INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIALTEAM

EDITORS

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

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

ISSN: 2582-6433

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

ADDRESSING LEGAL DEFICIENCIES IN INDIA'S CYBERCRIME LAWS

AUTHORED BY - DR. PRIYANKA PURI
Assistant Professor Laws
Rayat Bahra Professional University, Hoshiarpur, Punjab, India

ABSTRACT

Cyber-crime mainly involves activities that use internet and computers as a tool to extract private information of an individual either directly or indirectly and disclosing it on online platforms without the person's consent or illegally with the aim of degrading the reputation or causing mental or physical harm. With the advancement in technology a steep increase in the rate of cyber-crimes has been observed. With the increase of dependency on cyberspace internet crimes committed against women have also increased. This is mainly because around more than half of the online users are not fully aware of the functioning of online platforms, they are ignorant towards technological advancements and have minimal adequate training and education. Thus, cybercrime has emerged as a major challenge for the law enforcement agencies of different countries in order to protect women and children who are harassed and abused for voyeuristic pleasures. Women are commonly targeted for cyber stalking, cyber pornography, impersonation etc. India is one of the few countries which has enacted the IT Act 2000 to deal with issues pertaining to cyber-crimes in order to protect the women from exploitation by vicious predators however this act doesn't address some of the gravest dangers to the security of the women and issues involving women are still growing immensely.

Keywords: Cybercrime, Women, It Act, technology, law

I. INTRODUCTION

This is an Era we are most things in the world happen on internet ranging from internet management to online transactions. Because website is considered a global platform so anyone can access our resources from anywhere on the internet. Many people use internet technology for committing crimes like unauthorised access to website or committing frauds etc.

The unique thing about cyber crime is that the victim and preprietor may never meet. criminals

ISSN: 2582-6433

often choose operating countries with weak or non existent laws to reduce the chances of detection and prosecution. The term "cyber law" was introduced to stop or punish such kind of Cyber criminals. Internet law can be defined a part of legal system that operates on the internet.[1]

Computers of made a person's life easier and is helpful in making a variety of applications worldwide from individual to large organisations. Briefly it can be defined as a machine that stores and can process information or instructions given by the user.

Cybercrimes can be defined as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including chat rooms, emails, notice boards and groups) and mobile phones".

Cyber-crime involves the use of internet and computer. It threatens an individual's privacy by disclosing or publishing their personal or confidential information online with the aim of degrading their reputation and causing them physical or mental harm either directly or indirectly. Women are generally the targets of these offenders because they are inexperienced and lack knowledge of the cyber world, thereby falling prey to the technological fancies.

II. HISTORY AND EVOLUTION

Human civilization has come a long be from the abacus to modern supercomputer. This transition is one of the most important human activities as it changes the way of life and affect the lights of everyone except the choice of a few people living far away. Although this transaction took time long enough for technological evolution to occur. Cyber criminals have evolved over time and adapted this strategy according to the advancement of technology in committing cybercrime. Technically, criminals prefer to operate in cyber space as no actual activities involved in cyber crime as financial rewards and risk of arrest due to unknown factors involved in cyber crime on the Internet. Cyber criminals have used sophisticated propaganda to promote the sustainable development of the country. There has winner increase of world wide use of Internet in recent years the more people connect to the e-world the greater the chance of phoenix force to malware viruses and pishing attacks.

[1] Debarati Halder & K. Jaishankar, *Cyber Crimes Against Women in India* (SAGE Publications India Pvt. Ltd., New Delhi, 2016).

ISSN: 2582-6433

III. TYPES OF CYBER CRIME

- **Cyberstalking**

In today's modern world, it is one of the most commonly committed crimes. It involves following a person's movements and pursuing him/her stealthily. It involves gathering data that maybe used to harass a person or making false accusations or threats. A cyber stalker uses internet to stalk someone and thus, doesn't pose a direct physical threat to an individual but due to the anonymity of the interactions that take place online the chances of identification of the cyber stalker becomes quite difficult which makes this crime more common than physical stalking.

One of the major targets of cyber stalking is women and children who are stalked by men and adult predators namely, for revenge, for sexual harassment and for ego. Most of the times, the victim is unaware of the use and rules of the internet and the anonymity of the users has contributed to the rise of cyber stalking as a form of crime. The offender for committing this offence maybe charged for breach of confidentiality and privacy under section 72 of the IT Act, 2000 as cyber stalking is yet not covered under existing cyber laws in India. Also, section 441 and 509 of IPC are also applicable for the same.

- **Cyber Pornography**

It is a major threat to women and children security as it involves publishing and transmitting pornographic pictures, photos or writings using the internet which can be reproduced on various other electronic devices instantly. It refers to portrayal of sexual material on the internet.

According to A.P. Mali, "It is the graphic, sexually explicit subordination of women through pictures or words that also includes pornography is verbal or pictorial material which represents or describes sexual behaviour that is degrading or abusive to one or more of participants in such a way as to endorse the degradation. The person has chosen or consented to be harmed, abused, subjected to coercion does not alter the degrading character of such behaviour." Around 50% of the total websites on the internet show pornographic material wherein photos and pictures of women are posted online that are dangerous to women's integrity.

According to IT Amendment Act 2008 "crime of pornography under section 67-A, whoever publishes and transmits or causes to be a published and transmitted in the electronic form any material which contains sexually explicit act or conduct can be called as pornography. Section 292/293/294, 500/506 and 509 of Indian Panel Code, 1860 are also applicable and victim can file a complaint near the Police Station where the crime has been committed or where he comes

ISSN: 2582-6433

to know about crime. After proving crime, the accused can be called as first conviction with an imprisonment for a term which may extend to five years including fine which may extend to ten lakh rupees. In the second conviction the term of imprisonment may extend to seven years and fine may extend to ten lakh rupees".[2]

- **Cyber Morphing**

It is a form of crime in which the original picture is edited by an unauthorised user or a person possessing a fake identity. Photographs are taken of female users from their profiles and are then reposted for pornographic purposes by fake accounts on different sites after editing them. Due to the lack of awareness among the users the criminals are encouraged to commit such heinous crimes. Cyber morphing or Cyber obscenity is punishable under section 43 and 66 of Information Act 2000.

- **Cyber Bullying**

Cyberbullying involves the use of internet for causing embarrassment or humiliation to someone place by sharing their personal or private data by sending, posting or sharing harmful or false content over digital devices like computers, tablets, laptops and cell phones. It can take place through SMS, online gaming communities, online forums or social media platforms wherein information can be exchanged online and is available to a number of people. Cyberbullying is persistent and permanent and therefore, can harm the online reputation of not just the victim but both the parties involved. [3]

- **Email Spoofing and Impersonation**

It is one of the most common cybercrime. It involves sending e-mail which represents its origin. In today's times, this from of crime has become immensely common that it becomes really difficult to assess as to whether the mail that is received is truly from the original sender. Email spoofing is mostly used to extract personal information and private images from women fraudulently and are later used to blackmail them.

Email spoofing is an offence under section 66-D of the Information Technology Amendment Act, 2008 and section 417, 419 and 465 of Indian Panel Code 1860. It is a cognizable, bailable

[2] Prashant Mali, *Cyber Law & Cyber Crimes Simplified: with The Information Technology Act, 2000* (Cyber Infomedia, Mumbai, 6th edn., 2018).

[3] **Violence" Online in India: Cybercrimes Against Women and Minorities on Social Media**, Japleen Pasricha, *Feminism in India* (2016), available at [FII cyberbullying report] (http://feminisminindia.com/wp-content/uploads/2016/05/FII_cyberbullying_report_website.pdf).

ISSN: 2582-6433

and compoundable offence with permission of the court before which the prosecution of such offence is pending and triable by any magistrate.

- **Online Trolling**

It is a form of online violence on social media platforms where people are given the liberty to speak their mind. Online harassers often tend to target people who express their opinions and think differently from the prevailing societal norms. On such section constitutes of females who are targeted by social media bullies.

Social media bullying takes a toll on the mental as well as the physical health of the victims. Abuse, hate speech and mean comments are the most common elements of trolling. The most common consequences of trolling are self-censorship and mental health concerns. [4]

IV. THE LEGAL FRAMEWORK

There are two unique features of the Internet. Firstly, it is not confined to a particular boundary and the cyber-criminal can commit a crime from ay part of the world. The second unique feature is that it provide anonymity to its users which has its own boon and bane. For people who use this anonymity for putting out their opinion to the world it's a boon but the perpetrators who use this anonymity for commission of crime it is a bane. Therefore this features not only pose a challenge in crime prevention but also in the implementation of law. At present there is no specific law that deals with cyber-crime against women. Other laws which can be used in the specific case, most women are not aware of. Women does not know about their rights or that such rights exist.

There are many laws in statues and regulations which penalises cyber-crime. But the majority of the laws belong to the Indian penal Code (IPC), 1860 and the Information technology Act (IT Act), 2000. The IPC is the general criminal code of India which defines offences and prescribes punishment for the same. IPC covers laws and punishment pertaining to physical world and has been legislatively amended and judiciously interpreted to be applicable to cyber criminals.[5] Whereas the IT Act is a specific code pertaining to use of information technology and crime committed through it. In 2008 IT Amendment Act was enacted inclusive of certain crimes related to cyber world. Both IT Act and IPC are complementary to each other on cyber-crime against women. The below mentioned table is taken from a discussion paper published

[4] **Trolls Target Women: Dealing with Online Violence**, *The Citizen*, 21 January 2021.
[5] **Indian Penal Code, 1860** (repealed and replaced by **Bharatiya Nyaya Sanhita, 2023**, effective 1 July 2024).

ISSN: 2582-6433

by IT for Change it showcases the laws that a cyber-criminal can be charged with when he/she commits a crime against women. Following which the loopholes in the said laws is analysed.[6]

Act	**Clause**	**Details of the offence this provision addresses**	**What forms of online VAW can this provision help in challenging?**
IT Act	Section 66E	The capture and electronic transmission of images of private parts of a person, without his/her consent.	– Non-consensual circulation and malicious distribution of sexually explicit photographic and video material about an individual.
	Section 67	The publishing or transmission of obscene material in electronic form.	– Graphic sexual abuse on social media and blog platforms, including trolling. – Sending emails/social media messages with sexually explicit content and images to an individual, against his/her will.
	Section 67A	The publishing or transmission of sexually explicit content in electronic form.	– Graphic sexual abuse on social media and blog platforms, including trolling. – Sending emails/social media messages with sexually explicit content and images to an individual, against his/her will.
	Section 67B	The electronic publishing or transmission of material in electronic form that depicts children in obscene or indecent or sexually explicit manner.	– Circulation of child pornography
IPC	Section 354 A	Sexual harassment, including by showing pornography against the will of a woman	– Graphic sexual abuse on social media and blog platforms, including trolling. – Sending video and pictures with sexually explicit content and images to a woman, against her will.
	Section 354 C	Voyeurism, including watching or capturing the	– Non-consensual production, circulation and malicious distribution of sexually

[6] The Information Technology Act, 2000 (Act 21 of 2000).

ISSN: 2582-6433

		image of a woman engaging in a private act in circumstances where she would have a reasonable expectation of not being observed; and dissemination of images of a woman engaging in a private act under circumstances where she has agree to the capture of images but not to their dissemination.	explicit photographic and video material about a woman.
	Section 354D	Following a woman, contacting/ attempting to contact her to foster personal interaction repeatedly despite a clear indication of disinterest by such woman, or monitoring the use by a woman of the Internet, email, or any other form of electronic communication	– Cyber-stalking. Only women are recognized as potential victims by the law.
	Section 499	Criminal Defamation that leads to reputational harm	-Though this is a gender neutral provision, it could be invoked by women bloggers and women on social media fighting slander and libel.
	Section 507	Criminal intimidation by anonymous communication	– Though this is a gender neutral provision, it could be invoked by women fighting trolls issuing threats, whose identities are often anonymous.
	Section 509	Word, gesture, act or exhibition of an object intended to insult the modesty of a woman.	– Though this provision does not explicitly address online sexual harassment and abuse, it could be invoked in such cases.

ISSN: 2582-6433

V. STEPS TO PREVENT CYBER CRIMES

Following are some steps suggested that people can take to prevent cyber crime:-

- **You strong passwords:** The first line of defence in security is password protection. These maybe the words you see most often every time will login to your account but a strong password makes a big difference in the security of once account. This is a special important when it comes to Cyber stocking (someone searching for all your information or your computer or social media) and hacking (an authorised assess to your computer or information). You can also protect your password by using a secure password generator or by ensuring that the password you choose contains a combination of letters, numbers and symbols. People who are unaware of this fraud also fall into the strap.
- **Never provide your credit/debit card information to insecure site:** If the payment site does not support hhtps or request your credit/debit card information even though it is not required, never into your information. Additional a reliable page must have a good design to stop if you do not meet any of these criteria do not provide your credit card information.
- **Protect your Wi-Fi:** Secure unlock (since you have 8 sides make sure they are password protected). If you prefer a password, make sure only people in your household can access your Wi-Fi network. And other step you can take is to make sure your phone or computers Bluetooth is turned off if not needed.
- **Report crime quickly:** The information technology act 2000 was created to help businesses use information technology. It also shows at a process in the IT sector. The Indian penal code 1860 also included cyber price. Take websites, straightening messages via email hacking etc.

VI. CONCLUSION

"The law is not the be-all and end-all solution." Victims are still not getting justice despite of a strong legal base in spite of them remaining silent. Cyber-crime against women is just a reality check of what really is going on in the real world. The lines between the online and offline world is getting blurred. Cyber-crime happens because the criminals think that is a much easier way with less punishment. With millions of users in the online platforms complaint mechanisms has also become fruitless.

For instance in the recent boy's locker room case where group of teenage boys from Delhi

ISSN: 2582-6433

shared pictures of underage women and objectified them by passing derogatory comments on group chat in Instagram and Snapchat. When a girl shared the screenshots of the chats the group was busted. Women all over country raised voices but it could be seen that they were not shocked. The reason is that objectification of women has become quite normal in the society. Women have has accepted this mentality of objectification by male as every day new cases come into light. Years have passed and still women lives in the fear of going out alone outside in the real world. In fact the online world which she could go to in the safety of her home has also become an unsafe place.

It comes upon the women to take preventive measures such as usage of data security, not leaving digital footprint, keeping everything password protected. But this are all superficial ways. The major problem that has always been existing is the patriarchy and misogyny in the society. To solve this problem a long term measure need to be undertaken that will help in dealing with cyber-crime against women.

There is the need of the hour to evolve the societal and cultural norms with the development of information technology. Mandatory steps need to be taken. Steps like digital literacy, development of data security, providing access of technology to women and girls and most of all enactment of laws specifically on cyber-crime especially with reference to women.