ISSN: 2582-6433

# INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed6th Edition

VOLUME 2 ISSUE 7

www.ijlra.com

 ISSN: 2582-6433

# DISCLAIMER

ISSN: 2582-6433

# EDITORIAL TEAM

## EDITORS

### Megha Middha

*Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar*

*Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society*

### Dr. Samrat Datta

*Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board*

ISSN: 2582-6433


## *Dr. Namita Jain*

*Head & Associate Professor*

*School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.*


*Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019*


## Mrs.S.Kalpana

Assistant professor of Law


*Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.*


## Avinash Kumar


*Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.*

ISSN: 2582-6433

# ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN 2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

www.ijlra.com
Volume 2 Issue 7 | May 2023
ISSN: 2582-6433

# A STUDY OF LEGAL MECHANISM ADDRESSING CYBER CRIME AGAINST WOMEN IN INDIA

AUTHORED BY - ADV. NILAM SAMPAT SHEVKARILL.M
MODERN LAW COLLEGE, PUNE

## ABSTRACT

The author of this research article seeks to examine how the development of technology and the consequent ease of access to the internet and social media platforms play a significant part in the rise of cybercrimes against women in Indian culture. The internet users, particularly women, are particularly susceptible to cybercrimes, or illicit activities performed via the internet. The legal options as remedies for cybercrime against women are outlined in this article. Furthermore, the numerous reasons of an upsurge in cybercrimes targeting females and their repercussions on those who are victimized are emphasised.

## KEYWORDS

**Cyber, Crime, Pornography, Morphing, Stalking, Phishing, etc.INTRODUCTION**

Cybercrime may be described as a synthesis of technology and crime. Cybercrimes are simply, "any offense or crime that involves the use of a computer."[1]

In addition to the millions of deaths brought on by the pandemic, many people have experienced hardship as a result of losing their jobs or having to close their businesses due to lockdown, as well as families who have lost the sole breadwinner, young children who have lost both parents, and many others. Mobile and cybercrime spread like a virus as people battled the pandemic and resisted it. Many people used the internet and phone technologies to harass others as a way to vent their frustration with the lockdown, and many others did so to pass the time while the epidemic was going

[1] https://www.techtarget.com/searchsecurity/definition/cybercrime last seen on 20/03/2023

ISSN: 2582-6433

on. Cybercrime on the internet increased quickly and heavily during the epidemic.

Cybercrime can be defined as "The illegal usage of any communication device to commit or facilitate in committing any illegal act"[2]. A cybercrime is explained as a type of crime that targets or uses a computer or a group of computers under one network for the purpose of harm. Cybercrimes are committed using computers and computer networks. They can be targeting individuals, business groups, or even governments. Investigators tend to use various ways to investigate devices suspected to be used or to be a target of a cybercrime.

## Types of Cyber Crimes Against Women in India:[3]

The rate of cybercrime against women started growing at this time since the majority of women were using social networking websites and various other online resources for educational, professional, and recreational objectives. Women are most commonly exposed to the following types of cyber crimes.

**Sextortion**: It was the cybercrime committed against women the most frequently during the epidemic. The offenders began extorting money or sexual favours from their victims by using their private photos or altered images as a form of blackmail. The offenders threatened women and demanded that they engage in sexual videoconferencing or write messages to them as a way of venting their annoyance over the epidemic.

## Phishing:

To make money during the lockdown, criminals send fake e-mails with a link to a particular webpage in an effort to coerce the victim into entering personal information like contact details and passwords or with the purpose of infecting the victim's device with dangerous viruses assoon as the link is clicked. These texts and emails appear to be authentic. The attackers then carry out shady transactions from the victim's bank account to their own using the victim's bank account and other private information.

[2] https://indiaforensic.com/certifications/cyber-crimes-india/ last seen on 1/4/2023
[3] Amita Verma, Cyber Crimes and Law (Central Law House Publication, Allahabad 1st edn., 2009)

ISSN: 2582-6433

**Google under phishing attack (2017)**: Users of the Google email service "Gmail" allegedly received a legal notice from the Gmail team asking them to update their account name, password, occupation, birth date, and country of residence within seven days of receiving the warning, with the warning that if they did not update their details within seven days of receiving the warning, their account would be permanently lost. However, a Google official denied receiving any such legal letter, claiming that personal information was obtained through aphishing attack known as spoofing or password phishing.

## Revenge Pornography

Revenge porn could be specified as:

An act where the perpetrator expressed his resentment and frustration over an unsuccessful relationship by exhibiting a false, sexually obnoxious painting of the victim without usinginformation that he might have known naturally and that he might have stored in his own system,information that might have been passed to his electronic equipment by the victim herself, information that might have been stored in equipment with the consent of the victim herself, and that might essentially has been completed considering publicly defaming sufferer.

Suffering through way belonging to retaliation porn have become general phenomenon into India these days. It understanding which by the time retaliation porn importantly develops sexual violence towards women upon internet, it mandatory includes hacking, voyeurism, stalking(there is none of the particular law considering regulating retaliation porn. However, it might be assimilated through along of Section 354C[4] belonging to IPC (voyeurism), 66E belonging to IT Act (privacy violation) along with also Section number 509 belonging to IPC (punishment considering harming advancement particularly women) however it mandatory destroys the advancement that of women.

## State v. Jayanta Kumar Das (G.R. Case No.1739/2012)[5]

The complainant alleged that a fake profile was created in his wife's name in a pornographic website where derogatory and obscene comments were posted. Similarly, the complainant's mobile phone

[4] Ibid

[5] https://ijoslca.files.wordpress.com/2020/07/state-of-odisha-v.-jayanta-kumar-das-by-aditi-palit-chandrika-dutta.pdf

ISSN: 2582-6433

number was also uploaded on the said website which led to receipt of number of unsolicited calls and objectionable requests. The complainant had alleged that the accused was behind such acts because he had reported the accused RTI Activist's activities in newspapers.

Investigations revealed that fake e-mail account in the name of complainant and a fake profile in his wife's name had indeed been created by the accused, Das. The probe also revealed that accused was named in at least six criminal cases and charge sheets were also submitted by policein such cases. He was arrested and remanded in custody for about a month. The court considered the evidence produced for charges of forgery, identity theft and cyber pornography and convictedDas.

## Cyber stalking[6]:

It is a form of cyber stalking, which is essentially the behaviour of a group of people, a group of businesses, or an individual employing technology that has been made available and leaked information to harass one or more people.

As a consequence, these behaviours may include sharing the risk, making untrue accusations, identity theft, data theft, equipment damage, internet monitoring, enticing minors for sex, and confrontation. However, it is not just confined to this.

According to the Section 354D[7], IPC there were two stages of cyber stalking which were included. The provision states, Each and every man who founds involved in following a woman or tries to contacts her or even stalks her, than in such case a woman is accepted to nourish personal interaction again and again or interferes with the mental peace of such woman, commitsthe offence of stalking.

During the year 2020, Pune-based Archeology student Divya Sharma noticed that a random Instagram user liked nearly 200 of her photos. She took the incident lightly, until the boy started making inappropriate remarks and then the boy started sending her direct messages. That’s when Divya filed an online complaint with the cyber police, which resulted in the abuser’s account being suspended and the abuser being punished. She believes that, “no one has the right to threaten you in

[6] https://blog.ipleaders.in/everything-about-cybercrimes-against-women/last seen on 4/4/2023
[7] Indian Penal Code 1860

ISSN: 2582-6433
DMs or comments."

The cyberstalker could be charged under Section 509 of the IPC for invading a woman's modesty, as well as the Information Technology Act of 2000.

## Cyber hacking:

During the pandemic, people started reading the news online. There are more examples of false news and information now than ever before. After clicking on malicious URLs, the women were the victims of cyber hacking. The malware downloaded all of their personal information to their phones, turned on the microphone and camera, and took their intimate photos and videos. Then, criminals use these bits of information and pictures to carry out extortion and other offenses.[8]

## Kumar v. Whiteley

The accused, i.e Kumar gained unauthorised access to the Joint Academic Network (JANET)and deleted, added files, and changed the passwords to deny access to the authorised users whichled to a loss of Rs 38,248 to the users.

The Additional Chief Metropolitan Magistrate of Chennai sentenced N G Arun Kumar, the accused to undergo rigorous imprisonment for one year with a fine of Rs 5,000 under Section420 IPC (cheating) and Section 66 of the IT Act (Computer related Offense).

## Cyber-bullying:

This includes, sending rape and death threats to the victim and posting false, misleading, and abusive statements about the victims on social media sites, and demanding money to have them removed. It also includes leaving hurtful comments on the victim's posts[9].

[8] Atul Jain, Cyber Crime- Issues, Threats and Management (Chawla Offset Press, Delhi 1005)

[9] https://timesofindia.indiatimes.com/readersblog/aashank-dwivedi/crime-against-women-through-social-media- 48132/last seen on 29/03/2023

ISSN: 2582-6433

# Legal Provisions Dealing With Cyber Crimes In India

Despite the lack of a comprehensive regulatory framework for laws governing the cyber realm, including such conduct, particular legal remedies pursuant to various statutes may assist victims of cyber violence.

## The Indian Penal Code 1860

Prior to 2013, there was no law specifically addressing online abuse or crimes against women in cyberspace. Section 354A of the 2013 Criminal Amendment Act amends the Indian Penal Code, 1860 by adding Sections 354A to 354D.

**Section 354A**: A man who commits any of the following events – a demand or plea for sexual services; or displaying pornography against a woman's will; or making sexual remarks – commits sexual harassment and may be penalized with stringent imprisonment for a period up to 3 years, or with a fine, or with both. In the instance of the first two, and with a period of imprisonment for a period of up to one year, or by a fine, or with the both.

**Section 354C:** It defines 'voyeurism' as the act of photographing and/or publishing a picture of a woman engaged in a private act without her consent. To qualify as 'Voyeurism,' the conditions must be such that the lady would "typically expect not to be seen, either by the offender or by any person acting at the perpetrator's direction." A person convicted underneath this sectionfaces a fine and up to three years in prison on the first conviction and 7 years on successive convictions.

**Section 354D:** Added a stalking prohibition that includes online stalking. Stalking is described as an act in which a male pursues or contacts a woman despite the woman's evident disinterest insuch contact, or watches a woman's cyber activity or usage of the Web or electronic communication. A man convicted of stalking faces up to three years in prison and a fine for the first offence, and up to five years in prison and a fine for successive convictions.

Besides the specific amendments to the Code, there are a number of other provisions that providefor the reporting of cyber attacks and the prosecution of those who are responsible.. Theseinclude the following:-

ISSN: 2582-6433

**Section 499**: To slander, someone is to commit an act with the goal of slandering their reputation. When committed with the intent to injure the woman's reputation, defamation through the publishing of immediate and clear representation of imputation is punished with imprisonment for a period not exceeding two years, a fine, or both.

**Section 503**: Threats to harm a person's reputation, either to cause her panic or to compel her to modify her course of conduct about whatever she would normally do/not do, constitute criminal intimidation. The act of cyber-blackmailing a person, as was done in the aforementioned example, can be placed within the range of this law.

**Section 507**: This section establishes the maximum penalty for Criminal Intimidation committed by an individual whose identity is unknown to the victim. Any anonymous communication that constitutes criminal intimidation in violation of the preceding Section 503 is penalized under this section.

**Section 509**: Any individual who utters a word, makes a sound or gesture, or displays an object with the intent that such word, sound, gesture, or object is heard or seen by a female and insults her modesty, or intrudes on her privacy, may be charged underneath this section and sentenced toup to three years in prison and a fine. This section may penalize instances of sexual remarks or comments made over the Net, as well as other explicit photos and content that are forcibly transmitted over the web.

## The Information Technology Act 2000

**Section 66C**- Identity theft is a punished offense under Section 66C of the IT Act. This clause would apply to instances of cyber hacking. Under this provision, anyone who uses another person's electronic signature, password, or other unique identifying feature fraudulently ordishonestly faces up to three years in prison and a fine of up to Rs. one lakh.

**Section 66E-** Deals with a person's right to privacy being violated. Capturing, publishing, or sending an image of a person's private area without her agreement, or in circumstances that violate her privacy, is penalized by up to three years in prison and/or a fine.

ISSN: 2582-6433

**Section 67**- Makes it illegal to publish, transmit, or cause the distribution of obscene content and punishes violators with up to three years in prison and a fine on the first conviction and up to five years in prison and a fine on the second conviction.

**Section 67A**- Makes the publishing, transmission, or facilitating the transfer of sexually explicit content a misdemeanour punishable by up to five years in jail and a fine on the first offence, and up to seven years in prison and a fine on the second conviction.

# Emerging Cyber Crime against women in India:

India was catching up with legal response to online activities and infractions when it came up with its first cyber legislation namely, the IT Act, 2000. The Act has been amended in 2008, enforced in 2009 and has responded well to the menace of cyber crime in the country.

The situation currently is more troubling. Internet trolls primarily target women on social media platforms and chat apps like WhatsApp and Instagram. Some of these women's sexual appeal and degree of ability to sexually and attractively offer men were described by trolls in foul language. It is important to recognize that as information communication technology has progressed, traditional physical space crimes like rape, sexual molestation, blackmail, stalking, and other similar offences have taken on a new significance. In both the physical world and the virtual world, privacy is actually dwindling. Women are the group that suffers most in this respect.

Some common forms of cyber crime in India recently in practice includes:

## 1. Offensive speech and expressions on internet targeting women:

In India, Right to speech and expression is not unlimited. Art.19(1)(a)[10] guaranteeing right to speech and expressions has been expanded over time by courts in India within the meaning of eight limitations that are specified in art.19(2) and the latest judgment in Shreya Singhal case where the Supreme court held that a vague law such as S.66A[11] of the IT Act, 2000 which didnot explain the grounds of restrictions of speech cannot stand in a way of exercising right to speech and

[10] Art.19(1)(a) of Constitution of India

[11] IT Act, 2000

ISSN: 2582-6433

expression especially in case of internet speech. As such court specified the criteria by which the speech and expression can be illegal.

**Shreya Singhal v. Union of India**[12], Supreme Court focused upon criteria right for information by free speech, however on part equally big interim was fully ignored. This kind of interim was regarding suffering of women upon internet along with by internet. Suffering of given kind is being made out by misapply of right for expression, speech upon internet. This kind of misuse considering rights, expressions upon internet could turn severely dangerous considering women specifically since internet nature through medium knowledge, that is varied extracted traditional nature print media. In Shreya Singhal's episode additional Solicitor General India discussing considering manifesting relaxed level belonging restriction reasonableness figured out given different internet attributes.

## 2. Trolling and Gender bullying:

The most under-researched issues in the arena of cyber crime against women in India are gender bullying and trolling on the internet.[13] We know the online bullying has attracted much attention of researchers, especially in relation to school children, adolescent children and so on. Even though suicide due to cyber bullying has been found as a common ultimate risk factor even whenboth the bully and his/her victim are children it may be presumed that adults may be more dangerous bullies due to their maturity and exposure to the world as compared with children. Trolling creates hate crimes and brutally destroys the reputation of women.

## 3. Online grooming:

In general, grooming refers to broadening one's perspective, improving one's lifestyle, andpreparing one for a specific role, image, or future education. Online grooming, however, is oneof the most serious offences when it comes to grooming in the digital age. It either directly or tangentially fuels criminal activity aimed at specifically targeting women online.[14]

[12] Shreya Singhal v. Union Of India, AIR 2015 SC 1523.
[13] http://ncrb.nic.in/Stat Publicatios/last seen on 30/03/2023

[14] https://vikaspedia.in/social-welfare/women-and-child-development/women-development-1/legal-awareness-for-women/cyber-crimes-against-women last seen on 2/3/2023

ISSN: 2582-6433

The online 'motivators' performs very dangerous roles. It results in increasing the more crime rates and harms more to the victims.

There are various tactics which are being used by the groomers for finding an appropriate groom who can easily befool the victim and commits the offense easily. Most often while reporting crimes against a woman victim must not only mention about the groomers' role, but also directly speak about the harassment.

Methods, Platforms and Definition of Online Grooming:

Online grooming is basically a process in which two different individuals comes into the contact with each other over the online network. They do not even know each other in real life or they have never met each other. A virtual relation is created between the both. The online grooming aims at targeting the female by doing some sex text, taking nude pictures, using web-cam for recording the video talk forcing the victim to share nude pictures, clips etc.

According to the other report published in NDTV news, a racket running fearlessly on internet had been identified by the police. In which they make the use of the matrimonial sites to grab thebrides and make fake promises only to cheat them financially[15].

Most of the fraudsters befool the girls by pretending themselves as NRIs. Even the report states that they use the fake SIM cards using the foreign number. The report highlighted it with an example of a person who predicts himself as a doctor in front of the victim and also said that heis working in foreign. Therefore, he wins the trust of the victim by being in continuous touch with the victim in the form of communication. The best technique to won over the victim was sending the gifts on different occasions to her address. Later, a huge amount is being asked from her for getting the good packages. Then, after the report done by the victim put the police in the situation to tighten their shoes and found the fraudsters who were involved in this activity and they found that it's in trend to befool innocent female and make their possible use.

[15] https://www.ndtv.com/world-news/facebook-suggests-teenage-girls-to-befriend-middle-aged-men-says-report- 1945627 published on Nov 11, 2018 last seen on 30/03/2023

ISSN: 2582-6433

## Ranjit D. Udeshi v. State of Maharashtra (Hicklin Test Adoption)[16]

In given case, Section 292 which IPC was being questioned as though erratic consideringfundamental right in order to freedom of speech, expression beneath Article 19 considering Constitution of India. Here, Court adhered Hicklin test for upholding its constitutionality since law forcing reasonable obstruction upon right for freedom of speech, expression upon morality and decency grounds, as allowable beneath clause (2) belonging to Article-19. This main clause, in truth, makes over greater fundamental law oppose vulgarity into India.

# CONCLUSION:

Social networking, online shopping, storing data, online studying, every possible thing that man can think of can be done through the medium of internet. Internet is used in almost every sphere. Now, as man have encountered the dark side of internet; therefore to counter the possible ill- effects it is required to have proper knowledge, awareness, law, agency and adequate use of technology. Before 2013, there was no legislation that specifically addressed cyber bullying or crimes against women committed online. To address the matter, Sections 354A to 354D had been added to the Indian Penal Code, 1860. The legal system has implemented a number of laws to combat cybercrime against women as a way to halt the advancement of technology through illicit and unethical means. The government should take steps to report fraudulent websites to theNational Cybercrime Reporting Portal.

[16] Ranjit D. Udeshi vs State Of Maharashtra on 19 August, 1964(1965 AIR 881, 1965 SCR (1) 65)