Cover Page

DOI: http://ijmer.in.doi./2022/11.01.24

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881; IMPACT FACTOR :7.816(2022); IC VALUE:5.16; ISI VALUE:2.286
Peer Reviewed and Refereed Journal: VOLUME:11, ISSUE:1(2), January: 2022
Online Copy of Article Publication Available (2022 Issues): www.ijmer.in
Digital Certificate of Publication: http://ijmer.in/pdf/e-Certificate%20of%20Publication-IJMER.pdf
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: 2nd January 2022
Publication Date:10th February 2022
Publisher: Sucharitha Publication, India

CYBERCRIME AGAINST WOMEN: A SERIOUS THREAT

Monika
PhD Research Scholar
Department Of Laws, Bhagat Phool Singh Women University
Khanpur Kalan Sonipat, Haryana, India

Abstract

It is an era of technology and the internet. India is growing faster by using modern digital technology. The common men are also using digital technology to explore themselves and to make life easy and comfortable. Digital technology is considered to be used to acquire knowledge and easily or quickly communicate with anyone even across the world. But at the same time, it has some disadvantages as everyone knows technology has some pros and cons like it opens the door for criminals to commit cybercrime. Cybercriminals misuse the cyber platform and mostly target women and children because of their vulnerability. They are a soft target for the perpetrator of cybercrimes. Women are harassed every day either directly or indirectly. Despite the several laws and law enforcement bodies that are safeguards for the women or the benefit them, the crime rate against women is increasing day by day. Cybercrimes are most common these days. In this paper, an attempt has been made to describe cybercrime and try to make a predictive analysis of cybercrime against women in India, and describe the related legal provisions which deal with or punish the wrongdoer. A positive effort has also been made to find out the lacuna and reason behind the increasing rate of cybercrime rate. Cybercrime is an emerging and serious threat to economic and national security. Some suggestive measures are also provided.

Keywords: Computer, Cybercrime, Information Technology, Internet, National Commission for Women, National Crime Records Bureau.

1. Introduction

Women are considered Goddesses or Devi in Indian culture. As per census 2011, the population of India was 121.06 crore and the female constituted 48.5% of the total[1]. It shows the women are almost half of society. They are pillars of a developed and developing society. With the advent of education and technology, they are getting more independent and making themselves empowered. The government is also making laws for the empowerment of women. The Indian Constitution enshrined the provisions for gender equality. The preamble, fundamental rights, directive provisions of state policy, fundamental duties[2] are the several parts of the Constitution which applicable on all equally even constitution of India empower the States to adopt positive discrimination [Article 15(3)[3]] in favour of women for their empowerment and to make them independent and strong. The Constitutional 73rd[4] and 74th Amendment Act (1992)[5] is an example of it which provides the reservation of women in panchayats and municipalities respectively. Business laws have changed the lives of women by providing them with a comfortable work environment at the workplace. Apart from it, our government signed international conventions[6] also which prevent discrimination against women. But at the same time the crime against women either direct physical assault like domestic violence, cruelty, murder, rape, harassment, kidnapping, or indirect cyber threat like stalking, e-mail spoofing, video or phone calls, photo morphing, profile hacking, etc.

Cybercrime is a serious threat against women throughout the world. It is increasing day by day like a disease. Safety of women has always been an issue of discussion. India is among those countries which enact Information Technology (IT) Act, 2000 to tackle cyber-crimes. Despite the law, the rate of crime is so high. In today's technological world where everybody has internet access, it is very easy to commit such a crime. Some questions to be answered here: where is the lacuna? Are the agencies not working properly like cyber cell or police?

Now, first of all, we must know about cybercrime what is it?

[1] Censusindia.gov.in
[2]The preamble, part -3, part-4, part-4 A of the Indian Constitution.
[3] Nothing in this Article shall prevent the State from making any special provision for women and children.
[4]Insertion of part-9 in Indian Constitution.
[5] Insertion of part-9 A in Indian Constitution.
[6] The convention on the Elimination of all Forms of Discrimination Against Women an international treaty adopted in 1979 by United Nations General Assembly.

Cover Page

DOI: http://ijmer.in.doi./2022/11.01.24

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881; IMPACT FACTOR :7.816(2022); IC VALUE:5.16; ISI VALUE:2.286
Peer Reviewed and Refereed Journal: VOLUME:11, ISSUE:1(2), January: 2022
Online Copy of Article Publication Available (2022 Issues): www.ijmer.in
Digital Certificate of Publication: http://ijmer.in/pdf/e-Certificate%20of%20Publication-IJMER.pdf
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: 2nd January 2022
Publication Date:10th February 2022
Publisher: Sucharitha Publication, India

2. What is Cybercrime

In short and in simple terms, cybercrime is any type of illegal activity that takes place via digital means. It can be committed against a person, an association, a company, children, women, and Government. Data theft is one of the most common types of cybercrime but it is not limited to it. It includes a wide range of malicious or illegal activities as well. Cybercrimes can be committed with anyone or anywhere in the world[7]. At the same time, it must be borne in mind that a crime is not a crime everywhere. It means maybe one county has laws on one issue and the other county does not have laws on it then the county having no laws on the issue will not consider it a crime. Some definitions on it given as follows:

- Cybercrime or a computer-oriented crime is a crime that involves a computer and a network.[8]
- Criminal activity or a crime that involves the internet, a computer system, or computer technology.[9]
- Crime is conducted via the internet or some other computer network.[10]
- Cybercrime is a criminal activity done using computers and the internet.[11]
- Any use of a computer as an instrument to further illegal ends.[12]

3. Types of Cybercrimes against Women

Some specific cybercrimes which are most common and committed against women are as follow:

i. **Cyberstalking:** It is on the rise in the present world because of easy internet access. The perpetrator is not directly involved in a physical threat but he keeps his eye on the internet activity of the victim to gather information and to harass her. Due to the privacy policy of the internet, the identity of the culprit remains unknown that making cyberstalking common.

ii. **Cyber defamation:** Cyber Defamation means publishing or sharing defamatory information about a person on the website or circulating it among the victim's friends or circle. It is also called cyber smearing.

iii. **Morphing:** In morphing, the perpetrator edits the original photo(take it from social media like Whatsapp, Facebook, Instagram) or image of a woman by editing it by using computer animation technique and uploading it on porn sites or other social media.

iv. **Harassment through e-mails:** Harassment via email includes blackmailing, threatening and constant sending of love messages in anonymous names or regular sending embarrassing emails.[13]

v. **Cyber grooming:** Cyber grooming is when a person builds an online relationship with a young person and tricks her into doing a sexual act.[14]

vi. **Cyber pornography:** Cyber pornography means publishing, distributing, or designing pornography by use of the internet. Pornographic includes any video, pictures, or movies that contain sexually explicit acts that are considered indecent by the public. In legal sense pornography means "obscenity".[15]

vii. **Phishing:** In Phishinganculprit attempts to gain personal sensitive data such as user name and password or banking and credit card details.[16]

viii. **Trolling:** Trolling is very common and most of the time we heard about it when someone said something on the internet and other people do not like the comment or disagree with that make some opposite or off-topic messages to troll her and make them feel embarrassed. In recent times it mostly happens on Twitter or other social media.

[7]Information technology Act,2000 available at: http://www.iovation.com<topics>what is cybercrime
[8]Information technology Act,2000 available at: http://en.wikipedia.org.in<wiki>cyber crime.
[9] Information technology Act,2000 available at: Dictionary.com.
[10] Information technology Act,2000 available at: Oxford dictionary.
[11] Information technology Act,2000 available at: Techterms.com
[12]Information technology Act,2000 available at: the free dictionary
[13]Vikaspedia.in>social welfare>cybercrime against women.
[14] ibid
[15]Information technology Act,2000 available at: blog.ipleaders.in.
[16] Information technology Act,2000 available at: www.Phishing.org.

Cover Page

DOI: http://ijmer.in.doi./2022/11.01.24

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881; IMPACT FACTOR :7.816(2022); IC VALUE:5.16; ISI VALUE:2.286
Peer Reviewed and Refereed Journal: VOLUME:11, ISSUE:1(2), January: 2022
Online Copy of Article Publication Available (2022 Issues): www.ijmer.in
Digital Certificate of Publication: http://ijmer.in/pdf/e-Certificate%20of%20Publication-IJMER.pdf
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: 2nd January 2022
Publication Date:10th February 2022
Publisher: Sucharitha Publication, India

4. Cyber Crimes in India against women: National Crime Records Bureau (NCRB) Report, 2017

NCRB is an agency of Government that keeps records of crimes committed under IPC and Special or Local law.

As per the NCRB report, 2017 total of 21,796 instances of cybercrime were recorded in 2017, an increase of 77%over the previous year's number of 12317. The number of cybercrimes increased dramatically in 2017 as compared to 2016, and nearly every fifth cybercrime in 2017 was committed against a woman.17

NCRB Crime data 2019[18]: **According to the latest govt data, India has recorded a massive increase of 63.5% in cybercrime cases in 2019. NCRB data shows 44,546 cases were registered.**

The highest number of cybercrime cases were registered in Karnataka (12,020) closely followed by Uttar Pradesh (11,416), Maharashtra (4,967), Telangana (2,691), and Assam (2,231).[19]

According to the data, in 60.4% of cases, registered fraud was the motive followed by sexual exploitation (5.1%) and causing disrepute (4.2%).[20]

The table on Cyber Crimes against women: Data by NCRB report[21]

Cyber blackmailing/ threatening against women	132
Cyber pornography/hosting/publishing obscene sexual material	271
Cyberstalking/ cyber-bullying of women	555
Defamation/ morphing	50
Fake profile	147
Other crimes	3,087
Total	4,242

5. Cybercrimes during a lockdown: Data as per National Commission for Women:

There has been a significant increase in cybercrime against women, especially sextortion, during the COVID-19-induced lockdown with "caged criminals" targeting them online. According to National Commission for Women (NCW) data, 54 cybercrime complaints were received online in April in comparison to 37 complaints - received online and by post - in March, and 21 complaints in February.[22] Due to lockdown complainants are advised to file their complaints through online modes.

There was a total of 412 genuine complaints of cyber abuse from March 25 till April 25 been received. Out of these, as many as 396 complaints were serious ones from women, (and these) ranged from abuse, indecent exposure, unsolicited obscene pictures, threats, malicious emails claiming their account was hacked, ransom demands, blackmail, and more.[21]

Sextortion is extorting money or sexual favours from someone by threatening to reveal evidence of their sexual activity through means like morphed images.[23]

6. Traditional law for females

i. Indian Penal Code,1860

- Section 354- Assault or criminal force to woman with intent to outrage her modesty
- Section 354- A, B, C, D
- Section 359, 360 and 361 – Kidnapping and abduction

[17]https://indianexpress.com/article/explained/ncrb-data-cyber-crime-jumped-by-77-in-2017-6082779/
[18]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
[19]https://m.dailyhunt.in/news/africa/english/republic+tv+english-epaper-repubeng/63+5+increase+in+cybercrime+cases+in+india+in+2019+most+cases+in+karnataka+ncrb-newsid-n218596098
[20]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
[21]Harikrishan Sharma
[22]https://cio.economictimes.indiatimes.com/news/digital-security/significant-increase-in-cybercrime-against-women-during-lockdown-experts/75500549
[23] Information Technology Act,2000 available at: https://www.hindustantimes.com/india-news/significant-increase-in-cybercrime-against-women-during-lockdown-experts/story-QNPwq5Jr1iAkAXzacLnc5K.html

Cover Page

DOI: http://ijmer.in.doi./2022/11.01.24

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881; IMPACT FACTOR :7.816(2022); IC VALUE:5.16; ISI VALUE:2.286
Peer Reviewed and Refereed Journal: VOLUME:11, ISSUE:1(2), January: 2022
Online Copy of Article Publication Available (2022 Issues): www.ijmer.in
Digital Certificate of Publication: http://ijmer.in/pdf/e-Certificate%20of%20Publication-IJMER.pdf
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: 2nd January 2022
Publication Date:10th February 2022
Publisher: Sucharitha Publication, India

- Section 509 - Eve Teasing
- Section 378-Chain snatching
- Sections - 376,376A, 376 AB[24]376B, 376C, 376D, 376DA, 376DB[25]-Rape
- Section 498-A- Cruelty
- Section 506 -Punishment for criminal intimidation
- Section 441 -Criminal trespass
- Section – 304-B Dowry deaths
- Sections - 326A and 326B-Acid attacks[26]
- Sections - Sec. 370, 370A, 372, 373 -Women trafficking[27]

ii. **Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013.[28] - It was enacted for the protection against sexual harassment of working women, to maintain the equal right to work with dignity.**

iii. **Protection of Child from Sexual Offences Act, 2012.[29]**

iv. **Cyber Law.**

In India, the Information Technology Act,2000 was passed with the object to give legal recognition for all transactions and activities carried out by electronic means.

IT, Act defines some cybercrimes and penalties for its commission, and most of the crimes are related to documents and contracts but the issue regarding women is nowhere defined. There are different kinds of punishment and many fines are provided for the different offences.

Cybercrime against women is at an alarming stage and the issue of a woman's safety and security is always an issue of debate and discussion at the national and international levels. India is considered as one of the very few countries to enact the IT Act, (2000) but it needs some amendment.

Mainly it is Chapter- 11 which deals with cyber offences some relevant provisions are as follow:

- Section 65 - Tampering with computer source documents.
- Section 66 - Computer-related offences.
- Section 67- Punishment for publishing or transmitting obscene material in electronic form.
- Section 70 - Access to a protected system.
- Section 72- Breach of confidentiality and privacy.
- Section 74- Publication for a fraudulent purpose.[30]

IT Amendment Act, 2008(Act 10 of 2009) inserted some new provisions for which the original act is not sufficient that are as follows:

- Section 67- A – Punishment for publishing or transmitting of material containing sexually explicit act etc., in electronic form.
- Section 67- B – Punishment for publishing or transmitting of material depicting children in sexually explicit acts etc., in electronic form.
- Section 67C- Preservation and retention of information by intermediaries.
- Section 66 – E- Punishment for privacy violation
- Section 66-F- Punishment for Cyber terrorism.[31]

7. What kind of crime is it?

Cybercrime is what kind of crime or offence whether it is cognizable or non-cognizable and bailable or non-bailable? Here it is important to know the meaning of terms used herein as before.

[24] The Criminal Law Amendment Act,2018.
[25] Ibid
[26] The Criminal Law Amendment Act,2013.
[27] Indian Penal Code,1860.
[28] Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013.
[29] Protection of Child from Sexual Offences Act, 2012.
[30] Information Technology Act,2000.
[31] Information Technology (Amendment), Act 2008

Cover Page

DOI: http://ijmer.in.doi./2022/11.01.24

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881; IMPACT FACTOR :7.816(2022); IC VALUE:5.16; ISI VALUE:2.286
Peer Reviewed and Refereed Journal: VOLUME:11, ISSUE:1(2), January: 2022
Online Copy of Article Publication Available (2022 Issues): www.ijmer.in
Digital Certificate of Publication: http://ijmer.in/pdf/e-Certificate%20of%20Publication-IJMER.pdf
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: 2nd January 2022
Publication Date:10th February 2022
Publisher: Sucharitha Publication, India

- **Cognizable offence: "**Cognizable offence" means an offence for which and "cognizable case" means a case in which, a police officer may, in accordance with the First Schedule or under any other law for the time being in force, arrest without warrant.[32]

- **Non cognizable offence:** non-cognizable offence means an offence for which, and "non-cognizable case" means a case in which, a police officer has no authority to arrest without a warrant.[33]

- **Bailable offence:** means an offence which is shown as bailable in the First Schedule, or which is made bailable by any other law for the time being in force; and

- **Non bailable offence:** means any other offence.[34]

Most of the cybercrime under the Indian Penal Code is cognizable.

8. Filing of complaint against cybercrime

Cybercrime cells have been set up to register cybercrime complaints. The Information Technology Act,2000 clearly provides that cybercrime has global jurisdiction [35]it means a cybercrime may be reported in any of the Cyber Crime Units of any city irrespective of the place of commission. If the cyber cell is not available in the city of its commission, one can file an F.I.R in the local police station of its commission. Even a Zero F.I.R can also be logged. If a complaint is not accepted by police, then the victim or her family member or close friend refers a complaint to the commissioner or judicial magistrate of the city.

9. Cases on cyber crimes

RituKohli Case[36](2001): It was the first Indian case that has been registered on cyberstalking. The accused name Manish kathuria was deliberately following the victim on the internet. He by using her identity chat over the internet to different people mostly in the Delhi channel. He gave her phone number to others so that they call her during odd hours. As a result of it, he received 40 calls in just 3 days. A complaint had been filed and the police trace the IP address and the culprit was arrested under section 509 i.e, insult the modesty of a woman.

DPS MMS ScandalCase[37](2004): In 2004 a minor male student of Delhi Public School of R.K.Puram Delhi shot a small video shoot of his fellow female student topless without her knowledge. The video got viral through multimedia sharing channels and porn sites. One engineering student from IIT Kharagpur was prosecuted for the selling of a video clip on baazee.com but later he was acquitted because he does not earn by selling the video.

After this scandal needs to arise to amend the IT, ACT 2000. Several judgments were passed to ban cell phones in schools.

Delhi Metro CCTV footage leaks case[38](2013): This is a case of privacy breach, a CCTV footage of a couple at a Delhi metro station leaked on porn website. The said couple indulged in an intimate scene. It was found that the video was recorded from the live feed inside the CCTV control room of the Delhi metro. Delhi Metro Rail Corporation lodged an F.I.R at Azadpur police station for the obscenity in a public place.

Air Force Bal Bharati School case (Delhi)[39](2001): It was a case of cyber pornography. A 16 years old boy to take revenge on his classmates who teased him for having a pockmarked face, created a website containing obscene messages about the girls and teachers of the school. A boy was arrested and later released on bail due to his minority.

A Case was registered by the Delhi Police Cyber Cell under section 67 of the IT Act,2000.

---

[32] The Code of Criminal Procedure,1973(2 of 1974), s.2(c).
[33] Id., s.2(l).
[34] Id., s.2(a).
[35] Information Technology Act,2000.
[36]Information Technology Act,2000 available at: http://cyberlaws.net/cyberindia/2CYBER27.htm
[37]http://en.wikipedia.org/wiki/DPS_MMS_Scandal
[38]http://zeenews.india.com/news/nation/porn-mmses-from-delhi-metro-cctv-footage_860933.html
[39]AbhimanyuBehera, " Cyber Crimes and Law In India," XXXI,IJCC 19 (2010).

Cover Page

DOI: http://ijmer.in.doi./2022/11.01.24

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881; IMPACT FACTOR :7.816(2022); IC VALUE:5.16; ISI VALUE:2.286
Peer Reviewed and Refereed Journal: VOLUME:11, ISSUE:1(2), January: 2022
Online Copy of Article Publication Available (2022 Issues): www.ijmer.in
Digital Certificate of Publication: http://ijmer.in/pdf/e-Certificate%20of%20Publication-IJMER.pdf
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: 2nd January 2022
Publication Date:10th February 2022
Publisher: Sucharitha Publication, India

State of Tamil Nadu v. SuhasKatti[40](2004): It is the first case in India to convict an accused for posting obscene messages on the internet. The accused was a family friend of the victim and wanted to marry her but she refused and got married to some other but later she got a divorce and separated. The accused secondly proposed to her for marriage but again she refused. The accused got annoyed and send obscene messages on yahoo messenger to defame her and insult her modesty. After that, she started receiving calls in the belief that she is a sex worker. A case was registered and the accused was held liable under sections 469 and 509 of IPC and section 67 of IT Act, 2000.

10. Reasons behind the increasing number of cybercrimes against women

- Cybercrime is a global issue in these days. Cybercrimes against women are highly lifted. The women generally avoid reporting a case immediately just after its commission, even after knowing that it is a crime. The main reason behind it may be societal fear of her image or the long process of reporting it. Sometimes the culprit is known to the victim and they easily gain the confidence of the victim and use the information to harass her mentally.
- In most of the cybercrimes, the victim hesitates or feels shy to file a complaint against it, because of some sociological reasons like what would people think about her, the name of her family involved in it and ultimately the reputation of her family in society get affected. In most cases family of the victim does not support the victim. The fear in the mind of the victim about her image in society. This fear restrains her to come forward and report the crime.
- The identity of the perpetrator remains unclosed or anonymous due to the internet privacy policy. It encourages the culprit's spirit to do more wrong.
- The jurisdiction under IT Act is extended overseas. It is the reason people are not fully aware of that where to file a case. Sometimes the culprit is a foreigner then it is difficult to find out where to register a case and it is more difficult when the one act is a crime in India but the said act is not a crime or law is absent on the act.
- In India, there is no strict or fixed definition of cybercrime in any act or law. Though in the Information Technology Act, 2000 some laws and remedies are provided but all these are mostly dealing with economic and financial issues. There is no provision that is related to the crime against women and children. The said Act also does not expressly mention terms like Cyber defamation, email spoofing, cybersex, hacking and trespassing into one's privacy, etc. which is very common nowadays. As comparatively Indian Penal Code, provides specific express provisions for the protection of women, for instance, the modesty of a woman is protected under section 509, rape under section 376, sexual harassment under section 354-A, etc. The Criminal Law Amendment Act,2013[41] contains several additions to the Indian Penal Code, such as to sections 354, 354- A, 354- B, 354- C & 354- D. Now with the help or assistance of these penal provisions the several issues like stalking, sexual harassment, MMS scandals, pornography, morphing, defamation are easier to deal with.
- Lack of awareness among the people using the internet. The following table shows some data on the lack of cyber awareness.

Table 1: Awareness of cyberculture among Indian internet users[42]

Awareness of cyberculture among Indian internet users	Yes	No
Knowledge of minimum age to join cyber communities like Facebook, Orkut, Myspace, etc	56.2%	43.8%
Allow others to use one's email id/ profile id/ passwords etc	46.6%	53.4%
Use safety tips like filtering emails, locking personal albums and information, personal walls of social networking sites, etc.	69.9%	30.1%
Mail back to unknown senders of spam/ pornographic / erotic / phishing mails	37.0%	63.0%
Share personal information/emotions with virtual friends/ chat room partners etc whom you don't know in real life.	74.0%	26.0%
Believe in controlling free speech while communicating in cyberspace.	37.0%	63.0%
Read policy guidelines of social networking sites, ISPs, etc;	28.8%	71.1%
Use pseudo names	45.2%	54.8%

- India has a patriarchal society and male dominating culture and women who are victimized and mostly blamed for the crime and online victims are no exception to it.

[40] State of Tamil Nadu v. SuhasKutt,4680 of 2004 Criminal Complaint.
[41] The Criminal Law Amendment Act,2013, sec15(w.r.e.f. 3-2-2013.
[42]JaishankarKaruppannan"Cyber Victimization in India- A Base line Survey Report(2010)" SSRN Electronic Journal, DOI 10.2139/SSRN 1759708. https://www.researchgate.net/publication/228226461_Cyber_Victimization_in_India_A_Baseline_Survey_Report_2010

Cover Page

DOI: http://ijmer.in.doi./2022/11.01.24

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881; IMPACT FACTOR :7.816(2022); IC VALUE:5.16; ISI VALUE:2.286
Peer Reviewed and Refereed Journal: VOLUME:11, ISSUE:1(2), January: 2022
Online Copy of Article Publication Available (2022 Issues): www.ijmer.in
Digital Certificate of Publication: http://ijmer.in/pdf/e-Certificate%20of%20Publication-IJMER.pdf
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: 2nd January 2022
Publication Date:10th February 2022
Publisher: Sucharitha Publication, India

- At last, but not at least police also do not cooperate with the victim. In most cases, they blame the victim itself. They make them feel you are responsible for the commission of the crime. Even after giving the contact details of the perpetrator police show themselves unable to trace them. It shows the irresponsible behavior of the police towards society and being this the common man has low faith in police actions. Ultimately victim restraint herself for reporting the crime.

11. Remedies and some suggestive measures to minimize cybercrime against women

Some suggestive measures have been provided for the prevention of cybercrime against women or that may help minimize cybercrime.

- Firstly, the making of strong laws or legislation against the cybercrime which is committed against women some crystal-clear definitions, for example- cyber defamation, e-mail spoofing, cybersex, hacking, etc. shall be provided.
- Although the Information Technology Act has been enacted and it is a good initiative because at present Indian IT Act is among the few legislations on cybercrime but most of the provisions in its deal with economic or business-related crime. There is an absence of provisions that protect women and children. So, there is a need to make some amendments to the present IT Act.
- Cyber awareness programs must be organized.
- Cyber education must be provided at schools and colleges. Some cyber laws must be added to the syllabus.
- It is the age of technology. So, the awareness of the pros and cons of the technology must be taught by teachers, parents, elders to the children at an early age or from time to time when needed.
- Sex education is also provided because it is the need of the present time.
- There must be immediate reporting of cybercrime by the victim and equally immediate action by the concerned authority is required. If the victim immediately files a complaint against the crime, then there may be chances to stop further commission.
- The victim shall not be blamed for the crime. In India, in most cases, we have seen or heard that society blames females and it is a common tendency among urban and rural people.
  The irresponsible attitude of police must be changed. The police instead of filing a complaint or taking action they started blaming the victim by putting in obscene questions. This kind of behavior of police must be changed and police must come forward to solve the crime.
- The family support or moral support must be with the victim so that she can gain her confidence again and fight against the crime strongly.
- Women are mostly targeted through social media sites. They shall be careful while posting any personal information, sharing photographs and sensitive data on Facebook, Instagram, WhatsApp, etc. She first needs to check the privacy policy of the site and set it for her data information and if needed she can lock her profile.
- Cyber cells are created only in particular cities though the victim is free to file a complaint anywhere the lack of awareness of the procedure to file a case is the major reason. The procedure will be made simpler without any technicalities.
- Justice delayed is justice denied. The judicial system should be fast and effective.
- There is a need to establish some cyber courts in the country which only deal with cybercrimes cases.
- The behavior of society towards the victim must be changed because most of the time it is the fear of societal impression on her image that stops her to come forward against the wrong which is committed with her. The attitude of society should be supportive and cooperative.
- Cyberage must be fixed though it is a controversial issue with the age of the majority. Presently we live in a cyber world and the current pandemic situation where from the child of school to the businessman, govt and private sector employees everybody depends on the internet.

12. Some Govt. initiatives or programs for the prevention of cybercrime against women

The government also taking some preventive measures in form of social schemes and programs.

- **Cyber Awareness Program:** The National Cyber Safety and Security Standards introduced Cyber Awareness Program (CAP) for women and children. Its main objective is to provide safety and security to women in the cyber world while using mobile phones, computers, and the internet. The main object of the CAP is to spread awareness about cybercrime and cyber-attack and to adopt proper measures to protect themselves. CAP focus on the women and children who highly indulge themselves to take the benefit of technology by adopting safety measures.[43]

[43]https://www.ncdrc.res.in/cap.php

Cover Page

DOI: http://ijmer.in.doi./2022/11.01.24

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881; IMPACT FACTOR :7.816(2022); IC VALUE:5.16; ISI VALUE:2.286
Peer Reviewed and Refereed Journal: VOLUME:11, ISSUE:1(2), January: 2022
Online Copy of Article Publication Available (2022 Issues): www.ijmer.in
Digital Certificate of Publication: http://ijmer.in/pdf/e-Certificate%20of%20Publication-IJMER.pdf
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: 2nd January 2022
Publication Date:10th February 2022
Publisher: Sucharitha Publication, India

- **The National Cyber Security Policy 2013:** The main object of the policy is to protect information and strengthen the defence from cyber-attacks. It was released on 12 JULY 2013 by the Govt. of India. The policy aimed to provide safety measures against cyber threats and to provide security to citizens, businesses, and the government.[44]
- **Cybercrime Prevention against Women and Children Scheme:** The Union Ministry of Home Affairs to provide an effective mechanism to curb cybercrimes against women and children started the Apex Coordinator center and the same at the state level. Apex centre is in Delhi. The National Commission for Women has made its monitoring unit. The scheme provides the platform for reporting online against cybercrime. A national level cyber forensic laboratory has set up to find out the obscene content.[45]
- **The National Cyber Safety and Security Standards:** It has been started to provide safeguard to the nation from cyber threats in the cyber world. NCSSS has researched to find out the nature of the cyber threat and cybercrime.[46]

Apart from this, there are several NGOs that are working for the well-being of women. Where the police and family of the victim fail to assist and support the victim then these NGOs play a vital role to address the violence and help in providing justice. NGOs spread awareness against crimes and also provide guidelines and strengthen the victim to stand against the crime.

12. Conclusion

India is a land of God and Goddess and woman are worshipped as' Devi'. But in modern times it seems that women are the object of joy and portray as sex objects. Crimes against women are on a high rise in different forms. Society must change its vision towards the victim. The police, Government, judiciary all are must be aware and come forward to curb the evil of cybercrime. They all are updated about the latest development in the cyber world and the websites so that they find the culprit quickly. At the same time, the women also make them strong and updated about the changes in the cyber world. They must adopt safety measures and other safety tools and be careful in sharing photographs and other personal information. Cybercrime has a virtual form culprit easily hide his identity and people does not take cybercrime seriously.

Social advancement, the need for cyber education at an early age, social programming about cybercrime, and the need for more stringent penal provisions, etc. will be helpful to fight cyber disease. Most important the women should raise their voice against the crime and make them strong enough to fight with it.

[44] Information Technology Act,2000 available at: https://idsa.in/idsacomments/NationalCyberSecurityPolicy2013_stomar_260813#:~:text=With%20an%20aim%20to%20monitor,citizens%2C%20businesses%20and%20the%20government.
[45]Information Technology Act,2000 available at: https://opengovasia.com/indias-initiative-for-cyber-crimes-against-women-and-children/
[46]Information Technology Act,2000 available at: https://in.linkedin.com/in/ncsss-ncdrc