Jus Corpus Law Journal
Open Access Law Journal – Copyright © 2022 – ISSN 2582-7820
Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

Cybercrimes and Increasing vulnerability of women in Cyberspace: Indian Perspective

Dr. Somlata Sharma[a] Himani Ahlawat[b]

[a]Associate Professor, MDU Centre For Professional & Allied Studies, Gurugram, India [b]MDU Centre For Professional & Allied Studies, Gurugram, India

Received 05 May 2022; *Accepted* 30 June 2022; *Published* 25 July 2022

The Internet has helped in empowering women and in raising their voices against injustice and unsocial acts. It has given them a platform to raise their voices. However, the cyber world is like virtual reality and anyone can choose to remain anonymous or fake their identity. Cybercriminals use this to their best advantage in targeting their victims. Widespread internet coupled with a global pandemic resulted in growing cyber crimes against women. There are no borders in the virtual world and courts suffer in deciding where the jurisdiction lies. Because of a huge gap between the nature of a traditional crime and cybercrime are challenges faced in dealing with cybercrime and evidence collection. Due to a global platform, it is very difficult to deal with cybercrime. The criminals are using this to their maximum benefit as they have the confidence of remaining anonymous which will help them in staying undetected. Since cybercrime has become a global phenomenon, it targets more victims than traditional crimes. Unfortunately, like many traditional crimes, some cybercrimes specifically target women and compromise their security. The National Commission for Women received many complaints regarding the same, especially during the covid-19 pandemic which led to a lockdown. In this research paper, the authors have analyzed the factors responsible for the growth of cybercrimes against women and various barriers to combatting such crimes. The complex nature of cybercrimes coupled with the sensitive issue of the safety of women gives rise to several issues and challenges. The paper also critically analyses the loopholes and deficiencies in the law regarding the same. The authors have also discussed the impact of such crimes and their societal implications. The paper

concludes with the response by the judiciary in dealing with cybercrimes against women and by providing recommendations for the same.

Keywords: *internet, lockdown, cybercrimes, barriers, covid-19, pandemic, women*

INTRODUCTION

The role of technology has evolved at a rapid pace. Its dynamic nature has helped change many traditional works and made them less time-consuming and cheaper. In the past years, the widespread use of the internet all over the globe has helped users to communicate and share information in the fastest way possible. The Internet has become a part of our daily lives especially since the pandemic led to work from home and online classes. It has now become a necessity rather than a luxury. Its efficient use at a low cost has helped the development of businesses and governments. Distance is no longer a barrier as the internet has no boundaries. The internet has led to the betterment of human life but this also comes with a very heavy price. The negative sides of the internet are equally alarming. As a famous saying goes 'excess of everything is bad it is also applicable to the vast digital space which only keeps expanding. The world of technology has also given birth to a number of cybercrimes like hacking, cyberterrorism, cyber pornography, cyberstalking, invasion of privacy, financial and data thefts, cyberwarfare, phishing, and many others. These crimes are only increasing day by day as cyberspace allows cybercriminals to target more victims while hiding their own identities. Technological advancement has also benefitted women in a great way. It has allowed them to expand their knowledge, work conveniently and socialize. However, cyberspace has also led to an increase in the victimization of women. Cybercrimes are evolving at a fast pace and there is a variety of them. These are growing in all directions targeting business, property, common man, government, women, and children. However, recently there have been a number of cybercrimes against women.[1] These include online harassment, cyberpornography, revenge pornography, image morphing, blackmailing, cyberbullying, cyberstalking, online trolling, etc.

[1] 'Corona Lockdown Is Giving Rise To Cybercrim' (*ABP Live,* 8 April 2020) <https://news.abplive.com/trending-news/coronavirus-pandemic-cause-cybercrime-to-rise-1193085> accessed 05 April 2022

Cybercrimes against women have been increasing for a number of reasons. Perpetrators perceive women as a soft target. Many women do not report such crimes due to fear of further harassment and societal concerns. Some are not aware of their rights and cyber law while others are still caught in the web of pending cases.[2] The vulnerability of women in cyberspace poses a great threat to not just the victims but also the society at large. There are a number of factors responsible for this scenario. It includes social factors, lack of awareness, deficiency in cyber laws, etc.[3]

MEANING OF CYBERCRIME

Cybercrime is a criminal activity that either attacks a computer/internet or any other device/technology mentioned in the Information technology Act 2000. In other words, if a computer or internet is used either as a tool or as a target or both for any illegal activity then it falls under the category of cybercrime.[4] The term cybercrime has not been defined in any act or provision in India. Many might view this as a loophole or a legislative gap but it is indeed not possible to come up with an exact definition of cybercrime. The definition needs to have a wide scope as limiting it to just a few words won't do justice. The technology is changing at a fast pace because of which it would not be practical to form a definition as it would have to be amended from time to time. It is growing at a fast pace and poses a great threat in Modern India.

NATURE, SCOPE, AND IMPACT OF CYBERCRIME AGAINST WOMEN

The Internet has helped in empowering women and in raising their voices against injustice and unsocial acts. It has given them a platform to raise their voices. However, the cyber world is like virtual reality and anyone can choose to remain anonymous or fake their identity.

---

[2] Prof. S. I. Kumbhar & Raju Gaikwad, 'Cybercrimes against Women-perception and opinion of cyber cell officials' (2019) 8 (42) Scholarly Research Journal for Humanity Science & English Language <https://oaji.net/articles/2021/1201-1610009923.pdf> accessed 05 April 2022

[3] Deepshikha Sharma, 'Cybercrime in India: Are Women a soft target?' (*Legal Service India*) <https://www.legalserviceindia.com/legal/article-639-cyber-crime-in-india-are-women-a-soft-target.html> accessed 05 April 2022

[4] Michael Aaron Dennis, 'Cybercrime' (*Britannica,* 19 September 2019) <https://www.britannica.com/topic/cybercrime> accessed 05 April 2022

Cybercriminals use this to their best advantage in targeting their victims. Widespread internet coupled with the global pandemic resulted in growing cyber crimes against women. There are no borders in the virtual world and courts suffer in deciding where the jurisdiction lies. Because of a huge gap between the nature of a traditional crime and cybercrime are challenges faced in dealing with cybercrime and evidence collection. Due to a global platform, it is very difficult to deal with cybercrime. The criminals are using this to their maximum benefit as they have little to no fear of detection. Since cybercrime has become a global phenomenon, it targets more victims than traditional crimes. Unfortunately, like many traditional crimes, some cybercrimes specifically target women and compromise their security. Women are mostly victims of crimes like pornography, cyberstalking, cyberbullying, online harassment, etc.[5]These can harm their minds and lives. They may cause mental trauma and injury, especially to the young victims.[6] These rights are also violative of the right to privacy guaranteed to citizens. Internet grants access to cybercriminals to invade the privacy of others and gravely violate these rights.[7] It is of utmost importance that the cybercrimes which are committed via social networks should have strict and stringent punishment because they impact deterrent. There are thousands of instances of cyber harassment which are not even reported. Cyber stalking and cyber harassment can lead to rape threats and other forms of violence. Many threaten women with leaking their personal photographs or information online.

Often people simply say that the solution to these problems is to not use social media or limit its use. Victim blaming is not the solution in such cases as we cannot ask them to limit their access to online media and hamper their right. By asking the victim to stay offline it is a deprivation of their opportunities and rights. Many people are cyberstalked by their former

[5] Tanaya Saha & Akancha Srivastav, 'Indian Women at Risk in the Cyber Space: A Conceptual Model of Reasons of Victimization' (2014) 8 (1) International Journal of Cyber Criminology, 57, 62 <http://www.cybercrimejournal.com/sahasrivastavatalijcc2014vol8issue1.pdf> accessed 05 April 2022

[6] Dr. Monika Jain, 'Victimization of women beneath cyberspace in Indian upbringing' (*Manupatra*) <http://docs.manupatra.in/newsline/articles/Upload/786274E9-B397-4610-8912-28D6D03230F9.monika_jain_pdf_1-1111.pdf> accessed 05 April 2022

[7] Priyanka Devi & Satish Kumar, 'A Discourse on Cyber Crime Against Women: Problems and Prospects' (*Jus Dicere*) <https://www.jusdicere.in/a-discourse-on-cyber-crime-against-women-problems-and-prospects/> accessed 05 April 2022

spouses or ex-partners of their significant other.[8] This obsession could turn dangerous and might even lead to violence. Perpetrators can harass their victims and send them threatening messages. They can also spy on the victims with the help of following their social media updates. They can also gather personal information of the victims by searching it online and misusing it for illegal purposes.

KINDS OF CYBERCRIMES AGAINST WOMEN

Some of the cybercrimes that target women are as follows:

1. Cyber harassment
2. Cyberstalking
3. Cyber pornography
4. Cyber defamation
5. Morphing images/videos
6. Email spoofing

Cyber harassment often happens via e-mails. It is actually an old concept that can be linked to harassment by sending physical letters. Harassment can be caused by sending threatening, bullying, or blackmailing messages. Even cheating can amount to harassment. Cyber harassment takes on a more dangerous role as unlike harassment via letters, cyber harassment often takes place via fake accounts or IDs. This makes it difficult to identify and catch the perpetrator. Cyberstalking cases are emerging daily and are on a rise. Cyberstalking means consistently following a person's cyberspace movements and sending or posting messages which can sometimes be even threatening in nature. It involves following the victims in chat rooms used by them frequently and continuously sending messages and emails. The problem with this kind of activity is that even if you block the person's account who has been stalking

[8] Shweta Sankhwar & Arvind Chaturvedi, 'Women harassment in digital space in India' (2018) 118 (20) International Journal of Pure and Applied Mathematics, 597-598 <https://www.academia.edu/66950306/Woman_Harassment_in_Digital_Space_in_India> accessed 05 April 2022

you, they can make countless new or fake accounts and continue to stalk. Usually, cyberstalking is done by men who stalk women online or pedophiles who target children.[9]

The reason why cyberstalking is increasing rapidly is because of easy and cheap internet availability, free and unlimited creation of online accounts, and anonymity.[10] The majority percentage of cyberstalking victims are females.

There can be different motives for cyberstalking: -

- Sexual harassment
- Obsession (for love)
- Revenge or hatred
- Ego and power trips.

The Internet has made facilitating pornographic material quite easy and simple. There is no dearth of pornographic sites and materials online. There are almost negligible regulations and policies on pornographic content. A simple google search will allow anyone to access pornographic content. These materials are not just limited to images but also include video clips and movies. The most common trend, especially amongst teenagers that leads to cyberstalking or harassment is that by making new friends online. Words such as 'sexy', 'hot' etc. are often used by males to refer to their online female friends. This is considered the beginning of obscenity online by normalizing such behaviour. These men then start gaining the confidence of their female friends online. As they keep getting familiar, they start sharing their personal problems and life details. The perpetrators also encourage victims to reveal more information by acting as fake friends. Later on, the same can be manipulated and used against the victims. It is advised that in such situations, female victims should immediately report the matter and threaten the perpetrator with legal action. As such cybercrimes add to

[9] Anastasia Powell & Nicola Henry, *Sexual Violence in a Digital Age (Palgrave Studies in Cybercrime and Cybersecurity)* (1st edition, Palgrave Macmillan 2017) 77

[10] S hanu, 'Cyber Stalking And Harassment on Women' (*Legal Service India*) <http://www.legalserviceindia.com/legal/article-909-cyber-stalking-and-harassment-on-women.html> accessed 05 April 2022

violence against women it is very important to raise awareness and educate women on online safety measures.

REASONS FOR INCREASE IN CYBERCRIME AGAINST WOMEN

- **Easy availability of victims' (women's) personal information:** There are billions of users of social media websites. Many of them keep updating their profiles with recent pictures and status of what is going on with their lives. Even though some details are optional while registering on these applications many provide sensitive information including addresses and phone numbers.[11]
- **Ignorance and carelessness of the users:** There are ways to restrict other users and have some privacy on social media but these options are not known to all. In order to protect oneself from online harassment, the user can set up restrictions in the security and privacy settings for locking their accounts or personal pictures and limiting access to messages from unknown users. Some people are also unaware of the option of blocking and/or how it works. One can opt for a private account or a public. Some social websites also allow users to report particular messages and/or users online in cases of infringement of their legal rights.[12]
- **Nexus with Pandemic and Lockdown:** There is sufficient evidence linking the rise of cybercrimes against women with lockdowns during a pandemic. According to the 2021 report of the National Commission for Women, it was noticed that cases of cybercrimes against women would increase drastically during the lockdown.[13] So, it can be said that lockdown has been another major cause of the increase in cybercrimes against women. During the lockdown, people were forced to rely on the internet for work, leisure, education, and social reasons. Because of lockdown unsocial elements and criminals

[11] Abhinav Sharma & Ajay Singh, 'Cyber Crimes against Women: A Gloomy Outlook of Technological Advancement' (2018) 1 (3) IJLMH, 5 <https://www.ijlmh.com/cyber-crimes-against-women-a-gloomy-outlook-of-technological-advancement/> accessed 05 April 2022

[12] Shashya Mishra, 'Dimensions of Cybercrime Against Women in India- An Overview' (2018) 5 (4) IJRAR, 970 <https://www.ijrar.org/papers/IJRAR1944342.pdf> accessed 05 April 2022

[13] Rahul Tripathi, Cases targeting women with explicit content double in 3 years' (*The Economics Times,* 6 January 2022) <https://economictimes.indiatimes.com/news/india/cases-targeting-women-with-explicit-content-double-in-3-years/articleshow/88719638.cms> accessed 05 April 2022

could not physically cause trouble to their victims. Hence, they started causing mental and emotional harassment to women online.[14]Some infamous cases like the 'bullbar application' incident, 'Bois lockerroom, etc took place during this time.

- **The cloak of anonymity:** This is probably the biggest reason that encourages cybercriminals to involve in cybercrimes without the fear of being caught. They can easily hide their identity or create multiple fake accounts. It is difficult to detect the exact location of the perpetrator. IP addresses can be traced but hard-core cybercriminals or professionals know how to hide their IP addresses as well.[15]
- **Lack of responsibility on social sites and intermediaries:** Although there are rules and laws that websites and intermediaries have to adhere to yet some policies are vague.[16] For example, websites have their own policy regarding what they consider defamatory or harassment. One may report a particular message, post, or user but the reasons must match the terms and conditions of the website. Many social websites do not have a minimum legal age barrier or do not ask for proof of the same.
- **Lack of adequate legal protection:** It is a sad reality that even after the enactment of the IT Act 2000 and its amendment in 2008 there are many crimes and issues regarding women that are still not covered by the Indian legislation. It fails to mention the crimes that specifically target women and children. No doubt that the Act has some noteworthy provisions, such as hacking and publishing obscenity but it fails to cover the gravity of the threat to women's security. The present cyber laws lack the force of implementation and do not match the ground reality.[17]
- **Hesitation to report cases:** Female victims do not report these crimes due to fear of victim blaming and social stigma. Also, they receive threats from the perpetrators to not

---

[14] 'Cyber threat in times of coronavirus outbreak' (*Financial Express,* 8 April 2020) <https://www.financialexpress.com/opinion/cyber-threat-in-times-of-coronavirus-outbreak/1921878/> accessed 05 April 2022

[15] Sanjeev Kumar & Priyanka, 'Cybercrimes against women: right to privacy and other issues' (*Research Gate,* October 2019) <https://www.researchgate.net/publication/344153821_CYBER_CRIME_AGAINST_WOMEN_RIGHT_TO_PRIVACY_AND_OTHER_ISSUES> accessed 05 April 2022

[16] Dr. Jyoti Rattan, *Cyber Laws & Information Technology* (Bharat Law House Pvt. Ltd. 2017) 94

[17] Shreyaa Mohanty, 'Cyber Crimes Against Women: What do the Indian Laws Say?' (*ProBono India,* 6 May 2020) <https://www.probono-india.in/blog-detail.php?id=118> accessed 05 April 2022

register complaints against them. Usually, complaints regarding harassment are filed by teachers, airline staff, students, and celebrities who become victims of defamatory, derogatory, or morphed content.[18]

- **Unsupportable Behavior of Police and Administration:** In absence of concrete proof and evidence police often do not encourage such cases and refuse to take complaints. Some other reasons for cybercrime against women include the boundaryless and everchanging nature of the internet, its cost-effectiveness, numerous vulnerable targets, etc.[19]

LEGAL FRAMEWORK OF CYBERCRIMES AGAINST WOMEN

A broad generalization of cyber laws protecting women can be laid down in certain provisions of the Indian Penal Code 1860, Information and Technology Act 2000, and Indecent Representation of Women Act.

The Indian Penal Code has the following provisions:

- Section 499[20] deals with defamation (includes spreading false information about someone online or offline)
- Section 503 and 507[21] deal with criminal intimidation (includes threats made against reputation and also deals with blackmailing)
- Section 509[22] deals with an insult to modesty of women and violation of privacy.

[18] Advocate Kriti, 'Growing Indecencies or Obscenity In Cyber World And Legal Regime In India' (*Legal Service India*) <http://www.legalserviceindia.com/legal/article-1593-growing-indecencies-or-obscenity-in-cyber-world-and-legal-regime-in-india.html> accessed 05 April 2022

[19] Dr. Kasturi Bora,Cyber socializing and the growth of Hi-tech crimes against women' (2019) 6 (1) & (2) Law Mantra <https://journal.lawmantra.co.in/wp-content/uploads/2019/09/6.pdf> accessed 05 April 2022

[20] Indian Penal Code, 1860, s 499

[21] Indian Penal Code, 1860, ss 503 and 507

[22] Indian Penal Code, 1860, s 509

The Criminal Amendment Act 2013 made way for a few more provisions in the Indian Penal Code 1860 to deal with cybercrime against women. These are as below:

- Section 354A[23] deals with sexual harassment of women (includes both online and offline sexual harassment)
- Section 354C[24] which deals with Voyeurism
- Section 353D[25] which deals with stalking (includes cyberstalking)

The IT Act which was enacted in 2000 and amended in 2008 covers certain cyber crimes against women in the following provisions:

- Section 66 C[26] (Identity theft and hacking)
- Section 66 E[27] (violation of privacy and accessing private pictures without consent)
- Section 67[28] (obscene content)
- Section 67A[29] (sexually explicit materials)
- Section 67B[30] (sexually explicit materials depicting minors)
- Section 72[31] (Breach of confidentiality and privacy)

DRAWBACKS IN LEGAL PROVISIONS

- There are a few provisions offering protection to women against cybercrime of pornography and related offences, unfortunately, Section 77[32] of the IT Act 2000 has made all such offences bailable. Thus, it renders the above-mentioned provisions inefficient.[33]

[23] Indian Penal Code, 1860, s 354A
[24] Indian Penal Code, 1860, s 354C
[25] Indian Penal Code, 1860, s 353D
[26] Information and Technology Act, 2000, s 66C
[27] Information and Technology Act, 2000, s 66E
[28] Information and Technology Act, 2000, s 67
[29] Information and Technology Act, 2000, s 67A
[30] Information and Technology Act, 2000, s 67B
[31] Information and Technology Act, 2000, s 72
[32] Information and Technology Act, 2000, s 77
[33] Satish Chandra, *Cyber Law in India* (ABS Books 2017) 84

- At an age where intermediaries and service providers should be held responsible/accountable for illegal content, Section 79[34] of the IT Act grants immunity to them. The words mentioned in the provision are "due diligence" with respect to the role of intermediaries when a third-party posts offensive or illegal material.[35]
- The term cybercrime is not defined in the IT Act and its reason can be perfectly attributed to its dynamic nature which makes it quite impractical to define the term. However, the IT Act also fails to define important terms such as cyber-defamation. Its definition can only be traced through the Indian Penal Code.
- It is pertinent to note that the IT Act has successfully covered the majority of economic and commerce-related crimes protecting businesses. However, women are harassed by major cybercrimes such as cyberstalking, morphing, spoofing, etc. but these have not been specifically mentioned in the Act.[36]
- Even though obscenity is an offence under the Act, viewing it privately isn't.
- The IT Act was amended in 2008 and after that, no notable changes have been made. Technology has changed drastically in the last decade leading to the birth of new cybercrimes but nothing is being done to address the same.

JUDICIAL RESPONSE

The case *of Suhas Katti v State of Tamil Nadu*[37] resulted in the first conviction of cyberpornography in India. The accused (SuhasKatti) had sent obscene, derogatory, and defamatory messages about the complainant who was a divorced woman. These messages were sent on e-mails and in the message group (Yahoo). He had created a fake email account of the woman and sent e-mails stating that the woman was soliciting sex. The court held the accused guilty under Sections 67 IT Act, 469, and 509 of IPC. In India, the first conviction of

[34] Information and Technology Act, 2000, s 79
[35] Dr. Ishita Chaterjee, *Laws on Information Technology* (2nd edition, Central Law Publications 2018) 69
[36] Mayura U. Pawar & Archana Sakure, 'Cyberspace and Women: A Research' (2019) 8 (6) IJEAT, 1670 <https://www.ijeat.org/wp-content/uploads/papers/v8i6S3/F13130986S319.pdf> accessed 05 April 2022
[37] *Suhas Katti v State of Tamil Nadu* (2004) C No. 4680/2004

cyberstalking was in *Yogesh Prabhu v State of Maharashtra*.[38] Accordingly, the accused was convicted under Section 509 of IPC and Section 66 E of the IT Act.

SMC Pneumatics (India) Pvt. Ltd. v Jogesh Kwatra[39] was the first Cyber defamation case in India. The jurisdiction was assumed by a Delhi Court. The case was concerned with defaming a corporate's reputation via emails. The defendant was an employee of the company who sent derogatory, obscene, vulgar, abusive, and defamatory emails to the employers and various subsidiaries of the company in order to defame the company and the Managing Director. The court heard both the parties and passed an ex-parte interim injunction based on the prima facie case made by the plaintiff company and restricted the defendant from sending such defamatory emails and messages. *Fatima Riswana v State Representative by A.C.P, Chennai &Ors*[40] dealt with the procedural challenges for sensitive cases like cyber pornography. In the *Baazee.com*[41] case, Avnish Bajaj was the CEO of an online auction site. He was accused of distributing pornographic material online. Somebody sold pornographic content via Baazee.com and the same was sold on a CD in Delhi Markets. He was granted bail on the condition that he would participate and assist in investigating the case. The *Air Force Bal Bharti, Delhi Cyber Pornographic Case (2001)*[42]*:* the accused in this was a student of this school who was being teased by his classmates with cruel jokes regarding his face blemishes and scars. To get back at them, the student created a website on which he uploaded morphed nude photographs of his teachers and classmates. A complaint was registered by the father of one of the victims who saw this content online. However, the case was compromised and was dropped later on.

[38] *Yogesh Prabhu v State of Maharashtra* (2009) C.C. NO. 3700686/PS/2009
[39] *SMC Pneumatics (India) Pvt. Ltd. v Jogesh Kwatra* (2014) Suit No. 1279/2001
[40] *Fatima Riswana v State Representative by A.C.P, Chennai & Ors.* (2005) Appeal (Criminal) No. 61-62/2005
[41] *Avnish Bajaj v State (NCT of Delhi)* (2008) 150 DLT 769
[42] Nidhi Chhillar, 'Cyber Pornography' (*Ipleaders,* 9 July 2019) <https://blog.ipleaders.in/cyber-pornography/> accessed 04 February 2022

ISSUES AND CHALLENGES FACED IN DEALING WITH CYBERCRIME AGAINST WOMEN

1. **Geographical Challenge and the virtual world:** There are no borders or boundaries when it comes to the internet. While cybercrime itself is done in cyberspace, the criminal is actually outside cyberspace. A human commits the act but that act is in a virtual world. Unlike traditional crimes, cybercrime involves many territories making it difficult to determine the jurisdiction.[43]
2. **Evidence collection:** Another challenge that is faced due to the nature of cybercrime is the gathering of evidence. It is very difficult for investigating agencies to collect the evidence and prove them in court. The police and investigating authorities are not able to collect or store this evidence.[44] This makes it difficult to prove the crime and hold the accused guilty without reasonable doubt. This lack of evidence and anonymity further gives encouragement to criminals to indulge in cybercrime. Criminals can easily destroy their own evidence making it more difficult for law enforcement agencies.
3. **Non-reporting of cases:** Either victims are not aware of their rights or they hesitate to report. In cases of crime related to women, generally, people are afraid about how society will react due to this fear girls and their parents do not report the crime. Another fear in a child's and his family's mind is that the law on cybercrime isn't so strong and powerful yet. The criminal might go to jail today and come out tomorrow to be more revengeful. Due to cybercrime, common people are harassed mentally, financially, and emotionally.
4. **Technical Complexities:** These include the use of proxy servers, international law, untraceable evidence, unawareness of the people on how to deal with digital evidence, etc. Cybercriminals are often located by tracking IP addresses. However, it is even difficult to track them as there is a whole other dimension of the internet that many are

[43] Dr. Amita Verma, *Cyber Crimes and Laws* (Central Law Publication 2012) 102
[44] Anirush Rastogi, *Cyber Law- Law of Information Technology and Internet* (Lexis Nexis 2014) 68

not aware of. Deep Web does not show up in traditional search engines and is a hidden part of the internet.[45]

5. **Lack of competent authorities:** Dealing with digital evidence requires high competency. However, police officials are not well trained or well equipped in such matters. Special units and cyber cells also face the unavailability of forensic tools for the gadgets with the latest technology.[46]

CONCLUSION AND SUGGESTIONS

To conclude, the present IT Act focuses more on economic and commercial issues while leaving out crimes against women. It is a sad reality that even after the enactment of the IT Act 2000 and its amendment in 2008 there are many crimes and issues regarding women that are still not covered by the Indian legislation. No doubt that the Act has some noteworthy provisions, such as hacking and publishing obscenity but it fails to cover the gravity of the threat to women's security.

Easy accessibility to the Internet and the attraction of surfing the Internet without having proper knowledge are some of the major responsible factors for increasing cyber crimes against women. The majority of the women victims faced the problems like mental disturbance, obstacles in marital life, and also arrangement of marriage. Also, there are adverse effects on the social life of women due to cybercrime victimization. The Indian IT Act 2000 is not been effectively enacted due to some deficiencies and therefore, there is an increase in the rate of cybercrimes against women in India. Cybercrimes against women are already tough to deal with due to jurisdiction issues, lack or loss of evidence, and ineffectiveness of law enforcement agencies. To add to these challenges, the IT Act 2000 fails to provide provisions and stringent punishments relating to the same. Moreover, female victims do not report these crimes due to fear of victim blaming and social stigma. Also, they receive threats from the perpetrators to not register complaints against them. The biggest weapon to curb the

[45] Vakul Sharma, *Information Technology Law and Practice* (Lexis Nexis 2017) 56
[46] Vicky Nanjappa, 'Our cyber cells are not equipped to deal with cyber crime' (*Rediff*, 20 September 2009) <http://news.rediff.com/interview/2009/sep/20/inter-our-cyber-cells-cant-deal-with-cyber-crimes.htm> accessed 07 April 2022

problem is to first make women aware of the existence, dangers, and prevention of cybercrimes. The law regarding cyber crimes against women should be strict and stringent to avoid further fear for the victims and police authorities should not be lax in acting and dealing with it. The police officials should also be trained and educated on how to deal with such cases. Many states lack the technology to collect and preserve evidence related to cybercrime in electronic form. Therefore, it is important to invest in cyber forensics and acquire the latest technology. Awareness amongst the younger generation to make them understand what cybercrime is and how to prevent it is equally important. They need to be taught not to disclose their identity online to strangers which could lead to cyberstalking.