

**INTERNATIONAL JOURNAL OF LAW
MANAGEMENT & HUMANITIES**
[ISSN 2581-5369]

Volume 3 | Issue 4

2020

© 2020 *International Journal of Law Management & Humanities*

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com>)

This Article is brought to you for “free” and “open access” by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in International Journal of Law Management & Humanities after due review.

In case of **any suggestion or complaint**, please contact Gyan@vidhiaagaz.com.

To submit your Manuscript for Publication at **International Journal of Law Management & Humanities**, kindly email your Manuscript at editor.ijlmh@gmail.com.

Enactment of Law for the Protection of Women against Cyber Crime

SURUCHI YADAV¹ AND SRIJANA CHANDEL²

ABSTRACT

As far as innovative technology promotes our brilliance and provides social connectivity, it also affects our uprightness and confidential life. Cybercrime leads to downtrodden which may cause social assault all over the world. The intimate existence of men and women are affected by these cyber criminals. "are the women in 21st century safe?" NO, on a daily basis women's are abused in front of the community due to cybercrime women's are forced to become the victim of social assault like rape, molesting, harassment, etc. which causes mental disorder which also leads to affliction of physical health care. In order to provide protection against cybercrimes government has introduced Indian IT act, 2000. It is the primary Indian law which deals with CYBER

CRIME and E- COMMERCE. This act covers whole of India and recognizes electronic records and digital signatures. In order to empower society in cyber security the young generation has to be encouraged.

The present paper seeks to clarify how the cybercrime is demolishing our young innovative generation and exploiting women esteem by menacing, this paper also elaborates the various measures which have been taken by Indian government to curb exploitation of women through electronic mediums like cyber cell, police helpline, cops, etc.

Keywords- cybercrime , rights of women , , forced , crime , helpline , harassed , penalties, punishments , fundamentanl rights

I. INTRODUCTION

Today's advancement of technology has captured the whole society. In these days most of the people are wholly curved around the technology but we are unaware of these facts. Computer and internet has transformed the whole world into a global community by generating cyber space, cyber space is an ordinary patrimony of human race but in Today's generation some people take disadvantage of these ordinary patrimonies thus cyber space has also become a new perimeter of various types of crimes. Cyber space is a super highway of

¹ Author is a student at Amity Law School, Amity University, Chhattisgarh, India.

² Author is a student at Amity Law School, Amity University, Chhattisgarh, India.

dispatching of knowledge and information across the world through unseen microwaves. As we observe that our society have become very dependent on these advanced technologies, For example payment of grocery stores, booking of movie tickets and also the accommodation of hotels has become very easy for people as all these can be done easily through internet. During all these evolution of technologies, criminals have also taken the advantages of these situations and used it for their benefits, advanced technologies has only made it easier for the criminals to commit their crimes. Victims unknowingly become target of these criminals as people don't protect their identities on social media and they reveal their whole routine. For criminals it becomes more easier to collect the information about the victim unfortunately victims themselves unknowingly help the criminals. With the rapid growth of technology cyber crimes are also growing along with it. As safety is one's own responsibility people should start taking precaution of their security. Cyber crimes have serious impacts on the society which also cause psychological destroy, threat to national defence, hacking of intimate identification, Online bank information theft and unauthorized computer access, etc. and for all these crimes we have some severe punishments which are imposed on conviction.

In every second one or the other women gets deceived to be a victim of cyber crime. The online platform is a new platform where women's position, privacy and security are being challenged in every moment. Molesting, harassment, body shaming, revenge porn, black mailing and many other forms of indecent depiction of women are widespread in the cyber world. The cyber crimes against women causes mental disorder more than the affliction of physical health care. Criminals target to defame women by sending of obscene messages, E-mail, stalking women by using chat rooms, and the worst of all by developing pornographic videos. One of the major causes of harassment these days is cyber bullying.

Why people commit cyber crime? People who commits cyber crime are are mostly well organized they commit cyber crime as committing cyber crimes online allows a person to hide their location and identity. The word cyber crimes alludes to a different variety of crimes through computers, laptops, tablets, smart phones, internet connected televisions. Cyber stalkers steal confidential data which is stored online

II. GROWING ISSUES OF CYBER CRIMES AGAINST WOMENS

CYBER STALKING is a commitment of crime where a victim gets harassed by the attacker where women's are the main victims. They are stalked through obscene E-mails or IM (instant messaging), flaming. Women's are mainly stalked by men which have brutal impact on their

private life through electronic mediums such as internet or (www) World Wide Web women are used to pursue, harassed which again leaves a great impact on their psychology. According to the report of IC3 (crime complaint center) 2017 internet crime report which was published on may

2018 the report represents the total of 301,580 complaints were reported by the victims and the main complaints of violence against women where women are being victimized, molested, intimidated and due to all these issues women's are being treated brutally by their own family members and society which forces them to commit suicide and self harm which causes mental disorder. It is sad to accept but Cyber stalking is a creepy part of the modern society cyber stalkers have some really bad intentions – To embarrass, threaten, or to harass their victims the difference is they do all these brutal crime online behind the walls of real world. Everything on the internet are used by cyber stalkers to make ill-suited contact with their victims. Is cyber stalking and social media stalking has a same meaning? the answer is NO, we must not get confused between cyber stalking and social media stalking cyber stalking is really serious as it has evil intention ranging from defamation to sexual harassment and the cyber stalkers also encourages other people to harass the victims, social media stalking is not as cruel as cyber stalking Have you ever undergone the irritating or vexatious experience of being stalked? it really doesn't matter to cyber stalkers that you are a working women or a college student, or a house wife, or a school going student most of the time the cyber stalkers are our own close friends, family members too. a women said that she feels like a trapped animal whenever she gets stalked by cyber stalkers it feels like an frightening or a very horrible experience around 20 percent of the women are affected by cyber stalking due to the fear of being stalked many women don't like to even come out alone in the public, women quit using social media sites like instagram, face book, orkut, yahoo, twitter, snap chat. Some remedies to cyber stalking is? Filing a complaint online? women's who are being stalked can file a complaint to National Commission for women(NCW)and the commission will help the women to get rid of these cyber stalking problems and if needed commission will take the issue of cyber stalking to the police. In some serious cases the commission forms an committee for inquiry then the commission asks the police to accelerate the investigation. Commission has powers to summon the criminal. the enquiry committee of the commission starts an spot inquiry, examines witness, and collects the evidence against the cyber stalker National Commission for women's allows all the women across the country to file a suit against the cyber stalkers. Also the government of India has introduced many HELPLINE NO. Like if women are being stalked in DELHI, she can call 1096. For the rest women of India can make a call to National

commission for women (NCW) contact them on 0111-23219750. women's should always collect evidence they must not feel scared they must always collect the evidence against the cyber stalkers is she has any doubt on anyone even 1% then also she must collect the information even though women will not be asked to submit the evidence when she first report but for her own safety she must take some precautions for herself and must save the evidence safely because sometimes crime branch also needs your support to solve the case we must collect some evidence like chat room or a newsgroup text, printed copies of E-mails, screenshots of social media messages, etc. recently a case is being shown of NEW DELHI, : A law student of Delhi university has been accused of threatening and stalking a woman online. He created fake profiles on social networking sites and he tried to defame her identity the woman has filed a complaint with DELHI POLICE against the boy that the accused has been harassing her for over an year she told that the law student is making obscene phone calls and sending threatening, vulgar messages to her. FACTS: the accused asked the woman to get married to him but when she refuse to do so, he started blackmailing the woman and threaten her that he will kill her if she will not marry him and after all this she filed a suit against the boy in Sarita Bihar police station where he apologized and also promised her that he will not disturb her. but when the victim went to Goa to peacefully live along with her parents the boy again disturbed her, he created a fake profiles on social media websites and he uploaded some pictures with her and he stated or proclaimed that she is her wife this case is under section 66-A of Information Technology Act 2000 was registered at the economic offences wing in a complain she stated that that she is a victim of cyber staling and also the victim of personal identity theft ²

III. HACKING

Hacking is an unofficial access to computer and the people who are involved in hacking are known as hackers. Hacking is done for both positive as well as negative purpose but, mostly it is only used or done for negative purpose. Hackers used to break the security system of computer or website without the honest knowledge and it damages the system. Hacker's practices theft by hacking the personal data, because of hacking not only men and their personal data are affected but also, women and their private life are affected. Hackers hacks the personal account of women and they edit their profiles and starts to blackmail them and they demand for greater amount of money or for the sexual intercourse. Mostly because of the fear of society and because of her own in-laws she hesitates to go to the police and file a complaint about the case, because of the fear of the self image and the reputation of the family

often some women commits self harm. Hacking may cause serious affect to the future of E – commerce, a huge investment is required to protect E-commerce as we know, that now hacking has become a severe major problem of our country. We can take an example from an earlier

CASE - where hackers had inserted a link to a pornographic websites from the website of SEBI (stock exchange board of India) which left out a great negative impact on SEBI's reputation.

Cyber crime cells are one of the most appropriate solutions for tracking for combating and tracking cyber crimes. Cyber crime is an act of cyber crime which includes the act of online banking or credit scams, proliferation software viruses, stalking, etc. these cyber cells are the masterminds of the criminal investigation department of the cities in India .under each department of the cities in India cyber cells have been opened only to handle the issues of internet or website based crimes which are governed under the information technology act, 2000 the act also penalized such act:-

1. The computer as a target where a personal computer is used to beat other personal computers which are involved in crime for example hacking, virus/worm assaults, pos assaults and many other.
2. The personal computer as a weapon- where a personal computer is used to execute and commit actual and real world's criminal activities.

For example – digital terrorism, IPR, credit card scam, pornographic and so on. In one of the case of major cyber attack infringement, hackers have stolen Rs 94 crore by hacking the ATM switch server of the cosmos bank, one of in India's oldest co- operative banks in Pune. The hackers have stolen all the details of multiple visa and rupay debit card of the owner. Around 12000 foreign transaction were made of rupees 78 crore and another transaction of rupees 12 crore, was sent to Hanseng bank which is located in Hong Kong. The case was filed by the cosmos bank with Pune police cyber cell and other than Pune police foreign investigative agencies were also involved in the case.³

IV. CYBER FRAUD AND CHEATING

In every day news we hear that an individual have being fraud or being cheated by one or the other person. The growth of internet fraud is rapid, in every sector of this world internet is used for all the transactions, communication etc. whether it be financial institutions, household work or any other business , in short cyber fraud and forgery also affect the e-commerce and

act as a barrier in the profitable growth of e-commerce. These cyber criminals also cheats the women, women often talk to the unknown people on social medias and these unknown people starts cheating the women by winning their trust, chatting on social media and the women are trapped into their plans of being molest, the criminals become very familiar with the girls, and afterwards they ask for obscene pictures and pornographic videos. Mostly women afraid to go the police and file a complaint of being molested and even if they go, most of the time the police fails to trap them. After committing crime these criminals disappear and never gets caught, this deformity of police promotes the cyber criminals to repeatedly do the same crime but there are several agencies which control and decline the growth of cyber crimes. The FBI (federal bureau of investigation) which is formally known as the bureau of investigation, It is the federal agency for investigating cyber crimes done by criminals, terrorists etc. it also identifies the escapee who use to runaway after committing bank fraud and trafficked counterfeit devices that access personal electronic information. The FBI also tells us how to report against cyber crime and keep us updated by giving information about the latest cyber crimes. Section 420 of the Indian penal code which says that **cheating** and dishonestly inducing delivery of property is a crime and an accused will get the maximum punishment which includes imprisonment for a term of 7 year along with fine.

SONY.SAMBANDH.COM CASE

It was the first case of cyber crime in India where a company named SONY INDIA PRIVATE LIMITED filed a suit, which runs a website that is www.sonysambandh.com which targets the non residential Indians that is NRI. This website allows nonresidential Indians to deliver SONY products to their relatives and to their friends living in INDIA. And the payment for this transaction can be done online the case begins with when a person logged into the website with an identity of Barbara camp she ordered a cordless headphones and a SONY television and she gave her credit card number and requested to deliver the products to Mr. Arif Azim in Noida and the transaction proceeded following all the relevant procedures company delivered the products to Arif Azim after the delivery company took some digital photographs which shows the delivery is being accepted by Arif Azim, after one and a half months the credit card company informant SONY company that this transaction was unauthorized the real owner of this credit card has denied this transaction. The SONY Company lodged a complaint for at the central bureau of investigation of online cheating under section 418, 419 and 420 of the Indian penal code. After the investigation Arif Azim was exposed and he got arrested he convicted that while working in an call centre he gained access to the credit card number of an American national and he misused on the company's site the court convicted Arif Azim

under section 418, 419 and 420 of Indian penal code. This was the first case of cyber crime convicted.

V. CYBER PORNOGRAPHIC-

As we all know that cyber crime is a global issue and many people are affected by this, one of the main objects of cyber criminal are WOMEN. Women are continuously affected by the computer oriented crime which is done by cyber criminals. Women are being trapped in the bunch of net by the cyber stalker or hacker. They are repeatedly being abused in front of the society and are left for nowhere, they are continuously being molested and being victimization by the cyber stalker and hackers. Most commonly two unknown people become friend on social media like on face book, instagram etc. and starts conversation, after some days they become very good friends and started being very familiar but after all this friendship the fraud starts asking obscene photos by giving the hope of trust of being believed by her. After getting the pictures the fraud start blackmailing the girl and start demanding for money or to get into the sexual relation. After being trapped mostly the women hesitate to go to the police and file a suit because of the fear of their image in the society and she also has a fear that her bare pictures does not get leaked, this type of practices leave a heavy impact on women and this leads to mental pressure/harassment and disorder of physical health care. After being abused in front of the all women are mentally as well as physically tortured by the society mainly by the men, women are discriminated and are treated as different individual of the society.

According to section 67 of the information technology act,2000 following act are punishable with imprisonment of 3 year and fine up to 5 lakh-

1. Publication- it involves whatsapp group or any other website where third party can have access to the content.
2. Transmission- it involves transfer of obscene photos or image to any person through email, whatsapp, messaging or in any other form.
3. Causing to be published or transmitted- this terminology end up making the intermediary portal liable, and by using which the lawbreaker has published such obscene content. The information technology act provides a guideline where it says that it is the responsibility of the intermediary to practice due attentiveness to ensure that the portal of any individual does not get misused.

Section 67A of the information technology act makes transmission, publication and causing to be published and transmission in any electronic form matter containing sexually explicit

conduct, punishable with imprisonment up to 5 year and fine up to 10 lakhs. In a recent case, a 21 year old boy who was an engineering student was arrested for sending obscene pictures to a woman by whatsapp. In another case of AVNISH BAJAJ VS. STATE⁷⁸ where Avnish Bajaj the CEO who was arrested for an advertisement by a user to sell out the DPS sex scandal video, although the video was not displayed on the portal but he was arrested under section 67 of the information technology act.

Many laws and portal are made in order to provide justice to the victims, one of them is cyber crime portal. It is the result of the initiatives of the government of our country under the national mission for the safety of the women to facilitate complainants where a women can report any kind of cyber crime online, It has been proved very helpful for the women. At present the cyber crime reporting portal cater to complaints pertaining to online child pornography (CP)/child sexual abuse material (CSAM) or sexual explicit content. The reported complaints on this cyber crime reporting portal are distributed by the respecting police authority of the particular state and according to the information of the matter of complains given by the complainants, police start its work to detect the criminal they trace the mobile and try to get their location and trap him.

VI. PROTECTION AGAINST CYBER CRIME

Cyber crime is a crime which demolishes the country's security system. A person once said that 'our mouse is as dangerous as bullet or bomb'. All the cyber attackers should get brutal punishments. Our government and law agencies have proposed recently many new laws and plans to fight against cyber crimes. Information technology Act- 2000 accordingly it says that for different crimes there are different types of penalties but All cyber crimes are not handled by information technology act, 2000 Indian penal code also deals with some of the cyber crimes like publication of obscene information in electronic form, hacking, tampering of source code, etc. some of the crimes like sending defamatory messages by emails are covered under section

500 of IPC another like sending threatening messages comes under section 506 of IPC, forgery electronic records under section 465 of IPC, web jacking under section 348 of IPC, E-mail spoofing under section 465 of IPC, bogus website, cyber fraud under section 420 of IPC., online sale of drugs and following cases are covered under information technology act 2000, like section 43(d) to section 43(h) deals with a compensation for the damages to the victims whether it is the honor of the computer or person in charge. Section 65 of Indian technology act deals with tampering with computer source documents where if a person intentionally or

knowingly keep out of site or demolish code or changes the code of any other computer will be punishable and will be held in imprisonment for 3 years and fine which can extend to 2 lakhs. Section 66 (A) says, that if a person sends derogatory messages through communicative services will be punished further section 67 of IT act, says that if a person transacts obscene material in electronic form will be punished for imprisonment and fine up to 10 lakhs the penalty for accessing a computer illegally scopes from 6 months to 5 years and the penalty for unofficial moderation on a computer which scopes from 5 years to 10 years and if a person hacks the computer or hacks the social media accounts will be brutally punished and will get an imprisonment for up to 3 years and a fine. and if a person trying to get access to government system will be in imprisonment for 10 years and charge with an heavy fine after the instigation of these penalties it leads to an extreme depletion in cyber crimes as more and more lawbreakers are becoming aware of the punishments and penalties related to cyber crime. Different countries have their own penalties and punishments for cyber crimes.

Training of Personnel- cyber crime is an continuously growing danger in today's world where hackers goes on stealing the personnel and financial information of an individual. After listening to the cyber crime cases people tempted to stop using the internet but this is not the solution, in order to get rid of this type of computer oriented crimes one should take proper measures and learn to prevent cyber crimes like-

- Keep strong and safe password- one should keep different password for different sites and keep on changing your password regularly. Password should be complex one that no one can have access to it.
- One should have knowledge of what should be done if he/she become victim- if a person feels that he/she have victim of cyber crime then immediately they should contact to the local police and if the case is sever then one should go to the FBI or to the federal trade commission, they will help to the victim to get prevention.
- One should take some measures to protect yourself against identity theft- a person may knowingly takes your personal data with the intention of fraud and deception, for the protection against this type of crime one should have guard for their personal data or information. VPN (virtual private network) helps in protection of our data.
- Training of staff- management should teach their employees how to avoid threats. If an employee feel like something is wrong or doubtful then he should immediately
- Communicate to the appropriate agencies like to the IT(information technology)department or to MSP(managed service provider).

- Make it strengthen to the home network- people should make strong encode password as well as effective private network. People should use VPN in public wifi network like in café, library, hotels or in airport etc. to protect their encode data.
- minors should be updated about the technology- parents should regularly teach their children's about the new emerging technology and parents should make it sure that their children's are comfortable in sharing problems if they face any issue regarding social media bullying, stalking, harassment etc.
- Internet security suite must be fully used- as the security suite helps to remove viruses, and it also helps to protect your pecuniary data and also protects our private data whenever you go online.

VII. CONCLUSION

Even if all the people are not victimized but they are still on risk. Due to cyber crime life of many people had already being affected their personnel as well as financial information's are being hacked by the hackers. We see today that with the increase in technology robbers don't need to go to the banks and rob it. They can easily commit the crime by sitting in their home. They have everything available in their own computer. This type of practice encourages the criminals to commit the crimes without the fear of being caught. Women are the foremost target of the cyber stalkers, they try to abuse her in front of the society. Women are continuously molested, harassed and exploited which has a great impression on their mind, women face mental torture and pressure from the society. There are various portals which listen to the women and help her to get justice, although the government has taken many initiatives to deal with cyber crime. They introduced IT act, FBI, VPN ETC. these are the body of different agencies involved in dealing with the problems.
