INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA).*

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

Copyright © International Journal for Legal Research & Analysis. All rights reserved.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

CYBER CRIMES AGAINST WOMEN IN INDIA

AUTHORED BY - VEDANT SINGH

Abstract

The convergence of computer network and telecommunications facilitated by the digital technologies has given birth to a common space called 'cyberspace'. It has become 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.[1]there is hardly any human activity that is not touched by the internet. Therefore, Internet has something to offer to everybody and in the process, it only increases and never diminishes. Cyberspace has bestowed many 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 with impunity and people with intelligence, have been grossly misusing the aspect of the internet 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.[2] It has been observes that criminal activity on the Internet has become progressively more sophisticated. Perpetrators carry out cybercrimes through small, targeted Internet attacks, as well as launching significant attacks using large networks of commercially leased, hijacked computers. Furthermore, cybercrime does greater damage to society than traditional crime and is more difficult to investigate.

Introduction

Over the last few years, cybercrimes have become more intense, sophisticated and potentially debilitating for individuals, organizations and nations. Law enforcement agencies are finding it difficult to check and prevent the crimes in the cyberspace because the perpetrators of these crimes are faceless and incur very low cost to execute a cybercrime whereas the cost of prevention is extremely high. Targetshave increased exponentially due to the increasing reliance

1. Farooq Ahmad, *Cyber Law in India- Law on Internet*, 367(New Era Publication, Delhi, 2008).
2. M. Dasgupta, *Cyber Crime in India, A Comparative Study*, 8(Eastern Law House, 1st Edn, 2016).

ISSN: 2582-6433

of people on the internet.

India is becoming increasingly vulnerable to this menace because of rapid digitization and proliferation of mobile data without matching pace of cyber security and cyber hygiene. India has bypassed Japan to become the world's third largest Internet user after China and the United States, and its users are significantly younger than those of other emerging economies, India now has nearly 74 million Internet users, a 31 per cent increase over March 2012, the report says[3]. Andhra Pradesh (undivided), Karnataka and Maharashtra have occupied the top 3 positions when it comes to cyber-crimes registered under the new Information Technology Act in India.Interestingly, these three states together contribute more than 70 per cent to India's revenue from IT and IT related industries. This clearly indicates that the impact of Information Technology is very profound. Both Society and the Technology areoperating in a way so as to harmonize with the pace of each other's growth. As the World is developing, more technology is emerging with each passing day and thus there is more development taking place in the society. All the facets of human life including education, health, entertainment and communication are being influenced by and have been impacted by the advent of the Information and Communication Technology. This way it is serving with several advantages like greater efficiency, increased communication channels through email, discussion groups and chat rooms, beneficial motivational influence on learning and knowledge, e governance and citizens contribution, expanding global business and alike. With boon comes the bane and thus the World of Information and Communication Technology (in short 'ICT') isno except ion to this rule. Along with abundant opportunities that it has brought about,there are also some challenges too. Broadly speaking, it has posed certain major concerns like privacy threat, over riding cultural impact, more reliance on technology,boycott of societal engagements, computer virus, malware, spam phishing and many more. One of the major challenges in this era of ICT is of an increasing number of cybercrimes taking place in the World today.

The incredible development in the field of ICT coupled with an increased frequency of use of internet for different activities has also given rise to several mischievous activities taking place in the form of Cyber Crimes. To put in a layman's language, Cyber Crime is a technology based crime committed by the technocrats.

At present, India is ranked third in terms of cybercrime incidents behind the United States

[3] National Crime Records Bureau (NCRB) Ministry Of Home Affairs, Cyber Crimes in India, 2015, //ncrb.nic.in *National Crime Record Bureau (NCRB) Report 2012* visited On 1/3/17

ISSN: 2582-6433

and China as per data shared by a leading security vendor, which compiled data of bot-infected systems controlled by cyber criminals in differentcountries. As per Indian Computer Emergency Response Team (CERT-IN), one cybercrime was reported every 10 minutes in India during 2017[4]. These statistics are quite alarming and therefore, merit focused and collective attention from Law Enforcement Agencies. It is evident from the data revealed by National Crime Record Bureau (NCRB) in year 2016, where in about 12,317 Cybercrime cases were reported in India which is 6 percent higher than 2015. According to the annual report released by the NCRB in 2016, with 762 cases, Bengaluru had the second-highest number of cybercrime cases among the metros, behind Mumbai with 980 cases. Other metros in the list were far behind, with Hyderabad recording 291 cases, Kolkata 168, Delhi 90 and Chennai 36. From 762 to 5,035, the numbers of cases have seen a sharp increase in Bengaluru. The increase in Mumbai is not so pronounced. Experts and officials have attributed the high reporting of cybercrimes in Bengaluru to higher incidences and greater awareness among residents, among other factors. "In the other metros, such a step was not even considered. The station also had all the powers of other stations and a wide jurisdiction. Secondly, Bengaluru is an IT hub and the number of IT companies here is very high, even by global standards. Therefore, people with awareness on filing complaints against cybercrimes are also high in number. In short, there are a greater number of cyber literates in Bengaluru," In India the technology users are prone to become the victim of Cyber-crimes because of their level ofeducation and more precisely awareness about the nature of Technology and its use.

In the decade-and-half since it was incepted, the cybercrime cell of Karnataka's criminal investigation department has registered 586 cases. Charges have been filed in a mere 158 cases and none has converted into a conviction. Nationally, of the more than 14,000 cases of cybercrime fraud since 2012, according to the National Crime Records Bureau, only 40 have ended up in convictions, an abys record considering that India with its deep mobile penetration is among the fastest-growing internet markets globally.[5]

[4] https://timesofindia.indiatimes.com/india/one-cybercrime-in-india-every-10 minutes/articleshow/59707605.cms visited on 20/02/24

[5] https://m.economictimes.com/news/politics-and-nation/not-one-cybercrime-conviction-in-bengaluru-in-the-past-15-years/articleshow/51546770.cms visited on 15/02/24.

ISSN: 2582-6433

Considering the significant increase in number of Cybercrimes reported these days, it becomes important and imperative to enquire as to meaning of the term CyberCrime, the categories of Cyber Crimes. Cyber-crime is a crime done with the misuse of information technology for unauthorized or illegal access, electronic fraud; like deletion, alteration, interception, concealment of data, forgery etc., Cyber-crime is an international crime as it has been affected by the global revolution in information and communication technologies (ICTs). The number of Cyber Crimes committed isincreasing with each passing day, and it is very difficult to find out as to what actuallya cyber-crime is and what the conventional crime is. However, to deal with this challenge, knowingly or unknowingly internet users becoming the victims of differenttypes cyber-attacks. Cybercrimes on the basis of nature and different types of attacks are classified into following main categories.

Cybercrimes against individual - These are the crimes against person, against property of an individual are included. Against persons include harassment through e-mail, cyber stalking, and dissemination of obscene material on the Internet, defamation, hacking / cracking and by indecent exposure. Cybercrimes against property of an individual include computer vandalism, transmitting virus, Internet intrusion, and unauthorized control over computer system and hacking / cracking etc.

Cybercrime against Government - includes crimes against government, private firm, company, group of individual etc. These crimes can be made by hacking and cracking, by possession of unauthorized information and through cyber terrorism against the government organization. Distribution of pirated software also covered under these attacks.

Cyber Crime against Property-Involve credit card frauds, crimes related to intellectual property and internet time theft etc.,

Cybercrimes against Society - These crimes not only affect individual or any organization but the society at large. They include Pornography (especially child pornography), polluting the youth through indecent exposure and trafficking etc.

1.2 Cyber Crime against Woman

The use of cyberspace and its attendant features of anonymity continue to influence both positively and negatively on social, economic, cultural, and political aspects of every society. Nevertheless, while the cyberspace have provided secure tools and spaces where women can enjoy their freedom of expression, information and 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

ISSN: 2582-6433

to stalk, abuse, traffic, intimidate and humiliate women is palpable in developing countries including 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 cybercrime and cyber security issues on the person and specifically women.

Women are the worst victim of cyber-crimes; in an incident where a Delhi school student circulated a mobile video clip of two co-students having sex initiated a heated debate on right of privacy of women and even compelled authorities to ban mobile 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 of our 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 cybercrimes and 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 focusof 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 of images for pornographic content by using various software's available online. Indian women are not able to report cybercrimes immediately asthey 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 the abuser about taking strong legal action. Cybercrimes incept generally through fake Idscreated on Facebook, Twitter and other social media platforms causing grave harm to women, as through these platforms, major blackmailing, threatening, bullying, or cheating 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

ISSN: 2582-6433

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 thyroidailments due to e-harassment. Victimization of women in the cyber space and the nature 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 are as follows;[6]

Cyberstalking: Cyberstalking is on the rise and women are the most likely targets. Cyberstalking is a way to use the Internet to stalk someone for online harassment and online abuse. A cyber stalker does not engage in direct physical threatto 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 involves publishing 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 few seconds 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 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.

6 Dhruti M Kapadia, "If there is cybercrime, women start reporting right now" (2008) Available athttps://www.livelaw.in/cyber-crimes-against-women-and-laws-in- india/.

ISSN: 2582-6433

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 cyber space 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 just and unjust, but it only provides a platform for the activities which take place in humansociety. Law as the regulator of human behaviour 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[7] 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 since, the IT Act 2000 is in place in India for curbing cybercrimes, but the problem is that still, this statute is more on papers than on execution because lawyers, police officers, prosecutors and Judges feelhandicapped in understanding its highly technical terminology.

Moreover cybercrime is not a matter of concern for India only, but it is a global problem and therefore the world at large has to come forward to curb this menace. 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

[7] Act No. 21 of 2000.

ISSN: 2582-6433

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 or espionage 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 behind the 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 in India have caused disruptions of immense magnitude with far reaching implications. On one hand, these have been enablers for good governance, smart policing, better medical 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 so on. The protagonists have graduated from being opportunistic individuals to organized criminal groups who offer cybercrime-as-a-service at a minimal cost over the dark net.

To confront these new age cyber criminals, a well thought and effective cybercrime management strategy needs to be devised. If the law enforcement agencieshave to win this battle, there is a need for a paradigm shift in the approach to policing.The focus needs to shift from conventional to contemporary methods with the right blend of upskilling and upgrading the three pillars–people, processes and technology. Predictive policing is needed to disrupt the expanding web of crime. Policy changes atnational and international levels are required to synergize the efforts of all agencies against these faceless and borderless enemies striking across time zones. Greater collaboration is needed to build a responsive framework to carry out effective cybercrime management. Enhanced citizen awareness, quick response mechanisms, technical augmentation and capacity building of law enforcement officers can go a long way in controlling cybercrimes. In addition to international cooperation, law enforcement officials must also be provided access to the tools and technologies like big data analytics, artificial intelligence, robotic process automation and block chainto get ahead of the cyber criminals.

1.3 Statement of the Research Problem

The emergence of the ICTs provides an unparalleled opportunity for People[8] to exploit their capabilities to improve their quality of life as well as the contribution for the welfare of the

ISSN: 2582-6433

society. Nevertheless, while the cyberspace have provided secure tools and spaces where people can enjoy their freedom of expression, information andprivacy 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 violenceagainst women. The use of mobile phones and internet to stalk, abuse, traffic, intimidate and humiliate women is palpable in developing countries including India. While, the Information Technology Act, 2000 which was amended in the year 2008, begins to deal with the problem, it does not explicitly deal with all cybercrime and cyber security issues on the person and specifically women. Further, due to lack ofusage of technology either by men or women, there has been a constant increase incybercrime.

1.4 Objectives of the Study-

The objectives of this research work are to touch[9] all the important facets of thecyber- crimes in a comprehensive way and study is to contribute to the development ofcyber security legislation and regulatory framework in India in order to provide a secure safe space, for People to exercise their right to communicate without fear of abuse, harassment, and violence. In order to achieve this larger goal, the Researcher has identified the following objectives**:**

- To comprehend the basic concepts of the cyberspace.
- To trace the Origin and Historical Development of Cyber-Crimes in India.
- To examine the Cyber Security Laws and Policies to regulate Cyber Crime inIndia.
- To find out the International Initiatives to curb Cybercrime Menace.
- To analyse the role of Indian Judiciary in prevention of Cyber Crime.
- To conduct case study on Cyber Crime against Women and to explore how Cyber-crime affects Women employed in IT/ITes Industries.
- To find out workable solutions and remedial measures for the prevention andcontrol of cyber-crimes.

[8]Dr.Vishwanath Paranjape, *Legal Dimensions of Cyber Crimes and Preventive Laws with SpecialReference to India*, (Central Law Agency Publication, 2010).

[9] R.K. Chaubey, *An Introduction to Cyber Crime and Cyber Law*, (Kamal Law House Publication,2009).

ISSN: 2582-6433

1.5.Hypotheses

- Absence of comprehensive laws to combat cybercrime may encourage the cyber criminals to carry on their illegal activities in cyberspace
- The Information Technology Act, 2000 seems to be ineffective and inefficient enough for controlling the recent developments in Cyber world especially cyber- crimes against women in India.
- Due to the Legal, Technical, Jurisdictional and Operational issues and challenges in regulating cybercrimes may cause difficult task to the authoritiesto detect and prosecute Cyber Criminals.

1.6 Importance of the Study

The significance of the study is to decipher the cyber law as developed in India as well as to do critical comparative analysis of the cyber laws as developed in other countries. The study is important both from the theoretical and practical point of view. On a theoretical level, it reveals the judicial appreciation of all the important facts regarding cyber-crimes. On the practical level, it clearly shows the extent to which judicial approach meets the requirements of the day by protecting the people against various cyber offences. The result of the study would provide hitherto unknown criteria to evaluate the legislative and judicial philosophy in the research area. The practical utility of the work lies in the fact that policy making institutions may remove ambiguities surrounding the cyber laws. They may also enact specific cyber legislations pertaining to cyber-crimes against women.

1.7 The Scope and Limitations of the Study

The present study is limited to analyse the existing domestic cyber security laws in India and the study intends to highlight on judicial response in relation to cyber- crime and also to suggest some remedial measures to prevent cyber-crime. Further, the scope of the study is limited to analyse the cyber violence confronted by of women employed in 30 IT /ITes industries located in Bangalore city, Karnataka

1.8 Review of Literature

Present study deals with Legal Regime on Cyber Crime in India with special reference to study of Cyber Crimes against Women. For the purpose of this study, the Researcher[10] had gone through various books written by eminent authors and jurists, articles, documents, reports, journals, case laws and relevant material available on internet through different

ISSN: 2582-6433

websites. Review of literature relating to the field of study isessential to gain the background knowledge of the research topic and to identify the appropriate research design. Cyber-crime investigations are still a relatively new phenomenon. Methods used by practitioners are still being developed and tested today. While, attempts have been made to create a methodology on how to conduct these types of investigations, the techniques can still vary from investigator to investigator, agency to agency, corporation to corporation, and situation to situation. No definitive book exists on cybercrime investigation and computer forensic procedures at this time. Many of the existing methodologies, books, articles, and literature on the topic are based on a variety of research methods, or interpretations onhow the author suggests one should proceed. Researcher unsure that cyber-crime investigation and the computer forensic methodologies are still in their infancy stages and that the definitive manual has yet to be written.

BOOKS:

I. **Dr. Vishwanath Paranjape** in his book *"Legal Dimensions of Cyber Crimes and Preventive Laws with Special Reference to India",*[8] has pointed out that with the rapid development of computer technology and internet over the years, the problem of cyber-crime has assumed gigantic proportions and emerged as a globalissue. He has suggested the need for international cooperation to combat cyber- crimes and in this regard he has comprehensively discussed various national and international conventions, conferences, summits etc. relating to cyber-crimes along with the municipal cyber legislations of different countries like UK, USA, India, Canada, China, Japan, Germany, Australia, and France etc. In his book he has made efforts to investigate and find out the relevant legislation and judicial trends towards cyber-crimes and cyber criminals. He has also traced the origin of these types of crimes and its impact on the criminal justice administration system. He has suggested that there is a need of international cooperation between nations for curbing the cyber-crimes.

II. **R.K. Chaubey** in his book "*An Introduction to Cyber Crime and Cyber Law*"[9] has emphasized on the significance of 'right to privacy' in digital age, stating that the new technologies have enhanced the possibilities of invasion into the privacy of individuals and

10 Dr. M. Dasgupta, *Cyber Crime in India: A Comparative Study*, (Eastern Law House Publication, 2009).

ISSN: 2582-6433

provided new tools in the hands of eavesdroppers. Thus, individual privacy is at greater stake than ever before.

III. **Dr. M. Dasgupta** in his book *"Cyber Crime in India: A Comparative Study"*[10] has succinctly defined the meaning, nature, scope, characteristics and elements of cybercrimes. Commenting on the scope of cybercrimes he has stated that "it is very essential to emphasize that the world is not run by weapons anymore, or energy, or money. It is run by ones and zeros….little bits of data ….it is all electrons. There's a war out here, a world war. It is not about who has the most bullets. It is about who controls the information – what we see and hear, how we work, what we think etc. it's all about information." Further, he has critically analyzed the modus operandi of some important cybercrimes like cyber hacking, cyber terrorism, cyber pornography, cyber fraud etc. and also stated the national and international initiatives to prevent and control such cybercrimes.

IV. **Vivek Sood** in his book '*Cyber Law Simplified*'[11] cyber-crime is the deadliest epidemic confronting our planet in this millennium. This is an important book, particularly for those scholars who see cyber law simply as a social problem from which participants should be cured. It aims to offer us an understanding of cyber law. This book is structured in to four parts beginning with an analysis of the IT Act 2000 and next part cyber-crime, e-commerce, IPR. In this book there are nine chapters which are related to [11]cyber-crime. Cyber-criminal can destroy web-sites and portals by hacking and planting viruses, carry outline frauds by transferring funds from one corner of the globe to another, gain access to highly confidential and sensitive information, cause harassment by email threats or obscene material, pay tax frauds, indulge in cyber pornography involving children and commit innumerable other crimes on the internet. It is said that none is secure in the cyber world. The security is only for the present moment when you are actually secure. With the growing use of the internet cyber-crime would affect us all, eitherdirectly or indirectly. In this book there is much useful information for any scholar interested in the field of cyber-crime. The book is target audience is the educated general public. This book is helpful for the students, research [12]scholars, teachers, trainees, academicians, scientists etc.

V. **Nandan Kamath** in his book *"Law relating to Computers, Internet and E- commerce:*

---

11 Vivek Sood, *Cyber Law Simplified*, (Tata McGraw-Hill Education, 2001).

12Nandan Kamath, *Law relating to Computers, Internet and E-commerce: A Guide to Cyber Laws andthe Information Technology Act, 2000*, (Universal Law Publishing Co., 2009).

ISSN: 2582-6433

A Guide to Cyber Laws and the Information Technology Act, 2000"[12] has commented on the emerging field of 'electronic evidence[13]' in the cases of cyber-crimes. He has made an in-depth study about the admissibility and authenticity of electronic records, burden of proof in cyber offences, and of certainother concepts like production and effect of such evidences, video-conferencing, forensic computing and best evidence rule etc.

VI. **S.K. Verma and Raman Mittal** in their book "Legal Dimensions of Cyber Space"[13] have explained the basic concepts of cyber world like meaning, types, features and major components of computers; history and development of internet;merits and limitations of internet; various computer contaminants like virus, worms, Trojans etc. Emphasizing on the importance of computers and internet in day-to-day chores they have opined that "today it touches and influences almost every aspect of our lives. We are in the information age and computers are the driving force.

VII Vakul Sharma in his book *"Information Technology; Law and Practice"* [14] has evaluated the issue of jurisdiction in cyber space. While discussing the role of international law in deciding jurisdiction of cyber offences he has made referencesto various principles like territorial principle, nationality principle, protective principle, passive personality principle, effects principle and universality principle. Further, he has made deep insight into the controversial issue regarding extradition of cyber criminals. Moreover, he has examined the US, European and Indian approaches towards personal jurisdiction at a greater length.

Authored has stressed on the controversial issue of extradition of cyber criminals and personal jurisdiction regarding cyber-crimes. He has made a great attempt by interpretation to find out the true intention of legislature behind the passing of Act by referring and applying the Supreme Court Judgements for betterunderstanding the various provisions relating to cyber- crimes. He has critically analysed and pointed out the powers and functions of the cyber Regulatory Appellate Tribunal, Controller of Certifying Authorities, Adjudicating Officers and Police officers under the Information Technology Act.

Brian, Loader and Douglas, Thomas, in their book *"Cybercrime Law Enforcement,*

[13] S.K. Verma and Raman Mittal, *Legal Dimensions of Cyber Space,* (Indian Law Institute Publication, 2004).

ISSN: 2582-6433

Security and Surveillance in the Information Age"[14], has emphasized on the enforcement of cyber-crime[15] legislations by stating that "proper enforcement of law in its letter and spirit is more important than its enactment." Further, they have focused on the enhanced role of law enforcement agencies in investigating cybercrimes.

VII. **Stephenson, Peter** in his book *"Investigating Computer- related Crime",*[16] has observed that traditional methods of investigating traditional crimes are of not much use in the investigation of hi-tech crimes committed on e-way. Thus, he has enumerated various modes, methods and techniques to investigate the crimescommitted via computers and internet.

VIII. **Maarc D.Goodman D Susan W.Brennerg-** in his book '*The Emerging Consent on Criminal Conduct in Cyberspace'*- explores the historical aspect of victimization of women users in the internet. This includes the discussion on why mostly women are targeted in the cyberspace and what methods the offenders use to attack them in the cyber space. The time periods or the spaces in which women are attacked are also discussed& also provided the reasons why we chose to writea book on only women victims of internet crimes. It also gives a detailed description on the research done to write this book. This book also gives the aims and the audience that the book is aiming to attract. In addition, the scope and the expected implications of the book are presented.

IX. **Dr. Pawan Duggal** in his book "Text Book on Cyber Law"[16] has comprehensively and simply discussed the emerging developments in cyber law and its legal consequences and control mechanism for understanding the phenomenon of cyber-crime. This book covered not only the emerging developments in cyber law but also the dark side of Internet and World Wide Webwith its consequences. He has covered all the concepts relating to cyber-crime. According to him, cyber law is a phenomenon which is the most latest andcomplex in legal jurisprudence.

X. **K. Jaishankar,** *Cyber Criminology: Exploring Internet Crimes and Criminal2011* **-** This volume explores all aspects of this nascent field and provides a window on the future of Internet crimes and theories behind their origins.

Ronald J. Deibert, '*Black Code: Inside the Battle for Cyberspace 2013'* This book

[14] Brian, Loader and Douglas, Thomas, *Cyber-Crime Law Enforcement, Security and Surveillance inthe Information Age*, (Routledge Publication, London, 2000).

[15] Vakul Sharma, *Information Technology: Law and Practice*, (Universal Law Publication Co., 2010).

[16] Stephenson and Peter, *Investigating Computer- related Crime*, (CRC Press, New York, 2000).

ISSN: 2582-6433

highlights on the Governments and corporations are in collusion and are setting the rules of the road behind[17] closed doors. This is not the way it was supposed to be.

XI. **Debarati Halder, & K. Jaishankar** *'Cyber [18]Crimes against Women in India [18]* The book is a significant contribution to socio-legal research on online crimes targeting teenage girls and women. It shows how they become soft targets of trolling, online grooming, privacy infringement, bullying, pornography, sexual defamation, morphing, spoofing and so on.

XII. **Bhushan,** has revealed that awareness of cybernetics in India is abysmally low and thus has gained a reputation[19] as a country where foreign investors can do business in cybersecurity and have been investing heavily in cybersecurity.

ARTICLES:

a) **Behra, Abhimanyu** in his article "*Cyber Crime and Law in India*",[19] has discussed various types of cybercrimes and also suggested strategies to curb them.

b) **Paranjape, Vishwanath** in his article "*Cyber Crime:* A *Global Concern*",[20] has focused on the global nature of cybercrimes and also presses the need for global measures to curb them.

c) **Tanaya Saha and Akancha Srivastava** in their article '*Indian Women at Risk in the Cyber Space: A Conceptual Model of Reasons of Victimization* '[21] they have made an attempt to find out the various reasons[20] behind the fact to why Indian women are being victimized and a conceptual model of cyber victimization of Indian women are proposed.

d) **Shobhna Jeet** '*Cyber-crimes against women in India: Information Technology Act, 2000* '[22] *researcher highlighted on the types of cyber-crimes against women inIndia in the light of Information Technology Act, 2000 and observed that there is no specific provision to protect security of women.*

e) **Mukta Batra** in the article '*Cyber-Bullying in India: The Search for a Solution Why*

17 Pawan Duggal, ***Text Book on Cyber Law*** **(Universal Law Publishing Pvt. Ltd., 2013).**

18 Debarati Halder and K.Jaishankar, *Cyber Crime against Women in India*, (SAGE Publications IndiaPvt Ltd., New Delhi, 2017)

19 Paranjape, Vishwanath, "Cyber Crime: A Global Concern", pp. 20-27, *IPJ*, Jul.-Sep. (2007).

ISSN: 2582-6433

Model of Reasons of Victimization", IJCC, Vol 8, Issue 1, January - June (2014). *the Current Law in India is Ill- Equipped',*[21] Cyber bullying is, arguably, a milder offence when compared to offences such as murder. This problem can be effectively controlled by non-legal or indirect legal controls.

f) **Pandey.K** '*Low security makes netizens vulnerable to cyber* crimes' [24]concluded that lack of awareness about internet and low level of internet security is fast making Indore a heaven for cybercriminals. There has been a steady increase in the number of cybercrimes as people are not aware about the rapid developments in the cyber-world. Increasing dependence of common citizens on cybernetics without [22]proper security has made the job easy for cybercriminals. In the absence of experts and cyber sleuths, Indore has become more vulnerable to cybercriminals, the researcher concluded.

g) **Saxena.P** '*A Cyber Era Approach for Building Awareness in Cyber Security for Educational System in India'*[23] has concluded that proactive actions on the part of Government and enhanced participation of education system in the cybersecurity awareness approach may lead to a strongly secured nation.

a. Saroj Mehta & Vikram Singh, '*A Study of Awareness About Cyber laws in the Indian Society'*[26] they have suggested that there is proper awareness about cyber law and observed that there is difference between the awareness level of male and female users[24] of internet services and it was established that the male netizens are more aware for Indian cyber laws in comparison to their female counterparts.

b. Dalal.P, "*Awareness of Cyber Law in India*[27], one area that requires special attention is the cyber law awareness in India. Very few users, practitioners and organizations are aware about disputes arising out of IT Act, 2000 and its various amendments.

c. Nappinai.N.S, *Cyber Crime Law in India: Has Law Kept Pace with Emerging Trends? An Empirical Study*[28] found that cybercrime prosecution is not resorted inmany instances due to lack of awareness amongst both the victims and the enforcement authorities about the applicability of general laws to cybercrimes

d. *Seth.K* *'India – Cyber-crimes and the arm of Law – An Indian Perspective'*[29],has

[22] Behra, Abhimanyu, "Cyber Crime and Law in India", *IJCC*, p. 16-30 (2010).
[23] Shobhna Jeet, "Cyber-crimes against women in India: Information Technology Act" pp. 8891-8895,ECLJ 47, (2012
[24] Batra Mukta, "Cyber-Bullying in India: The Search for a Solution -- Why the Current Law in India isIll-Equipped", SSRN, (2014).

ISSN: 2582-6433

noticed that with increasing awareness and provision of training on the subject of cybercrime[25], enhanced technological and legislative steps being taken to further strengthen the IT laws and enforcement framework, India will effectively succeed in combating the problem of cybercrimes

(e) Rohit K. Gupta, '*An Overview of Cyber Laws vs. Cyber Crimes: In Indian Perspective'*[30]. This paper focus on immense increase in the use of Internet and dependency of individuals in every field, a number of new crimes related to Computer and other gadgets based on internet have evolved in the society. Such crimes where use of computers coupled with the use of Internet is involved are broadly termed as Cyber Crimes. There was no statute in India for governing Cyber Laws involving privacy issues, jurisdiction issues, intellectual property rights issues and a number of other legal questions. With the tendency of misusing of technology, there arisen a need of strict statutory laws to regulate the criminal activities in the cyber world and to protect the true sense of technology "Information Technology Act, 2000" [ITA- 2000] was enacted by Parliament of India to protect the field of e-commerce, e-governance, e-banking as well as penalties and punishments in the field of cyber-crimes. The above Act was further amended in the form of IT Amendment Act, 2008 [ITAA-2008].

(f) Preethi A Nayak, Anandatheertha. –'*Cyber Crime and Role of Law in India'* – This paper mainly focus on Crime is both a social and economic phenomenon. Itis as old as human society. Crime is any form adversely affects all the members ofthe society. In developing economics, cybercrime has increased at rapid strides, due to the rapid diffusion of the Internet and the digitization of economic activities. In a cybercrime, computer or data itself the target or the object of offence or a tool in committing some other offence, providing the necessary inputsfor that offence. All such act of crime will come the broader definition of cybercrime. The misuse of the technology has created the need of the enactment and implementation of the cyber laws. As the new millennium dawned, the computer has gained popularity in every aspect of our lives. This includes the use of computers by persons involved in the commission of crimes.

g. Brian C. Lewis, '*Prevention of Computer Crime amidst International Anarchy'***, -**In this, author considers reliance solely on an international legal framework for the prosecution

[25] Seth K, India – Cybercrimes and the arm of Law – An Indian Perspective, (2007). retrieved from http://www.sethassociates.com/%E2%80%9Ccyber-crimes-and-the-arm-of-law-an- indian-perspective.html

ISSN: 2582-6433

of computer-related offences to be inadequate and proposed a framework for prevention as a better alternative. The author endorses a "prevention-based" legal regime utilizing such novel approaches as "privately- sponsored corporate bounties", instituting a tort liability regime for ISPs, "hack-in contests", and a "market trading system" to control private sector solutions, etc.all involving an active role for IS.

h. A.S. Chawla, *'Cyber Crime – Investigation and Prevention',* **-**this paper focus on internet as a global media, need for international cooperation to combat cybercrime and efforts at the global level to curb cyber menace.

i. Rajlakshmi Wagh, '*Comparative Analysis of Trends of Cyber Crime Laws in USA and India'*.[31] This article mainly emphasises on Today's Global era needs laws governing fast paced cybercrime. The popularity of on-line transaction is on the rise thereby having attempts made by unscrupulous entities to defraud internet users. The modus operandi may be in the form of Hacking, Spoofing, Pornography, Scanners, Device, Fake card and the like. The Educational sectors, Defence sector, Law Enforcement Bodies, Bank sectors are exposed to risk as the information sought usually includes data such as username, passwords, bank account and credit card number, revelation of which is huge loss for not only every individual but also the state at large. The paper is an analysis of the USA Laws for Cyber Crime with a comparative analysis with the Indian Laws. The aimis to analyze the conviction rate in cybercrime with comparison to both thecountries and suggest various remedies.

1.9 Research Methodology

In pursuing this study, the methodology adopted is both Doctrinal study . The research is combination of descriptive in nature for the purpose of this Doctrinal study, The Researcher is relied on various source of information including Laws, Policies, Judicial Guidelines, International Conventions, articles published in several national & international journals, Judicial Decisions, Legal Text Books, Reports of Law Commission, Periodicals, Academic writings, Commentaries, Websites, & Statements of Administrators etc.