VOLUME 4 | ISSUE 3

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

A CRITICAL STUDY OF CYBER CRIMES IN INDIA WITH SPECIAL REFERENCE TO OFFENCE AGAINST WOMEN

- Abhinav Vijayran[1]

ABSTRACT

The critical study of cyber crimes in India, particularly focusing on offenses against women, is paramount in understanding the multifaceted challenges posed by the digital age. In recent years, the proliferation of technology has facilitated various forms of cyber crimes targeting women, including online harassment, cyber stalking, revenge porn, and financial exploitation. This study aims to delve into the intricate dynamics of such offenses, analyzing their prevalence, underlying causes, and the efficacy of existing legal frameworks in addressing them. By examining case studies and statistical data, it seeks to unravel the complex interplay of socio-cultural factors and technological advancements that contribute to the vulnerability of women in cyberspace. Furthermore, the study endeavors to propose recommendations for enhancing legal and technological mechanisms to combat cyber crimes against women, ultimately advocating for a safer and more inclusive digital environment.

I. INRODUCTION

The convergence of computer network and telecommunications facilitated bythe digital technologies has given birth to a common space called ‘cyberspace’. It hasbecome a platform for a galaxy of human activities which converge on the internet.The cyberspace has, in fact, become the most happening place today. Internet is increasingly being used for communication, commerce, advertising, banking, education, research and entertainment etc.[2]there is hardly any human activity that isnot touched by the internet. Therefore, Internet has something to offer to everybodyand in the process, it only

[1] Law Student, Amity Law School, Noida

[2] FarooqAhmad, *Cyber LawinIndia-LawonInternet*,367(NewEraPublication, Delhi,2008).

increases and never diminishes. Cyberspace has bestowedmany gifts to humanity but they come with unexpected pitfalls. Due to the anonymousnature of the internet, it is possible to engage into a variety of criminal activities withimpunity and people with intelligence, have been grossly misusing the aspect of theinternet to perpetuate criminal activities in cyberspace.It is increasingly being used for pornography, gambling, trafficking in human organs and prohibited drugs, hacking, infringing copyright, terrorism, violating individual privacy, money laundering, fraud, software piracy and corporate espionage, to name a few. Cybercrimes, uniquely different from traditional crimes, are often harder to detect andprosecute.[3] It has been observes that criminal activity on the Internet has becomeprogressively more sophisticated. Perpetrators carry out cybercrimes through small,targeted Internet attacks, as well as launching significant attacks using large networksof commercially leased, hijacked computers. Furthermore, cybercrime does greaterdamageto societythan traditionalcrimeand ismoredifficultto investigate.

CYBER CRIME AGAINST WOMAN

The use of cyberspace and its attendant features of anonymity continue toinfluence both positively and negatively on social, economic, cultural, and politicalaspects of every society. Nevertheless, while the cyberspace have provided securetools and spaces wherewomen can enjoy theirfreedom of expression, informationand privacy of communication, the same benefits of anonymity and privacy also extend to those who employ ICTs for criminal activities and use the internet to commit violence against women. The use of mobile phones and internet to stalk, abuse, traffic, intimidate and humiliate women is palpable in developing countriesincluding India. While, the Information Technology Act, 2000 which was amended inthe year 2008, begins to deal with the problem, it does not explicitly deal with all cyber crime and cyber security issues on the person and specifically women.

Women are the worst victim of cyber-crimes; in an incident where a Delhischool

[3] M. Dasgupta,*CyberCrimeinIndia,AComparativeStudy*,8(Eastern Law House, 1st Edn, 2016).

student circulated a mobile video clip of two co-students having sex initiated aheated debate on right of privacy of women and even compelled authorities to banmobile phones in educational institutions. The biggest fear are the IT and computer science students who are constantly making new discoveries on their cell phones. Such incident of pornographic MMS is repeatedly occurring at the various places ofour country. Another incident, where a landlord in Pune has installed a webcam in rented rooms occupied by college girls, has also aroused heated debate on laws relating to privacy of individuals, particularly women, in the country.

Every second, one woman in India gets tricked to be a victim of cybercrimesand the online platform is now the new platform where a woman's dignity, privacy and security are increasingly being challenged every moment. Trolling, abusing, threatening, stalking, voyeurism, body-shaming, defaming, surveillance, revenge pornand other forms of indecent representation of women are rampant in the cyber world.In cybercrimes against women, the effect is more mental than physical while the focus of the laws ensuring women's security is more on physical than mental harm. It is true that the National Crime Records Bureau (NCRB) of India does not maintain any separate record of cyber-crimes against women. Technology is the resource used by some perpetrators who target to defame women by sending obscene WhatsApp messages, e-mail, and stalking women by using chat rooms, websites, and worst of allby developing pornographic videos, mostly created without their consent, spoofing e-mails, morphing ofimagesfor pornographic content by using various software's available online. Indian women are not able to report cyber crimes immediately as they are not really aware as to where to report such crimes or are not serious about reporting the same due to social embarrassment they don't want to face. Their mind-set needs to broaden and they must be the whip to curb down by taking derring-do against such perpetrators that is to go ahead and lodge an immediate complaint. Most of the problems can be solved if women report the crime immediately and warn theabuser about taking strong legal action. Cybercrimes incept generally through fake Idscreated on Facebook, Twitter and other social media platforms causing grave harm towomen, as through these platforms, major blackmailing, threatening,

bullying, orcheating via messenger messages and email are done by perpetrators. Ill-intentioned men perpetrate these cyber-crimes with malafide intention such as illegal gain, revenge, insult to the modesty of a woman, extortion, blackmailing, sexual exploitation, defamation, incite hate against the community, prank satisfaction of gaining control and to steal information. Some of the major well-known cybercrimes have put thousands of women into various health issues such as depression, hypertension and women suffer from anxiety, heart disease, diabetic and thyroid ailments due to e-harassment. Victimization of women in the cyber space and thenature of cyber-crimes that may happen to women may properly be understood if deeper research is done on the ethology of the crimes, the motives of the perpetrators, "crime hubs" and nature and characteristics of the victims and perpetrators. Some of the major cyber-crimes against women areas follows;[4]

Cyberstalking: Cyberstalking is on the rise and women are the most likely targets. Cyber stalking is away to use the Internet to stalk someone for online harassment and online abuse. A cyber stalker does not engage in direct physical threat to a victim but follows the victim's online activity to gather information, make threats in different forms of verbal intimidation. The anonymity of online interaction reduces the chance of identification and makes cyberstalking more common than physical stalking.

Defamation: Cyber defamation includes both libel and defamation. It involvespublishing defamatory information about the person on a website or circulating it among the social and friends' circle of victims or organization which is an easy method to ruin a woman's reputation by causing her grievous mental agony and pain.

Morphing and cyber pornography: Morphing is highly increasing it is done byediting the original picture to misuse it. Perpetrators due to internet access can in fewseconds download women's pictures from social media, WhatsApp or some other resources and upload morphed photos on other websites such as social media site, porn sites or for

[4]DhrutiMKapadia,"Ifthereiscybercrime,womenstartreportingrightnow"(2008)Availableathttps://www.livelaw.in/cyber-crimes-against-women-and-laws-in-india/.

registering themselves anonymously. Cyber-pornography is another threat to women because this includes publishing pornographic materials in pornography websites by using computers and internet wherein women will not even be aware of such immoral publication of their own very image.

E-mail spoofing: It refers to an email that emerges from one source but has been sent from another source. It can cause monetary damage.

Phishing: Phishing is the attempt to gain sensitive information such as username and password and intent to gain personal information.

Trolling: Trolls spreads conflict on the Internet, criminal starts quarreling or upsetting victim by posting inflammatory or off-topic messages in an online community (such as a newsgroup, forum, chat room, or blog) with the intention to provoke victims into an emotional, upsetting response).Trolls are professional abusers who, by creating and using fake ids on social media, create a cold war atmosphere in the cyberspace and are not even easy to trace.

Well, the new medium which has suddenly confronted humanity does not distinguish between good and evil, between national and international, between justand unjust, but it only provides a platform for the activities which take place in human society. Law as the regulator of human behavior has made an entry into the cyberspace and is trying to cope with its manifold challenges. A legal framework for the cyber world was conceived in India in the form of E-Commerce Act, 1998. Afterwards, the basic law for the cyberspace transactions in India has emerged in the form of the Information Technology Act, 2000[7] which was amended in the year 2008.The IT Act amends some of the provisions of our existing laws[5] i.e. the Indian Penal Code, 1860; the Indian Evidence Act, 1872; the Bankers Book Evidence Act, 1891and the Reserve Bank of India Act, 1934. Though

[5] ActNo. 21 of2000.

since, the IT Act 2000 is in place inIndia for curbing cybercrimes, but the problem is that still, this statute is more onpapers than on execution because lawyers, police officers, prosecutors and Judges feel handicapped in understanding its highly technical terminology.

Moreover cybercrime isnot a matter of concern for India only, but itis aglobal problem and therefore the world at large has to come forward to curb thismenace. Further complicating cybercrime enforcement is the area of legal jurisdiction.Like pollution control legislation, one country cannot by itself effectively enact laws that comprehensively address the problem of internet crimes without cooperation from other nations. While the major international organizations, like the Organisation for Economic Co-operation and Development (OECD) and the G-8, are seriously discussing cooperative schemes, but many countries do not share the urgency to combat cybercrimes for many reasons, including different values concerning piracy orespionage or the need to address more pressing social problems. These countries, inadvertently or not, present the cybercriminal with a safe haven to operate. Never before has it been so easy to commit a crime in one jurisdiction while hiding behindthe jurisdiction of another. Though the issue of jurisdiction in cyberspace cannot be settled spontaneously, but still a global effort in this direction is the need of hour.

Technological breakthroughs in the cyber landscape over the past few years inIndia have caused disruptions of immense magnitude with far reaching implications. On one hand, these have been enablers for good governance, smart policing, bettermedical care, etc., while on the other; there has been a surge in cybercrimes, frauds and data thefts. A frequent criminalization instance of the web has resulted in proliferation of illicit trading of arms and drugs, cyberstalking, cyberbullying, cyber extortion, child pornography and soon. The protagonists have graduated from being opportunistic individuals to organized criminal groups who offer cyber crime-as-a-service at a minimal cost over the dark net.

CONCLUSION

Crime is both a social and economic phenomenon. It is as old as human society. Many

ancient books right from pre-historic days, and mythological stories[1] have spoken about crimes committed by individuals be it against another individual likeordinarytheft and burglaryor against the nation like spying, treason etc. 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 [6]the digitisation of economic activities. Every person across the globe in one way or the other is using or becoming part of the cyber world. The advent of information technology has made our work easier but also it makes us vulnerable to number of crimes which are committed over the internet medium. Especially in a society that is dependent more and more on technology, crime based on electronic offences are bound to increase and the law makers have to go the extra mile compared to the fraudsters, to keep them at bay. The main problem lies with the control of cybercrime is that it is committed in borderless world and regulated by national laws, where the law is still struggling to define and redefine the boundaries for the control of cybercrimes.

The cybercrime is far different from conventional crimes. In cyber-crimes, the culprit is regularly significantly harder to find, distinguish, and in the end get. Numerous individuals utilize the web, content informing, and online networking to take cover behind a virtual character which, basically, can be anything and anybody they need, so it is very hard for the law enforcement agencies to deal with the cybercrime with the same old approach. Indeed it is important to have different outlook and adequate knowledge and training for the law enforcement agencies to control the rising cybercrimes.

REFERENCES

- CommissionontheStatusofWomen,*Beijingat15:Reportonthefiftyfourthsession,* E/2010/27 (SUPP) (2010).
- CommissionontheStatusofWomen,*PoliticalDeclarationontheoccasionofthetwenty-fifthanniversaryoftheFourthWorldConferenceonWomen*,E/CN.6/2020/L.1(2020).

[6] Kautilya's *Arthashastra*written around 350 BC, considered to be an authentic administrative treatise in India, discusses the various crimes, security initiatives to be taken bythe rulers, possible crimes in a state etc. and also advocates punishment for the list of some stipulated offences. Different kinds of punishments have been prescribed for listed offences and the concept of restoration of loss to the victims has also been discussed in it

- Convention for the Suppression of the Traffic in Persons and the ExploitationoftheProstitution of Others, 1949.
- Convention on Elimination of All Forms of Discrimination Against Women,1979.
- CouncilofEuropeConventiononPreventingandcombatingViolenceagainstWomenand DomesticViolence, 2011 (IstanbulConvention).

Reports

- Geetha Devi, Meghana, *et, al.,* Vimochana, "Getting away with Murder: HowLawCourts &Policefailvictims of DomesticViolence"(2000).
- GovernmentofIndia,"ReportofTheCommitteeonAmendmentstoCriminalLaw" (Justice Verma Committee on Amendments to Criminal Law, January23, 2013).
- Government of India, "Tackling Violence Against Women: A Study of StateIntervention Measures, Bhartiya Stree Shakti" (Ministry of Women and ChildDevelopment,2017).
- Law Commission of India, "226th Report on the Inclusion of Acid Attacks asSpecific Offences in the Indian Penal Code and a law for Compensation forVictimsof Crime" (July, 2008).
- LawCommissionofIndia,"172ndReportonReviewofRapeLaws"(2000).

A. Books

- A.L.Basham,*TheWonderthatwasIndia*(PanMacmillonIndia,NewDelhi,2005).
- A.K.Coomaraswamy,*Hinduism&Buddhism*(NewYork:PhilosophicalLibrary, 1943).
- A.S.Altekar,*ThePositionofWomeninHinduCivilization:FromPrehistoricTimeto thePresent* (Motilal Banarsidass, 2016).
- AhujaRam,*IndianSocialSystem*(RawatPublications,Jaipur,1993).

- AlbertSchweitzer,*IndianThoughtandItsDevelopment*(TheBeaconPress,1st ed., 1957).
- AlladiKuppuswami,*TheConstitution:WhatItMeansToThePeople*,(Gogia&Company, Hyderabad 2000).
- AparnaSundarandNandiniSundar(eds.),*CivilWarsinSouthAsia:State,Sovereignty,Development*(SAGEPublications IndiaPvt.Ltd., 2014).
- Aristotle,R.F.Stalley(ed.),ErnestBarker(translator),*Politics*,(OxfordUniversityPress, Oxford, 1998).