity in Cyber World and Legal Regime in India.  
[www.legalserviceindia.com/legal/article-1593-growing-indecencies-or-obscenity-in-cyber-world-and-legal-regime-in-india.html](http://www.legalserviceindia.com/legal/article-1593-growing-indecencies-or-obscenity-in-cyber-world-and-legal-regime-in-india.html).

provides that if a person is committing the offence of using child for pornography along with offence given under sections 3 or 5 or 7 or 9 by getting himself involved in the pornographic act, then such a person shall be punished under section 4 or 6 or 8 or 10 respectively in addition to section 14 of the POCSO Act.<sup>21</sup>

### **Under the Information Technology Act, 2000**

**Section 67B** of the IT Act punishes the act of publishing, transmitting, creating, collecting, browsing, downloading, advertising, promoting, exchanging, distributing, recording, etc. of any material in electronic form which shows a sexually explicit activity engaging a child. It also punishes the formation of online relationships with any child for sexually explicit act and abusing the child online. The punishment provided u/s 67B is imprisonment of 5 years and ten lakh rupees fine on first conviction, and in case of second conviction, it is 7 years of imprisonment and fine of Rs. 10 lakhs.<sup>22</sup>

It's important for everyone to understand that child pornography is a heinous crime that exploits and harms innocent children. We must all work together to prevent and report any instances of child pornography to the authorities. It's the responsibility of every individual to ensure the safety and well-being of children in our society.

#### **➤ CYBER STALKING PART OF CYBER SEXTORTION**

Stalking is the act of invading someone's privacy to terrify, torment, torture, or intimidate the victim. Cyberstalking is an extension of physical stalking, where the internet is used to pursue, harass or contact another in an unsolicited fashion. Cyberstalkers follow a person's movements across the internet by posting threatening messages on bulletin boards, entering chat rooms frequented by the victim, or constantly bombarding the victim with emails. Abused women are followed in the cyber world by their assailants, allowing the stalker to threaten, impersonate, and discredit the victim on the internet. Cyberstalking victims are as scared as those being stalked in

---

<sup>21</sup> Shingari Kirti .(2023) Cyber sextotion in India –An Analysis .dissertation

<sup>22</sup> Shingari Kirti .(2023) Cyber sextotion in India –An Analysis .dissertation

the real world, and cyberstalkers have no fear of physical retribution since they know they cannot be physically touched in cyberspace.<sup>23</sup>

Cyberstalking can be done by strangers or people who have or had a relationship with the victim. Gender-based stalking, also known as online gender-based violence, is common and can include rape threats, threats of violence, and posting personal information. Cyberstalking of intimate partners is a form of domestic violence used to control the victim and encourage social isolation and dependency. Cyberstalkers may send repeated insulting or threatening e-mails, monitor or disrupt the victim's e-mail use, and use the victim's account to send e-mails to others posing as the victim or to purchase goods or services the victim does not want. Celebrities and public figures are often targets of lies or made-up stories in tabloids, and stalkers may feel they know the celebrity even though the celebrity does not know them.

### ➤ **LEGISLATION IN INDIA**

The cyber stalking cases are dealt in India by the:

#### 1. Information Technology Act 2000

If any person is publishing or sending any salacious material in the form of electronic media is to be charged under section 67 of the Act. This does not involve the determination of the extent of liability of ISP (internet service providers) and their directors.

For the preclusion of cyber stalking the protection of the data is very important, which gets leaked easily by the hackers. According to the amended IT act, section 43 A is added for the inclusion of a Body corporate”, the allowing of the compensation in the case of a firm or a company which causes any wrongful losses or gain to any person by the way of transmitting any sensitive information and the maintenance of such type of security, then such body corporate shall be liable to pay damages by way of compensation.<sup>24</sup>

The Information Technology Act, 2000 also comes into picture when the cyberstalker posts or sends any obscene content to the victim. Section 67 of the Information Technology Act states that

---

<sup>23</sup> Naik, Yeshwant. “Cyber Obscenity and Victimisation of Women in India - iPleaders.” iPleaders, 10 May 2017, [blog.ipleaders.in/cyber-obscurity](http://blog.ipleaders.in/cyber-obscurity).

<sup>24</sup> Sebastian Wachs et al., How are consensual, non-consensual, and pressured sexting linked to depression and self-harm? the moderating effects of demographic variables International journal of environmental research and public health (2021), <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7967514/> (last visited Jun 3, 2024).

when any obscene material is published, transmitted or caused to be published in any electronic form, then it is a crime of obscenity, punishable with imprisonment for up to 5 years with fine of up to Rs. 1 lakh. A second or subsequent conviction is punishable by imprisonment for up to 10 years with a fine of up to Rs. 2 lakh.

### ➤ **NON CONSENSUAL SEXTING ANOTHER CRIME UNDE CYBER SEXTORTION**

Sending, receiving, or forwarding sexually explicit images or texts via electronic devices—a practice known as “sexting”—has become increasingly popular among teenagers. While some experts contend that consensual sexting can be a normal, even healthy, form of expression, concerns are intensifying about the potential health risks to adolescents from nonconsensual sexting or sharing a sexual photo without the subject's permission. The ability to share sexually revealing photos electronically with any number of people gives rise to growing worry among health care professionals about the consequences for teens.<sup>25</sup>

The term "sexting" was first coined in 2005 and refers to the act of sending and receiving sexual content, such as photos and videos, via the internet and mobile phones. However, there is no consensus among researchers on a definition of sexting, with some definitions being broad and including any type of sexual content, while others are narrower and only include image-based content. Additionally, some definitions include coercion as part of sexting behavior, while others exclude it. The existing literature on sexting also differs in the population samples used and the items used to measure sexting, which contributes to the lack of a unified definition.<sup>26</sup>

### ➤ **SEXTING AND ITS POSITION IN INDIA**

Sexting is considered a criminal offense in India under the Information Technology Act, 2000, and the Indian Penal Code. The act of sexting can be punishable with imprisonment and fines, and can

---

<sup>25</sup> Srivastava, D. K. Cybercrime in India Challenges and Solutions. 2021, [hdl.handle.net/10603/448897](https://hdl.handle.net/10603/448897).

<sup>26</sup> Sebastian Wachs et al., How are consensual, non-consensual, and pressured sexting linked to depression and self-harm? the moderating effects of demographic variables International journal of environmental research and public health (2021), <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7967514/> (last visited Jun 3, 2024).

have severe consequences for the victim, including emotional distress, reputational damage, and even job loss.

In recent years, there has been a growing concern about the rise of non-consensual sexting and revenge porn in India. According to a study conducted by Cyber Peace Foundation, a non-profit organization, there has been a significant increase in the number of cases of sextortion and revenge porn in India in the past few years. The study found that women and children are particularly vulnerable to such crimes, and that most cases of sextortion and revenge porn are perpetrated by people known to the victims, such as former partners or friends.

To address this issue, the Indian government has taken several measures to prevent non-consensual sexting and protect victims of such crimes. In 2018, the Ministry of Women and Child Development launched a portal called "Cyber Crime Prevention Against Women and Children" to enable victims of cybercrime to report incidents of sextortion, revenge porn, and other forms of online harassment. The portal also provides information on how to stay safe online and how to seek legal recourse in case of cybercrime.

In India, sexting is considered a criminal offense under the Information Technology Act, 2000, and the Indian Penal Code. In 2015, a case in Mumbai made headlines when a 23-year-old man was arrested for allegedly blackmailing and threatening a 20-year-old woman with her nude photos. The man was charged with sexual harassment, criminal intimidation, and extortion. The case highlighted the need for stronger laws and measures to prevent non-consensual sexting and protect victims of such crimes in India. Since then, there have been several other cases of sexting-related crimes reported in India, underscoring the importance of raising awareness about the risks and consequences of sexting.<sup>27</sup>

To address this issue, the Indian government has taken several measures to prevent non-consensual sexting and protect victims of such crimes. In 2018, the Ministry of Women and Child Development launched a portal called "Cyber Crime Prevention Against Women and Children" to enable victims of cybercrime to report incidents of sextortion, revenge porn, and other forms of

---

<sup>27</sup> M. Dasgupta, *Cybercrime in India - a comparative study*, 134 (Easter Law House, Kolkata 2016).  
179 Ashok Wade, *Obscenity in Electronic Form: Exploration of Regulations*, [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2196473](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2196473)

online harassment. The portal also provides information on how to stay safe online and how to seek legal recourse in case of cybercrime.<sup>28</sup>

In addition, several states in India have introduced laws to address non-consensual sexting and revenge porn. In 2018, the state of Maharashtra became the first state in India to introduce a law specifically targeting revenge porn. The Maharashtra Prohibition of People from Social Boycott (Prevention, Prohibition and Redressal) Act, 2016, makes it a criminal offense to publish or circulate any material that causes insult, humiliation or intimidation to a person.

In conclusion, sexting is a serious issue in India, and there is a need for stronger laws, better education, and greater awareness to prevent non-consensual sexting and protect victims of such crimes.

### ➤ CONCLUSION

Cyber sextortion is a growing problem in the digital age, and it is a term used to describe the act of using sexually explicit material to blackmail, extort, or manipulate someone. It is a form of online harassment that can have devastating psychological effects on the victim, and it is a crime that has become increasingly common in recent years.

The term cyber sextortion is a relatively new one, but the practice itself has been around for some time. The rise of social media and other online platforms has made it easier for people to share sexually explicit material, and this has led to an increase in the number of cases of cyber sextortion.

Cyber sextortion can take many different forms, but it typically involves the use of sexually explicit material to coerce or manipulate the victim. This can include the threat of releasing nude photos or videos, the threat of sharing intimate conversations or messages, or the threat of exposing embarrassing or compromising information.

The psychological impact of cyber sextortion can be severe, and victims often experience anxiety, depression, and other mental health issues as a result. In some cases, victims have even taken their own lives as a result of the trauma they have experienced.

To combat the problem of cyber sextortion, there are several things that can be done. First and foremost, it is important to raise awareness about the issue and to educate people about the risks

---

<sup>28</sup> Srivastava, D. K. Cybercrime in India Challenges and Solutions. 2021, [hdl.handle.net/10603/448897](https://hdl.handle.net/10603/448897).

and consequences of sharing sexually explicit material online. This can include educating young people about the dangers of sexting and the importance of respecting other people's privacy.

Secondly, it is important to have strong laws in place to protect victims of cyber sextortion. In many countries, including the United States and the United Kingdom, cyber sextortion is a criminal offense that can result in imprisonment and fines. However, there is still a need for stronger laws in many other countries to ensure that victims of cyber sextortion are protected and that perpetrators are held accountable for their actions. Finally, it is important to provide support and resources for victims of cyber sextortion. This can include counseling services, legal assistance, and other forms of support that can help victims to recover from the trauma they have experienced.

In conclusion, cyber sextortion is a serious problem that requires a multi-faceted approach to address. By raising awareness about the issue, strengthening laws to protect victims, and providing support and resources for those who have been victimized, we can work together to combat this growing problem and ensure that everyone can enjoy a safe and secure online environment.