INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :

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.

ISSN: 2582-6433

CYBER CRIMES TARGETING WOMEN IN INDIA: AN OVERVIEW

AUTHORED BY: SWETA UPADHYAY & PRASHANT KUMAR VARUN
LLM student: Law school ICFAI
The ICFAI University, Selaqui, Dehradun

ABSTRACT: Cyberspace has transformed communication, commerce, and social interaction, but it also increases the risk of cybercrime, especially against vulnerable populations like women and children. This article examines the dimensions of cybercrime against women and highlighting the legal framework, societal implications, and recommendations for addressing this pressing issue.
Nowadays, these crimes have taken on new forms in the cyber world. Instead of just physical harm, women now face cyber-crimes like harassment, bullying, abuse, and blackmailing. With the rise of information technology, cyber-crimes against women have become more common in India. These include things like email harassment, cyber stalking, revenge pornography, morphing, profile cloning and cyber defamation. Sometimes, these crimes don't get reported because people don't know what they can do legally, or a lack of trust in the law enforcement agencies to effectively investigate and prosecute these cases. Unfortunately, current laws in India aren't always effective in dealing with cyber-crimes. There's a need for stricter and more efficient laws to protect women from these digital threats. This article explores the evolution of cybercrime against women in India, examining its various form of cyber crime. And examine the legal provision to combat cyber crime against women in India
The article further highlights the reasons for the growth in cybercrime against women, including legal and sociological factors. Additionally, it discusses the impact of cybercrime on victims, emphasizing the need for comprehensive legal frameworks.

Keywords: Cyber-crime, Information Technology, Cyber Space, Women, Human Rights of Women, Dignity of Women, Cyber stalking, Cyber defamation, Cyber trolling, Pornography,

I. INTRODUCTION:

Human creativity has played a pivotal role in shaping the course of civilization. From ancient times to the present day, our innate curiosity and inventiveness have driven remarkable

ISSN: 2582-6433

breakthroughs and advancements. The discovery of fire stands as one of humanity's earliest achievements, enhancing survival, fostering social connections, and facilitating community growth. The invention of the wheel revolutionized transportation, enabling the movement of people and goods over longer distances and laying the groundwork for modern transportation systems.

In the modern era, the development of the Internet represents a groundbreaking milestone. Initially conceived in the 1960s as a means of communication among military personnel[1], the Internet has since evolved into a global network connecting billions of individuals worldwide. Its transformative impact spans across communication, business, education, and virtually every aspect of contemporary life, fundamentally altering how we interact, collaborate, and access information.

The internet has revolutionized communication, work, and information access, yet it has also introduced new challenges and threats on a global scale. The criminal mentality of human nature has leveraged the internet for malicious purposes, resulting in the proliferation of cybercrime. While these technological advancements have enhanced convenience in our lives, they have also brought about new risks, notably in the form of cybercrime[2].

Law is a dynamic concept[3] which undergoes changes with the changing need of the society. The development of law is a process which continued with the changes and advancement in social circumstances. Law is generally made to meet the needs of the society[4]. Gradually the lawmaker feels the need of strong legislation to regulate the criminal activities on cyber space. Many countries came with laws to regulate cyber-crime. Cybercrime is, a relatively modern form of criminal activity, has emerged as a significant challenge in the contemporary world. It encompasses various illegal activities conducted through computers, the internet, or other technologies.

On the one hand, technology and the cyber-criminal as well as cyber-crime are evolving at warp speed, but on other hand law at best has been developing at snail's pace and too, mostly as a knee-jerk[5].

The emergence of digital technology and the merging of communications and computers has

[1] In 1960, the internet was first created as a tool for interconnection of computer as amongst military personnel known as ARPANER (**Advanced Research Projects Agency Network**) to communicate and share data.
[2] N S Nappinai, Technology law Decoded, 36 (LexisNexis, New Delhi 1st edn., 2024)
[3] Justice Gavai said, "Law is not static, but it is dynamic. Available at https://indianexpress.com/article/cities/pune/law-changes-as-per-needs-of-society-sc-justice-gavai-6017386/#:~:text=During%20his%20speech%2C%20Justice%20Gavai,to%20the%20needs%20of%20society%E2%80%A6
[4] Dr. Ashok Jani, Cyber law (Information Technology Act) p.1, ASCENT Publications 2nd end., 2020.
[5] N S Nappinai, Technology law Decoded, 36 (LexisNexis, New Delhi 1st edn., 2024).

ISSN: 2582-6433

started changing our way of living. There are now greater opportunities for crime than ever before due to these changes. Two decades ago, it seemed unimaginable that criminal activity would occur today. Digital technologies now provide ordinary citizens, even juveniles, with the capacity to inflict massive harm. These incredible technological advancements have already had an immense impact on many of aspects of life.

Common types of cybercrime against women in India include hacking, stalking, cheating by impersonation, voyeurism, pornography, obscenity, and indecent representation of women in the cyber space. These crimes are committed through social networking sites, unlawful and uncivil networking sites, and other cyber platforms.

Women are particularly vulnerable to these crimes due to their addiction and over-dependence on internet, computer applications, information technology, and social networking sites. Cybercrimes against women have been increasing in India, and there is a need for greater awareness and education to prevent and address these crimes. The Indian Information Technology Act and 2000 have some loopholes that need to be addressed to ensure the safety and security of women in cyberspace.

II. BRIEF HISTORY OF CYBER CRIME AGAINST WOMEN IN INDIA:

IT CAN BE EVIDENTLY THAT WHEN INDIA STARTED HER JOURNEY IN THE FIELD OF INFORMATION TECHNOLOGY. THE DRAFTERS OF THE INDIAN INFORMATION TECHNOLOGY ACT, 2000, CREATED IT ON THE INFLUENCE OF THE MODEL LAW ON ELECTRONIC COMMERCE, WHICH WAS ADOPTED BY THE RESOLUTION OF THE GENERAL ASSEMBLY OF THE UNITED NATIONS IN 1997[6]***.***

THE ACT TURNED OUT TO BE A HALF-BAKED LAW AS THE OPERATING AREA OF THE LAW STRETCHED BEYOND ELECTRONIC COMMERCE TO COVER CYBER-ATTACKS OF NON-COMMERCIAL NATURE ON INDIVIDUALS AS WELL. WHILE COMMERCIAL CRIMES AND ECONOMIC CRIMES WERE MODERATELY MANAGED BY THIS ACT, IT MISERABLY FAILED TO PREVENT THE GROWTH OF CYBER-CRIME AGAINST INDIVIDUALS, INCLUDING WOMEN. Before the passage of the Information and Technology Act 2000, the punishment for Cyber Crime was given under the Indian Penal Code 1860.

III. MEANING AND DEFINATION OF CYBER CRIME:

Cybercrime generally termed, as offences committed by using computer or where the computer

[6] Available at https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce.

ISSN: 2582-6433

is the victim or merely facilitator for commission of an offences[7]. The Indian Legislature has not defined cybercrime in any statute, including the Information Technology Act of 2000 and its subsequent amendment act 2008, which specifically addresses cybercrime issues.

In other hand The Kerala Government's draw a comprehensive definition of "cybercrime" as "any criminal activity in which a computer or network is the source, tool or target or place of crime[8]. There are several other definitions which try to explain the cybercrime.

The Black's Law Dictionary defines "Computer Crime" as "A crime involving the use of a computer, such as sabotaging or stealing electronically stored data Also termed cybercrime"[9].

The oxford Dictionary defined the term cyber-crime as "Criminal activities carried out by means of computers or the Internet[10].

The Saudi Arabian Legislation has codified definition of "cybercrime" is defined as:

"Any action which involves the use of computers or computer networks, in violation of the provisions of this Law"[11].

Unfortunately, the current definitions and descriptions of cybercrime do not encompass the complexity and nuances of cybercrime against women.

IV. CYBER CRIME CAN BE BROADLY DIVIDED INTO THREE (3) CATEGORIES:

Cyber-crimes can be broadly divided into three major Categories[12] –

1. Cyber-crimes against persons, first category include various crimes like transmission of obscene messages, harassment of anyone with the use of a computer such as e-mail, cyber-bullying and cyber-stalking.
2. Cyber-crimes against Property, the second category of is that of Cyber-crimes against all forms of property. These crimes include illegal and unauthorized computer trespassing, and transmission of important and critical information outside the organization which can lead to a great loss to the organization.
3. Cyber-crimes against Government. The third category of Cyber-crimes relate to Cyber-crimes against Government which includes Cyber Terrorism[13], Cyber-Warfare and Cyber Espionage.

[7] N S Nappinai, Technology law Decoded, 36 (LexisNexis, New Delhi 1st edn., 2024).
[8] Available at http:// www.img.kerala.gov.in/docs/downloads/cyber%20crimes.pdf.
[9] Black's Law Dictionary (9th ed.) defines crime as "An act that the law makes punishable, the beach of a legal duty treated as the subject matter of a criminal proceeding Also termed criminal wrong.
[10] Available at http://www.oxforddictionaries.com/definition/english/cybercrime
[11] Article 1(8) Saudi Arabia Anti-Cyber Crime Law, Royal Decree No. M/17.
[12] Nidhi Agarwal & Dr. Neeraj Kasuhik, "Cyber Crime Against Women", GJRIM VOL.4, NO.1, 2014.
[13] Section 66F, of the Information Technology Act 2000.

ISSN: 2582-6433

V. CYBER CRIME AGAINST WOMEN:

1. **Cyber Bullying**: For the First time "The Canadian named Bill Belsey" defined the term cyberbullying[14].

   a term coined by Canadian Bill Belsey to describe 'the use of information and communication technologies to support deliberate, repeated, and hostile behavior by an individual or group, that is intended to harm others'[15].

   Harassing or insulting victims using electronic or communication devices such as computer, mobile phone, laptop, etc. or digital platform.

2. **Cyber Stalking:** Indian Penal Code Amendment 2013, Section 354D[16] talk about the term stalking. Cyber stalking means any man, follow a woman physically, tracing her movement or repeatedly tries to communicate her without her interest through internet or electronic or communication devices such as computer, mobile phone, laptop, etc. or digital platform. Cyber stalking is a way to use the Internet to stalk someone for online harassment and online abuse. Cyber Stalking is a punishable offence and attracts section 354 (D), 509 Indian Penal Code 1860, and section 67[17] under Information Tecnology Amendment Act 2008.
3. **Harassment through e-mails**: As name suggest harassment of the victims through e-mails and is not a new concept. It includes blackmailing, threatening, bullying, and even cheating via email.
4. **Cyber Defamation**: Black's law dictionary, defamation means, "the offense of injuring a person's character, fame, or reputation by false and malicious statements[18]". In simple words, defamation is an injury to the reputation of another person. There are two form of defamation Libel and Slander. Libel is a published/written defamation which is in permanent form. On the other hand, Slander is oral or by gesture which is temporary

[14] Available at https://billbelsey.com/?cat=13
[15] Available at https://extensionpubs.unl.edu/publication/1056/html/view#:~:text=Bill%20Belsey%2C%20creator%20of%20www,threaten%20or%20terrify%20an%20individu.
[16] Section 354 of the IPC states:
(1) Any man who—
(i) follows a woman and contacts, or attempts to contact such woman to foster personal interaction repeatedly despite a clear indication of disinterest by such woman; or
(ii) monitors the use by a woman of the internet, email or any other form of electronic communication,
commits the offence of stalking;
[17] Section 67 of the act attracted only when person publishes or sends salacious material through electronic or communication device or Internet.
[18] Available at https://thelawdictionary.org/defamation/.

ISSN: 2582-6433

form. Libel is actionable per se where Slander requires actual damage. Cyber defamation includes both libel and Slander.

5. **E- Mail Spoofing**: it generally refers to an e-mail that emerges from one source but has been sent from another source. It can cause monetary damage.
6. **Cyber Phishing**: Phishing where cyber criminals pretend as genuine service provider and try to collect the vital personal data such as password, username, bank details etc. of the victims, for financial gain. When phishing is conducted through mobile i.e. SMS it is called as Smishing, and if done through calling it is known as Vishing[19].
7. **Cyber Morphing**: Morphing is a new era cybercrime, it uses animation technology by criminals to morph (edit) the original picture of any person (women) and posted in social networking websites or digital platform.
8. **Cyber Pornography**: The term 'pornography' means any portrayal of sexual subject matter for the purpose of sexual satisfaction. In a legal sense, Pornography means "*obscenity*". The word obscene has not been defined in IPC as the concept of obscenity differs from society to society and from time to time[20]. But the test of obscenity laid down in the English decision, the landmark Hickling Case[21] is the basis of the test of obscenity given in Section 292(1)[22]. Section 67[23] which covers 'obscene act or conduct in general, Section 67A[24] specifically covers sexually explicit act or conduct and 67B[25] exclusively deal with child pornography.

VI. LEGAL INSTRUMENTS FOR COMBATING CYBER CRIME AGAINST WOMEN:

1. THE CONSTITUTION OF INDIA, 1950: The supreme law of the land protects the women against cybercrime. Article 19 and 21 provides protection to women. Fundamental right to speech and expression is protected under Article 19(1)(a) of the constitution. The right to speech and expression is not absolute and is subject to reasonable restrictions under Article 19(2). The

[19] Dr. Kanika Seth, (Computer, Internet and New Technology laws,00, LexisNexis, 3rd end, 2022
[20] PSA Pillai, Criminal Law 701,703 (K. I.Vibhute ed., 2009).
[21] R.v. Hicklin, (1868) LR 3 QB 360.
[22] Section 292(1) Indian Penal Code 1860.
[23] Section 67 of the Information Technology Act 2000, Punishment for publishing or transmitting obscene material in Electonic form.
[24] Section 67A of Information Technology Act 2000, Punishment for publishing or transmitting of material containing sexually explicit act, etc.
[25]Section 67B of Information Technology Act 2000, Punishment for publishing or transmitting of material depicting children in sexually explicit act.

ISSN: 2582-6433

right to live with human dignity[26] in cyber space is also protected under Article 21 of the constitution of India[27].

2. INDIAN PENAL CODE 1860: ***INDIAN PENAL CODE 1860 NOT ESPECIALLY DEALS WITH THE CYBERCRIME, BUT THE AMENDMENT ACT 2013 INSERTED*** section specifically deals with cybercrime related to women.

i. Obscenity and Pornography: section 292 to 294, 354A, 354B,354C, 509
ii. Section 354- Outraging the modesty of women
iii. Section 354A-Sexual Harassment
iv. Section 354C-Voyeurism (this inserted after Nirbhaya Rape Case,2012)
v. Section354D-Stalking
vi. Section 509- Word, gesture or act intended to insult women modesty

3. INFORMATION TECHNOLOGY ACT 2000:

Chapter IX of the Act covers penalties, compensation, & adjudication. According to Section 43 the person who harms the computer systems shall be liable to pay damages by way of compensation to the affected person.

i. Sections are 66A for Sending offensive messages through communication service,
ii. Section 65 for Tampering with computer source documents,
iii. Section 70 for Tampering of confidential information,
iv. Section 72 for Online stalking,
v. Section 42A and Section 66 of IT Act, 2000(r/w Section 379,406 of IPC, 1860) for Data hacking,
vi. Section 43B,66E and 67C for Data Theft,
vii. Section 67A for Pornography.
viii. Section 67B for Child Pornography

VII. LEADING CASE LAWS

[26] In Maneka Gandhi v. Union of India, the Supreme Court held that the right to live is not merely a physical right but includes within its ambit the right to live with human dignity.
[27] Protection of life and personal liberty No person shall be deprived of his life or personal liberty except according to procedure established by law.

ISSN: 2582-6433

Regina v Hicklin,'[28] as the tendency "to deprave and corrupt those whose minds are open to such immoral influences and into whose hands a publication of this sort may fall", and it was understood that this test would apply only to isolated passages of a work. Those "whose minds are open to such immoral influences primarily meant the young, as Lord CJ Cockburn explained in his Hicklin opinion, the danger of prurient literature was that it "would suggest to the minds of the young of either sex, and even to persons of more advanced years, thoughts of a most impure and libidinous character"

The test was slightly modified in United States v One Book Entitled "Ulysses"[29] "The superior court held that the criterion for obscenity was not the content of isolated obscene passages but rather "whether a publication taken as a whole has a libidinous effect". In Roth v United States,[30] the US Supreme Court tendered a basic redefinition of obscenity: "whether, to the average person, applying community standards, the dominant theme of the material taken as a whole appeals to prurient interests".

Whereas in Miller v California, the US Supreme Court declared that the states might prohibit the printing or sale of works, "which appeal to prurient interest in sex, which portray sexual conduct in a patently offensive way, and which, taken as a whole, do not have serious literary, artistic, political or scientific value".

In Miller v California,[31] the US Supreme Court set-out a three-prong test for obscenity, called the "Miller Test":

i. Whether "the average person", applying contemporary community standards would find the work, taken as a whole, appeals to the prurient interest,
ii. Whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by state law,
iii. Whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value.

In Ranjit Udeshi State of Maharashtra[32], case established a modified version of the Hicklin test as the test for obscenity in India. The Supreme Court has observed that the rest obscenity laid down by Cockburn C) should not be discarded. It held, "that the test of obscenity to adopt in India is that obscenity without a preponderating social purpose or profit cannot have the constitutional protection of free speech and expression and obscenity in treating sex in a manner appealing to

[28] Regina v Hicklin, (1868) 3 QB 360.
[29] United States v One Book Entitled "Ulysses", 72 NY 705. (1934).
[30] Roth v United States, 354 US 476 (1957).
[31] Miller v California, 413 US 15 (1973).
[32] AIR 1965 SC 881

ISSN: 2582-6433

the carnal side of human nature or having that tendency[33].

In the subsequent cases, the Supreme Court, further articulated on the test for obscenity. In Chandrakant Kalyandas Kakodkar v State of Maharashtra,[34] and others, the court held:

What is obscenity has not been defined either in section 292 IPC or in any of the statutes prohibiting and penalizing, mailing, importing, exporting, publishing and selling of obscene matters It is the duty of Court to consider the obscene matter by taking an overall view of the entire work and to determine whether the obscene passages are so likely to deprave and corrupt those whose minds are open to influences of this sort and into whose hands the book is likely to fall and in doing so one must not overlook the influence of the book on the social morality of our contemporary society.[35]

In Samaresh Bose v Amal Mitra[36], the court held that "the concept of obscenity would different from country to country depending on the standards of morals of contemporary society". The bout differentiated between "vulgarity" and "obscenity":

"*A vulgar writing is not necessarily scene. Vulgarity arouses a feeling of disgust and revulsion and also boredom but does nor bare the effect of depraving, debasing and corrupting the morals of any reader of the novel, whereas obscenity has the tendency to deprave and corrupt those whose minds ateopen to such immoral influence"*

VIII. REASON FOR GROWTH IN CYBER-CRIME AGAINST WOMEN:

Cybercrime, a significant threat to society, primarily affects women and children. The information of net surfers is easily disclosed by cybercafé owners, leading to illegal activities. Although technology is beneficial for development, it is also increasing the crime rate against weaker sections of society. The increasing cyber-crime rate against women can be attributed to two main reasons: legal reasons, such as the Indian IT Act 2000, which aims to combat cybercrimes, and sociological reasons, such as the fear of defamation of family names and the anonymity of perpetrators. Many women in India do not report cyber-crimes, fearing it may disturb their family life[37].

IX. *MPACT OF CYBER-CRIME ON VICTIMS:*

[33] Ranjit Udesin v State of Maharashtra, AIR 1965 SC 881 (1965) 2 Cr LJ 8: (1965) | SCR 65 (SC)
[34] AIR 1970 SC 1390
[35] Chandrakant Kalyanda Kakodkar v State of Maharashtra, AIR 1970 SC 1390: 1970 (2) SC) 217: (1970) 2 SCR 80
[36] Samaresh Bose v Amal Mitra, AIR 1986 SC 967: (1985) 4 SCC 289: 1986 C: LJ 24.
[37] Dr. Kasturi Bora," CYBER SOCIALIZING AND THE GROWTH OF HI-TECH CRIMES AGAINST WOMEN" (I.S.S.N 2321- 6417 (Online).

ISSN: 2582-6433

The internet has become a crucial tool in modern life, providing knowledge and efficient tasks. Despite the Covid pandemic increasing internet reliance, cyber-crime remains a significant threat, negatively impacting daily lives. Despite its positive impact, it is essential to address cyber crime's threats. Cyber-crime is a non-traditional threat utilizing computers for illegal activities, aiming to cause physical or mental harm through the internet and modern telecommunication networks. The threat of cyber-crime has risen due to the increased usage of the internet and reliance. The term cybercrime encompasses a wide range of crimes including cyber stalking, cyber harassment, email spoofing, defamation, and morphing of pictures[38].

With the increasing popularity of Artificial Intelligence (AI), technologies such as deep fakes which can manipulate facial expressions of people in pictures and videos using deep generative techniques pose a significant threat to people on the internet leaving them vulnerable[39]. The motive of cyber-crime is to directly or indirectly cause physical or mental harm to an individual or group of people using the internet and other forms of modern telecommunication networks.

X. CONCLUSION:

The primary challenge associated with cybercrime is its dynamic nature, driven by the continuous evolution of digital technology. As the internet continues to evolve and permeate every aspect of daily life, the risk of digital threats such as cyberbullying, stalking, defamation, and harassment has escalated, disproportionately affecting vulnerable populations like women. Despite the existence of legal frameworks such as the Indian Penal Code and the Information Technology Act, the current laws often fall short in effectively addressing the complexities of cyber-crimes against women.

In 2008, provision of punishment was made in the Information Technology Act, 2002 by including new Cyber Crimes. In view of the changing nature of Cyber Crime at present, there is still a need to make changes to the Information Technology Act, 2000. This act is still not able to provide full punishment for Cyber Crime against women. A separate law needs to be made. A comprehensive data protection regime needs to be incorporated in the law to make it more effective. Special training must be given be the officers to deal with the cyber-crime against women.

To safeguarding the rights and dignity of women in cyberspace requires a multi-faceted approach

[38] Misra, R. (2013, April 10). *Cyber Crime Against Women*.

39 Written by Jahnavi Chopra" Cyber Crime and it's Impact on the Lives of Women" Available at https://medium.com/@leveledlegislationldn/cyber-crime-and-its-impact-on-the-lives-of-women-b84d29c5814a#:~:text=As%20a%20result%2C%20people%20develop,crime%20try%20to%20commit%20suicide

ISSN: 2582-6433

that combines robust legal frameworks, awareness campaigns, support systems, and proactive measures to address the ever-evolving challenges of cybercrime. Only through concerted efforts and collective action can we create a safer and more inclusive digital environment for all women in India.

SUGGESATION:

For Users

i. A User must use a strong password minimum 12 characters which contain upper case and lower case at list one special or numeric character.
ii. A User must update the software frequently.
iii. Using anti-virus in a device, it can help to detect and prevent malware.

For Government

iv. The government should launch comprehensive awareness programs in collaboration with cybersecurity experts to educate the public about preventive measures against cybercrime.
v. These awareness programs should be designed to inform citizens about the various types of cyber threats targeting individuals, particularly women, in the Indian.
vi. The awareness programs should cover topics such as safe internet practices, recognizing phishing attempts, securing personal devices and online accounts, and responding to cyberbullying and harassment.
vii. Utilizing various platforms such as workshops, seminars, webinars, and social media campaigns, the government can reach a wide audience and promote cyber
viii. The government should issue a helpline number for cyber-crime victims.

REFERENCE:

A. BOOKS:
1. K. Jaishankar, Cyber Criminology: Exploring Internet Crimes and Criminal 2011
2. Dr. Vishwanath Paranjape, Legal Dimensions of Cyber Crimes and Preventive Laws, (Central Law Agency, Allahabad, 2010).
3. Debarati Halder and K. Jaishankar, "Cyber Crime and Victimization of Women",information science reference, ed1st 2012
4. Vakul Sharma and Seema Sharma,,Information Technology law and Practice, P318, LexisNexis, Eight Eidition,2023.
5. N S Nappinai, Technology law Decoded, 36 (LexisNexis, New Delhi 1st edn., 2024).

ISSN: 2582-6433

6. Dr. Kanika Seth, (Computer, Internet and New Technology laws,00, LexisNexis, 3rd end, 2022
7. Dr. Ashok Jani, Cyber law (Information Technology Act) p.1, ASCENT Publications 2nd end., 2020.

B. STATUTES:

1. INDIAN CONSTITUTION 1950
2. INFORMATION TECHNOLOGY ACT 2000
3. INDIAN PENAL CODE 1860
4. EVIDENCE ACT 1872
5. PROTECTION OF CHILDREN FROM SEXUAL OFFENCES ACT 2012
6. INDECENT REPRESENTATION OF WOMEN (PROHIBITION) ACT, 1986

C. ARTICLES:

1. Agarwal, M. (2022). Cybercrimes against women in India: A review of literature. Journal of Criminology and Criminal Justice, 14(1), 71-84.
2. Gupta, S. (2021). Cybercrimes against women in India: A study of the challenges and opportunities. Journal of Law, Technology and Policy, 14(2), 1-22.
3. Abbasi, A., & Abbasi, M. (2022). Cybercrimes against women: A global perspective. Journal of Cyber Security and Law, 7(1), 1-16.
4. Gupta, A., & Singh, S. (2019). Cybercrimes against women: A global perspective. Journal of Criminology and Criminal Justice, 11(3), 235-252.
5. Kumar, A., & Yadav, A. (2021). Cybercrimes against women: A study of the challenges and opportunities. Journal of Law, Technology and Policy, 14(3), 1-22.
6. National Crime Records Bureau. (2022). Cybercrime in India, 2020. Ministry of Home Affairs, Government of India.
7. Jaspreet Singh, VIOLENCE AGAINST WOMEN IN CYBER WORLD: A SPECIAL REFERENCE TO INDIA "International Journal of Advanced Research in Management and Social Sciences" (ISSN: 2278-6236)

D. INTERNET SOURCES

ISSN: 2582-6433

1. https://www.meity.gov.in/writereaddata/files/The%20Information%20Technology%20Act%2C%202000%283%29.pdf
2. https://www.meity.gov.in/writereaddata/files/The%20Information%20Technology%20Act%2C%202000%283%29.pdf
3. https://www.ijfans.org/uploads/paper/374cf990d6568e78319acc782da1
4. https://blog.ipleaders.in/overview-of-concept-of-cyber-bullying-in-india/#Cyberbullying_in_India
5. https://blog.ipleaders.in/cyber-stalking/
6. https://www.legalserviceindia.com/legal/article-3042--types-of-cyber-crime-and-its-causes.html
7. https://www.hindustantimes.com/india-news/cybercrimes-see-highest-spike-among-cognisable-offences-in-2022-says-ncrb-101701714486481.html.
8. https://economictimes.indiatimes.com/news/india/cases-targeting-women-with-explicit-content-double-in-3-years/articleshow/88719638.cms
9. https://vikaspedia.in/social-welfare/women-and-child-development/women-development-1/legal-awareness-for-women/cyber-c
10. https://onlinelibrary.wiley.com/doi/abs/10.1002/spy2.340
11. https://www.livelaw.in/cyber-crimes-against-women-and-laws-in-india/
12. https://docs.manupatra.in/newsline/articles/Upload/CE3E0AE8-DE2B-41EA-92A2-8A46035DECEB.pd
13. https://www.legalserviceindia.com/legal/article-8382-the-evolution-of-cyber-crime.html
14. https://blog.ipleaders.in/cyber-crime-laws-in-india/
15. https://legalserviceindia.com/legal/article-15164-evolutionary-theory-of-law-a-study.html
16. https://www.legalserviceindia.com/legal/article-4883-understanding-the-law-as-a-means-of-social-change.html