



ISSN 2582 - 211X

LEX RESEARCH HUB JOURNAL

On Law & Multidisciplinary Issues

Email - journal@lexresearchhub.com

VOLUME II, ISSUE I
OCTOBER, 2020

<https://journal.lexresearchhub.com>

Lex Research Hub
Publications

DISCLAIMER

All Copyrights are reserved with the Authors. But, however, the Authors have granted to the Journal (Lex Research Hub Journal On Law And Multidisciplinary Issues), an irrevocable, non exclusive, royalty-free and transferable license to publish, reproduce, store, transmit, display and distribute it in the Journal or books or in any form and all other media, retrieval systems and other formats now or hereafter known.

No part of this publication may be reproduced, stored, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other non-commercial uses permitted by copyright law.

The Editorial Team of **Lex Research Hub Journal On Law And Multidisciplinary Issues** holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not necessarily reflect the views of the Editorial Team of Lex Research Hub Journal On Law And Multidisciplinary Issues.

[© Lex Research Hub Journal On Law And Multidisciplinary Issues. Any unauthorized use, circulation or reproduction shall attract suitable action under applicable law.]

EDITORIAL BOARD

Editor-in-Chief

Mr. Shaikh Taj Mohammed

Ex- Judicial Officer (West Bengal), Honorary Director, MABIJS

Senior Editors

Dr. JadavKumer Pal

Deputy Chief Executive, Indian Statistical Institute

Dr. ParthaPratimMitra

Associate Professor, VIPS. Delhi

Dr. Pijush Sarkar

Advocate, Calcutta High Court

Associate Editors

Dr. Amitra Sudan Chakraborty

Assistant Professor, Glocal Law School

Dr. Sadhna Gupta (WBES)

Assistant professor of Law, Hooghly Mohsin Govt. College

Mr. KoushikBagchi

Assistant Professor of law, NUSRL, Ranchi

Assistant Editors

Mr. Rupam Lal Howlader

Assistant Professor in Law, Dr. Ambedkar Government Law College

Mr. Lalit Kumar Roy

Assistant Professor, Department of Law, University of GourBanga

Md. AammarZaki

Advocate, Calcutta High Court

ABOUT US

Lex Research Hub Journal On Law And Multidisciplinary Issues (ISSN 2582 – 211X) is an Online Journal is quarterly, 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, Essays in the field of Law and Multidisciplinary issues.

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. Lex Research Hub Journal On Law And Multidisciplinary Issues (ISSN 2582 – 211X) welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

CYBER CRIMES AGAINST WOMEN- A GROWING THREAT TO THE SOCIETY

Author –

Susmita Saha

Advocate

Mathabhanga Court

ABSTRACT:

Crimes against women in a patriarchal country like India are on the rise from ancient times. With the advent of technology or in other words the internet, women are harassed in the digital world in the same manner as they are harassed in the physical world and there is no exception to it. Crimes against women in this virtual world become a global phenomenon in recent days. Women become more victimized in cyberspace in comparison to men because of many reasons. The word “cyberspace” or “cyber world” is a word full of electronic devices. Cyber crimes are crimes which involve a computer and a network. There are several types of cyber crimes which are committed against women, like cyber defamation, cyber stalking, cyber pornography etc. Due to the high rate of involvement in social networking sites, women easily fall into the trap of miscreants, as they have no sufficient knowledge about privacy policy. Lack of awareness regarding cyber law and policy among the individuals especially among women, there is less number of reported cases on cyber crimes which encourage the offenders little more. Although India has its own law namely Information Technology Act, 2000 to curb the cyber crimes but it mainly focuses on e-commerce thus it fails to protect the privacy of women. This paper attempt to explore various reasons as to why women are more victimized in cyberspace, what are the several cyber crimes committed against women and to what extent Indian laws can protect the women from being harassed in this virtual world.

Key words: Cyberspace, Women, India, Cybercrimes, IT Act.

1. INTRODUCTION:

Safety of women has always been an issue in India, where the patriarchal system exists. Women are harassed every second in all the sphere of society. Internet is one of the greatest inventions of the modern era that make the life of people became easier. Because of the internet, people can communicate with each other around the world. It erases the distance between people across the world virtually belonging to a different country as well as culture. By using internet people not only communicate with each other but also doing business on online, online shopping, getting information about every corner of this earth within a minute. People are very much dependent on technology now- a- days to save time, even the education system also dependent on the internet. The social networking sites are the most popular way for socializing. Despite these several advantages of using the internet, it has some disadvantages also. Crimes in this virtual world are known as cyber crimes or computer crimes. The term “cyber crimes” or “computer crimes” may

be defined as an “illegal activity using a computer, and includes computer-related extortion, fraud and forgery and unauthorised access to or interference with data”.¹ Cyberstalking, email morphing, cyber defamation, cyber pornography are some serious crimes which are committed against women every day. Victimization of this vulnerable section of the society are on the high as because of lack of awareness, emotional dependence, inequality between men and women, lack of proper enforcement agency etc. Home is no more be considered as the safest place for women as well as for children also. As this virtual world has no physical boundaries, the violence against women knows no boundaries thus it is quite difficult to eliminate cybercrimes but it can be done by creating awareness among women about computer literacy and the safest use of smartphones, computer and internet browsing.

¹ Dr. J. P. Mishra, *An Introduction to Cyber Law* (Central Law Publications, 2nd ed. 2014).

2. CYBER CRIMES AGAINST WOMEN IN INDIA:

Almost every person in this world accesses internet services. Technology is one of the greatest inventions of modern days. The Internet brought the whole world in our drawing-room. Today people are dependent on the internet whether it for entertainment or information. India is the second-largest online market in the world after China with over 560 million users in 2020.² People are so busy to waste their valuable times by using several social networking sites. Some popular social networking sites in India recently are Facebook, Whatsapp, Instagram, Twitter, Youtube, Tinder and Snapchat etc. Every year the number of social network users increases, like from 326.1 million in 2018 to 376.1 million in 2020 and is also expected that the number would increase to 447.9 million by 2023.³ With the rise in internet users, the crimes in cyberspace also increase. As per the Government data, there is a drastic increase of 63% of cybercrimes in India in 2019. The National Crime Record Bureau's (NCRB) data showed that the registered cases of cybercrimes increased from 28,248 in 2018 to 44,546 in 2019.⁴

The criminals mostly targeted women to harass them in the cyber world either to take any type of revenge or to defame her or to make fun of them. This can be done by several means.

²Internet usage in India - statistics & facts, (Nov 3, 2020, 4:30 PM)<https://www.statista.com/topics/2157/internet-usage-in-india/>

³Number of social network users India 2015-2023, (Nov 6, 2020, 1 PM)<https://www.statista.com/statistics/278407/number-of-social-network-users-in-india/#:~:text=With%20the%20ease%20of%20internet,at%20326.1%20million%20in%202018.&text=Nevertheless%20the%20social%20network%20users,media%20platforms%20as%20of%202017.>

⁴ 63.5% Increase In Cybercrime Cases In India In 2019; Most Cases In Karnataka: NCRB, (Nov 6, 2020, 1 PM)<https://www.republicworld.com/india-news/law-and-order/63-dot-5-percent-increase-in-cyber-crime-cases-in-india-in-2019-most-cases-in-ka.html#:~:text=According%20to%20the%20latest%20government,compared%20to%2028%2C248%20in%202018>

2.1. KINDS OF CYBERCRIMES

2.1.1. Cyber Stalking: Stalking generally means following a person's movement and when we talk about cyberstalking this means the act of following happens in the virtual world. Due to cyberstalking, the good things of a person's life may be used in the worst possible manner by some miscreants. This act of stalking become possible due to the communication through e-mails, e-chatting, messages etc. Through these communication modes, the offender can easily gather personal information about a woman without her knowledge. As per the Merriam- Webster's dictionary meaning cyberstalking means, the repeated use of electronic communication to harass or threaten someone with physical harm.⁵

According to Webster's Dictionary, cyber-stalking as a verb stands for (i) using the internet, through chat rooms and e-mail, to find, identify, and arrange to meet a person whom one intends to criminally victimize; and (ii) sending multiple e-mails, often on a systematic basis, to annoy, embarrass, intimidate, or threaten a person or to make the person fearful that she or a member of her family of a household will be harmed.⁶

2.1.2. Cyber Pornography: Indian culture is the traditional one where morality prevails at the top. In a value-based society like India an offensive or indecent phrase or word or picture considered as a moral wrong. This wrong also violates one's right to privacy who is the victim. This is the most dangerous threat to a woman as well as to children as it involves the publishing or transmitting obscene materials of the victim in pornographic websites. Without the knowledge of the victim, the offender obtains the private pictures or videos of the victim either by hacking phone or

⁵cyberstaling(Nov 10, 2020, 10 AM) <https://www.merriam-webster.com/legal/cyberstalking>

⁶ Supra note 1.

computer or social media accounts and publish it in the virtual world which would adversely affect the life of the victim in this physical world.

2.1.3. Cyber Morphing: The act of cyber morphing includes editing a picture completely or partially by an unauthorized user. Here the wrongdoer downloaded female's pictures from different social media sites and then upload the edited one on various websites or use it to create a fake profile. By this act, one can easily threaten a woman whose photo is morphed and compelled her to do something against her wish.

2.1.4. Cyber Defamation: As in tort cyber defamation is also a civil wrong. The act of cyber defamation is committed by a person who publishes any defamatory statements or any obscene material on any websites to defame another.

2.1.5. Email Spoofing: Email spoofing is the misrepresentation of the original source of an email. Here one fraudulently changed the real origin of an email and send it to other people in such a way that one can easily mislead about its source.

Not only these crimes, but there are also some other types of harassment which are experienced by women while using the internet. For example, online trolling which destroys the peaceful condition of the browsing and phishing by which one attempts to obtain another's personal information like username, password etc.

In *State of Tamil Nadu v. Suhas Katti*⁷, considered as the first case of conviction under section 67 of the IT Act, 2000, a complaint was made against the accused for posting obscene, defamatory and annoying messages about the victim, a divorced woman in the yahoo message group. A false e- mail account was also opened by the accused in the name

⁷ CC No. 4680 of 2004.

of the victim through which several e-mails were sent to the victim for information. The court found the accused guilty of offences under sections 469, 509 of IPC and 67 of IT Act.

In *Habeas Corpus Petition No. 1956 of 2016 Palanisamy v. State of Tamil Nadu*, decided on 16 March, 2017, the habeas corpus petition filed by the petitioner was dismissed by the Court. Suresh the offender is a resident of Salem opened a Facebook account in the name of one Miss. Vinupriya without her knowledge and uploaded the obscene photos of her which he had edited from his phone. Because of this reason, Miss. Vinupriya out of depression committed suicide and the wrongdoer was branded by the court as “CYBER LAW OFFENDER”.

3. LAWS TO PREVENT CRIMES AGAINST WOMEN IN DIGITAL WORLD IN INDIA:

The Information and Technology Act, 2000 mainly deals cyberspace. This Act defines a few cybercrimes by name. It has some penal provisions also. Except this the Indian Penal Code, 1860 has some provisions which deal with cyber crimes against women. Although the IT Act is not a gender-specific statute it has some provisions which are specifically talked about gender-specific crimes and also prescribes punishments for those crimes. These two statutes are addressed cybercrimes against women to a large extent in India.

IPC enacted with the object to provide a general Penal code for India is the general law of the land. It defines almost all the offences and provides punishments for the same. At present because of several amendments to the Act and through case laws, some provisions are also applicable to cybercrimes against women. Besides the earlier provisions, the amendment of 2013 has inserted several other provisions to protect every woman from any kind of harassment. Some of them are as follows-

- i. Section 354D which is inserted by the Amendment Act of 2013 defines the crime of stalking includes cyber stalking also.

- ii. Section 292 of IPC, in general, prohibits the sell, distribution, advertisement of obscene materials by making the act punishable.
- iii. Section 354A which is inserted in the year 2013 deals with sexual harassment which includes the act of man showing pornography against the will of a woman and prescribes punishment for such an act.
- iv. Section 354C inserted in 2013 makes the offence voyeurism punishable with imprisonment for not less than one year but which may extend to three years and shall also be liable to fine. The offence of voyeurism includes watching or captures or disseminates the image of a woman engaging in a private act where she would usually expect not being observed by any person.

On the other hand, the IT Act, 2000 is the only Act which specifically enacted to deal with the matters of cyberspace. Some of the cybercrimes are specifically defined under this Act, they are as follows-

- i. Section 66 of the Act provides punishment for computer-related offences.
- ii. Section 66A makes punishable the act of sending offensive messages using a computer resource or a communication device with imprisonment for a term which may extend to 3 years and with fine. However, the section does not mention the term 'cyberstalking'.
- iii. Section 66C provides punishment for identity theft.
- iv. Section 66E makes the act of a person punishable for violation of privacy in terms of intentionally or knowingly captures, publishes or transmits the image of a private area of any person without her consent with imprisonment which may extend to 3 years or with fine not exceeding two lakh rupees or with both.
- v. Section 67 provides punishment for publishing or transmitting obscene material in electronic form.
- vi. Section 67A provides punishment for publishing or transmitting of material containing sexually explicit act in any electronic form.
- vii. Section 67B punishes the act of publishing or transmitting any material depicting children in sexually explicit act etc. In an electronic form.
- viii. Section 72 provides a penalty for breach of confidentiality and privacy.

- ix. Section 72A prescribes punishment for disclosure of information in breach of lawful contract.

4. REASONS BEHIND THE GROWTH OF CYBER CRIMES AGAINST WOMEN:

Thousands of females of all age groups in India are subjected to deliberate violence everyday because of their gender. The fastest-growing of technology and the rapid spread of the internet, on one hand, can take a nation at the top of development but on the other hand, it also results in the rise of offences against the weaker section of the community. The Internet Crime Report for 2019 of the Federal Bureau of Investigation(FBI), released by USA's Internet Crime Complaint Centre (IC3) has revealed that India ranks **third** among top 20 cybercrime countries.⁸ Major victims of cybercrimes are females due to several reasons which are discussed below-

- a. Psychological Reasons:** Due to urbanization in India the traditional joint family system has changed to the nuclear family system. Now everyone is busy with their work and nobody has time for their family members. In between this, it is the woman who stuck in home alone and as a result, they became depressed. To overcome from this depression and loneliness, they started to find support from outside of her family circle. Because of this technological advancement they easily get the chance to interact with strangers in several social networking sites. They blindly trust those strangers and started sharing their personal information. Thus it became easier for the miscreants to grab this opportunity and misuse it. Further women feel hesitations to report cybercrimes due to associated stigma and the fear of being future victimization. This encourages the criminals to commit more wrongs and women became prone to cyber victimization.

⁸India stands third among top 20 cyber crime victims, says FBI report, (Nov 16, 2020, 10 AM)
<https://www.newindianexpress.com/nation/2020/feb/23/india-stands-third-among-top-20-cyber-crime-victims-says-fbi-report-2107309.html>

A report from India shows that only 35% of women of the country have reported their victimization... women often prefer not to report cyber violence against women for fear of social repercussions.⁹

- b. Insufficient Computer Knowledge:** People of India especially females have partial computer knowledge. Although they know how to browse the internet or how to use different social networking sites, they less aware about the terms and conditions of various networking sites and the policy guidelines before opening their accounts on the social networking sites. Different social networking sites like Facebook, WhatsApp etc. have the settings to keep one's profile private and secure but most of the women do not know about such policies. The sites also have the setting to block a stalker or harasser permanently and

with whom one wants to share photos or albums. Even after all these facilities, women are more prone to cyber victimization than men in the cyber world. Women are less expert in handling technology.

- c. Lack of Adequate Knowledge about Cyber Laws:** In India, the literacy rate of women is less than men. They also have inadequate knowledge about cyber laws. They do not know how to file a complaint about cybercrime and where to file. Even sometimes they don't know which act constitutes a wrong. This made women more vulnerable in society.

Even the appropriate officers, i.e. police officials, investigating officers do not have sufficient knowledge about cyber law which delays the investigation proceedings and unable to give justice.

- d. Loopholes in the Present Statute:** Most of the cyber crimes go unreported because of unawareness of women about such crimes. This encourages an

⁹ Combatting Online Violence Against Women & Girls: A Worldwide Wake-up Call, Final report of the Broadband Commission Working Group on Gender, September 2015, (Nov 22, 2020, 10:45 PM)
<https://en.unesco.org/sites/default/files/highlightdocumentenglish.pdf>

offender to repeat the crime again and again. Although the IT Act, 2000 defines some of the cyber crimes committed against women and also prescribes punishments for the same but the Act mainly focused on commercial and financial issues. There is no specific mention about such serious offences like email spoofing, email morphing, cyberstalking etc. There are no Standard Operating Procedures formulated to deal with cyber issues. Further according to the criminal investigation can be done only by a police officer not below the rank of an inspector which sometimes result in inappropriate enquiry due to shortage of manpower.

5. CONCLUSION AND SUGGESTIONS:

Cybercrime is a serious issue of the present day which require attention from the Govt. as well as from the society. It is time to take immediate action to protect the women of India from the harassment in cyberspace. People make the internet as a vital part of their life which brings with it both pros and cons. Harassment of women in cyberspace is not a new phenomenon now but it is the time to wake up and fight against this evil with unity. As per the experts report, there is a significant increase in cybercrime against women during the COVID- 19 lockdowns. The National Commission for Women's (NCW) data shows that 54 online cybercrime complaints were received in April while 37 complaints were received in March both by online and by post.¹⁰ In spite of the fact that India has its own cyber law, there is increasing number of cyber crimes because of lack of enforcement agency. Cybercrimes against women are on rise which must be prevented by adopting some measures, such as:

Public sensitization is the most important preventive measure. First of all, the public should be educated about the seriousness of cyber crimes and the attitudes of the society towards women should be changed.

¹⁰Significant' increase in cybercrime against women during lockdown: Experts (Nov 24, 2020, 3 PM)
<https://cio.economictimes.indiatimes.com/news/digital-security/significant-increase-in-cybercrime-against-women-during-lockdown-experts/75500549>

The legislature of India should make strict and separate legislation relating to crimes committed in cyberspace or should amend the existing laws, i.e. IPC and IT Act in such a manner to exclusively deal with the matters about crimes against women committed in the cyber world. There must be a provision to prevent the creation of a fake profile on the internet.

Indian women must educate about the various privacy policies and term and conditions of several websites. Without knowing the privacy settings of social networking sites a girl is unable to protect herself from a stalker or hacker etc. They should change the passwords of their accounts frequently. They should avoid the accepting of friend requests from strangers.

The Govt. of India and NGOs should organise awareness programmes about cybercrime against women in schools, colleges of every level as girls of all age groups are using the internet at present. Further seminars and workshops on cyber laws must be organised for the better understanding of cyber laws. Women should know the cyber law to live with dignity. Awareness camp should also organise in the rural areas also to educate the women about their rights to not be a victim of cybercrime and to make a complaint in case of any violence. The law is of no use unless women themselves are aware of their rights.

The police officials dealing with this matter should also be trained on cyber laws. They must be well equipped with the knowledge of technology so they become able to catch the offenders. Police officials and cyber forensic laboratories should collaborate for the better enforcement of cyber law.

However the Ministry of Home Affairs, Govt. of India recently developed a centralized online reporting portal namely, **www.cyberpolice.gov.in** to deal with complaints of cyber crimes.