International Journal of Law, Justice and Jurisprudence

E-ISSN: 2790-068
P-ISSN: 2790-0673
IJLJJ 2024; 4(1): 38-49
Received: 15-11-2023
Accepted: 23-12-2023

Savita Chaudhary
Ph.D. Research Scholar, Shoolini University of Life Sciences and Business Management, Solan, Himachal Pradesh, India

Dr. Renupal Sood
Associate Professor, Shoolini University of Life Sciences and Business Management, Solan, Himachal Pradesh, India

Correspondence Author:
Savita Chaudhary
Ph.D. Research Scholar, Shoolini University of Life Sciences and Business Management, Solan, Himachal Pradesh, India

Prevention of cyber-crime against women in India

Savita Chaudhary and Dr. Renupal Sood

Abstract
The Internet has become a basic fact of everyday life for millions of people worldwide, from e-mail to online shopping. Ever faster and more accessible connections available on a wider range of platforms, such as mobile phones or person to person portable devices, have spurred new e-commerce opportunities. Online shopping and banking are increasingly widespread and over the next 10 years, the Net is expected to become as common as gas or electricity. The invention of the computers has opened new avenues for the fraudsters. It is an evil having its origin in the growing dependence on computers in modern life.

Keywords: Cyber-crime, online shopping, e-commerce, computers

Introduction
At the Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, in a workshop devoted to the issues of crimes related to computer networks, cyber-crime was broken into two categories and defined thus:

a. **Cybercrime in a narrow sense (computer crime):** Any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them.
b. **Cybercrime in a broader sense (computer-related crime):** Any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession [and] offering or distributing information by means of a computer system or network. The OECD Recommendations of 1986 included a working definition as a basis for the study: Computer-related crime is considered as any illegal, unethical or unauthorized behaviour relating to the automatic processing and the transmission of data.

Cyber crime
First case of cyber crime
The first recorded cyber-crime took place in the year 1820! That is not surprising considering the fact that the abacus, which is thought to be the earliest form of a computer, has been around since 3500 B.C. in India, Japan and China. The era of modern computers, however, began with the analytical engine of Charles Babbage. In 1820, Joseph-Marie Jacquard, a textile manufacturer in France, produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics.

Division of cyber crime
There can be no one exhaustive definition about Cybercrime. However, any activities which basically offend human sensibilities can also be included in its ambit. Child Pornography on the Internet constitutes one serious Cybercrime. Cybercrimes can be basically divided into major categories being Cybercrimes against persons, property and Government. Cybercrimes committed against persons include various crimes like transmission of child-pornography, harassment of any one with the use of a computer such as e-mail, and cyber-stalking.
The trafficking, distribution, posting, and dissemination of obscene material including pornography, indecent exposure, and child pornography, constitutes one of the most important Cybercrimes known today. The potential harm of such a crime to humanity can hardly be overstated. This is one Cybercrime which threatens to undermine the growth of the younger generation as also leave irreparable scars and injury on the younger generation, if not controlled. Similarly, Cyber harassment is a distinct Cybercrime. Various kinds of harassment can and does occur in cyberspace, or through the use of cyberspace.

Harassment can be sexual, racial, religious, or other. Persons perpetuating such harassment is also guilty of cyber-crimes. Cyber harassment as a crime also brings us to another related area of violation of privacy of netizens. Violation of privacy of online citizens is a Cybercrime of a grave nature. No one likes any other person invading the precious and extremely touchy area of his or her own privacy which the medium of internet grants to the netizens. Another Cybercrime against persons is that of Cyber stalking. The Internet is a wonderful place to work, play and study. The Net is no more and no less than a mirror of the real world. And that means it also contains electronic versions of real life problems. Stalking and harassments are problems that many persons especially women, are familiar with in real life. These problems also occur on the Internet, in what has become known as "Cyber stalking" or "on-line harassment" The second category of Cybercrimes is that of Cybercrimes against all forms of property. These crimes include unauthorized computer trespassing through cyberspace, computer vandalism, and transmission of harmful programs and unauthorized possession of computerized information. Hacking and cracking are amongst the gravest Cybercrimes known till date. It is a dreadful feeling to know that someone has broken into your computer systems without your knowledge and consent and has tampered with precious confidential data and information. Coupled with this, the actuality is that no computer system in the world is hacking proof. It is unanimously agreed that any and every system in the world can be hacked. Using one's own programming abilities as also various programmes with malicious intent to gain unauthorized access to a computer or network are very serious crimes. Similarly, the creation and dissemination of harmful computer programs which do irreparable damage to computer systems is another kind of Cybercrime. Software piracy is also another distinct kind of Cybercrime which is perpetuated by many people online who distribute illegal and unauthorised pirated copies of software.

The third category of Cybercrimes relate to Cybercrimes against Government. Cyber Terrorism is one distinct kind of crime in this category. The growth of Internet has shown that the medium of Cyberspace is being used by individuals and groups to threaten the international governments as also to terrorise the citizens of a country. This crime manifests itself into terrorism when an individual "cracks" into a government or military maintained website. Since Cybercrime is a newly specialised field, growing in Cyber laws, a lot of development has to take place in terms of putting into place the relevant legal mechanism for controlling and preventing Cybercrime. The courts in United State of America have already begun taking cognizance of various kinds of fraud and Cybercrimes being perpetuated in Cyberspace. However, a lot of work has to be done in this field. Just as human mind is ingenious enough to devise new ways for perpetuating crime, similarly, human ingenuity needs to be channelized into developing effective legal and regulatory mechanisms to control and prevent Cybercrimes.

Cyber-crime against women in India

The role of information technology is remarkable in today's world. It has widened itself over the last two decades and has become the axis of today's global and technological development. The world of internet provides every user all the required information fastest communication and sharing tool making it the most valuable source of information. It has extended efficiency, cost effectiveness and accelerated productivity at individual as well as the business or governmental level. It has brought world under one umbrella. The expanding reach of computers and the internet has made it easier for people to keep in touch across long distances. The internet plays an important role in our day-to-day life activities from home to office like in connecting with friends, searching study materials and in attending important video conferences.

In present scenario, cyber-crime is emerging as a very serious threat. At the same time, however, it has some negative sides too. This is evident in the growing proliferation of cyber-crimes in cyber space such as cyber warfare, cyber terrorism, hacking, data thefts, invasion of privacy, phishing attacks, intellectual property infringements and identity theft and other computer related crimes. The anonymity and speed with which these crimes can be committed online renders cyberspace an attractive medium to cyber criminals. Such as it invades the privacy of an individual or in accelerating crimes on cyberspace. With the numerous advancements of internet, the crime using internet has also widened its roots in all directions. The cyber-crimes not only pose serious threats to national security but also to the individual mainly women. In the context of cybercrime, one must be aware that the cyber criminals are always in a search to find out the new ways to attack the possible internet victims. In present days, everybody is using the computers i.e., from white collar employees to terrorists and from teenagers to adults, from men to women.

Cyber Space is a powerful way for women to realise their rights, from accessing information, to expressing themselves freely and even anonymously. However, cyber-crime is a global phenomenon and women are the soft targets of this new form of crime. The vulnerability and safety of women is one of the biggest concerns of any criminal and penal law, but unfortunately women are still defenceless in cyber space. Cybercrime against women is on at alarming stage and it may pose as a major threat to the security of a person as a whole.

The World Wide Web allows users to circulate content in the form of text, images, videos and sounds. The widespread circulation of such content is particularly harmful for women. In recent years, there have been numerous reports of women receiving unsolicited emails which often contain obscene and obnoxious language. Cyber-crimes against women are on the raise and women have been drastically victimized in the cyberspace. Some perpetrators try to defame women by sending obscene e-mails, stalking women by using chat rooms, websites etc., developing pornographic videos where women are depicted in compromising positions mostly created without their consent, spoofing e-mails, morphing of images for pornographic content etc. The sex-offenders look for their victims on social network websites, and also on job or marriage websites where people post their personal information for better prospect. The revealing of personal information has made women more a casualty of cybercrime. It is evident that victimization of women is leading to cybercrime and vice versa.

India is considered as one of the very few countries to enact IT Act 2000 to combat cyber-crimes. This Act widely covers the commercial and economic crimes. Even though

issues regarding women still remain untouched in this Act. Social Networking and other websites are created and updated for many useful purposes, but they are nowadays also used to circulate offensive contents. Individuals who post personal information about themselves on job and marriage websites or social networking websites are often at the receiving end of 'cybercrime'. Women and minors who post their contact details become especially vulnerable. As many as 80,000 cyber-crime related complaints have been registered with police in Kerala in 2012, of which 50,000 relate to harassment of women through new hi-tech devices. On the one side, the internet is serving as boon, but on the other side, it has made the life of women insecure due to rising cybercrime in the virtual world. Women of all ages and milieu are in jeopardy with the coming up of internet. While many women are victimized online, the question arises as to what makes Indian women unique. India is predominantly patriarchal and orthodox country and women who are victimized are mostly blamed and online victims are no exception. There are instances where marriages of women victims were stopped due to their online victimization. Also, there is less legal protection to them compared to their western counterparts and the Indian women victims do not get adequate solutions for their victimization from the ISPs governed predominantly from a western cultural perspective. Internet is the most chosen mode of the offenders to harass and victimize women. The foremost aim of such sorts of victimization remains the same as that of pre-internet era, i.e., damaging the reputation of the woman victim and creating fear factor in the victim's mind. The behavioural factors that contribute to such victimization may include broken relationships, ex-partner harassments, professional rivalry, male dominance and chauvinism, sudden exposure to digital technologies, mischievous intentions to experiment with online adult entertainment in a digital way and even for monetary gains. Victimization may begin by numerous methods, such as, either befriending the victim with original name but portraying as a 'good Samaritan', or winning her trust under a camouflaged identity, or shadowing her cyber activities, or encouraging others to add to the ongoing victimization process of the victim. Cyber technology has become a prime tool to carry out such victimizations in an almost successful manner due to digital ways and similarly, cyber space has provided the biggest platform to harass women in a most cruel way as the victimization can be viewed by millions of digital audiences. Emails, public and private chat rooms, search engines Emails, public and private chat rooms, search engines, social networking sites and web sites along with various digital technologies are the chosen modes of many offenders who victimize innocent women. There could be three factors for offenders to commit cyber-crime against women; *viz*. a. It successfully generates instant fear and trauma in the minds of the victims; b. The perpetrator is omnipresent, yet no one can find him out and prevent his atrocious activities; c. Once the electronic devices through which these communications were accessed by shrewd perpetrator(s) are destroyed, it becomes really hard for the victim as well as the government reporting agencies like the police to nab him/them. If we divide the cyber era in separate 'periods' depending upon the usage of cyber communications, we can see that so far three distinct periods have been formed:

a. **The email-period (could be said to have begun since the 1990s):** When emails were the only ways of digital communications and no strong universally accepted regulation other than the EU convention on cyber-crime, 2001, ruled the cyber world;
b. **The chat-room period (could be said to have begun in late 1990s and early 2000):** After the digital communication saw a boom through email period, came the public and private chat room period, where by people could exchange their personal information, see their pictures and chat instantly during these two 'periods' domestic laws on digital communication were being framed in many leading cyber savvy countries and cyber psychology and behavioural patterns were getting highlights due to new and unique reports of misuse and abuse of digital identities.
c. **The cyber social networking period (begun in early 2000):** In 1997, the launching of social networking website named "sixdegrees.com" in the United States could be said to be the beginning of this age. Even though, this website failed to survive for a long time, the concept became immediately popular among other entrepreneurs, internet users and numerous social networking sites were born in the US in, and around 2000 - 2001.

This period also saw booms in social interactions through blogs, adult dating sites, online bulletin boards etc. From the above, it could be seen that with each of these "periods", new methods of have been adopted by the perpetrators to victimize innocent women on the internet. The statistical resources of WHOA would show that in the year 2000, 87% victims were female and the highest chosen mode of victimization was through emails. There are various factors, which instigate cyber-crime against women to grow. One of the main factors is the patriarchal approach of the law and justice machineries of most of the cyber savvy nations towards this grave issue. Most crimes in the internet are judged by cybercrime conventions and the domestic laws of the countries from three basic angles, i.e., economic crimes, crimes against State including hate speech through the web-forums to instigate violence, and crimes against children. On the other hand, cries of the women victims of crimes of the internet are often ignored; as such, these crimes mostly do not fall in the categories mentioned above. For instance, bullying or teasing a woman in the open web space never attracts any law enforcement intervention as the female victim is expected to be matured enough to handle the situation as an adult. Using of the female models for pornographic websites cannot bring any criminal charges against the concerned website authority, especially when the site exhibits the 'consent notice' of the models. However, truth is, many women are actually depicted as 'models' in these sites without their valid consents. This is mostly done by men who contribute to these sites by misusing the private information including still pictures or video images of innocent women. Unless the victim is establishing the fact that her rights has been infringed (which in majority of cases is extremely painful and traumatizing for the victim), the law guarding the freedom of speech and expression of the individuals, will remain a silent motivator for enhancing the defamation of the victim herself. The most contemporary form of victimization of women is "sexting"

where mostly teenagers and young adults are involved. In such cases, either the victim's sexted messages may be misused or she may suddenly see her mailbox flooded with sexted images from male acquaintances accompanied with obscene or harassing text messages. These sorts of harassments make the situation more complicated as the victim is expected to be mature enough to not to indulge in these sorts of activities. A sudden raise of sexting offences in the time period of 2006-09 in the US saw the huge metamorphosis of provisional as well federal criminal laws to adapt and adjust to the concept of victim turned offender.

However, this new trend of offence is becoming rapidly popular among young adults worldwide and still needs to be recognized as another add up in the wagon of cyber-crime against women. There are various cyber-crime counsellors, victims, cyber security experts, police personnel, professors of cyber law and cyber-crime and common individuals who had never heard of cyber-crime against women. Going through the various statistics like cyber stalking statistics of Haltabuse.org (WHOA) for the period from 2000 till 2023. It can be seen that in 2000, among 353 victims who approached WHOA, 87% were women and 13% were men; among the harassers, there were 68% men and 27% women. In 2001, among 256 victims, 79.3% were women and 16% were men; whereas 58.6% harassers were men and 32.5% were women. In 2002, among 218 victims, 71% victimizations, which happen to women. Almost all these scholars and counsellors opined that women are more prone to cyber-attacks due to various reasons including patriarchal social outlook towards women and various legal drawbacks. When a man's email id or private data stored in websites and also personal computers are accessed and modified in an unauthorized way, he can afford to live on by informing the police and his acquaintances. Unlike a woman victim, he may not be subjected to gross humiliation by the society as a whole; he may neither be reduced to a mere 'sex item' like his female counterpart. His victimization may be judged onlyfrom the perspective of economic losses. On the contrary, a woman victim may be ostracized by the society. Unlike her male counterpart, she may not be able to take the online humiliation so easily; it may engulf her in the feeling of shame and hatred for herself. Besides the risk of being reduced to a sex avatar, a woman victim may find it hugely difficult to gain back her social and professional reputation. Virtually vandalized women amuse the world more than digitally robbed men or digitally threatened security of the nations. It can be said that researches on this issue have not gained momentum. Majority of the researches were done from the US perspective, with an exception of few researches from European perspectives. This has limited the scope of analysing the issue from transnational perspective, especially from the orthodox viewpoints of the oriental societies. It has considerably influenced the law and justice machinery as well. The cyber savvy nations still need to develop rules and regulations to implement the promises of the CEDAW as well as the guarantees of fundamental freedoms to provide safe and dignified cyber-life to women. We do not deny the fact that new laws are being drafted and old laws are being refined in countries like US, Canada, UK, Australia and India to deal with the traditional cyber-crimes that may target the safety of women and children both online and offline. However, an analysis of such laws would reveal that the drafters are not acquainted with the present cyber cultures to draft gender protective regulatory laws for online communications as well as stronger online data privacy laws. A need has arisen now to consider broadening the scope of "unprotected speech" under the US Federal constitution for the sake of women. Similarly, it has become very essential to recognize the malicious web activities that are done women as could be seen from our discussions in the above paragraphs, each new period of 'cyber era' unfolded new trends of victimizations of women. Some of these trends are the traditional methods to victimize women in the offline world. Some methods adopted by the perpetrators are, sending derogatory letters about the character of the victim to her family members and also work place colleagues, spreading reputation damaging rumours about her in the society, threatening her with dire consequences and blackmailing her banking upon her good virtues, children and family, physical assaults, offline stalking etc. However, when these methods are utilized by the perpetrators in the cyber space, they create newer models for victimization. The laws dealing with cybercrimes in general may have recognized some of these new modes of victimization. However, the global approach to the issues of cybercrimes against women has narrowed down the scope of these laws for combating online victimization of women. We claim that this vacuum has further instigated the growth of ongoing experiments with digital technologies to victimize women. There is a rapid growth of non-governmental private policing agencies to help the victims of online crimes since the mid Nineties, and women victim's growing reliance on these agencies. These agencies are expected to monitor the unwanted offensive contents with strict confidentiality. The Internet Watch Foundation (IWF) of UK, was established in 1996 and it works towards preventing child sexual abuse, criminally obscene contents targeted towards adults, abusive racial hate speech etc. The NGO, working to halt online abuse (WHOA) was founded by Jayne Hitchcock in the US in 1997 to help primarily online stalking victims.

Cyber angels were created in 1995 in the US for promoting online safety education programmes for children. Wired safety is another notable non-governmental US based organization who work for internet safety of men, women and children. In India, an NGO, Centre for Cyber Victim Counselling (CCVC), was established in 2009, to help victims of cybercrimes. They prefer to rely on the advice of the non-governmental agencies like the CCVC, cyber safety tips discussed in various blogs and websites of various well-known cybercrime experts and scholars etc. From various experiences, it is been noticed a growing tendency among women victims to approach the professional hackers to stop the online harassment on an emergency basis, besides contacting the nongovernmental agencies. From the above discussion, it could be deducted that women victims need faster restorative procedures to avoid further escalation of agony and trauma, but they may feel reluctant to approach the police for such restorative procedures. It is observed that the lack of professionalism of the police in dealing with crimes targeting women and failure of the laws to protect the rights of women are two major contributing factors for this shifting of reliance. At this juncture, it has become almost an undisputable fact that the method of analysis of the data privacy laws by the police and the courts from the perspective of national security issues and individuals financial and health records, and the usage of the free speech guarantees by internet users have eclipsed the issues

of online victimization of women. A child victim could feel extremely stressful and even suicidal due to paedophilia or bullying. To save the children from vicious internet traps, the States have extended child protection laws to cover child pornography, online grooming and online bullying. Victims of financial frauds are protected by numerous legislations preventing identity theft, online monetary scams and anti-phishing guidelines. Women victims on the contrary, do not get emergency help from the State as crime patterns remain unrecognized and overshadowed by general trends of cyber-crimes.

Review of literature

Violence against women in cyber world

By Jaspreet Singh: The research paper acmes that the violence against women is a violation of human rights and not a new phenomenon. It is always taking it shapes time to time in Indian history. With the passage of time, many feminists fought against women violence and for their empowerment in the society, but there is no end of her vulnerable life and her exploitation. This paper presumes the cyber violence against women, how it is impacting their social life in the context of India. It highlights the reasons and forms of cyber-crime and explores some suggestions how to curb cyber-crime against women. Open to immediately report the cyber abuse or cyber-crime. The biggest problem of cyber-crime lies in the modus operandi and the motive of the cyber-criminal. Cyber space is a transit space for many people, including offenders. While people do not live-in cyber space, they come and go like any other place. This nature provides the offenders the chance to escape after the commission of cybercrime. Many websites and blogs provide security tips for the safety of women and children in the net. But still then cyber-crime against women are on rise.

Mapping cyber-crimes against women in India

By Dr. Shalini Kashmirithe research paper highlights cyber-crimes against women in India which is a completely new phenomenon. To make the paper effective, a comparative analysis has been done between the cyber laws regulating cyber-crimes in India, United Kingdom and United States of America. The scholar observed in detail the various crimes against women and the legal framework regulating these crimes in India. Finally, the study provides with appropriate suggestions where necessary.

Cybercrime: The transition of crime in the information era

By Shailza Dutt, Dr. Suneyna, Asha Chaudhary the research paper acmes that Computer crime also called as Cybercrime has increased in acuteness and occurrence in the current years. This paper. Cybercrime, which is firstly increasing in frequency and in acuteness, requires us to rethink how we should implement our criminal laws. The present model of reactive, cybercrime, its types, modes of cyber-crime and security measures including stoppage to deal effectively with cybercrime. The scholar observed that there is a requirement for a timely review of existing approaches to fighting this new phenomenon of cybercrime in the information technology. Though it is impossible to remove Cyber Crime from the world but we can reduce it to a large amount by creating alertness in Society. The scholar further suggested a system of administrative regulation backed by criminal sanctions that will cater the incentives necessary to create a workable limiting to cybercrime.

Cyber-Crimes and their Impacts: By Hemraj Saini, Yerra Shankar,Rao T.C. Panda

The research paper highlights the current era of online processing, maximum of the information is online are prone to cyber threats. There are a huge number of cyber threats and their behaviour is difficult to early understanding hence difficult to restrict in the early phases of the cyber-attacks. Cyber-attacks may have some motivation behind it or may be processed unknowingly. The scholar noted that the attacks those are processed knowingly can be considered as the cybercrime and they have serious impacts over the society in the form of economical disrupt, psychological disorder, threat to National defence etc. Restriction of cybercrimes is dependent on proper analysis of their behaviour and understanding of their impacts over various levels of society. The scholar further observed that this paper provides the understanding of cyber-crimes and their impacts over society with the future trends of cybercrimes.

Cybercrime: A threat to Network Security by Ammar Yassir and Smitha Nayak

This research paper discusses the issue of cyber-crime in detail, including the types, methods and effects of cyber-crimes on a network. In addition to this, the study explores network security in a holistic context, critically reviewing the effect and role of network security in reducing attacks in information systems that are connected to the internet. The scholar observed that, all this adversely affects the efficiency of information security of any kind of security that exists and is used in information systems. Since hackers and other offenders in the virtual world are trying to get the most reliable secret information at minimal cost through viruses and other forms of malicious soft-wares, then the problem of information security - the desire to confuse the attacker: the scholar further observes that the Internet is a large computer network, or a chain of computers that are connected together. This connectivity allows individuals to connect to countless other computers to gather and transmit information, messages, and data. Unfortunately, this connectivity allows criminals to communicate with other criminals and with their victims.

Cybercrimes: Another dimension of women victimization by Paridhi Saxena & Anisha Malka

The research paper highlights various cyber-crimes highlighting cyber pornography, cyber bullying, cyber-stalking against women. This paper also addresses about various lacunas in IT ACT 2000 and also made some suggestion in regard to these crimes. The scholar observed various crimes against women which are prevailing in India and noted down the suggestions and observations made therein.

Cyber-crime against women in India by Debarati Halder, K. Jaishankar (2017) [51]

Analysed various cyber-crimes against women in India which are very much prevalent nowadays. It discusses cyber-crimes against women in India, various forms of the online crimes including hate speech, trolling and gender bullying, online grooming, infringement of privacy and sexual offences on the internet. The scholar observed the

various above mentioned crimes against women and further noted the preventive measures that the police and judiciary and the victims should adopt to combat the offences. The scholar also noted about the liability of the websites and service providers. The scholar identified the factors associated behind the cyber-crime against women in India. The study revealed that there is no uniform law, the police, prosecutors and the courts have to look into existing laws which are scattered in traditional criminal laws such as Indian Penal Code (IPC), the Evidence Act or the recently developed laws such as information technology (IT) Act and so on for providing justice to the victims. Furthermore, it has been noted that many websites have their servers outside India and harassers take huge advantage of this.

Cyber-crime and victimization of women laws, rights and regulations, Debarati Halder, K. Jaishankar (2012) [52]

This book is to identifies and explain the mostly unexplored crimes of the Internet targeting women in particular. This book is designed to define cyber victimization from women victim's perspective, analyze the trends of victimization, formulation of core rights of women internet users and examine the legal protections towards women victims of cyber-crimes in five prime countries. The scholar observed definition, typology and patterns of Victimization Legal Treatment of Cyber Crimes against Women in USA, Canada, U.K. Australia. The scholar he scholar identified the factors associated behind the victimization of women in cyber space. The study revealed that Women victims are near invisible in the eyes of universal cyber-crime conventions and domestic internet and cyber communication related laws. The effect of this lawlessness is so huge that government-reporting agencies also sometimes deny any help to the woman in need.

Computers, internet and new technology laws by Karnika Seth (2016)

Is a comprehensive work that aptly highlights new laws, policies, cases, concepts, events and studies that have evolved cyber laws in the national and international spheres. The scholar noted that it specially focuses on the development of laws in India including new bills and guidelines that were passed such as Electronic Delivery of Service Bill, 2013, the cabinet approval of the New Consumer Protection Bill 2015 and the new guidelines for the introduction of e-authentication technique using Aadhar-eKYC services. It also discusses land mark cases, including Shreya Singhal v UOI, which struck down Section 66A of the IT Act, 2000 as unconstitutional and Anwar Vs P.K Basheer which clarified the law on appreciation of electronic evidence in India. The scholar further noted the emerging crimes such as trolling, sexting, and revenge porn and new developments such as Net Neutrality that have impacted the cyber world. The scholar noted basic concepts of cybercrime and its classifications. It has been observed that with the increase in use of technology the cybercrime is also on rise which is required to be checked.

Objectives of Study

- To understand the meaning of cyber-crime against women.
- To find out causation behind the victimization of women.
- To analyse law dealing with in checking cyber-crime against women in India, and to find out the loopholes in the law if there is any.
- To find the gap between legal actions & technological advancement.
- To situate the growing threat of cyber-crime against women and girls within the broader context and challenge of cyber-crime, Internet growth and governance and human rights.
- To find out the steps which should be taken by the government for checking cyber-crime against women in India.

Cyber Crime against Women: Indian Scenario

In India, cyber-crime against women is relatively a new concept. It can be noted that when India started her journey in the field of Information Technology, the immediate need that was felt to protect the electronic commerce and related communications and non-cyber socializing communications. The drafters of the Indian Information Technology Act, 2000, created it on the influence of the Model Law on Electronic Commerce, which was adopted by the resolution of the General Assembly of the United Nations in 1997. The Act turned out to be a half-baked law as the operating area of the law stretched beyond electronic commerce to cover cyber-attacks of non-commercial nature on individuals as well. While commercial crimes and economic crimes were moderately managed by this Act, it miserably failed to prevent the growth of cyber-crime against individuals, including women.

Main types of Cyber Crime against women are

Cyber pornography / obscenity, Cyber Stalking, Cyber Bullying, Cyber Morphing, Cyber Pornography

This would include pornographic websites; pornographic magazines produced using computer and the Internet (to down load and transmit pornographic pictures, photos, writings etc.) predominantly sexually explicit material, lascivious in nature intended primarily for the purpose of arousal of sex desires or erotic activity over the internet and includes pornographic websites, e- magazines containing porn stuff which could be downloaded from the internet, transferrable porn pictures, photos writings etc. Because of the advantage of lack of territorial restrictions, anonymity and fastest means of communication pornographic materials can be reproduced more quickly and cheaply on new media like hard disks, floppy discs and CD-ROMs. Apart from still pictures and images, full motion video clips and complete movies are also available. Another great disadvantage with a media like this is its easy availability and accessibility to children who can now log on to pornographic web-sites from their own houses in relative anonymity and the social and legal deterrents associated with physically purchasing an adult magazine from the stand are no longer present pornography industry is contributing approximately $ 20 billion annually to the global economy. For example In India Videsh Sanchar Nigam Limited (VSNL) and number of other internet service providers such as Reliance, Vodafone, Airtel, cyber cafes, online portals etc provides for various kinds of internet schemes without restrictions on the nature of persons permitted to avail these services. Moreover the social websites like Facebook, Twitter, Whatsapp, Orkut, free music downloading sites etc do not

check the kind of material that is being uploaded and downloaded. They do not have any parameter to differentiate between what we call as an art or pornography. What is more shocking is children (between 8-16 years) indulgence in viewing porn sites. Approximately twenty six popular children's characters such as Pokemon, Action Man, My Little pony reveals thousands of links to porn sites.

The most embarrassing aspect of pornography industry is the child pornography. The Air Force Bal Bharti, Delhi Cyber Pornographic Case (2001) and the Bombay Swiss Couple Case (2003) are the leading examples in this context. It is to be noted that Traditional law of obscenity is contained under sections 292-293 of Indian Penal Code, 1860.Section 292deals with the sale of obscene books and section 293 provides punishment to person dealing in cyber pornography that is accessible to person under twenty years of age with imprisonment up to three years and fine up to two thousand rupees on first conviction and with imprisonment up to seven years and fine up to five thousand rupees on second or subsequent convictions. The IT Act, 2000 was deficient in dealing with obscenity and consist of a single section 67 dealing with the crime. IT (Amendment) Act, 2008 amended section 67. The combined effect of sections 66-E, 67, 67-A and 67-B obscenity has been brought under the legal regime and child pornography has been separated from mainstream pornography. Section 67 provides that whosoever publishes or transmits obscene material in electronic form shall on first conviction be punished with imprisonment up to three years and fine which may extend up to five lakh rupees and on second or subsequent convictions, imprisonment up to five years and fine up to ten lakh rupees. Section 67A deals with mainstream pornography and provides punishment for publishing or transmitting of material containing sexually explicit act, etc in electronic form with imprisonment up to five years and fine up to ten lakh rupees on first conviction and with imprisonment up to seven years and fine up to ten lakh rupees on second and subsequent convictions. Section 67-B is related to child pornography. This section provides punishment for publishing or transmitting of material depicting children in sexually explicit act, etc, in electronic form or creates text, digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in electronic form depicting children in sexually explicit act or entices or induces children for online relationship with one or more children or facilitates abusing children online with imprisonment up to five years and fine up to ten lakh rupees on first conviction and imprisonment up to seven years and fine upto ten lakh rupees on second or subsequent conviction. Other acts having an impact on cyber pornography are indecent representation of Women's Act, 1986 and Young Persons (Harmful Publication) Act, 1950.

In many countries like India and Malaysia, British law (the Hicklin test for obscenity) left over from a colonial legacy is still used to determine what is obscene. The Hicklin test of obscenity is whether "the tendency of the matter charged as obscenity is to deprave and corrupt those whose minds are open to such immoral influences and into whose hands a publication of this sort may fall." The test defines 'obscene' as all visual or written material that is "lascivious or appeals to the prurient interest", and has the capacity to corrupt those exposed to it. These standards are relevant in the context of Internet governance as well, since most countries are either extending existing legislation for other media (television and cinema) to the Internet. New laws enacted for the Internet adopt the same definitions regarding obscenity or sexually explicit material, inheriting also the weight of precedents that have determined what is obscene. This definition of obscenity and the penalisation of it under the Indian Penal Code, 1860 (sections 292 and 293) is further extended by other laws that prevent the distribution of such material (Young Persons Harmful Publication Act, 1956, Indecent Representation of Women (Prohibition) Act, 1986). The case that laid down the Hicklin test i.e., was about the mass distribution of inexpensive pamphlets called provocatively "R. vs. Hicklin The Confessional Unmasked" described how priests extracted erotic confessions from female penitents. The publication of the pamphlet was encouraged by the Protestant Electoral Union and used by them to discredit the Catholic Church and specifically to prevent laws that would allow Catholics into the Parliament. A description of the social and political context of this case or even the content of the pamphlet found obscene is rarely found in discussions on obscenity law in the contemporary. In a handbook on pornography law, Thomas C. Mackey discusses this case – "Protestant Electoral Union sought to 'protest against those teachings and practices which are un-English, immoral and blasphemous, to maintain the Protestantism of the Bible and the liberty of England'. Further, the Protestant Electoral Union supported electing as Members of Parliament, men who shared their anti-Catholic sentiments and who wished to 'expose and defeat the deep-laid machinations of the Jesuits'. It is perhaps not so difficult to draw a link between the political and social connotations in this case and the use of obscenity law to control political speech, especially since the birth of print culture and urban spaces, led to the proliferation of explicit sexual writing in early stages of modern Europe that was used to satirise and criticise the church, state and monarchy and was controlled for its defamatory and blasphemous nature, more than its obscenity.

In the legal discourse pornography is missing as a category except as an aggravated form of obscenity (Ranjit Udeshi v. State of Maharashtra). In this case the obscenity of Lady Chatterley's lover was on trial, and it was held that the book as per the Hicklin test is obscene since it has the potential to deprave and corrupt by immoral influences. In essence the judgment deals with slang and colourful language and it was held that there was not enough preponderance of art or social purpose in the text. The judgment does make reference to pornography as "dirt for dirt's sake" further explained as "libidinous writings of high erotic effect unredeemed by anything literary or artistic and intended to arouse sexual feelings". It is this judgment that establishes the Hicklin test as the law to be followed in independent India as well.

In the recent fairly progressive judgment on M.F. Hussain's painting, this definition was reiterated, giving some degree of distinction to the category of pornography apart from it being an aggravated form of obscenity and to say that it is a class of objects, images, paintings, videos designed for sexual arousal, while other material which may or may not be obscene is layered with other meanings (aesthetic, patriotic, narrative). But as such it is not a much more evocative definition than "dirt for dirt's sake". Does this missing descriptive category assist in the rampant

circulation of pornography, either online or offline? But perhaps the more interesting question to ask is how the legal discourses side step the question of pornography, while minutely examining material that could be described as obscene. This intensity of the legal gaze is obvious than in the judgments on obscenity of film, books, magazines (in Indian law) where the material is minutely examined for traces of obscenity.

In the legalistic drive to categorize and label, the court has also drawn fine distinctions between obscenity and vulgarity stating that – "A vulgar writing is not necessarily obscene. Vulgarity arouses a feeling of disgust and revulsion and also boredom but does not have the effect of depraving, debasing and corrupting the morals of any reader of the novel, whereas obscenity has the tendency to deprave and corrupt those whose minds are open to such immoral influences." This case deals with a fiction story published in a relatively popular magazine Prajapati about a character called Sukhen whose slide into the life of decadence and squalor is narrated in first person. Sukhen hates his teachers, hypocritical politicians and is often violent or at least regarded as a goonda by others. This story of all those encountered by the law seems to be indeed the most erotic and fascinating – here is an excerpt of the court's description of the story/novella "Seeing Shikha in that position with the butterfly on her palm and Shikha trying to fix the severed wing in its place in the body of the butterfly, Sukhen is reminded of what happened to Zina, a daughter of one of the officers of the factory at the picnic party of the factory owner and its big executives. Sukhen remembers how at that party Zina, a girl of about 14 years of age was being fondled by the elderly persons holding high posts in the factory and whom Zina would call 'Kaku' (Uncle). Sukhen also recalls that how he thereafter had taken Zina away from those persons to a sugarcane field and had an affair with her there. This part of the affair with Zina in the sugarcane field had been considered to be obscene. Sukhen feels that the butterfly resting in the palms of Shikha resembled Zina in the sugarcane field while she was there with him. After remembering this incident Sukhen turns to Shikha and goes near her. There he notices Shikha's dress and he finds Shikha had only a loose blouse with nothing underneath and a good part of her body was visible and there is some description by Sukhen of what was visible and of his feelings on seeing Shikha in that position. Sukhen's kissing Shikha and going to bed with Manjiro, his friend's sister, are other parts of the book considered obscene. The affairs of Sukhen's 'Mejda' (second elder brother) with the maidservant's daughter and Sukhen's description of the same have also been hold to be obscene."

In the same judgment, pornography was described a little bit more in the words of the High Court judge who held the book to be obscene, and the Supreme Court overruled his decision. The High Court judge stated that the book is in fact pornography – "Pornography it is and with all the gross taste not because it has sacrificed the art of restraint in the description of female body and also because in some part it has indulged in complete description of sexual act of a male with a female and also of lower animal." In the Supreme Court judgment, it was held that the judge must apply his mind dispassionately to the question of whether the book is obscene, and not allow for personal preference or subjective element in the subconscious mind to influence his decision. Eventually while deciding that the book was indeed not obscene, the court justified this by saying that the book would shock readers rather than deprave them, consequently serving as a moral warning for all the sins and vices described. The decision of the court to not ban the book is also buttressed by interventions of scholars from Jadavpur University in support of the book and the moral stand it takes eventually.

It is also perhaps relevant that Sukhen, the main character is on his way to being reformed, from his restlessness, sexual drives and finding solace and peace with himself, especially with the help of his new lover Shikha, when he gets injured in violent clashes between rival political parties and dies. It is from this bleak ending that the court salvages the moral resurrection of this book as not obscene – the dire punishment of those who succumb to sexual and other vices is most evidently laid out.

The decision in which there was an appeal to the courts to declare that precentorship of cinema in India is unconstitutional is K. A. Abbas v. Union of India and Another. This appeal was not accepted and it was held that pre-censorship in cinema is necessary because of the impact that cinema has on the senses, unlike other mediums such as books, magazines, paintings, etc., – "with trick photography, vista vision and three dimensional representation thrown in has made the cinema picture more true to life than even the theatre or indeed any other form of representative art". The decision relies on Mutual Film Corporation v. Ohio, in spite of an acknowledgement that this decision was no longer relevant to American jurisprudence that does indeed give protection to cinema as well under the First Amendment (freedom of expression).

The description of cinema in Mutual v. Ohio is probably the most indicative of the fear and suspicion with which the image and especially the moving image as perceived in law. Cinema is likened to magic and sorcery – it is said that "indeed (moving pictures, cinema) may be mediums of thoughts, but so are many things, so is the theatre, the circus and all other shows and spectacles. Rather than being organs of public opinions, of ideas and sentiments, published and known, vivid, useful and entertaining no doubt, but as we have said, capable of evil." Echoing this general distrust, it was held in K.A. Abbas that the reason for treating cinema or moving image differently is that "the motion picture is able to stir up emotions more deeply than any other product of art. Its effect particularly on children and adolescents is very great since their immaturity makes them more willingly suspend their disbelief than mature men and women. "The justification of censorship based on the paternalistic role of the State that must protect the infantile public is often repeated in Indian jurisprudence on obscenity, not only as a rationale for classification of material but also for the banning and censorship of different material.

In the introduction to The Public is Watching: Sex, Laws and Videotapes, Lawrence Liang states that rather than giving an account of censorship as incursions into the right of freedom of expression or receiving information, perhaps it is more useful to have a productive account of censorship. This is inspired from Annette Kuhn's work on early British cinema and the linkages she draws between discourse around birth control and censorship paradigms. Annette Kuhn's emphasis on the productive discourse of censorship allows for the shift away from looking only at the content/material that is to be censored to the forces,

institutions, notions, ideologies that are pulled into play and are produced for censorship to take place; to move away from a straight forward account of power. Kuhn says – "To question this model is by no means to deny that censorship has anything to do with power. On the contrary, what I want to suggest in fact is that an understanding of power as a purely prohibitive gesture - especially where the object of prohibition is taken to be the representation of some pre-existing reality - does not go far enough, and may actually inhibit our understanding of how, and with what effects, the powers involved in film censorship work. The prohibition model of censorship is usually associated with a further assumption: that censorship is something that takes place within certain organisations, especially in organisations with an explicit institutional remit to censor."

Liang takes this thesis further to state that the prohibitive idea of censorship doesn't allow us to see that the law is building a theory of cinema, of spectatorship and the idea of the public – "The law of instance, is not merely interested in prohibiting a particular kind of 'seeing', but also equally interested in suggesting the proper way of seeing." In other words, the productive project of law is also about a discursive crafting of the ideal viewer of cinema – where he (and this ideal is not inclusive of she) will view cinema, what he will see and read from it. Hence, each judgment that lays down the meaning of an object – whether Bandit Queen and Prajapati as not erotic but shocking and containing a moral regarding social evils (of vice, alcohol and caste violence) or Hussain's painting Bharat Mata as not erotic/obscene but as patriotic, is also stating that this is what the ideal viewer/spectator would see – this is the meaning that is attached to the image (like a caption) with which it must be read.

The court has a heavy investment in the question of aesthetics and especially narrative as is evident in the decision on Shekhar Kapur's Bandit Queen (Bobby Art International &Ors. v. Om Pal Singh Hoon&Otrs 1996 AIR (SC) 1846). In Bandit Queen, Phoolan Devi is raped and walks through the street of the village, naked. This caused much consternation and led to the case coming up before the court. Aesthetic opinions on the film varied – even as Arundhati Roy described it as the 'great Indian rape trick'the court held that it is a film that attempts to show the reality of a social evil. Consequently, it must show that social evil in the film. The narrative demands that the rape sequence that puts Phoolan Devi on the path to becoming a cruel, vengeful dacoit is essential – "in aid of the theme and intended not to arouse prurient or lascivious thoughts but revulsions against the perpetrators and pity for the victim."

Perhaps the most important decision in this regard, that characterizes the slippage between obscene and pornographic objects, is the case of Pratibha Naithani v. Union of India. The court was called upon to decide whether English movie channels (like HBO and Star Movies) should be pulled off the air for broadcasting adult content, and what controls should be put on the channels (censoring bad language, timings of adult movies, etc.). This case exemplifies the blurry borders of obscenity as a category – whereby innocuous objects are pointed at, as aspects of a sleazy modernity that are separate from Indian culture, and thereby rendered obscene. Indian culture plays an important referent role in most of the judgments on obscenity – to answer the question of what affect is produced in people by allegedly obscene objects and sometimes to emphasize the existence of erotic, sexual texts within Indian culture that are not found objectionable and point to a tradition of eroticism that should be taken into account.

Subsequent judgments have dealt with as varied objects as newspapers and their erotic content, a documentary film by Anand Patwardhan which contains a scene of an aphrodisiac being sold and eventually M. F. Hussain's painting Bharat Mata. This painting depicts India in the shape of a nude woman distressed or grieving and was put up on a website for auctioning for a worthy cause. However, this led to a case about the painting and the court eventually decided that it was not obscene in one of the more progressive judgments about obscenity in India. The purpose of this short account of obscenity jurisprudence in India is perhaps merely to point at how various objects, most of them barely obscene and innocuous, have been examined by the law in much detail. It is this detailed and minute examination that is intriguing. Pornography itself has very blurred boundaries – as various objects slip into this category, whether it is Hollywood films with very minor sexual content, soft porn films often called blue films, BF, films like Choker Bali that are circulated in cinema halls that are meant for blue films21 Soft porn itself points to how there exists various gradations of material – some of them marked only by slang, suggestive language, minimal dressing and references to sexual activity rather than sexual explicitness (nudity, genitalia or sexual activity). Hard core pornography is circulated largely through CDs, DVDs in video parlours and piracy markets and through the Internet; it ranges from material from Europe and America and a smattering of Indian pornography which is mostly heterosexual. Amateur pornography or sexually explicit material which is made and put online either as part of the porn industry, which is not very large especially in comparison to the global North, or by people themselves, is a relatively new phenomenon assisted by digital technologies and the Internet. In the last decade, the leaking of such material, and consequently the swarm of moral, ethical, social dilemmas that have arisen has led to most of the 'scandals. It is these scandals that are literally pushing the category of pornography out of the grey zones of being a public secret; out of rampant and unexamined illegality into the realm of the law – its imperatives, violence and descriptive plenitude.

Cyber Privacy and Related Problems for Women

The cyber space regulatory laws are partly gender sensitive in the US especially for cases covering stalking, domestic violence, dating violence and the extension of the same in the cyber space. While considering general privacy issues (excluding financial crime), we note that women still remain vulnerable victims. Hacking and stalking are the most sorted crimes that invade the privacy of the victim. Video voyeurism and adult sexting are the two essential component parts of online privacy invading activities.

Legal Treatment of Cyber Crime against Women in UK

This is more evident from the available statistical reports of cyber-crime in the UK. Analysing the 2018-2019 report of "Garlik", "The online experts", it can be seen that among 29.7 million adult internet users in UK, there are approximately 2,374,000 instances of online harassment. By online harassment, the report indicates cases of mental distress of the victim, stalking, sending unwanted abusive mails containing hate messages, racial messages,

threatening messages and blackmailing mails etc. This report shows that among other crimes, there were 86,900 instances of identity theft and identity fraud (which includes impersonation, using of other's identity card, identity theft etc mainly for financial gain), 207,700 instances of financial frauds (which includes losses of plastic cards, bank frauds etc), 137,600 instances of computer misuse (the report does not include virus infections) and 609,700 instances of sexual offences which cover victimization of children mainly. Apart from the Garlik report, we did not find any detailed analysis of cyber victimization, especially of women in UK. This could be an indication as how individuals, especially women are conservative about reporting the online crimes that happen to them. A victimization survey to unearth online crimes against women in the UK is the need of the hour. Unauthorized Access and Related Activities.

Hacking and hacking related activities may not always be restricted to crimes committed against the nation or the corporate entities alone. We see it as a crime when done to stored computer data or the computer as a machine of any female victim. To access her personal information including pictures without proper authorization, with intention to misuse it, distribute it in the internet, modify the contents and give a false impression of the victim etc, are also criminal activities like stalking or bullying. Strangely enough, in UK, these sorts of cyber-criminal activities against women have been never given a separate legal treatment on the pretext that these are also one of the hacking related activities which are done to individuals. We feel that the core reason for the growth of internet crimes against women could be lackluster attitude of the law and justice machinery to understand the nature of hacking related activities targeted especially to the women. Such sorts of unauthorized access towards personal data may lead to several other cyber offences including public defamation and humiliation, impersonation, unwanted exposure of the victim in adult entertainment industry etc. Unlike the US, the UK does not have any women – special regulation to cover cyber offences originating from domestic violence or dating violence; rather the offences related to unauthorized access are regulated by a compact legislation called "Computer Misuse Act, 1990". Under this Act, three offences are penalized, namely, unauthorized access to computer material, or to enable any such access to secure unauthorized access, intention to create further menace with such unauthorized access and unauthorized modification of the computer material. As mentioned earlier, this Act was created to protect both men and women victims. Notably, the drafting of the language could very well suit the needs for preventive actions against harassment of women also when it says that the men's rea must be directed to the 'act' that the offender knows would successfully accomplish his intention to harm his victim. In brief, the offender can be held guilty for unauthorized access if it is proved that he used his technological knowledge to access the computer material or data with intention to harm the victim. The penalties for such offences are on a summary conviction in England and Wales to imprisonment for a term of 12 months or to a monetary fine not exceeding statutory maximum, or both. In case of summary conviction in Scotland, the law prescribes imprisonment for six months or to a fine not exceeding statutory maximum, or both.

Conclusion and Suggestion

Crime in any form adversely affects all the members of the society. In developing economies, cyber-crime has increased at rapid strides, due to the rapid diffusion of the Internet and the digitisation of economic activities. There is huge penetration of technology in almost all walks of society right from corporate governance and state administration, up to the lowest level of petty shop keepers computerizing their billing system, we find computers and other electronic devices pervading the human life. The penetration is so deep that man cannot spend a day without computers or a mobile. Snatching some one's mobile will tantamount to dumping one in solitary confinement! Cyber Crime is not defined in Information Technology Act 2000 nor in the I.T. Amendment Act 2008 nor in any other legislation in India. To put it in simple terms 'any offence or crime in which a computer is used is a cyber-crime'. Interestingly even a petty offence like stealing or pick-pocket can be brought within the broader purview of cyber-crime if the basic data or aid to such an offence is a computer or an information stored in a computer used (or misused) by the fraudster. In a cyber-crime, computer or the data itself is the target or the object of offence or a tool in committing some other offence, providing the necessary inputs for that offence. All such acts of crime will come under the broader definition of cyber-crime.

Cyber-crime can occur against data and against individual (men and women), in which cyber-crime against women is on rise and serious subject of concern. In the cyber space, women are victims not only in the hands of individuals, but also in the hands of technology as well as the law and governmental systems. Women are humiliated, made fun of and left to be an object to be ridiculed. The reason lies in the volume of rapid growth of a typical 'cyber culture' where basic fundamental rights are given least importance. This volume of growth could not be matched by law makers of any country or any global organizations. Indeed, when the law fails to take note of the ongoing victimization, the harm escalates more. It can be seen that there is a peculiar trend of the law makers to approach cybercrimes from three basic angles, namely crime against government, financial crime and crime against children. Further, crime against government and financial crimes are often clubbed by creating numerous hacking related laws as well as anti-money laundering laws. Crimes against children however are gaining highlights due to increased legal barricades through laws on child pornography and bullying etc. Millions of women and men, who use internet as a way of life from other aspects, like leisure, non-economic communications, socializing etc also continue to experience the curse of technology in a lawless state. Users create their own rules and regulations to carry on their virtual lives. No one bothers about the wrongs that can be done to others and prolong in exercising their own free rights without knowing any limits. The cyber space turns as a Utopia to some and hell to others. Sadly, enough online victimization and subsequent damage to reputation harms women more than men. This is mainly because damage to reputation may often lead to piercing of privacy and women are more susceptible in such cases. Furthermore, it needs to be understood that traditional physical space crimes such as rape, sexual molestation, blackmailing, stalking and so on

have gained new significance due to the development of information communication Technology. There are incidences of rape and consequent storing of images of the rape scene in the mobile phone devices, extraction of money by threatening to publish photographs of intimate moments, grooming to subsequently use women for online porn markets, physical sexual exploitation of matured teen girl students by showing them sexually explicit images in mobile phones or in computer devices by the teachers. There are also hundreds of instances of crimes through digital telecommunication systems as well whereby women are repeatedly harassed by offending phone calls, SMSs and MMSs, instant messaging services and so on. Also, the existing social norms play a major role in making women soft targets in the digital space. Considering the fact that their place in the patriarchal social structure of the country makes them more responsible for the good or bad reputation of the family, especially when the reputation of a women as a 'modest woman of good character' often guarantees the good reputation of the whole family, many harassers target to vandalise women victims profiles not only to destroy the woman's reputation but also destroy the reputation of immediate family members, including father, brother, sisters, husband and so on.

As the world moves into the new century we are faced with an ever-unceasing reliance upon technology and particularly the internet, in our day to day lives. The element of anonymity and lack of territorial borders in cyber space makes internet an attractive medium for criminals to commit crimes. Not only the conventional crimes such as thefts, extortion, defamation or forgery are committed through computers but also new forms of crime have emerged such as hacking, spoofing, email bombing, spreading Trojans, virus and worms, data diddling, phishing attacks etc.

"Cyber-crime" is not defined on any act or statute. A generalised definition for cybercrime is crimes wherein computer act as a tool or as a target or both. In data theft cases, unauthorised access or damage to a computer system(s), a computer is the target of a cyber-crime. In this category also fall the hacking, corporate espionage, theft of intellectual property and other offences. In case conventional crime is committed using computers and the internet, the computer or internet functions as a tool to commit the crime. In this category fall the credit cards frauds, extortions, defamation, criminal intimidation and fraud, cheating by impersonation and phishing attacks.

There are certain crimes where computer can be said to be incidental to a crime that is committed, such as child pornography, money laundering. Another type of cyber-crime is where a computer is used to aid or serves as an accomplice such as software piracy, copyright violations and privacy of video and audio tracks.

On the internet 'vishing' is becoming common i.e., use of voice protocols to commit financial frauds where the victims are made to believe that sensitive information such as credit card information is being requested by a genuine service provider such as a bank where the victim holds an account. Crimes such as frauds, theft, criminal intimidation, forgery are caused by using computers to commit conventional crimes. There is a proliferation of these crimes due to inherent anonymity, the lack of cyber awareness, complexities in enforcing cyber laws that renders this medium as an attractive mode to commit cyber-crimes.

In India, the Information Technology Act, 2000 and Indian Penal Code, 1860 are the principle statutes containing provisions related to computer related crimes. IT Act, 2000 basically covers financial crimes but then also it lacks in giving proper definitions to the crimes. Even the penalties and punishment given under this act is also quiet less or not stringent. This section however does not speak about sexual activities of the victim unlike the Canadian, British or American anti voyeurism laws. We presume that the words "private body parts" also cover nude body parts and usage of such body parts for sexual activities. Section 67A may also be used to prohibit such voyeur sexual activities, as the wordings of Section 67A strongly prohibit distribution of sexually explicit acts or conduct.

Reference

1. Beza, F. The History of Cybercrime [Internet]. Available from: http://www.bezaspeaks.com/cybercrime/history.htm
2. Duggal P. Email: pduggal@vsnl.com; pavanduggal@hotmail.com
3. Fatima T. Cyber Crime. Lucknow: Eastern Book Company; c2011.
4. United Nations. International Review of Criminal Policy United Nations Manual on the Prevention and Control of Computer Related Crimes [Internet]. Available from: http://www.uncjin.org/Documents/EighthCongress.html
5. The Indian Express; c2024.
6. WHOA Statistics for 2000 [Internet]. Available from: http://www.haltabuse.org/resources/stats/2000stats.pdf
7. Cyberbullying adults still awaits any legal tag, even though most countries like the US, have developed laws to prevent cyberbullying against children.
8. Spinderella. Another woman claims Tony Parker was sexting her. The Soul of DFW [Internet]. 2010 Nov 22 [cited 2023 Nov 22]. Available from: http://thesoulofdfw.com/national/news-gossip/spinderella/another-woman-claims-tony-parker-wassexting-her/
9. WHOA Statistics for 2000 [Internet]. Available from: http://www.haltabuse.org/resources/stats/2000stats.pdf
10. WHOA Statistics for 2001 [Internet]. Available from: http://www.haltabuse.org/resources/stats/2001stats.pdf
11. MacKinnon C, Dworkin A. An Act to Protect Civil Rights of Women and Children [Internet]. Available from: http://www.nostatusquo.com/ACLU/dworkin/OrdinanceMassComplete.html
12. Wired Safety [Internet]. Available from: http://www.wiredsafety.org/
13. Cyber Victims Organization [Internet]. Available from: www.cybervictims.org
14. Megan Meier Cyberbullying Prevention Act, 2008.
15. Fatima T. Cyber Crime. Lucknow: Eastern Book Company; c2011.
16. Paranjape V. Cyber Crimes and Law. Allahabad: Central Law Agency; c2010.
17. Indian Penal Code, 1860, s. 292.
18. Indian Penal Code, 1860, s. 293.
19. Information Technology (Amendment) Act, 2008, s. 67.
20. Information Technology (Amendment) Act, 2008, s. 32.
21. Information Technology (Amendment) Act, 2008, s. 32.
22. Information Technology (Amendment) Act, 2008, s. 32.

23. Miller v. California, 413 U.S. 15 (1973); K.A. Abbas v. Union of India (1970) 2 SCC 780.
24. R. v. Hicklin (1868), L.R. 3 Q.B. 360, Cockburn C.J.
25. Mackey TC. Pornography on Trial: A Handbook with Cases, Laws and Documents. p.134.
26. O'Toole L. Pornocopia: Porn, Sex, Technology and Desire. London: Serpent's Tail; c1999.
27. AIR 1965 SC 881.
28. Samaresh Bose v. Amal Mitra, AIR 1986 SC 967.
29. AIR 1971 SC 481.
30. Mutual Film Corporation v. Industrial Commission of Ohio, 236 U.S. 230 (1915).
31. Kuhn A. Cinema, Censorship and Sexuality. London: Routledge; c1988.
32. Roy A. The Great Indian Rape Trick [Internet]. Available from: http://www.sawnet.org/books/writing/roy_bq1.html
33. Bobby Art International & Others v. Om Pal Singh Hoon & Others, 1996 AIR (SC) 1846.
34. AIR 2006 (Bom) 259.
35. Raj Kapoor v. State, AIR 1980 SC 258.
36. Sexting and privacy issues may trigger legal debates as consensual transmission of images could be misused by the recipient, invoking a "fear factor" to establish victimization.
37. Garlik [Internet]. Available from: http://www.garlik.com.
38. Garlik Cybercrime Report [Internet]. Available from: http://www.garlik.com/cybercrime_report.php
39. Ibid.
40. Ibid.
41. Ibid.
42. Ibid.
43. Ibid.
44. Computer Misuse Act, 1990, s. 1.
45. Police and Justice Act, 2006.
46. Computer Misuse Act, 1990, s. 2.
47. Computer Misuse Act, 1990, s. 3.
48. Computer Misuse Act, 1990, s. 1.
49. Police and Justice Act, 2006.
50. Information Technology Act, 2008, s. 67A. Retrieved from: http://cybercrime.planetindia.net/ch11_2008.htm.
51. Halder D, Jaishankar K. Love marriages, inter-caste violence, and therapeutic jurisprudential approach of the courts in India. InTherapeutic jurisprudence and overcoming violence against women, IGI Global; c2017. p. 30-42.
52. Halder D, Jaishankar K. Definition, typology and patterns of victimization. InCyber Crime: Concepts, Methodologies, Tools and Applications. IGI Global; c2012. p. 1016-1042.