REVENGE PORN AND BLACKMAILING UNDER CYBERCRIME AGAINST WOMEN IN INDIA: A SOCIO-LEGAL STUDY IN LUCKNOW CITY

Thesis

SUBMITTED TO THE
BABASAHEB BHIMRAO AMBEDKAR UNIVERSITY, LUCKNOW

FOR THE AWARD OF DEGREE OF

Doctor of Philosophy

IN

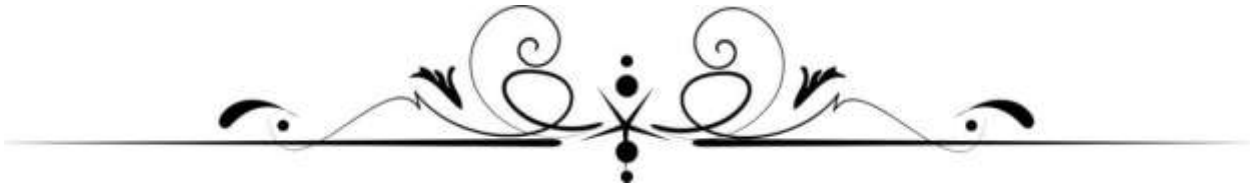
LAW

SUPERVISOR
PROF. (Dr.) SUDARSHAN VERMA
DEPARTMENT OF LAW
SCHOOL OF LEGAL STUDIES

SUBMITTED BY
IRSHAD AHMAD
ENROLLMENT NO. 160/15

DEPARTMENT OF LAW
SCHOOL OF LEGAL STUDIES
BABASAHEB BHIMRAO AMBEDKAR UNIVERSITY
(A CENTRAL UNIVERSITY)
VIDYA VIHAR, RAEBARELI ROAD, LUCKNOW-226025 (U.P.), INDIA

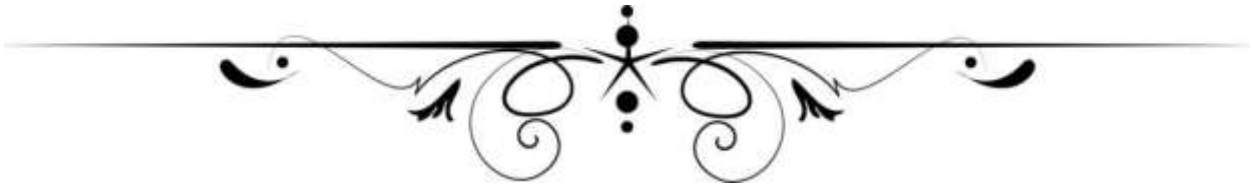
2022



THIS THESIS IS DEDICATED

TO

MY BELOVED AMMI & ABBU



DECLARATION

I, **Irshad Ahmad**, hereby declare that this research work embodied in this Ph.D. thesis titled **"Revenge Porn and Blackmailing under Cybercrime against Women in India: A Socio-Legal Study in Lucknow City"** has been carried out by me under the supervision of **Prof. (Dr.) Sudarshan Verma**, Former Dean, School of Legal Studies & Head, Department of Law, Babasaheb Bhimrao Ambedkar University, Lucknow.

This research work is an original work and it has not been previously submitted in part or full for any other degree or diploma in this or any other University. This is also declare that the thesis is essentially free from all kinds of plagiarism.

Date: 06.06.2022

Place: Lucknow

(Irshad Ahmad)

Research Scholar
Enrollment No.160/15
Department of Law
School of Legal Studies
Babasaheb Bhimrao Ambedkar University
Lucknow-226025 (U.P.), India

CERTIFICATE

This is to certify that the thesis titled "**Revenge Porn and Blackmailing under Cybercrime against Women in India: A Socio-Legal Study in Lucknow City**" submitted by **Mr. Irshad Ahmad** is an original research work and has not been previously submitted in part or full for the award of any other degree or diploma to this or any other university.

This thesis submitted to Babasaheb Bhimrao Ambedkar University, Lucknow satisfies all the requirement as stipulated in the Doctor of Philosophy (Ph.D.) Regulation, 2016 as amended in 2017 and it is fit for submission and evaluation for the award of degree of Doctor of Philosophy of the University.

Date: 06.06.2022

Supervisor

06/6/22

Head of Department

HEAD
Department of Law, SLS
B.B.A. University Lko- 226025

ACKNOWLEDGEMENT

"In the name of Allah the most merciful and beneficent"

Praise be the Allah the most merciful and beneficent, the benevolent, the compassionate who showed me the path of righteousness, and gave me the courage, strength, capability and understanding, that I have been able to complete my present venture to fulfill the requirements of Ph.D. Degree from this prestigious and most loving Babasaheb Bhimrao Ambedkar University, Lucknow, that is like Heaven on Earth for me where I got the wisdom of knowledge to serve the humanity.

It is my pleasant duty to express my sense of gratitude and obligations towards those without whose help and encouragement this work could not have been produced in this form.

I am extremely thankful to our Hon'ble Vice-Chancellor ***Prof. Sanjay Singh*** *for providing me a suitable platform and academic environment to carry out my research work.*

I express my deep sense of gratitude to my eminent and erudite Supervisor ***Prof. (Dr.) Sudarshan Verma (Former Dean & Head)*** *Department of Law, SLS for her excellent and blissful monitoring, motivation, precious suggestions and encouragement to keep my endeavor intact towards the preparation and completion of this work. It is an honour for me to work under her supervision.*

I am very thankful to ***Prof. Preeti Misra,*** *Dean, School of Legal Studies, Head, Department of Human Rights, for providing all necessary academic and administrative support to carry out my research work.*

I am equally thankful to the learned ***Prof. Sanjeev Kumar Chadha,*** *Head Department of Law, SLS, who has provided an excellent academic environment in the Department, where I groomed my personality as a Ph.D. student. I am thankful for his relentless motivation, guidance and suggestions.*

I feel immense pleasure and honour to record my sincere gratitude and veneration to my learned, and kind teachers who are galaxies of intellectuals especially to, ***Dr. Sufia Ahmed, Dr. Anis Ahmad, Dr. Pradeep Kumar and Dr. Mujibur Rehman,***

Asst. Professor *in Department of Law, SLS, for their vision, direction, encouragement, guidance, high teachings and suggestions which have been a source of inspiration and knowledge for me from the very first day of joining department.*

I am very thankful to my friend, especially ***Dr. Sanober Ameer, Dr. Asim Hasan, Dr. Jamal Nasir, Shadab Alam, Abdul Mueed Ansari, Sateesh Kumar, Dinesh Singh, Prashant, Nitesh Chaturvedi, Shalini, Ashwini and my fiancée Aarifa Saghir*** *and all other class fellows for their constant support, valuable suggestions, exchange of knowledge and information, kind co-operation at all stages of this work.*

I express my thanks to ***Dr. Muneesh Swaroop, Dr. Milind Raj Anand, Dr. Pankaj Rawat, Dr. Raj Kumar Paricheta, Dr. Ragini, Dr. Ankita,*** *Resource Person in Department of Law for their support and valuable suggestions.*

I express my thanks to the entire library staff especially to ***Dr. O. P. Saini,*** *Assistant Librarian of Gautam Buddha Central Library, BBAU, Lucknow, for providing access to all high level Research Database.*

I express my thanks to all SHOs of Police Station of Commissionrate, Lucknow, for their co-operation especially to ***N. Chaudhary****, Joint Police Commissioner, Lucknow.*

I wish my heartiest gratitude to my revered most loving and dearest parents ***Mr. Iftekhar Ahmad*** *and* ***Mrs. Mazharun Nisha*** *for their perpetual blessings, love, care and compassion, patience, guidance and high ideals of life that encouraged and inspired me throughout the course of this study.*

I also express my sincere gratitude and admiration from the core of my heart to my most loving sisters, ***Razia Begum, Shazia Khatoon, Aliya Begum, Fareeda Beghum, Sayeeda Khatoon*** *and* ***Tabassum Jahan*** *for their progressive ideas, valuable suggestions, co-operation and encouragement in all my academic and legal pursuits.*

My sincere thanks to the whole staff of Department of Law especially to ***Mr. Avadhesh Yadav, Aniket Kumar, Dharmendra Yadav, Alok*** *and others for their immense co-operation.*

Last but not the least, I am grateful to all those who toiled behind the scene and assisted me in completing this Ph.D. work.

Irshad Ahmad

TABLE OF CONTENT

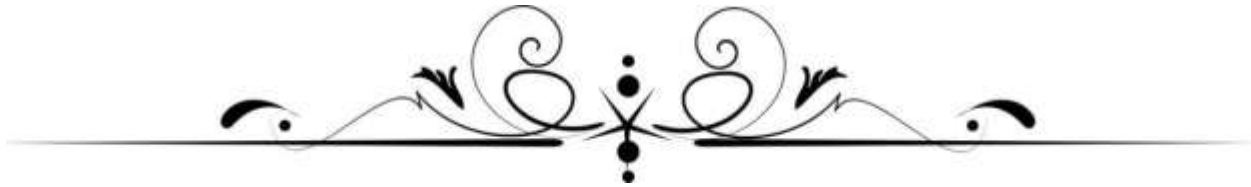
LIST OF CASES

- *Raj Kapoor* v. *State of Maharashtra*
- *Ram Jethmalani* v. *Union of India*
- *Ram Narain* v. *State of Bombay*
- *Ranjit D. Udeshi* v. *State of Maharashtra*
- *Regina* v. *Hicklin*
- *Rishi Narula* v. *The State NCT of Delhi and Ors.*
- *Romesh Thappar* v. *State of Madras*
- *Roth* v. *United State*
- *Rustom Cavasjee Cooper* v. *Union of India*
- *S. Khushboo* v. *Kanniamal & Ors*
- *Sakal Papers (P) Ltd. & Ors.* v. *Union of India*
- *Samaresh Bose* v. *Mr. Amal Mitra*
- *Saumya Tiwari* v. *State Of U.P.*
- *Sharat Babu Bigumati* v. *Government (NCT of Delhi)*
- *Sharda* v. *Dharmpal*
- *Shivaprasad Sajjan* v. *R/At No. 560/B*
- *Shreya Singhal* v. *Union of India*
- *Shri Chandrakant Kalyandas Kakodkar* v. *The State of Maharashtra and Ors.*
- *State of Maharashtra* v. *Madhukar Narayan Mardikar*
- *State of Tamil Nadu* v. *Suhas Katti*
- *State* v. *Charulata Joshi*
- *Subhranshu Rout @ Gugul* v. *State of Odisha*
- *Syed Asifuddin* v. *State of Andhra Pradesh and Ors.*
- *T. T. Antony* v. *State of Kerala*
- *The State of Tamil Nadu* v. *Dr. L. Prakash*
- *Vishaka* v. *State of Rajasthan*
- *Von Hannover* v. *Germany (No 2)*
- *West Bengal* v. *Boxi*

ABBREVIATIONS

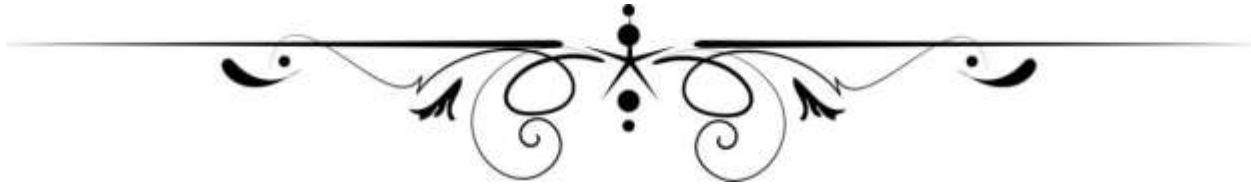
AC	:	Appellate Court
AIR	:	All India Reporter
Art.	:	Article
Al	:	Artificial Intelligence
ARPA	:	Advanced Research Projects Agency
ARPANET	:	Advanced Research Project Administration Network
B.C.	:	Before Christ
CJCA	:	Criminal Justice and Courts Act
Cr. LJ	:	Criminal Law Journal
Cr.P.C.	:	Criminal Procedure Code
DoD	:	Department of Defence
ECHR	:	European Commission on Human Rights
ECOSOC	:	The United Nations Economic and Social Council
Ed.	:	Edition
EDVAC	:	Electronic Disket Variable Automatic Computer
ENIAC	:	Electronic Numerical Integrator and Calculator
EU	:	European Union
H.C.	:	High Court
Hon.	:	Honorable
Ibid	:	In the Same Place
IBM	:	International Business Machine
IMPs	:	Interface Message Processors
Ins.	:	Inserted
IPC	:	Indian Penal Code
ITU	:	International Telecommunication Union
MoU	:	Memorandum of Understanding
NCDRC	:	National Consumer Disputes Redressal Commission
NCRB	:	National Crime Records Bureau

NSF	:	National Science Foundation
NSFNET	:	National Science Foundation Network
Ors.	:	Others
p.	:	Page
Para	:	Paragraph
PC	:	Personal Computers
Retd.	:	Retired
SC	:	Supreme Court
SCC	:	Supreme Court Cases
Sec.	:	Section
SLLs	:	Special Laws
SNW	:	Social Network
Supra	:	Before this
U.K.	:	United Kingdom
U.N.	:	United Nations
U.S.	:	United States
U.S.A.	:	United State of America
UDHR	:	Universal Declaration of Human Rights
UNIVAC	:	Universal Automatic Computer
UNODC	:	United Nations Office on Drugs and Crimes
v.	:	Verses
Vol.	:	Volume
VSNL	:	Videsh Sanchar Nigam Limited
WSIS	:	World Summit on the Information Society
www	:	World Wide Web



CHAPTER-I

INTRODUCTION



CHAPTER-I

INTRODUCTION

1.1. Introduction

The development of technology has given us hope and brought enormous changes in pattern of our lives. These evolutions of Information Technology (IT) gave birth to the cyber space which became more familiar to the people, wherein internet provides equal opportunities to all without any gender discrimination to access any information, data storage, analyses etc. with the use of high technology. The revolution brought by information & technology and communication in twentieth century brought enormous changes in the way people organized their lives, economies, industries and institutions. These changes have brought enormous development in modern times and enhanced the quality of lives. At the same time, these have led to manifold problems including the problem of cybercrime.[1] Women too are using the cyber space and they are much vulnerable to cybercrime. The physical world crime against women is now committed in the virtual world too and the crime of virtual world is known as the cybercrime against women. The women are much targeted in committing the cybercrime because of their vulnerability in cyberspace. The Information and Communication Technologies (ICTs) have replaced the lethal weapons of guns and swords in the hand of criminals with the feather touch board. The situation is further accentuated by the unpredictable nature of cybercrime, particularly cybercrime against women.

The term 'cybercrime against women' in India is mostly used to denote sexual crimes and sexual abuse on the internet, such as morphing the picture and using it for purposes of pornography, harassing women with threatening mails or messages, cyber stalking, etc. Traditional physical space crimes such as rape, molestation, blackmailing and stalking have gained new significance due to the development of information and communication technology.[2]

Technology is the resource used by some perpetrators who target to defame women by sending obscene messages through Whatsapp, e-mail, and stalk women by using chat rooms, websites; and worst of all by developing pornographic videos,

[1] Uchenna Jerome Orji, *Cyber Security: Law and Regulation* 2 (Wolf Legal Publisher, 2012).
[2] Barkha and U. Rama Mohan, *Cyber Law & Crime: IT Act 2000 & Computer Crime Analysis* 10 (Asia Law House, Hyderabad, 2006).

mostly created without their consent, spoofing e-mails, morphing of images for pornographic content by using various software available online. Popular perception predict that women in India make most vulnerable targets on the internet and digital communication technology due to their gender and easy access of images of Indian women as porno-materials.

The technology changes the pattern of people's life. The computer, smart mobile-phone, and easy and inexpensive access of internet mould people's life into virtual reality. Since 2000, two decades have got over but before it people could not think about owning mobile phone or computer so easily, but presently everyone has mobile phone and computer, laptop, tablet, smart watch etc. Due to the development of the technology these equipment became cheaper and non-accessibility vanished. Presently the maximum population of the world can access internet at economical price. The technological development changes every dream into reality. Day by day, people's dependency has increased on the computers, internet and cellular technology. Now people want to connect everything to everything through network. The human behavior has also changed with the technological development. People now shop, communicate and share information in digital form, which was previously impossible. The development of technology has brought the virtual world in parallel to the physical world and today they run together. In India, most of the people frequently use the cyber space but due to the widespread illiteracy or lack of knowledge of cyber space, they are not able to understand the vices of internet and hence are susceptible to fall into the hand of cybercriminals usually young women.

Violence against women is not new phenomena. They are the subject of violence in all ages.[3] The vulnerability and safety of women is one of the biggest concerns of any criminal and penal law, but unfortunately, women are still defenseless in cyberspace.

The issue of privacy and dignity of women in cyber space also needs more concern of the authorities, as it is the responsibility of the State to protect them. The concept of right to privacy for women and girls in relation to electronic media has often been narrowly understood as right to protection against sexual perpetrators. Art. 17(1) of the International Covenant on Civil and Political Rights says, "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home

[3] Sahanaudupa, "Virtual Crime and Women*"* 43(4) *Economic & Political Weekly*, 101-109 (2018).

or correspondence, nor to unlawful attacks on his honour and reputation". In ***Justice K.S. Puttaswamy (Retd.) Case,***[4] Supreme Court of India declared right to privacy as a Fundamental Right, which is protected under Art. 21 of the Constitution. The victimization by way of revenge porn has become a common phenomenon in India. The revenge porn, a cybercrime against women is advanced form of the violation of right to privacy.

The accessibility of Internet-enabled devices like, computers, laptops tablets and mobile phones, as well as social media networks and social applications, which facilitates increased opportunities for some form of digital based sexual harm.[5] In the last several years, a concept known as revenge pornography or 'revenge porn' has seen disgruntled ex-partners, without the consent of former partners, distribute private sexual images and videos on the Internet that were self-produced with the consent of those depicted. Revenge porn typically involves the use of text messaging or sexting. Sexual images and videos can include both images taken by the victim (a 'selfie') or a partner where consent was given, as well as images that have been obtained without consent through coercion or hacking a victim's devices, or through hidden video recordings, or through doctoring or superimposing the victim's face or identity with an existing pornographic image. The impetus for the distribution is the vengeance sought by an ex-partner following the breakdown of the relationship and aptly captured by the anonym 'revenge porn'.

The term 'revenge porn' was originally generated by the media to indicate that sexually explicit images were distributed without the consent of the person depicted in the pictures and videos.[6] This term indicates that the reason for distributing such images or videos is for revenge. However, there are other motivations for distributing sexually explicit images without the consent of the person depicted, which includes a desire to embarrass, humiliate or blackmail the victim.

The concept of revenge porn or image based sexual abuse is extended with blackmailing (sextortion). It is not only the illegal distribution of (consensually) produced image and videos addressed, but also the creation and production thereof. Therefore, revenge porn with blackmailing is a crime.

---

[4] *Justice K. S. Puttaswamy (Retd.)* v. *Union of India*, (2017) 10 SCC 1.

[5] N. Henry and A. Powell, "Sexual Violence in the Digital Age: The Scope and Limits of Criminal Law" 25(4) *Social & Legal Studies*, 397- 418 (2016).

[6] N. Henry and A. Powell, "Sexual Violence in the Digital Age: The Scope and Limits of Criminal Law" 25(4) *Social & Legal Studies*, 397-418 (2016).

In India, there is no specific law for regulating revenge porn and blackmailing.[7] But, regulated by the way of various provision of the scattered laws. Due to the lack of specific and appropriate law to administer these crimes, the criminals are committing these crimes fearlessly. Hence, the crime rate is increasing day by day.

In India the rate of cybercrime against women is ascending as per the 2016 National Crime Records Bureau (NCRB). The NCRB report 2016 states that in 2016 there has been 48,31,515 incidences of crime in India under Indian Penal Code (IPC) as well as under special laws (SLLs), which is 2.9% more than the crime incidences of 2015. Of these total crimes, the number of cybercrimes is 12317, which form 0.25% of the total crimes. This is inclusive of cybercrimes against women. The cybercrime incidences have increased at a rate of 6.3% during 2015-16 and 20.5% during 2014-15. The number of cybercrimes in India in 2014 and 2015 have been 9622 and 11592 respectively. It shows either there are not adequate laws to cover all incidences or there is lack of awareness of what constitutes cybercrime and seeking the help of law. The position becomes more critical when it comes to cybercrimes against women. The figures of cybercrime against women are not clearly available and we have to assume it from relevant Indian Penal Code and special law crimes and crimes booked under relevant sections of the Information Technology Act, 2000. Most of the cybercrime against women are included in crimes under Information Technology Act.[8]

The number of cybercrime reported in Uttar Pradesh in 2016 is 2639 which is too low as compared to other crimes under Indian Penal Code and Special Law. This shows that there is lack of awareness as to what constitutes a cybercrime and which authority to report to. This figure is inclusive of cybercrime against women.[9]

India does not have any uniform law to regulate internet or digital crimes targeting women. In 2000 the Information Technology Act, 2000 (IT Act) was introduced in India to govern cyber related issues which came into force on 17th October 2000. The scope of this provision was limited to provide legal recognition to electronic commerce-filing of electronic records and creation and management of

[7] Debarati Halder, K Jaishanker. *Cyber Crimes against Women in India 133* (Sage Publication, New Delhi, 2017).
[8] Government of India, "Report of National Crime Record Bureau" (Ministry of Home Affairs, 2016) *available at*: https://ncrb.gov.in/en/crime-india.(last visited on 2nd March, 2022).
[9] *Ibid.*

digital signature. The Indian Penal Code, 1860; Indian Evidence Act, 1872; Bankers Book Evidence Act, 1891 and The Reserve Bank of India Act, 1934 were also amended in consonance with the IT Act, 2000. Apart from this, the Information Technology Act had limited provisions for penalizing certain types of offences including damage to computer system, hacking, publication of obscene materials in the digital form.

To facilitate smooth performance of this IT Act, 2000 several rules were also made. However, this version of the Information Technology Act, 2000 suffered multiple drawbacks including those related to governing cybercrime against women. To rectify this, new amendment version of the Information Technology Act was brought in, which was made functional from 2008. Some extend to fill the gap but severely failed again to provide any effective solution for hate crime or for cybercrime against women.

As mentioned above, India does not have any consolidated focused laws on governing cybercrime against women. Similarly, the present Information Technology Act 2000 also suffered from several drawbacks, which have made the concept of cyber jurisprudence still a half- baked legal philosophy.

After *Delhi Gang Rape Case*[10] there has been a huge outcry over bringing out new reforms and penal provisions so as to protect to women against the crime. Therefore, in 2013, The Criminal (Amendment) Act passed and several new sections were inserted and some were amended in the Indian Penal Code such as sections 354, 354A, 354B, 354C, 354D. With the help of these new or amended provisions in Indian Penal Code, now the issues of MMS Scandals, pornography, morphing, defamation can be dealt in proper manner. But no amendment was made in the Information Technology Act 2000 to protect women from cybercrime in cyber space.

It is crystal clear from the preamble of the Information Technology Act 2000 which confirms that, it was formed for the regulation of the e-commerce, hence this Act 2000 mainly covers commercial and economic crimes i.e., hacking, fraud, breach of confidentiality etc. but the drafters did not insert the provision which provides protection to the net users. Gradually the domain of cyber space is increasing day by day but the Information Technology Act, 2000 does not provide any specific sections and provisions specially for the protection of women from cybercrime such as

[10] *Nirbhaya Case* in 2012.

revenge porn and blackmailing, etc. As long as there is no uniform law, the police, prosecutors and the courts have to look into the existing laws which are scattered in traditional criminal codes, such as The Indian Penal Code, 1860; The Code of Criminal Procedure, 1973; The Evidence Act, 1872 or the recently developed laws such as Information Technology Act, 2000 for providing justice to the victim.

The cybercrime against women, especially as per the researcher concern, the day by day increase of 'revenge porn and blackmailing' which has become a serious problem against the dignity of women in the Indian society. The criminal administration of justice system is also not well acquainted or equipped with digital technology to provide justice to victim of revenge porn and blackmailing and prevent them in future.

The vulnerability and safety of women is one of the biggest concerns of any criminal and penal law, but unfortunately, women are still defenseless in cyberspace. Indian women are not able to report cybercrime 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 which they don't want to face.

1.2. Review of Literature

A literature review is the body of text that aims to review the critical points of current knowledge including substantive findings as well as theoretical and methodological contribution to a particular topic. Review of literature is an important component of research by which multifaceted understanding of the phenomenon becomes the part of the researcher's cognitive personality.

1.2.1. Books

Debarati Halder and K Jaishanker in their book **"Cybercrime against Women in India"** published by sage publication (2017), the author has divided book into 9 chapters the first chapter start with an introduction. Second chapter deals with freedom of speech and expression on the internet from Indian perspective with special reference to crime against women. The third chapter deals with gender bullying and trolling targeting women in India. The fourth chapter explores the online grooming. Online grooming plays a significance part in trapping the victim. This chapter of this book has provides a definition of online grooming and discuss the methodology of

grooming and possible result of grooming and would find the legal solution for the legal solution for this problem from the existing laws. Chapter 5 of this book has addressed the infringement of privacy in the cyber space. There can be different pattern of cyber infringement of women and girls in the cyber space. Chapter 6 of this deals with the online sexual offence. We know that pornography and online obscenity are the most discussed topic when speaking about cybercrime against women in India.

Prashant Mali, **"Cyber Law & Cybercrime, Information Technology Act, 2000 With IT Rules, 2011",** published by Snow White Publication Pvt. Ltd. (2015), has discuss the various crime such as Data Theft, Hacking, E-commerce, E-taxation, E-contracts, Software Piracy, Cloud Computing, IPR in Cyber World, Electronic Evidence, Forensics & Investigation, Reasonable Security Practices and some Case Laws. This book has illustration and pictorial depiction of new age crimes.

Justice Yatindra Singh, **"Cyber Laws",** Universal Law Publishing Co., 4th edition (2010). This book is a comprehensive guide to the various legal issues which have arisen as a result of the unprecedented growth of Internet. It covers both academic and practical information regarding technology related issues and the underlying legal principles which have been applied in these areas. This book is divided into two Parts, Part I of the book deals with different aspects of cyber laws with discussions on various topics, controversies and practical solutions. Part II provides useful and important legal instruments including Acts, rule, regulations, treaties, policies, etc. These instruments are updated and so provide an invaluable resource for further research. In sum, the book aptly discusses how some people have been misusing the phenomenon of the internet to proliferate criminal activities in cyber Space.

Talat Fatima, **"Cybercrime",** published by Eastern Book Company, Lucknow, 1stedition (2011), this book emphasize on the issues relating to the various cybercrimes, origin of cybercrimes, how they different from the traditional crimes. It's also discusses the legal issues involved in countering the cybercrimes and provide preventive and enforcement strategies.

Vakul Sharma in his book **"Information Technology; Law and Practice**" published by Universal Law Publication (2010), 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 references to 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 comparatively the US, European and Indian approaches towards personal jurisdiction at a greater length.

Nandan Kamath in his book **"Law relating to Computers, Internet and Ecommerce: A Guide to Cyber Laws and the Information Technology Act, 2000",** published by Universal Law Publication (2009) has commented on the emerging field of 'electronic evidence' in the cases of cybercrimes. He has made an in-depth study about the admissibility and authenticity of electronic records, burden of proof in cyber offences, and of certain other concepts like production and effect of such evidences, video-conferencing, forensic computing and best evidence rule etc.

Nina Godbole and Sunit Belapure in their book **"Cyber Security; Understanding Cybercrime, Computer Forensics and Legal Perspective**", published by Willyindia (2011), firstly discussing the concept of cybercrime and methods used by cyber criminals in committing of cybercrimes, specially emphasized need for the cyber laws. In the context of the cyber security, author in this book defines the cyber security and various provisions of IT Act, 2000 to curbing the cyber security problems existing in the country.

Manish Kumar Chaube, in his book **"Cyber Crimes & Legal Measures**" published by Regal Publication (2013), divided the chapters in two parts, first part deals with the backgrounds of the cybercrimes and various aspect of cyber law and second part deals with the legal aspect of Information Technology Act, 2000 and concluded that law enforcement agencies are not well equipped and oriented about the cybercrime. Further, it provides the various preventive measures which have been taken to curb the increasing menace of cybercrimes.

1.2.2 Articles

Majid Yar and Jacqueline Drew, **"Imaged Based Abuse, Non-consensual Pornography, Revenge Porn: A Study of Criminalization and Crime Prevention in Australia and England &Wales" (2019)**. This paper charts briefly the rise of image based abuse as a social problem. It details the move to criminalize such online abuse, looking in particular at recent introduction of new laws in England & Wales

and Australia. It also draws upon formative development in the United States and elsewhere. This paper also maps the kinds of user-oriented crime prevention initiatives aimed at curtailing the incident of online image based abuse and bringing the offender to justice. The effectiveness of these legally based crime control initiatives is assessed and potential or actual impediment to effective responses are identified.

Danielle Keats Citron and Mary Anne Franks, **"Criminalize Revenge Porn" (2014),** this paper unfold the faulty assumptions that have obscured a full view of the damage that revenge pornography inflicts. Further this paper explores why civil law alone cannot effectively address nonconsensual pornography. Then, discussed the deficits of current criminal law. And considers current legislative proposal to prohibit revenge porn.

Debarati Halder and K Jaishankar, **"Revenge Porn by teens in the United States and India: A Socio- Legal Analysis"** (2013), this paper discusses the number of issues related to privacy, offensive speech, child pornography, the liability of the parents and also Internet Service Providers (ISPs) and above all, the treatment of the super intelligent minor offenders by the courts. This paper is divided into four parts, first part deals with revenge porn by the teens. Its highlights the possible usage of stored data for online revenge by teens and typology of revenge porn by teens. Further chapters deal with the judicial philosophy from the United States and Indian Perspective regarding misuse of sexted as well as other data which may have been stored with the consent of the victim. In this paper, author taken up two cases, viz., the 2001 case of Airforce Balbharti School boy who created porn websites with the images and information of the female student of his class and female teachers of his school; the 2004 Delhi DPS MMS case. Then deals with the role of Therapeutic Jurisprudence in the management of revenge porn by teens.

Rajat Misra, **"Cyber Crime against Women" (2013).** This article conveys the idea that the crime against women is on a rise in all fields and being a victim of cybercrime could be most traumatic experience for a woman, especially in India where the society looks down upon the women and the law doesn't even properly recognize cybercrimes. This paper discusses upon the various types of cybercrimes that can be inflicted upon a woman and how they adversely affect her. It briefly examines the various laws that exist to protect women in such cases such as the

Information Technology Act, 2000 and the new laws that are coming upon in this field such as the Criminal Amendment Bill (2013). This paper focused upon the options available to the victims to cybercrime and the changes required in legal system to effectively curb the rising spirits of cyber criminals.

Sahanaudupa, **"Virtual Crime and Women" (2018).** This paper discussed the comprehensive list of the online offences and acts of violence and how to bring them into legal frame work of the cybercrime. The author provides in this paper an upto date discussion of the existing legal structure and policy challenges.

Anita Gurumurthy, Niveditha Menon, **"Violence against Women *via* Cyber Space" (2009).** The paper is a report on consultation on women and the use of information technologies that addressed how policy choices need to avoid narratives of fear around new technologies, narrative's that can effectively constrain women's freedom to use digital space.

1.3. Aim and Objective of Research

It is said that identifying a problem is what gives us power and energy to solve them as every problem has in it the seeds of its own solution. The present research work has aim and objective as follows:

- To provide holistic picture of cybercrime against women in India.
- To analyze crime against woman in the light of the cyber law in India.
- To analyze the related laws, which would protect the interest of women victim of the cybercrime.
- To find out the socio-cultural criminological reason for the growth of crime against women in cyber space especially revenge porn and blackmailing.
- To examine all the laws whether traditional or modern relating to revenge porn and blackmailing.
- To examine the role of cyber cells to inquire into the cases of cybercrime particularly in City of Lucknow.
- To analyse the system of police to investigate the cybercrime.
- To suggest measures to safeguard the golden triangle of Constitution of India, equality, freedom, life and liberty i.e., Art.14, 19 & 21.
- To lay down a pathway for solution of cybercrime against women for revenge porn and blackmailing.

1.4. Hypothesis of Research

- Revenge Porn and related offences violate the right to privacy of women victims.
- Honor related social norms prevent the women victims of cybercrime to file the case against perpetrators.
- Inadequacy of specific laws for the protection of women against cybercrime, despite the plethora of laws.
- The administration of criminal justice system is not acquainted and equipped with digital technology to provide justice to women victims of revenge porn and blackmailing and prevent such happenings.

1.5. Result of Hypothesis Tested

1. The First hypothesis of the research is that, Revenge Porn and related offences violate the right to privacy of the victims. Right to privacy is one of the precious fundamental rights conferred under Art. 19(1) (a) and Art. 21 of the Constitution of India, through the liberal interpretation of freedom of speech and expression and right to life by Indian judiciary. The researcher, while conceptualizing the revenge porn and blackmailing under Chapter III and through judicial interpretation of right to privacy under Chapter VI came to the conclusion that revenge porn cybercrime violate the right to privacy. Privacy is considered to be the extension of liberty of human beings. The protection of privacy requires the attention of state and non-state actors, where the 'informational confidentiality' is linked with the private matters like sexual integrity, autonomy on the person's body. Therefore, the second hypothesis has been proved.
2. Second hypothesis is that, Honor related social norms prevent the victims of cybercrime to file the case against perpetrators. The real fact the researcher collected the data from more than 500 respondents. After analysis the data is collected in Chapter VII. The researcher came to the conclusion that most of the respondent accepted the fact that most of the time aggrieved women always faced the apathy of family and society which blamed her for such crime, as society considered that women through her beauty, dressing sense etc, provoked the criminals to commit the crime against her. The women are

both the co-partner (accomplice) and victim of the crime. The women are blamed for sexting, sharing of intimate images and other activities at social media. Therefore, the first hypothesis found proved.

3. The third hypothesis is the, inadequacy of specific laws for the protection of women against cybercrime, despite the plethora of laws. Researcher in chapter IV and chapter V discussed the plethora of laws in India and at international level but their effectiveness to address the issue is lacking due to several reasons. Researcher under these chapters tried to find out the law addressing the cybercrime in general and revenge porn and blackmailing in specific. The researcher analysed under chapter IV traditional laws dealing specifically for crime against women i.e., Constitution of India, 1950; Indian Penal Code, 1860; Immoral Trafficking (Prevention) Act, 1956; The Dowry Prohibition Act, 1961, Domestic Violence Act, 2005; The Protection of Children From Sexual Offences Act, 2012 and Sexual Harassment of Women At Workplace, 2013 and critically analysed the Information Technology Act, 2000 *vide* amended in 2008 for protective laws for protection of women against cybercrime. In chapter VI international conventions, treaty, MoU of organizations and UN General Assembly resolution for protection of women from cybercrime specifically revenge porn and blackmailing have been discussed. Researcher found that the laws are not defining the cybercrimes adequately due to which the conviction is getting tougher for the judicial pronouncements. The reason behind is fast development of technology and the privacy policies of the internet platforms where the protection of the victim is not considered in terms of dignity and human rights but to facilitate the business model of the platforms.

There is no comprehensive law in India which can be able to deals the cybercrime against women particularly revenge porn and blackmailing. However, there are several laws but they have not considered the technicality involved while defining the crimes which provide the loophole for the escape of the accused, as the procedural aspect of the legislations is not compatible in respect of technological infrastructure and skills required for the same. Under these edges laws have not addressed the subject matter of modern development like revenge porn and blackmailing under cybercrime against

women. Therefore, the third hypothesis is partially proved and partially disproved.

4. The fourth hypothesis is that, the administration of criminal justice system is not acquainted and equipped with digital technology to provide justice to women victims of revenge porn and blackmailing and prevent such happening in future. The cybercrime and its severity have been increasing day by day to combat this crime. A technically and legally sound criminal administration of justice system is required. During the research, the researcher contacted with the police administration system which was basically the investigating authority of the crime. The decision of the judiciary is based on the inquiry report & presentation of the case before court by the police authority. The researcher during the research work contacted to various authorities of the police stations to know the process of investigation of the cases of cybercrime, particularly in the matter of cybercrime against women. The information was gathered from the police officials through the questionnaire. After discussing with the police officers in Lucknow, researcher did analysis of questionnaire in Chapter VII filled by them. In Chapter VII, the primary data with police administration collected strongly suggests that the technical skill, infrastructure and expert human resource for the same is lacking in the administrative agencies, where the police administration is the prime focus of the study. The researcher concludes that police lacks the relevant training and understanding of the technology behind revenge pornography and blackmailing to respond effectively against the crime. Therefore fourth hypothesis has been proved.

1.6. Research Methodology

The methodology used in this research work is doctrinal as well as empirical. The doctrinal method involved in depth study of the source materials, text reviews, case studies and extensive analysis of both descriptive and analytical content. It also traces the legislative development at national and international level. In empirical method, the researcher collected the data through the survey method as well as by questionnaire method and analyzed the data and interpreted them. This method required field work study which made the research data more authentic and reliable.

Primary as well as secondary sources like legal texts, books, articles, encyclopedias, research papers, newspapers and the internet material have been referred in order to get the most pertinent information.

In empirical study, questionnaire method has been adopted for the collection of data from the respondents who primarily belonged to the academic institutions and administrative agencies in "Lucknow City of Uttar Pradesh". The questionnaire was structured accordingly and the communication with the administrative agencies was through such questionnaire on interpersonal communication method was also need.

For the purpose of elaborative analysis of the data through empirical study, researcher divided the respondents in different age groups and gender sections particularly belonging to academic institutions. The questionnaire was circulated specifically targeting the female institutions and crossed the academic standard of undergraduate level at least.

1.7. Limitation of Research

The researcher limits the research up to the legal and preventive measure of the cybercrime instead of technical measures adopted to protect the computer system. It is limiting the scope further to evaluate the crime with the prospective of human agency and their rights and not in terms of technological developments and tech-based requirement for the protection of cybercrime.

A further limitation of this study was that, it was unable to directly analyze the respondents under the age group of 17 due to near absence of disclosure experiences of revenge porn and blackmailing cybercrime to researcher. This non-disclosure and non-participation of such age group in the analysis restricted the vision for the registration, awareness and understanding of responsive measure of this age group. Whilst this absence was significant in and of itself, future work might focus on directly interviewing young women, in order to discern whether their experiences of revenge porn and blackmailing connected to their experiences.

1.8. Framework of the Thesis

The whole research work has been divided into eight chapters

Chapter I: Introduction

This chapter of introduction comprises the brief introduction and statement of problem as to the cybercrime against women especially the revenge porn and blackmailing. Researcher introduced research work and outlined research problem, hypothesis, research methodology and hypothesis testing by findings of data and the qualitative debates under the subject matter. Brief of the chapters of the research thesis is also included in this chapter.

Chapter II: Origin and Historical Development of Cybercrime in India

In this chapter, the researcher has mentioned the history of computer and various phases of development of generations of computer, how this computer development introduced the internet and invented the cyberspace where, all the computer activities are done. The criminals with the help of the computers commit the crime in the cyberspace and physical world crime deviated into cybercrime.

Chapter III: Conceptualization of Revenge Porn and Blackmailing under Cybercrime against Women

This chapter highlights the cybercrime against women in India especially cybercrime such as revenge porn and blackmailing which has been gaining much attraction now a days. The objective of this chapter is to clarify the concept of revenge porn and blackmailing. Revenge porn has the potential to severely harm victim and society as a whole, yet no research has been done as to the content of the concept. Revenge porn and blackmailing is advance form of violation of women's privacy rights and dignity. The conceptualization of revenge porn and blackmailing is necessary to be able to understand the severity of the harm caused by this offence on victim and to develop appropriate law governing specifically revenge porn.

Chapter IV: Cybercrime against Women: National Legal Perspective

In this chapter, researcher has made a detailed study of Indian laws dealing the issue of cybercrimes especially related to women. For this purpose, researcher has first provided the provisions available under the traditional laws i.e., under Constitution of India, under Penal Laws and under Special Law i.e., The Information Technology Act, 2000 and then tried to evaluate the remedies available in the specific law dealing with the problem of cybercrime especially for the victims of revenge porn and blackmailing.

Chapter V: Cybercrime against Women: Global Legal Perspective

After going through the cybercrime against women, a national legal protection in the previous chapter; in this chapter the researcher has taken an analysis of the existing International legal Instruments for cybercrimes related problems. Researcher has also tried to analyse the available legal protection at international level for tackling the problem of revenge porn which is adversely affecting the right to privacy in the present day and age.

Chapter VI: Judicial Articulation towards Revenge Porn and Blackmailing under Cybercrime against Women.

In this chapter the researcher has tried to analyse the decisions of the judiciary in various case laws related to privacy, decency, dignity in physical world which came to be applied to the virtual world. The researcher also analysed the cases wherein judiciary interpreted the crime of revenge porn and blackmailing through cybercrime to give justice to the victims of such crime.

Chapter VII: Analysis of Data Collected From Lucknow City Related Social Awareness and Impact of Cybercrime against Women

This chapter presents and analyses the primary data collected from the 542 participants of various colleges and universities with different academic background and it also includes the analysis of the data collected from 22 Police Stations in the City of Lucknow, Uttar Pradesh.

In this chapter the researcher attempts to provide an idea about the state of awareness about cybercrimes especially targeting women, considering the technological requirement and rapid development in this field. The Researcher also tried to bring out the similarity of status and perceptions between the general crime against women and cybercrimes, through data analysis and in the form of chart and tabular representation.

Chapter VIII: Conclusion and Suggestions

This chapter is prepared on the basis of research study, certain conclusions are drawn, and some suggestions are also placed for consideration.

CHAPTER-II

ORIGIN AND HISTORICAL DEVELOPMENT OF CYBERCRIME IN INDIA

CHAPTER-II
ORIGIN AND HISTORICAL DEVELOPMENT OF CYBERCRIME IN INDIA

"Technology is a useful servant but a dangerous master."

Christian Lous Lange

2.1. Introduction

A computer is an electronic device used to store, retrieve and manipulate data. A computer is also defined as "a programmable electromechanical device that accepts instruction (program) to direct the operations of the computers". Four words can be deducted from the above definition for further illustration, i.e., Store: To put data somewhere for safe keeping, Retrieve: To get and bring the data back, Process: To calculate compare arrange.[1]

Therefore, computer and the cybercrime are correlated to each other. The computer can be used in a commission of a crime or it can be a target. Commission of crime through computer or any other electronic device and internet are generally called cybercrime. Literally the term cybercrime is a misnomer and the concept is not defined anywhere. It refers to any crime that involves a computer and a network. Cybercrimes refer to criminal exploration of internet and cybercrimes are defined as an offence that is committed against individuals or a group of individuals. Today it has become a complicated problem in cyber world & is very difficult to tackle. Presently, Cybercrimes have become deadliest epidemic of our planet and have emerged as a major source of government concern across the globe. In the present chapter, an attempt is made to define and conceptualize cybercrimes, its development from primitive to modern day's technology, determine their nature and scope, point out essential ingredients of these crimes, and highlight the reasons for this form of criminality.

2.2. Origin of Computer

The history of computer dated back to the period of scientific revolution (1543-1678). The calculating machine invented by *Blaise Pascal* in 1642 and that of *Goffried*

[1] Subhash Pathirana, "History of Computer", *available at:* https://medium.com/@subhashpathirana/history-of-computer-7504d590f989 (last visited on 1st July, 2018).

Liebnits marked the genesis of the application of machine in industry. This progressed up to the period 1760-1830 which was the period of the industrial revolution in Great Britain where the use of machine for production altered the British society and the Western world. During this period, a machine was used in textile industry 'the weaving machine' invented by *Joseph Jacquard*.[2]

Originally, the computer was born not for entertainment or email but out of a need to solve a serious number-crunching crisis. By 1880, the United State (U.S) population had grown so large that it took more than seven years to tabulate the U.S. Census results.[3] The government sought a faster way to get the job done, giving rise to punch-card based computers that took up entire rooms. This led to the development of the computer machine. Today, we carry more computing power on our smart phones which was not available in these early models. The following brief history of computing is a timeline of how computers evolved from their humble beginnings to the machines of today that surf the Internet, play games and stream multimedia in addition to crunching numbers.[4] The computer is the means and target for the cybercrime.

2.3. Historical Evolution of Computer

The history of modern computer may be traced back to 2000 B.C., that is about four thousand years ago, when the first mechanical device called abacus was developed by the Chinese for being used as a calculating machine. Centuries later, many similar devices were developed but it was in 1642 A.D. that "Blaise's calculating machine" became the most popular calculating device which could be used by dialing numbers 0 to 9 on its dial disk. Subsequently, *Joseph Jaquard* a French weaver devised a loom in 1820 that used punch cards to direct the weaving patterns. It was *Charles Babbage*, who is called the father of modern computers for his invention of an automatic computing machine designed to do additions at the rate of 60 per minute. It also had a memory where the machine was programmed by instructions coded initially on punched cards and

[2] *Ibid*.
[3] Kim Ann Zimmermann, "History of Computers: A Brief Timeline", *available at*: https://www.livescience.com/20718-computer-history.html (last visited on 1st July, 2018).
[4] *Ibid*.

then stored internally. Later, Babbage, who was a Professor of Mathematics in U.K., invented the first general purpose computer which he called as the Analytical Engine.[5]

The historical evolution of computer will remain incomplete without the mention of *Augusta Ada King*, a disciple of Babbage, who contributed to the machines design of computer. Her thorough understanding of the machine and its mechanism led to the development of instruction routine which was fed into the computer.

Babbage's analytical engine as modified by *Augusta Ada King* consisted of over 50,000 components and input devices in the form of perforated cards containing operating instructions in stored memory of 1000 numbers upto 50 decimal digits. It also consisted of a 'mill' with a controlled device that allowed processing instructions in any sequence and output devices to produce printed results. Subsequently, an American inventor, *Herman Hollerith* further developed the Jacquar's Loom concept to computing. But instead of using Babbage's machine, he used cards to store data information fed into the machine which compiled the results mechanically. Each punch on a card represented one number and a combination of two punches represented one letter. As many as 80 variables could be stored in single car.[6] Besides speedy compilation of *Augusta Ada King* was the Countess of Lovelace and a daughter of well-known English poet Lord Byron. She earned fame as the first woman computer programmer.[7]

Later, Hollerith introduced punch card reader and founded his Tabulating Machine, in 1896, which eventually transformed into International Business Machine (IBM) around 1924. Thereafter, a German engineer *Konard* devised a computer Z-3 to be used in aeroplanes and missiles which helped the Germans to strengthen their, strategic potential against the British Allied Forces during World War II. As a counter strategic measure, a more powerful computer called *Collossus* was developed by the British engineer who had secret code breaking mechanism that could easily decode German messages. Thus, these two developments were essentially an outcome of the World War

[5] R. K. Tiwari and P. K. Shastri, *Computer Crime and Computer Forensics* viii. (BioGreen Books, New Delhi, 2002).
[6] Deepti Coora and Keith Merrill, *Cyber Cops, Cyber Criminals and the Internet* 198 (IK Books, New Delhi, 2002).
[7] Quoted from Fundamentals of Cyber Law 70 (Asian School of Cyber Laws, 2005).

II which were instrumental in accelerating the progress of computer technique in times to come.

Taking inspiration from the importance of computers for defence services, American scientist *Howard H. Aiken* who was working with IBM developed an all-electronic calculator which was used by the American Naval Forces for creating ballistic charters. It was called Automatic Sequence Controlled Calculator. A year later, *John Von Neumann* designed a computer which he named as World War II. Electronic Disket Variable Automatic Computer (EDVAC) with a memory to hold stored program as well as data. It consisted of a central processing unit, which allowed functioning of the computer to be controlled and coordinated from a single source.

The advances made in computer technology during mid-fifties of the 20th century brought more sophisticated and efficient computers which were much smaller, faster and more reliable than the earlier ones. They became so popular that most companies, business enterprises, industries and even the Government in U.S.A. switched over to computerization in next decade.

The credit of producing a commercially usable computer goes to Remington Rand Corporation. It was initially launched in 1951 and called Universal Automatic Computer (UNIVAC). A decade later, *Rand Paul Baran* of the Rand Corporation was requested by the U.S. Air Force to study and device a computer which could maintain its command on missiles and bombs in the event of nuclear attack. It was to be a military network which could survive a nuclear attack. It leads Baran to prepare a switched network.[8]

In 1965, most of the large business houses, firms and industrial establishments routinely switched over to IBM computers for maintaining their records and processing their financial information through computer because of its vast storing capacity and cost effectiveness.

Though, these newly developed computers contained transistors as a replacement for vacuum tube, they generated considerable heat which often damaged their internal parts and also affected their sensitiveness. In order to eliminate this problem, *Jack Kilby* of United States developed the integrated circuit in 1968 which combined three electronic

[8] Ian Watson, *The Universal Machine: From the Dawn of Computing to Digital Consciousness* 89 (Springer, 2012).

components into one small silicon disk made from quartz. Later, semiconductors were also squeezed in the form of a single chip. The device came to be known as ARPANET (Advanced Research Project Administration Network). Thereafter, the first e-mail program was created by *Ray Tomlingson* of BBN in 1972. By this time computer had become more user friendly because the software package therein offered an array of applications even to a non-technical user. With the advance of time there was thrust on having computers smaller in size so as to be easily portable, as a result of which laptops and even pocket computers were introduced which are commonly in use these days.

ARPANET was developed by U.S. Department of Defence in 1968. IBM introduced Personal Computers (PC) in 1981 for use in homes, offices, educational institutions etc.[9] They could be linked together or networked to share memory space and communicate with each other. As a medium of communication, computer has brought about revolutionary changes in transmitting information and has increased the capacity to store, search and retrieve any information through its application. It has not only made human life easier and comfortable but virtually acts as a substitute for human mind so for storage and assimilation of knowledge and information is concerned. From the functional point of view, the computer has even excelled human mind. The expansion of internet network enables a person to visually see and talk to a person who is sitting thousands of Kilometres away in any part of the world.

2.4. Generations of Computers

The history of computer is considered with the generations of a computer from first generation to fifth generation. In 19th century English mathematics professor name *Charles Babbage* referred as a "Father of Computer". He designed the Analytical Engine and it was this design that the basic framework of the computers of today are based on. Generally speaking, computers can be classified into five generations.[10] Each generation lasted for a certain period of time and each gave us either a new and improved computer or an improvement to the existing computer. The generations of computer are as follows:

[9] P. Gnannasivam, *Telecommunication Switching and Networks* 3 (New Age International Publication, New Delhi, 2007).

[10] Introduction to Information Technology ITL Education Solution Ltd. Research and Development Wing (Pearson Education, 8th Impression, 2009).

2.4.1. First Generation of Computer (1937-1946)

The first electronic digital computer was built by *Dr. John V. Atanasoff* and *Clifford Berry* in 1937. It was called the *Atanasoff-Berry Computer* (ABC). Then an electronic computer name the *Colossus* was built for the military in 1943. Other developments continued until in 1946 the first general purpose digital computer, the Electronic Numerical Integrator and Calculator (ENIAC) was built. It is said that this computer weighed 30 tons, and had 18,000 vacuum tubes which was used for processing. When this computer was turned on for the first-time lights dim in sections of Philadelphia. Computers of this generation could only perform single task, and they had no operating system.[11]

2.4.2. Second Generation of Computer (1947-1962)

Second generation of computers used transistors instead of vacuum tubes which were superior to vacuum tubes. In 1951 the first computer for commercial use was introduced to the public; the Universal Automatic Computer (UNIVAC 1).[12] In 1953 the International Business Machine 650 and 700 series computers made their mark in the computer world. During this generation of computers over 100 computer programming languages were developed, computers had memory and operating systems.[13]

2.4.3. Third Generation of Computer (1963-1975)

The invention of integrated circuit brought us the third generation of computers. With this invention computers became smaller, more powerful more reliable and they are able to run many different programs at the same time. This allow the device to run many different applications at one time with a central program that monitor the memory. For the first time computer become accessible to mass audience because they are smaller and cheaper.

---

[11] Ishaq Zakari, "History of Computer and its Generations", *available at*: https://www.researchgate.net/publication/336700280Historyofcomputeranditsgenerations.(last visited on 18th July 2019).

[12] *Ibid.*

[13] Subhash Pathirana, History of Computer, *available at*: https://medium.com/@subhashpathirana/history-of-computer-7504d590f989.(last visited on 18th July, 2019).

2.4.4. Fourth Generation of Computer (PC 1975-2020)

At this time of technological development, the size of computer was re-divided to what we called Personal Computers (PC). This was the time the first Microprocessor was created by Intel. The microprocessor was a very large scale, that is, VLS integrated circuit which contained thousands of transistors. Transistors on one chip were capable performing all the functions of a computer's central processing unit.

2.4.5. Fifth Generation (Present and beyond) - Artificial Intelligence

The dream of creating a human-like computer that would be capable of reasoning and reaching at a decision through a series of 'what-if-then' and analysis has existed since the beginning of computer technology. Such a computer would learn from its mistakes and possess the skill of experts. These are the objectives for creating the fifth generation of computers. The starting point for the fifth generation of computers had been set in the early 1990s. The process of developing fifth generation computers is still in the development stage. However, the expert system concept is already in use. The expert system is defined as a computer system that attempts to mimic the thought process and reasoning of experts in specific areas. Three characteristics can be identified with the fifth-generation computers. These are:[14]

Mega Chips: Fifth generation computers will use Super Large Scale Integrated (SLSI) chips, which will result in the production of microprocessors having millions of electronic components on a single chip. In order to store instructions and information, fifth-generation computers require a great amount of storage capacity. Mega chips may enable the computer to approximate the memory capacity of the human mind.

Parallel Processing: Computers with one processor access and execute only one instruction at a time. This is called serial processing. However, fifth-generation computers will use multiple processors and perform parallel processing, thereby accessing several instructions at once and working on them at the same time.

Artificial Intelligence (Al): It refers to a series of related technologies that try to simulate and reproduce human behavior, including thinking, speaking and reasoning. Al

[14] Alexis Leon and Mathews Leon, Introduction *to Computer* 76 *(*Leon Tech World, 2008).

comprises a group of related technologies: expert systems (ES), natural language processing (NLP), speech recognition, vision recognition and robotics.

2.5. Emergence of Internet

At the end of the 20th century, the Internet has emerged as the world's newest, and perhaps most unique, communication medium. The early Internet was used by computer experts, engineers, and scientists. There was nothing friendly about it. There were no home or office personal computers in those days, and anyone who used it, whether a computer professional or an engineer or scientist, had to learn to use a very complex system. It was only in 1995 that the World Wide Web (www.) became an integral part of the USA society, but today countries across the globe are dependent on the Internet. In the early days of the commercialization of the Internet and the growth of Internet connected countries, attention primarily focused on the development and use of information and communication technology.[15]

2.5.1. History of Internet

The internet's roots are firmly embedded within the scientific and technological development that followed the end of World War II. The origin of the internet's basic architecture can be traced back to the search for a 'survivable communications' system. During the late 1950s, the U.S. Department of Defence (DoD) was concerned about the need for a failure resistant communication method. In 1961 *Paul Baran* developed such method, which has become known as *packet switching*. *Baran* admits that 'the origin of packet switching itself is very much cold war'.[16] Package switching (originally called "message switching") works by breaking up a message into fixed sized units or 'packages'; each package is "labeled with its origin and destination and is then passed from node to node through the network". This technology was also being separately developed by *Donald Davies*, a British expert on computer security, who was the first to

[15] Watney, Murdoch, "The Evolution of Internet Legal Regulation in Addressing Crime and Terrorism" 2 *Journal of Digital Forensics, Security and Law* 3 (2007).
[16] P. Baranetd., "On distributed Communications", MIS. I-XI" *RAND Corporation Research Documents*, Aug. 1964.

use the term 'packet' in reference to data communications. Davies also built an experimental packet-switching network in the mid-1960s.[17]

The first large-scale packet-switching network that was developed based on the insights of *Baran* and *Davies* was the work of the Advanced Research Projects Agency (ARPA), a research agency of the DoD, which financed high-tech research. In the late 1960s, the DoD provided generous grants to universities and corporations to establish a communications network between major research centers in the United States, including universities such as MIT and Stanford. It recruited *Lawrence Roberts* of MIT's Lincoln Laboratory to oversee the construction of the ARPANET, the first incarnation of what is now known as the Internet.[18]

The original ARPANET grew into the Internet. Internet was based on the idea that there would be multiple independent networks of rather arbitrary design, beginning with the ARPANET as the pioneering packet switching network, but soon to include packet satellite networks, ground based packet radio networks and other networks. The Internet as we now know it, embodies a key underlying technical idea, namely that of open architecture networking. In this approach, the choice of any individual network technology was not dictated by particular network architecture but rather could be selected freely by a provider and made to interwork with the other networks through a meta-level 'Internetworking Architecture'. Until that time, there was only one general method for federating networks. This was the traditional circuit switching method where networks would interconnect at the circuit level, passing individual bits on a synchronous basis along a portion of an end-to-end circuit between a pair of end locations.[19] The basic infrastructure of the ARPANET consisted of several timesharing host computers, packet-switching interface message processors (IMPs), and leased telephone lines.

By the end of 1971, the primitive ARPANET was up and running. Its primary goal was supposed to be resource sharing, that is, enabling connected sites to share hardware processing power, software, and data. But the network's users soon discovered

[17] Richard A. Spinello, *Cyber Ethics Morality and Law in Cyberspace* 67 (Jones & Bartlett Learning, Burlignton, 6th edn. 2016).
[18] *Ibid*.
[19] Barry M. Leiner and Vinton G. Cerf, *et al.*, "Brief History of Internet" 39 *ACMSIG COMM Computer Review* 22-31(2009), *available at*: https://www.internetsociety.org/wp-content/uploads/2017/09/ISOC-History-of-the-Internet_1997.pdf . (last visited on 10th July, 2019).

another function i.e., electronic mail. Instead of using the network primarily to leverage remote hardware resources, users began sending huge volumes of email. As a result, this popular application soon began to dominate traffic on this fledgling network.

According to *Abbate*, "Network users challenged the initial assumptions, voting with their packets by sending a huge volume of electronic mail but making relatively little use of remote hardware and software. Through grassroots innovations and thousands of individual choices, the old idea of resource sharing that had propelled the ARPANET project forward was gradually replaced by the idea of the network as a means of bringing people together".[20]

In the early 1980s, this system was subdivided into two networks, the ARPANET and Milnet. Furthermore, connections were developed so that users could communicate between the two networks. The interaction between these networks came to be known as the Internet. The term 'Internet' was actually first used in a research paper written by *Cerf* and *Kahn* in 1974; that paper described a 'network of networks' that would eventually link together computers all over the world. In the late 1980s, the National Science Foundation Network (NSFNET), which relied on five supercomputers to link university and government researchers from across the world, replaced the ARPANET.[21] The NSFNET began to encompass many other lower-level networks such as those developed by academic institutions, and gradually the Internet as we know it today, a maze of interconnected networks, was born.

In these early days the federal government generously subsidized the Internet, and as a consequence there were restrictions on any commercial use. The Internet was the exclusive domain of government researchers, scientists, university professors, and others who used it primarily to share their research findings or other academic information. However, the NSF no longer subsidizes the Internet, which has assumed a strong commercial character during the last decade. During the early 1990s the Internet quickly became available to corporate users; email providers such as MCI and Computers opened up email gateways. In the year 1993, 29% of the host computers connected to the Internet

[20] Abbate, Janet. "Government, Business, and the Making of the Internet" 75 *The Business History Review* 147–176(2001), *available at:* www.jstor.org/stable/3116559.(last visited on 10th August, 2019).

[21] V. G. Cerf and R. E. Kahn, "A Protocol for Packet Network Interconnection" 5 *IEEE Trans. Comm. Tech*. 627-641 (1974).

belonged to corporations. Commercial use now accounts for the vast majority of all Internet traffic. Management of the network has been transferred to private telecommunications carriers that manage the backbone, that is, the large physical networks that interconnect. Thus, the network's vitality depends on the cooperation and goodwill of these telecom providers.

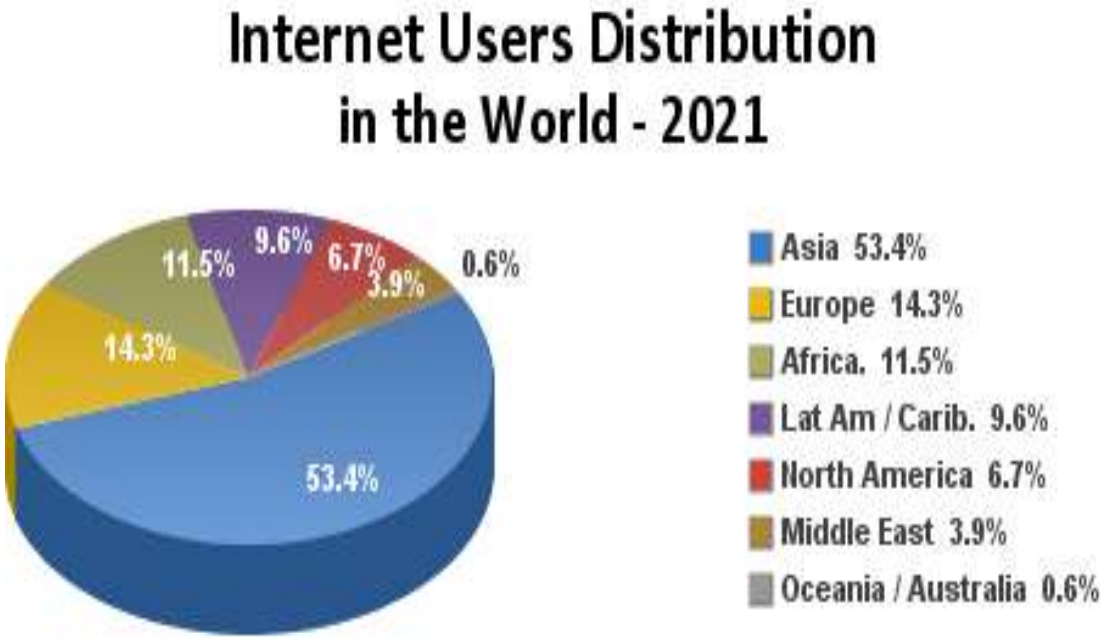


Chart No. 2.1[22]

The global diffusion of Internet usage during this period has been an extraordinary phenomenon. In 1983 there were a mere 500 host computers (computers with unique Internet protocol addresses) connected to the Internet. In the year 2000 there were 360 million Internet users. In the year 2014, the number of Internet users worldwide had grown to 3 billion, approximately 40% of the population.[23] Although the rapid development of the global Internet has been extraordinary, there is still a disparity between developed and developing countries. Africa still lags far behind the rest of the world in Internet usage. However, in some developing countries, Internet use is

[22] Cisco Annual Internet Report (2018–2023) White Paper, *available at:* https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html. (last visited on 20th March 2021).

[23] World Internet Usage Statistics, *available at:* https://www.internetworldstats.com/stats.htm (last visited on 20th March 2020).

expanding rapidly.[24] Nearly two-thirds of the global population will have Internet access by 2023. There will be 5.3 billion total Internet users (66 percent of global population) by 2023, up from 3.9 billion (51 percent of global population) in 2018.[25]

Until recently, there was no public internet access in India. The only organizations that were able to use the internet were educational institution and certain scientific department of the Government. These organizations were operated on the ERNet backbone that was reserved exclusively for nonprofit organizations. Until the VSNL network was officially launched, this was India's only access to internet.[26] The Videsh Sanchar Nigam Limited (VSNL), India's international telecommunication organizations, launched the countries first public internet service by offering subscribers dialup access to the internet.[27] A Press Note released by the Telecom Regulatory Authority of India on 11th May, 2021, is indicative of the prevalence of telecom services in India as on February 2021. All number of Internet subscribers increased from 665.31 million at the end of Jun-19 to 687.62 million at the end of Sep-19, registering a quarterly growth rate of 3.35%. Out of 687.62 million internet subscribers, numbers of Wired Internet subscribers are 22.26 million and numbers of Wireless Internet subscribers are 665.37 million. There were 439.99 million urban subscribers and 247.63 million rural subscribers. The total number of internet subscribers stood at 687.62 million reflecting a 3.35 % change over the previous quarter. 625.42 million were broadband subscribers. 665.37 million is the figure of wireless internet subscribers. The total internet subscribers per 100 population stood at 52.08; urban internet subscribers were 104.25 per 100. [28]

For the first time, the NFHS-5 sought details on percentage of women and men who have ever used the Internet. According to this, only an average of 42.6 % of women ever used the Internet as average of 62.16 % among the men. In urban India, 10 States

[24] *Ibid*.
[25] Cisco Annual Internet Report (2018–2023) White Paper, *available at:* https://www.cisco.com/c/en /us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html. (last visited on 20th March 2021).
[26] Rahul Matthan, *The Law relating to Computers and the Internet* 428-429 (Butterworths India Publication, New Delhi, 2000).
[27] *Ibid*.
[28] Performance Indicator Report, July-September, 2019, The Indian Telecom Services Performance Indicators, *available at:* https://trai.gov.in/sites/default/files/PR_No.04of2020.pdf. (last visited on 21st September, 2021).

and three Union territories reported more than 50 % women who had ever used the Internet.[29]

The internet is one of the most significant inventions in the communication sector with the help of which, people living across the globe can communicate with each other without realising the distances between them. It has diminished the boundaries among people and provided them with opportunities to make better relations at both the personal as well as the professional fronts. The number of social network users in India has increased drastically from 181.7 million in 2015 to 216.5 million in 2016 to a projected 250.8 million in 2017. It is expected that the same would increase to at least 336.7 million by 2020.[30] Cybercrime has increased due to increasing number of the internet users and broadening of cyberspace.

2.5.2. Development of Cyberspace

Cyberspace, this is a term coined by William Gibson, A science fiction writer, in his sci-fi novel *Neuromancer* which is published in 1984 and he suggested it as a 'consensual hallucination'. According to his vision about near future computer network (as at the time when he coined the term in 1984), "Cyberspace" is where users mentally travel through metrics of data. Conceptually, "Cyberspace" is the "nebulous place" where human interacts over computer networks. The term "Cyberspace" is now used to describe the internet and other computer networks. In the terms of computer science, cyberspace is a worldwide network of computer networks that uses the transmission and exchange of data. A common factor in almost all definition of cyberspace is the sense of place that they convey. Cyberspace is most definitely a place where you chat, explore, research and play.[31]

Governance of the Internet, specifically legal governance, is very relevant to the discussion of the evolution of legal regulation of the Internet. Although the Internet was

[29] National Family Health Survey (NFHS-5) 2019-2021, *available at:* http://rchiips.org/nfhs/NFHS5 FCTS/Final%20Compendium%20of%20fact%20sheets_India%20and%2014%20States_UTs%20(Phase-II).pdf . (last visited on 23rd December, 2021).

[30] Mayura U. Pawar and Archana Sakure, "Cyberspace and Women" 8 *A Research, International Journal of Engineering and Advanced Technology* 1670 (2019).

[31] Nina Godbole and Sunit Belapure, *Cyber Security: Understanding Cybercrimes, Computer Forensics and Legal Perespective* 16 (Wiley Publication, New Delhi, 2017).

not designed as a single entity with a single authority that governs the legal development and use of the Internet, dominant western 'powers' have emerged in respect of the legal 'governance' of the Internet, such as the USA and European Union (EU). Data protection (information privacy protection) and now data retention illustrate the role and influence of the dominant powers. It is important to briefly look at data protection as it is affected by state control and specifically, the method of data retention.[32]

While the Internet serves as a tremendous resource for information, products, and services, the same technology provides companies and individuals the ability to collect information about Internet users and to distribute that information to others. Many Internet users feel that this collection of data is an illegal invasion of privacy, specifically information privacy which is defined as the right of an individual to control the acquisition, disclosure and use of personal information. The aim of regulating the use of state surveillance technology is to ensure judicial checks and balances in respect of the use of such invasive, non-obtrusive but extensive technology in respect of Internet users. If surveillance technology is applied without legal regulation, it can easily be abused. From above discussion it's clear that the cyberspace is the place created by the internet, where the cybercrime has been committed.

2.6. Meaning and Definition of Cybercrime[33]

In order to better understand the link between cyberspace and crime, it's important to first examine the transition from the real world to the virtual world. There is no society that is not confronted with the problem of criminality. Its form changes; the acts thus that characteristics are not the same everywhere; but everywhere and always, there have been men who always behaved in such manner as to draw upon themselves penal repression. Crime is not per se a legal term. It derives its meaning and has a connotation in the background of a society than the State as such. Thus, it defines an attempt to lay down a straight jacket definition with clearly defined boundaries. However,

[32] Watney and Murdoch "The Evolution of Internet Legal Regulation in Addressing Crime and Terrorism," 2 *Journal of Digital Forensics, Security and Law* (2007), *available at*: https://commons.erau.edu/jdfsl/vol2/iss2/3 (last visited on 21st March, 2020).

[33] Nandan Kamath, *Law Related to Computers Internet & E-Commerce* 35 (Universal Law Publication, New Delhi, 4th ed., 2009).

usually it is put synonymous to something which is 'a wrong', 'an offence', 'a misdemeanour' or 'a felony'. Crime is both a social and an economic phenomenon. It is as old and historical as the human society itself. Many ancient books, right from the pre-historic days, and mythological stories have spoken about crimes being committed by individuals; be it committed against an individual like ordinary theft and burglary or against the nation at large like the crimes of spying. *Kautilya's Arthashastra*, a document written around in the 350 BC is considered to be one of the most authentic administrative treatises in India which discusses the various crimes committed in the society, security initiatives to be taken by the rulers to curb them, possible crimes in a State, etc. It also advocates awarding different punishments for different offences listed therein. Further, the concept of restoration of loss to the victims has also been discussed in it. In his theory of probable crime, he has discussed as to how with the changes in society, different crimes emerge.

The crimes against women increased in the society; with the strong position of a specific sector, the abuse of power will result in commission of crimes associated with the power-play. Certainly, the advent of Information and Communication Technology has lead to the emergence of a new kind of crime called the Cybercrime. To clearly understand the meaning of cybercrime, one should first understand the meaning of the term crime and then the meaning of cybercrime.[34]

2.6.1. Meaning of Crime

Crime is as old as the human race. The origin of crime may be traced back to the days where mankind depends purely upon the nature for food and other necessities. Whenever, demand is more for any substance than its availability there prevailed the crime.[35] However, an attempt is made by erudite legal scholars to define it. *Sir William Blackstone* defines crime as "*an act committed or omitted in violation of a public law, forbidding or commanding it*".[36] Here the word public law used in the definition is a confusing expression as it includes not only constitutional law but municipal or all laws

[34] Cybercrime Law and Practice 11(The Institute of Company Secretaries of India, New Delhi, 2016).
[35] Batuk Lal, *Commentary on the Indian Penal Code, 1860* 30 (Thomas Reuters, 3rd edn. 2016).
[36] Blackstone, Commentaries on Laws of England, Vol.4 P. 5.

made by the state in which the ambit of crime will become too wide including every legal wrong as crime. Some writers define crime only in the context of moral feelings but as we see, while some crime may be moral wrongs yet there are good number of crimes which nothing to do with the morals. Not paying taxes to the State may not be a moral wrong but it is a crime. Travelling without ticket, carrying inflammable goods in trains, is not an immoral act but it is an offence. *Prof. Kenny* defines crime as "*wrongs whose sanction is punitive and is in no way remissible by a private person, but is remissible by Crown alone, if remissible at all*".[37] The definition is not without lacuna as in India and also in many countries, certain crimes are compoundable by the victim or private individual. The more exhaustive definition which is open to less criticism is given by *Allen* when he says that "*a crime is the commission or omission of an act which law forbids or commands under pain of a punishment to be imposed by the state by a proceeding in its own name*".[38]

Salmond define a '*crime' as "an act deemed by law to be harmful for society as whole although its immediate victim may be an individual"*.[39] Crime in any form does adversely affect the members of the society. According to **Merriam Webster Dictionary,**[40] "Crime is an act or the commission of an act that is forbidden or the omission of a duty that is commanded by a public law and that makes the offender liable to punishment by that law, especially a gross violation of law".[41] **Black's Law Dictionary** defines the "crime" as "an act that the law makes punishable, the breach of a legal duty treated as the subject matter of a criminal proceeding".[42] These are the definition given in the English dictionaries which particularly emphasizes on the act in violation of law. *Blackstone* defines crime as "an act committed or omitted in violation of a public law either forbidding or commanding it". *Stephen* observed, "A crime is a violation of a right considered in reference to the evil tendency of such violation as

[37] S. W Stewart, *A Modern View of the Criminal Law* 14 (Pergamon Press, 1969). David C. Ormerod and Karl Lair, *Smith and Hogan's Criminal Law* (Oxford University Press, London, 2015).
[38] Allen, *Legal Duties Winfield, Province of Law of Tort* 221-52 (Tagore Law Lectures, 1930).
[39] *Ibid*. at p.230.
[40] "Crime", Merriam Webster 2011, *available at:* https://www.merriam-webster.com/dictionary/crime (last visited on 10th August, 2021).
[41] D. Williams, *Race, Ethnicity, and Crime: Alternate Perspective* 45 (Algora Publication, United States, 2012).
[42] Black's Law Dictionary, 8th Ed. 2000, p.399.

regards the community at large". [43] **Oxford Dictionary** defines "Crime as an act punishable by law as forbidden by statute or injurious to the public welfare".[44] There is no exclusive definition of crime given by any jurist. In a layman's language, a crime can be defined as an unlawful act punishable by a State or other authority.

The term 'crime' does not, under the modern criminal law, has a simple and universally accepted definition, though statutory definitions have been provided for certain purposes. The most popular view is that crime is a category created by law; in other words, something is a crime if it is declared as such by the relevant and applicable law. One proposed definition is that a crime or an offence (or criminal offence) is an act harmful not only to an individual or individuals but also to the community, society or the State at large 'a public wrong'. Such acts are thus forbidden and punishable by law. Crime is a revolt against the whole society and an attack on the civilization of the day.[45]

Therefore, an inclusive definition of the term crime can be that it is an act or an omission which is prohibited by law. Deducing from the definitions of the term 'crime' above, cybercrime can be defined as an act or omission prohibited by law which is carried out either with the means of or where the target is a computer, computer source or computer network.

2.6.2. Traditional Approach to Crime

Crime, the subject-matter of criminal law, is not a new thought; it is as old as human life, though the term crime is used at a later stage of legal evolution. Punishment is the *sine qua non* of crime; hence whenever civil remedy or damages were regarded insufficient for certain civil injuries or torts; they were erected into crimes. In the ancient society, where many facets of human life like agriculture, political institutions, health services, medical science and basic amenities of life were at a rudimentary stage, crimes too were fewer in number and whenever occurred, they were simple in nature and

[43] O. P. Srivastava, *Principles of Criminal Law* 8 (State Mutual Book & Periodical Service, Limited, New Delhi, 2006).
[44] Hugh J. Klare, *Changing Concept of Crime and its Treatment* 16 (Pergamon Press Oxford, 1st edn., 1960, reprint 1969).
[45] *Harpreet Kaur* v. *State of Maharastra*, AIR1992 SC 979.

percolated from baser human instincts like lust, greed, vengeance, jealousy and sexual drive.

However, in England as anywhere else where the process of turning of private wrongs into public ones is not yet complete, but it is going forward year by year. For instance, the maiming or killing of another man's cattle was formerly civil wrong but they were made crimes in the Hanoverian reign. Then again, it was not until 1857 a crime for a trustee to commit a breach of trust. So also, incest was created a crime in 1908. In fact, the categories of crimes are not closed. In our own country, since Independence, many acts have now been enacted into crimes which we could not even have conceived of, for instance, practice of untouchability or forced labour or marrying below a certain age and so on. A socialistic State does conceive of much anti-social behaviour punishable as crimes more frequently.[46]

Thus, at such a period of time, it was easier to define crime and to bring it within the four falls of definition but even then, from Blackstone to Kenny, and from Russell to R.C. Nigam, no perfect or exhaustive definition of crime is found. The reason is that crime is not a static term. It is like a mirror which reflects the religious and moral beliefs, social standards, ethics and above all, public opinion of a society at a given period of time. It is like changing sands; ever changing shapes according to the direction of the wind, hence a scientific and precise definition of crime is not possible.

Thus, the traditional approach to crime focuses on the watertight definitions of crime which are neither perfect nor exhaustive as the concept of crime, as stated above, is a variable term.

2.6.3. Meaning of Cybercrime

It is rightly said that everything has a cost associated with it and so is the case with growing popularity and convenience of digital networks. The ease, convenience and swift communication provided by the Information and Communication technology does also come at a cost. As the businesses and societies are increasingly relying on computers and internet-based networking, the cybercrimes and digital attack incidents have increased many folds. These attacks are generally classified as crimes that involve the use

[46] R.C. Nigam, *Law of Crimes in India, Principles of Criminal Law* 30 (Asia Publishing House, 1956).

of a computer or computer source or computer networks. The instances of different cybercrimes being committed include the financial scams carried out through the mode of computer, computer hacking, downloading pornographic images from the internet, virus attacks, e-mail stalking and creating websites that promote racial hatred.

The first major instance of a cybercrime being committed was reported in the late 90's, when a computer virus mailed to the masses affected nearly 45 million computer users worldwide.[47]

As in the developed world, in developing economies too, the cybercrimes have increased manifold, owing to the rapid diffusion of Internet and the digitalization of economic activities. Thanks to the huge penetration of technology in almost all areas of operation of society, from corporate governance and state administration to the 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 we cannot think of operating without being associated with computers.[48]

The terms "computer crime" and "cybercrime," which are often synonymous and used interchangeably, refer to criminal acts in one or more of three categories: a "traditional form of crime … committed over electronic communication networks and information systems," the "publication of illegal content over electronic media," or any "crime unique to electronic networks" (Commission of the European Communities 2007)[49].

In a cybercrime, the computer or the data itself is either a target or the object of an offence or a tool employed in commit ting some offence, and thus providing the necessary inputs for that offence. All such acts of crime come under the broad definition of the term cybercrime.

According to *Pavan Duggal*, "cybercrime is species and the conventional crime is genus, where the computer is either an object or a subject of the cyber-criminal

[47] Cyber Crime Law and Practice, The Institute of Company Secretaries of India (2016), *available at:* https://Www.Icsi.Edu/Media/Webmodules/Publications/Cyber_Crime_Law_And_Practice.Pdf. (last visited on 21st July, 2020).

[48] *Ibid*.

[49] J. Bregant, and R. Bregant, "Cybercrime and Computer Crime". In The Encyclopedia of Criminology and Criminal Justice, J.S. Albanese (ed.) 2016, *available at:* https://doi.org/10.1002/9781118517383.wbeccj244. (last visited on 2nd September 2020).

activities".[50] Cybercrimes are technology-based crimes wherein the computer or internet itself is used as a weapon or means to commit such crimes. They are organized and white-collar crimes like cyber frauds, hacking, data theft, phishing, identity theft, etc. Cybercrimes are committed with the help of technology and cyber criminals have a deep understanding of technology. In fact, cyber criminals are technocrats who understand the intricacies of Information Technology. Cybercrimes do not know or recognize any territorial boundary or barrier.

In general, a cybercrime can be classified into the following three categories:

(i) *Target Cybercrime:* It is a crime wherein a computer is the target of the offence.

(ii) *Tool Cybercrime:* It is a crime wherein a computer is used as a tool in committing the offence.

(iii) *Computer incidental:* It is a crime wherein the computer plays only a minor role in the commission of the offence.

This however is not an exhaustive definition as the Indian Penal Code also covers certain cybercrimes, such as email spoofing and cyber defamation, sending threatening emails, etc.

2.6.4. Definition of Cybercrime

The term "Cybercrime" has neither been defined in the Information Technology Act, 2000 nor in the Information Technology (Amendment) Act, 2008 nor in any other legislation in India. In fact, it is quite difficult, if not impossible, to define the word cybercrime. The word 'Offence' has had been defined under the Indian Penal Code, 1860 and also in quite a few other legislations too[51]. In order to define cybercrime, we can say, it is a crime associated with or committed with the help of computers. To put it in simple words 'an offence or a crime in which a computer is used can be said to be a cybercrime'. Interestingly, even a petty offence like stealing or pickpocketing can be brought within the broader purview of cybercrime, if the basic data or aid to such an offence is given through a computer or the information stored in a computer is used (or misused) by the

[50] Pavan Duggal, *Cyber Law - An Exhaustive Section Wise Commentary on The Information Technology Act* 17 (Universal Law Publishing, New Delhi, 2nd edn., 2017).

[51] The Indian Penal Code, 1860 (Act 45 of 1860), s.40; The Code of Criminal Procedure, 1973 (Act 2 of 1974), s. 2(n).

offender. The Information Technology Act, 2000 does define words like computer, computer network, data, information and all other associated terms that form a part of the term cybercrime, about which we will now be discussing in detail.

There are almost as many terms to describe cybercrime as there are cybercrimes. Early description included 'computer crime', 'computer related crime' or crime by computer.[52] The advent of internet brought us cybercrime and internet or net crime.[53] Cybercrime is a term used to broadly describe criminal activity in which computers or computer networks are tools, target, or a place of criminal activity and include everything from electronic cracking to denial-of-service attacks. It is also including traditional crime in which computer or networks are used to enable the illicit activity. Cybercrimes are committed while in cyber space. They included crimes like cyber terrorism, intellectual property infringement, hacking, industrial espionage, online child exploitation, internet usage policy abuse, illegal purchase of goods, sexual assault, internet fraud, software piracy, viruses, impersonation and many more.

Thus, cybercrime can generally define as a criminal activity in which information technology systems are the means used for the commission of the crime.

❖ **Encyclopedia Britannica Definition of 'Cybercrime'**

The encyclopedia Britannica defines cybercrime as any crime that is committed by means of special knowledge or expert use of computer technology. So, what exactly is cybercrime, cybercrime could reasonably include a variety of criminal offences and activities.[54]

❖ **Webopedia Definition of Cybercrime**

Cybercrime encompasses any criminal act dealings with computers and networks (called hacking). Additionally, cybercrime also includes traditional crimes conducted through the internet. For example; hates crimes, telemarketing and internet fraud, identity theft, and credit card account theft are considered to be cybercrime when illegally activities are committed through the use of the computer and the internet.

---

[52] S W Brenner, "Cybercrime metrics: Old wine, new Bottles?" 9 *Virginia Journal of Law and Technology (*2004), *available at:* https://www.researchgate.net/publication/265032559CybercrimeMetricsOldWine_New_Bottles/link/5743026108ae298602ee6bd5/download. (last visited on 25th December 2020).

[53] Jonathan Clough, *Principles of cybercrime* 10 (Cambridge University Press, 2nd edn., 2015).

[54] *Available at*: http://tnsja.tn.gov.in/article/Cyber%20Crime%20by%20KNBJ.pdf (last visited on 25th July 2020).

❖ **CBI manual Defines Cybercrime**

CBI Manual defines cybercrime as:

a) Crimes committed by using computers as means, including conventional crime.
b) Crimes in which computers are targets.[55]

Cybercrime is criminal activity done by using computers and the internet. This includes non-monetary offences, such as creating and distributing viruses on the other computers or posting confidential information on the internet. The most prominent form of cybercrime is identity theft, in which criminals use the internet to steal personal information from other users. Cybercrime done is through phishing and farming. Both these methods lure users to fake websites, where they are asked to enter personal information. This includes login information, such as usernames and passwords, phone numbers, addresses, credit card numbers, bank account numbers, and other information criminals can use to "steal" another person identity.

The word crime is defined as an act which, subject the doer to legal punishment or any offence against morality, social order or any unjust or shameful act. Or a crime an action or morals or to the interest of the state and that is legally prohibited. The offence is defined in the Indian penal code 1860 to mean as an act or omission made punishable by any law for the time being in force.

❖ **United Nations Definition of Cybercrime**

Cybercrimes span not only state but national boundaries as well. Perhaps we should look to international organizations to provide a standard definition of the crime. At the tenth *United Nation Congress on the Prevention of the crime and Treatment of offenders*[56], in a workshop devoted to the issues of crimes related to computer networks, cybercrime was broken into two categories and defined thus:

a) *Cybercrime in a narrow sense (computer crime):* Any illegal behavior directly by means of electronic operation that targets the security of the computer system and the data processed by them.

[55] *Ibid*.
[56] United Nation, Crime related to Computer Network, A/CONF.187/1.3 February 2000, *available at:* https://www.unodc.org/documents/congress//Previous_Congresses/10th_Congress_2000/017_ACONF.187.10_Crimes_Related_to_Computer_Networks.pdf (last visited on 23rd September, 2020).

b) *Cybercrime in a broader sense (computer-related crime):* any illegal behavior committed by means of, or in relation to, a computer system or network, including such crime as illegal possession and offering or distributing information by means of a computer system or network. Of course, these definitions are complicated by the fact that an act may be illegal in one nation but not in other.[57]

❖ **Professor S. T. Viswnathan Definition**

Prof. S.T. Viswnathan has given three possible definitions of cybercrime in his book and these are as follows:

a) Any illegal action in which a computer is a tool or object of the crime; in other words, any crime, the means or purpose of which is to influence the function of computer.
b) Any incident associated with computer technology in which a victim suffered or could suffered loss and a perpetrator, by intention, made or could have made a gain.
c) Computer abuse is considered as any illegal, unethical or unauthorized behavior relating to the automatic processing and transmission of data.[58]

Cybercrime can be plainly defined as "crimes directed at a computer or computer system".[59] Cybercrime are different from the conventional crimes in cybercrimes; the crime is committed in an electronic medium and here *mens rea* is not requirement but is rather a general rule under the penal provisions of the Information Technology Act, 2000. The element of *mens rea* in internet crimes is that the offender must have been aware at the time of causing the computer to perform the function that the access thus intended to be secured was unauthorized.[60]

2.7. Transformation of Traditional Crime to Modern Form of Crime

Modern approach to crime is a functional approach. It aims at the function played by law in a civilised society. Industrial revolution, scientific developments, refinement of political institutions, academic and education enlightenment of the individual, the

[57] *Ibid*.
[58] S.T. Viswanathan, *The Indian Cyber Laws: with Cyber Glossary* 81(New Delhi, 2001).
[59] Peter Stephenson, *Investigating Computer- Related Crime* 3 (CRC Press, Washington DC, 2000).
[60] Manish Kumar Chaubey, *Cybercrime and Legal Measures* 6-8 (Regal Publication, New Delhi, 2013)

loosening of religious grip over society and the fading moral norms have changed the configurations of crime in modern society more so in the information society.[61] Accordingly, the function of law has become diverse. The Wolfenden Committee Report (1958)[62] has spotlighted the functional approach to crime in England and observes that the function of criminal law is preservation of public order and decency, the protection of citizens against exploitation and corrupt behavior of others; it particularly protects the weaker, the fragile, the crime prone and the inexperienced; The aim of law the is function thus to preserve of law does public not good go beyond this. The aim of law is thus to preserve public good and check individual behavior whenever it challenges that and the concept of morality has little said in the legal lexicons.

2.8. Essential Ingredients of Crime with Reference to Cyberspace

The definition of a crime has always been regarded as a matter of great difficulty. It is a general principle of criminal law that a person may not be convicted of a crime unless the prosecution has proved beyond reasonable doubt that:[63]

(i) He has caused a certain event, or responsibility is to attributed to him for the existence of a certain state of affairs which is forbidden by criminal law;

(ii) He had a defined state of mind in relation to the causing of the event or the existence of the state of affairs.

Thus, a crime essentially consists of two elements, namely, *actus reus* and *mens rea*. What will follow will be an analysis of how the theory of criminal law can be applied to internet crimes. For this purpose, hacking, a crime of the internet age has been used to illustrate the points sought to be made.

2.8.1. Role of *Actus Reus* in Crime

The word *actus reus* connotes a 'deed', a physical result of human conduct. The *actus reus* includes all the elements in the definition of the crime except the accused

[61] R.C. Nigam, *Law of Crimes in India, Principles of Criminal Law* 30 (Asia Publishing House, vol.1, 1956).

[62] Wolfenden Report, 1957, *available at*: https://www.bl.uk/collection-items/wolfenden-report-conclusion. (last visited on 11th July 2019).

[63] J. C. Smith and Brian Hogan, *The Element of a Crime in Criminal Law* 31 (Butterworth & co., 1988).

mental element. It is not merely an act but may consist in a state of affairs not including an act at all. A well-known definition of *actus reus* is "such result of human conduct as the law sleeks to prevent".[64]

The *actus reus*, then, is made up generally, but not always, of conduct, and sometimes its consequences and also the circumstances in which the conduct takes place, or which constitute the state of affairs, in so far as they are relevant. Sometimes a particular state of mind on the part of the victim is required by the definition of the crime. If so, that state of mind is part of the *actus reus*.

2.8.2. Status of *Actus Reus* in Cybercrime

The element of *actus reus* in cybercrime is relatively easy to identify, but is not always easy to prove. The fact of the occurrence of the act that can be termed as a crime can be said to have taken place when a person is:

(i) Trying to make a computer function;

(ii) Trying to access data stored on a computer or from a computer which has access to data stored outside;

(iii) If he or she uses the internet to attempt to gain access, signals pass through various computers. Each of these computers is made to perform a function on the instruction which the person gave to the first computer in the chain. Each such function can be said to constitute *actus reus*;

(iv) Attempting to login, even if those attempts fail. This is because most hackers have an automated system of trying passwords, the very running of which can be considered to be a function being performed.

2.8.3. Role of *Mens Rea* in Crime

The second essential constituent of a crime is what is often called "a guilty mind", also known as *mens rea*. Until the 12th century, a man could be held liable for a harm simply because his conduct caused it, without proof of any blameworthy state of mind, whatsoever, on his part. However, this interpretation under vent a gradual change until

[64] J.W. C. Tunner, *Kenny's Outline of criminal Law* 17 (Cambrige University Press, London, 19th edn., 1966).

modern common law came to regard a guilty mind of some kind or some other such mental element as always being necessary.

Mens rea may comprise a number of different mental attitudes including intention, reckless and negligence. "Intention", here refers to the state of mind of men who not only foresee but also wills the possible consequences of his conduct. There cannot be intention unless there is foresight, since a man who intends a particular act must have reasonable foresight of the consequences of such act.[65]

Though intention cannot exist without foresight, the converse is not necessarily true, i.e., there cannot be foresight without intention. A person who does not intend to cause a harmful result may take an unjustifiable risk of causing it. If a man foresees the possible or even probable consequences of his conduct and yet, without desiring them, still persists with such conduct, he knowingly runs the risk of bringing about the unwished result. Such conduct may be defined as recklessness.

Finally, a man may bring about an event without having any intention or foresight. He may never have considered the possible consequences of his conduct and the end result may come as a surprise even to him. Under Common Law, there is no criminal liability for harm caused by ones inadvertent or unintended and unforeseen conduct.

2.8.4. Status of *Mens Rea* in Cybercrime

An essential ingredient for determining *mens rea* on the part of the offender is that he or she must have been aware at the time of causing the computer to perform the function that the access intended to be secured was unauthorized. There must be, on the part of the hacker, intention to secure access, though this intention can be directed at any computer and not at a particular computer. Thus, the hackers need not be aware of which computer exactly he or she was attacking. Further, this intention to secure access also need not be directed at any particular or, particular kind of, programmes or data. It is enough that the hacker intended to secure access to prograammes or data per se.
Thus, there are two vital ingredients for *mens rea* to be applied to a hacker:

[65] Anthony Hooper, "General Principles of Criminal Responsibility" in Harris, *Criminal Law* 29 (Sweet & Maxwell, London, 1968).

(i) The access indented to be secured must have been unauthorized;

(ii) The hacker should have been aware of the same at the time he or she tried to secure the access.

The second ingredient is easier to prove if the accused hacked is a person from outside who has no authority whatsoever to access the data stored in the computer or the computers, however, it is difficult to prove the same in the case of a hacker with limited authority.

2.9. Classifications of Cybercrime

With the increasing use of internet number of cybercrimes is also increasing. Criminals now very commonly and frequently use some of these crimes where some are in their infancy and growing at a very fast speed the frequently committed crimes are committed basically under four categories:

2.9.1. Cybercrime against Individuals

Cybercrime committed against persons includes transmission of cyber porn, transmission of child pornography, harassment via email, fake avatar. The trafficking, distribution, posting and dissemination of obscene material including indecent exposure, posting of intimate image and pornography.[66] The humanity can hardly explain the impact of this form of cybercrime.[67] There are certain offences which affect the personality of individual can be defined as**:**

(i) **Infringement of Privacy**: In today's world, increasing use of computer networks including internet for storing and transmitting of personal data, under person which he himself may not even aware of. Thus, availability of information in the cyberspace, for anyone with capability to access, has brought up the issue of criminal infringement of privacy. Right to privacy is considered as fundamental right in all most civilized nation and in India too.[68] Infringement

[66] Harpreet Singh Dalla and Geeta, "Cyber Crime-A Threat to Persons, Property, Government and Societies" 3 *International Journal of Advanced Research in Computer Science and Software Engineering* 235 (2013).

[67] *Ibid.*

[68] Mark S. Merkow and James Brietharyst, *the E-Privacy Imperative* 45 (American Management Association, New York, 2002).

of privacy means unauthorized access of the personal information stored in computer without his/her consent.

(ii) **Identity Theft**: The term identity theft refers to a host of frauds, thefts, forgeries, false statements and impersonations' involving the use of another person are identifying information.[69]

(iii) **Cyber Staking**: It is expressed or implied a physical threat that creates fear through the use of computer technology such as email, phone, text massage, webcam, internet, website or videos.

(iv) **Revenge Porn and Blackmailing:** Revenge porn means an act whereby the perpetrator satisfies his anger and frustration for a broken relationship through publicizing false, sexually provocative portrayal of his/her victim, by misusing the information that he may have known naturally and that he may have stored in his personal computer, or may have been conveyed to his electronic device by the victim herself, or may have been stored in the device with the consent of the victim herself; and which may essentially have been done to publicly defame the victim.[70] Blackmailing in respect of revenge porn means threaten the victim that the stored explicit image/ video will be published to fulfill the unfavorable demand.

(v) **Sextortion:** A sexual coercion or ''sextortion,'' a form of coercion where a person procures ''sexual cooperation by putting some kind of pressure on a victim''. This may be in the form of blackmail, bribery, or threats such as demanding that the victim engage in either online or in-person sex acts or demanding the release of intimate images or information.[71]

(vi) **Cyber Defamation**: It involves any person with intent to lower down the dignity of the person by hacking his mail account and sending some mails with using vulgar language to unknown persons mail account.

---

[69] G. S. Bajaj (ed.), *Cyber Crime & Cyber Law* 187(Serial Publication, New Delhi, 2011).

[70] D. Halder, "Examining the Scope of Indecent Representation of Women (Prevention) Act, 1986, In the Light of Cyber Victimization of Women in India," 11 *National Law Journal* 88-208 (2013).

[71] Nicola Henry and Anastasia Powell, "Technology-Facilitated Sexual Violence, Trauma, Violence & Abuse" 19 *A Literature Review of Empirical Research* 195-208 (2018), *available at: https://www.jstor.org/stable/10.2307/26638194. (last visited on 16th April, 2020).*

(vii) **Harassment via E-Mails**: This is very common type of harassment through sending letters, attachments of files & folders i.e., via e-mails. At present harassment is common as usage of social sites i.e., Facebook, Twitter, Orkut, Instagram etc. increasing day by day.

(viii) **Cyber Bullying:** Cyber bullying means the use of electronic communication to bully a person, typically by sending message of an intimidating or threatening nature.[72]

2.9.2. Cybercrime against Society

(i) **Racial & other Hate Crime**: It means "distribution or otherwise making available, racist and xenophobic material to the public through a computer system". Such material is defined as "any written material, any image or any other representation of thought or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individuals or group of individuals, based on race, color, descent or national or ethnic origin as well as religion if used as a pretext for any of these factors".[73]

(ii) **Child Pornography**: It includes the use of computer networks to create, distribute, or access materials that sexually exploit the children below the age of 18 years.

(iii) **Gender Trolling**: Gender Trolling involves specifically gender-based insult including the widespread use of pejorative term that is leveled particularly at women.[74]

(iv) **Online Gambling**: Online gambling is a general term for gambling using the internet. Computer, in online gambling, is used merely as a medium. Gambling in many countries is illegal. The problem is that most virtual casinos are based offshore, thus making them difficult to regulate.

(v) **Financial Cybercrime**: Financial cybercrime means criminal perform the illegal activities in terms of money. It includes cheating, credit card frauds, online gambling, salami attacks, and hacking.[75]

---

[72] According to Oxford Dictionary (2018).

[73] "Hate-Speech Protocol to Cybercrime Convention" 96(4), *The American Journal of International Law*, 973-975 (2002), *available at:* https://www.jstor.org/stable/3070700. (last visited on 8th February, 2020).

[74] Karla Mantilla, "Gendertrolling: Misogyny adapts to New Media" 39 *Feminist Studies* 563-570 (2013). *available at:* https://www.jstor.org/stable/23719068.(last visited on 21st January, 2020).

2.9.3. Cybercrime against State

Indian law recognized the "Cyber Terrorism" as a cybercrime against the State. The term "Cyber Terrorism" defined under section 66F[76] of The Information Technology Act, 2000. As per the Information Technology Act, such terrorist activities are done through using information technology or computer technology is punishable. Offences against government could be hacking websites or breaching the privacy of government data. Then there can also be offences against corporate bodies.[77]

Cyberwarfare:[78] Cyber war is that war which is fought through internet between countries. When on country accesses the secret of other country by internet and uses that secret against that country is known as cyber warfare.[79]

---

[75] Ravi Kumar S. Patel and Dhaval Kathiriya, "Evolution of Cybercrimes in India" 2(4) *International Journal of Emerging Trends & Technology in Computer Science* 241 (2013).

[76] The Information Technology Act, 2000 (Act 21 of 2000), s. 66 F state that "Punishment for cyber terrorism.

(1) Whoever,

(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by--

(i) denying or cause the denial of access to any person authorised to access computer resource; or

(ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorised access; or

(iii) introducing or causing to introduce any computer contaminant,

and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70; or

(B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer data base that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer data base, with reasons to believe that such information, data or computer data base so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise,

commits the offence of cyber terrorism.

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.

[77] K. Brindaa Lakshmi "Revenge Pornography is Not Recognised by Indian Law," (2017), *available at:* https://www.hidden-pockets.com/debarati-halder-legal-reourse-revenge-pornography-cyber-stalking/. (last visited on 21st January 2020).

[78] S. Wall David, "Cybercrime: New Wine, no bottle? In invisible Crimes, Their Victims & Their Regulation, edited by Pam Davies, Peter Francis & Victor Jupp, London: Mac-Millan, 1999.

[79] V. S. Jaswal and S. T. Jaswal, *Cyber Crime and Information Technology Act, 2000* 29 (Regal Publication, New Delhi, 2014).

2.9.4. Cybercrime against Property

(i) **Cyber Squatting**: Cyber Squatting: means where two persons claim for the same Domain Name either by claiming that they had registered the name first on by right of using it before the other or using something similar to that previously. For example, two similar names i.e., www.yahoo.com and www.yaahoo.com.

(ii) **Intellectual Property Crime**: Intellectual property consists of a bundle of rights. Any unlawful act by which the owner is deprived completely or partially of his rights is an offence. The common form of Intellectual Property Rights violation may be said to be software piracy, infringement of copyright, trademark, patents, designs and service mark violation, theft of computer source code, etc.

(iii) **Internet Time Theft:** Internet time theft is a kind of theft in which perpetrator used the surfing hours of victim.[80]

2.10. Nature of Cybercrime

Since the beginning of the civilization, man has always been encouraged by the need to make progress and better the existing technologies. This has led to fabulous development and progress, which has been a launching pad for further development.[81]

When internet was developed, the founding fathers of internet hardly had any inclination towards the internet that it could transform itself into all-pervading revolution which could be misused for criminal activities and which requires legal regulation to regulate it. Today there are many disturbing things happening in cyberspace.[82]

People who commit computer crimes vary widely in skills, knowledge, recourses, authority and motives. In addition, motives are said to include greed, need (to solve personal problem such as gambling debts), inability to recognize the harm done to others, personification of computers (seeing computer as adversaries in a game) and Robin Hood syndrome (seeing corporations as so rich that stealing from them is morally justified).[83]

Due to the anonymous nature of internet, it is possible to engage into variety of criminal activities with impunity and people with intelligence, have been grossly

[80] Cyber Crimes-Technical Issues, Internet Time Theft, *available at:* http://www.asianlaws.org/cyberlaw/library/cc/what_cc.htm. (last visited on 3rd Feb, 2020).
[81] G. S. Bajpai, *Cybercrime & Cyber Law* 167 (Serials Publications, New Delhi, 2011).
[82] *Ibid*.
[83] Atul Jain, *Cybercrime: Issues threats and Management* 87 (Isha Books Publications, New Delhi, 2005).

misusing this aspect of the internet to perpetuate criminal activities in cyberspace. Hence, there is need of cyber laws to punish them. The new form of cybercrime present new challenges before law makers, law enforcement agencies, and international institution.[84]

2.11. Who Are Cyber Criminals?

Cybercrime involve such activities as child pornography; revenge porn; credit card fraud; cyber stalking; cyber defamation; gaining unauthorized access to computer system; ignoring copy right; software piracy; identity theft to perform criminal acts. Cybercriminals are those who conduct such acts. They can be categorized into three groups that reflect their motivation.[85]

Type I: cybercriminals-Hungary for recognition

- Hobby hackers;
- IT professionals (social engineering is one of the biggest threats);
- Politically motivated Hackers;
- Terrorist Organization

Type II: cybercriminals-not interested in recognition

- Psychological Perverts;
- Financially Motivated hackers (corporate espionage);
- State- sponsored hacking (National espionage, sabotage);
- Organized criminals.

Type III: cybercriminals-the insiders

- Disgruntled or former employees seeking revenge;
- Competing companies using employees to gain economic advantage through damage and / or theft

Thus, the typical "motives" behind cybercrime seems to be greed, desire to gain power and /or publicity, desire for revenge, a sense of adventure, looking for thrill to access forbidden information, destructive mindset and desire to sell network security service.

[84] G. S. Bajpai, *On Cybercrime & Cyber Law* 76 (Serials Publications, New Delhi, 2011).
[85] Nina Godbole and Sunit Belapure, *Cyber Security: Understanding Cybercrimes, Computer Forensics and Legal Perspectives* 16 (Wiley Publication, New Delhi, 2017).

2.12. *Modus Operandi* of Cybercrime[86]

❖ **Ways of direct access**

This covers damaging, deletion, deterioration, alteration, suppression or copying of the computer data and includes unauthorized hindering of computer, computer system or network functioning by inputting corresponding command from the computer where information is restored. Such direct access can be made both by the person working with the data and as well as by person intentionally penetrating in restricted areas or premises where information is restored. However, due to decentralization of information processing, direct access is decreasing and the perpetrator finds it easier to intercept computer networks. In order to seize information left by the user, the perpetrator looks around workplaces of programmers for drafts, examines and restores erase software.

❖ **Ways of indirect access**

Ways of indirect access to information includes access without right to certain computer or information system via computer networks from the computer located at certain distance.

❖ **Mixed method**

These methods consist of both direct and indirect (remote) access. They are

(i) Secret insertion of commands in programs that allow the performance of new unplanned functions, making this program workable.

(ii) Alteration of programs by way of secret placing of command sets that should come into action under specified conditions and in a given time.

(iii) Access obtained to data base and files of the authorized user through weak places in security system. This gives an opportunity to read and examine information stored in system and copy it.

(iv) Mixed method also includes using of bugs in program files. The programs are called "breaking" and malefactor inputs some amount of certain command that help to perform new unplanned functions making this programmer unable.[87]

[86] Talat Fatima, *Cyber Crimes* 67-69 (Eastern Book Company, Lucknow, 2016).
[87] *Ibid*.

Comprehension of such modus operandi which keeps changing with the technological advancements shall help in development of law regarding control of cybercrime.

2.13. Reason for Committing Cybercrime

There is no more to crime than opportunity. Crime requires a pool of motivated offenders. The motivations of those who would commit cybercrime are diverse, but hardly new. Computer criminals are driven time-honored motivations, the most obvious of which are greed, lust, power, revenge, adventure, and the desire to taste "forbidden fruit". Cybercrime has a unique victimological attributes the victim often does not know that he is or she is a victim. This is because the people are not aware about the cybercrime, whether it is a cybercrime or not. There is a lot of misconception prevalent with respect to the people committing cybercrimes, the cybercriminals. Hollywood movies have built into the mind of the people an image of smart intelligent and tech savvy cybercriminal. This was somewhat true a decade back. Today, however, both the net and the user friendliness of personal computer have made committing cybercrime easy for anyone willing to learn to do so.[88]

2.13.1. Legal Reason for Commission of Cybercrime

The global nature of cyberspace significantly enhanced the ability of offenders to commit crime in one country, which affects individuals in a variety of other countries. The transcendental jurisdiction of internet causes the major threat to the society in the form of cybercrime. The main victim of this transgression can be considered women and children. Acquaintance with technology is positive aspect that be considered important for the development of the country but at the same time it is becoming the source to increase the crime rate with the help of technology against the vulnerable group of the society. The cybercrime investigation is different and present serious enforcement challenge.

[88] Rahul Purohit and Varun Maheshwari, "Cyber Crime: Form and Control" in S. Bajpai, *On Cybercrime & Cyber Law* 130 (Serials Publications, New Delhi: 2011).

2.13.2. Sociological Reason for Commission of Cybercrime

Most of the cybercrime remains unreported due to lack of awareness that certain act in cyberspace constitutes an offence. Another reason for not reporting the cybercrime due to the hesitation and shyness of the victim; and fear of defamation of the family name fame, while a cybercrime committed is against women. The cyber criminal's identity remains anonymous and cybercrime perpetrator hides behind a veil in cyberspace, one of the sociological reasons for increasing cybercrime in the society.

2.14. Cybercrime in India

In the present situation where cyber control mechanism are most important, we need to push cyber laws. Cybercrime are a new form of crime to India rapidly expanding due to the extensive use of internet. Getting the right lead and making the right interpretation are very important in solving a cybercrime.

S. No.	Year	No. Of Cybercrime Reported	
		IT Act	IPC
1	2002	70	738
2	2003	60	411
3	2004	68	279
4	2005	179	302
5	2006	142	311
6	2007	217	339
7	2008	288	176
8	2009	420	276
9	2010	966	356
10	2011	1791	422
11	2012	2876	601
12	2013	4356	1337
13	2014	9626	
14	2015	11592	
15	2016	12317	
16	2017	21796	
17	2018	27248	
18	2019	44546	
19	2020	50035	

Table 2.1

(NCRB Report, 2002-2020)[89]

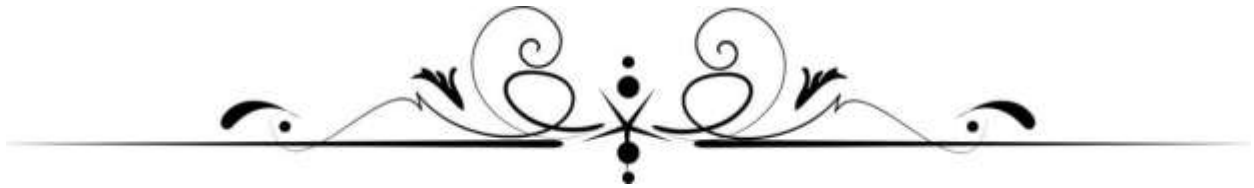
[89] Government of India, "Report of National Crime Record Bureau" (Ministry of Home Affairs, 2016) *available at*: https://ncrb.gov.in/en/crime-india.(last visited on 2nd March, 2022).

A total number of crimes recorded in India is 9,24,016 comprising 6,68,061 Indian Penal Code (IPC) Crime and 255955 special & Local Laws (SLLs) crime. During the year 2020, 50035 cases were registered under the Information Technology Act as compared to 70 cases registered during the year 2002, thereby reporting increased in many folds over 2002.

In year 2020, NCRB, published report on cybercrime against children and cybercrime against women under separate heading. Total cybercrime during year 2020 recorded as 1102 under cybercrime against children and 10405 recorded under cybercrime against women. These statics are but a fraction of the ground reality.

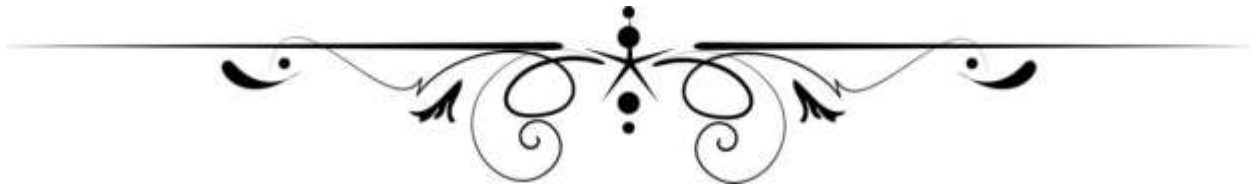
Conclusion

The development of the computer and internet bring the enormous changes in our life and the same time brings the monstrous thing such as cybercrime which makes the life of the women miserable especially. The cybercrime against women rapidly increasing and its form changes with the changing of the technology. The growth in internet access has accelerated due to the boom in access via mobile phone, and who make massive use of cyberspace are particularly vulnerable to cybercrime. 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. The revenge porn and blackmailing are one of the cybercrimes against women needs conceptual understanding and interpretation which seek attention of the legislator to frame laws at national as well as at international to curb this menace.



CHAPTER-III

CONCEPTUALIZATION OF REVENGE PORN AND BLACKMAILING UNDER CYBERCRIME AGAINST WOMEN



CHAPTER-III

CONCEPTUALIZATION OF REVENGE PORN AND BLACKMAILING UNDER CYBERCRIME AGAINST WOMEN

3.1. Introduction

Since the advent of the internet issues of online safety, privacy and abuse have been of central concern. Cybercrime is a global phenomenon. With the advent of technology, cyber victimization of women is on the high and poses a great threat to individual freedom, Privacy and Dignity. Safety of the women has always been an issue, especially in a country like India, where the worm of crime against women increases like a coconut tree. Cybercrime against women in India, quite an emerging new concept, however, cybercrime against women is a form of crime which committed with the help of technology. Women from ancient to modern societies have always been the subject of crime. Among all the groups in the society women are the most vulnerable and fall pray to cybercrimes. Therefore, women are most vulnerable in society for cybercrime. The crimes which are committed against women with the help of computers and computer networks are called cybercrime against women. The present study highlights the cybercrime against women in India especially emphasizing on cybercrime such as revenge porn and blackmailing.

Problematising the subject matter of the crime against women, researcher said that Crime against women is steadily rising in the present world in general particularly revenge porn and blackmailing. The changing nature and scope of internet usage as a platform, where one third of the users are female, has a shifting paradigm for the definition of these crimes and adding different notions of classification of crime through internet or on its platforms. Development of definitions are contributing to the rights of parties involved and enticing discussions of duties related to privacy, dignity and mental and physical well being of women.

Internet increases the scope of Information & Communication Technology (ICTs) for mobile information and communication technologies and the wide distribution of

social media have created new opportunities among the internet users.[1] Superintendent of Police (Cybercrimes) G.R. Radhika said that the NCRB data in 2018 revealed that 6,030 cybercrimes were registered by women. "In India 71 crore people are using the Internet, out of which, 25 crores are women. She said 80% of people are falling prey to cybercrimes and 63% of people don't know where to lodge complaints on cybercrimes".[2] Cyber violence against women and girls is emerging now as a global issue with serious implications for global societies and economies.

This chapter is proposes the theoretical grounds, crafting the concept of revenge porn and blackmailing. Revenge porn has the potential to severely harm the victim and society as a whole, yet no research has been done as to the content of the concept. Revenge porn and blackmailing is an advanced form of violation of women's right of privacy and dignity, as considered by the researcher. This conceptualization will reflect the social values and un-considered rights that are violated by the phenomenon, more importantly highlights the behavior of the offender and more clearly recognizes the harm inflicted on the victim or the society at large. Therefore, the conceptualization of revenge porn and blackmailing is necessary to be able to understand the severity of the harm caused by this offence on the victim and to develop an appropriate law governing specifically revenge porn.

3.2. Cybercrime against Women

In the virtual world, women and children have been found to be the most vulnerable group of the society; therefore, cybercrimes against women and children have witnessed a sharp rise in the last few years. Women are usually subjected to cybercrime such as cyber harassment, cyber stalking, cyber pornography, cyber defamation, revenge porn and cyber blackmailing and much more. Violence against women may include domestic violence, intimate partner abuse, sexual harassment at work place, women and child sex trafficking, female feticide, gendered online cybercrime etc. are also at a rise due to showing the power of gender masculinity.

---

[1] Shruti Bist, *Cybercrime against Women-Investigative & Legislative Challenges* 78 (Blue Rose Publication, New Delhi, 2020).

[2] "Cyber-crimes against women on the rise" *The Hindu News Paper*, 20th August , 2020.

There are other definitional aspects for categorizing the crime and determine the harm inflicted on women or society at large. Considering this crime category of not just dissemination of non-consensual pornography bit to widen its definition for sexual offenses. As it is argued in the other chapters that the actions of the administration for the prevention and response against such acts are not adequate in order to dispense justice in such cases.

3.2.1. Meaning and Definition of Cybercrime against Women

Considering the basic definition related to Crime against women at international level; The United Nations defines violence against women as "any act of gender-based violence that results in, or is likely to result in, physical, sexual or mental harm or suffering to women, including threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or in private life (Empowering women against cyber-violence 2011)."[3]

Online abuse is not just virtual, it's very real. "Individual women who experience online abuse understand that online violence is real violence, but very often their peers, friends, or families don't."[4]

That one is the non-consensual dissemination of private information of sexual explicit character or of other nature which diminished the identity of women, fixing the identity to a sexually diminished the women, causing harms to sexual integrity and autonomy of the individual where the offender has used arbitrary force to harass the women physically, mentally and economically by such dissemination in public sphere using internet or other media tools. This form of cybercrime is known as 'revenge porn'.

These above definitions are also applicable while dealing with cybercrime against women. Further, *Swapna Majumdar* defines the violence against women, as "Violence against women is neither culture nor region-specific; it cuts across community and class. Shocking though it is, the fact is that violence against women has become an acceptable

[3] *Available at:* https://www.un.org/womenwatch/daw/vaw/voverview.htm#:~:text=The%20Declaration%20defines%20vi olence%20against,public%20or%20in%20private%20life'. (last visited on 3rd June, 2021).

[4] United Nation Organisaion, UN Reporting on Violence against Women's and Girls, available at: https://www.un.org/sexualviolenceinconflict/wpcontent/uploads/2020/01/report/reporting-on-violence-against-women-and-girls-a-handbook-for-journalists/371524eng.pdf. (last visited on 5th July, 2021).

norm of life because women accept violence as a part of their married life until it becomes intolerable."[5]

The Internet and social media, changing and deviating the nature of such crime further where, internet is used as an extraordinary vehicle for communication, information and citizen mobilization, but it can also give discrimination, hatred and violence to a voice. New technologies and Internet based networks do not create the sexist behaviors that prevail in a particular social context, but they can enlarge and globalize them. In many cases, these acts of harassment are committed by relatives such as ex-husbands, classmates, colleagues, etc., but those responsible for these attacks can also come from the entire public sphere.

Considering these definitions that principal definition of the crime against women are more in the traditional sense where the crime against body and mind is actualised in physical space. However, the tools to establish the essentials of the crime are intention and coercion and arbitrary force is mentioned in the definitions, which is also true for the cyber or virtual spaces where the force or duress is applied in other forms. Mostly, the definitions are considering the social and cultural milieu and spaces where the objectification of women happens in society by arbitrary deprivation of liberty. Both of the definition can be considered to explain the basic essentials to establish a crime against women but limited in scope and doesn't include space and tools for such arbitrary deprivation of liberty to establish such crime by technology. Moreover, it also focused more on the action taken for the commission of crime and impliedly considering the omission of duty form the part of consent in dissemination of information, where there is consent for the production of such content.

Moreover, internet as a platform is not liable and equipped enough for the monitoring of such content and the owner of the platform is considered to be free from any liability of violation of privacy, dignity, sexual autonomy and liberty of the individual. Jurisprudential aspect of the law is either silent or having immunity against such disseminations as it is closely linked with the argument of freedom of expression which can impact the actions in good faith for relevant information in public interest.

[5] Majumdar, Swapna, "Sexual Control and Violence." *The Tribune* (2003).

3.2.2. Cybercrime against Women: A Deviance from Traditional Crime

Criminal jurisprudence is the boon of the civilized society. In India, criminal jurisprudence can be traced back to the days of Manu where Manu had recognized assault, theft, robbery, false evidence, slander, criminal breach of trust, cheating and rape as offences. The real notion of crime percolated from the Roman law in Western jurisprudence. The internet has revolutionised the conventional notion of crime.[6]

Historically, crimes against women and young girls have been gravely under-criminalized.[7] There has been, and continues to be, a systemic failure of the world's legislative bodies to adequately and effectively protect women from all kinds of victimization on a national and international level.[8] This has been especially true when the abuse endured is of a sexual nature whether physically, mentally, or emotionally. With the advent of legislative reform in the United States protecting women's rights, the criminal legal landscape has dramatically changed. Yet, our country is still plagued by a lack of recognition for women's rights to sexual, physical, and expressive autonomy a fundamental flaw underlining the reason why there may be a societal lack of empathy for victims of nonconsensual pornography.[9]

Therefore, physical world crime against women has been change into cybercrime against women following the technology driven crime. Cybercrime against women in India deserves a better analytical treatment from law and justice machinery as well as cyber criminologists, socio-legal researchers and activists.

---

[6] Talat Fatima, *Cyber Crime* 63 (Eastern Book Company, Lucknow, 3rd edn., 2021).

[7] Kim Swanson, Crime against Women- a Brief History of Laws in the US, *GET INCLUSIVE* (Mar. 28, 2014), *available at*: https://www.getinclusive.com/blog/crimewomen-brief-history-laws-us. (last Visited on 31st March, 2021).

[8] Sophie Edwards, "How the Legal System is failing to Protect Women and Girls from Sexual Violence," *DEVEX* (Mar. 6, 2017), *available at*: https://www.devex.com/news/how-the-legal-system-is-failing-to-protect-women-and-girls-from-sexualviolence-89573. (last visited on 31st March, 2021).

[9] Katherine A. Mitchell, "The Privacy Hierarchy: A Comparative Analysis of the Intimate Privacy Protection Act *vs*. the Geolocational Privacy and Surveillance Act", 73 *University Miami Law Review* 569 (2019).

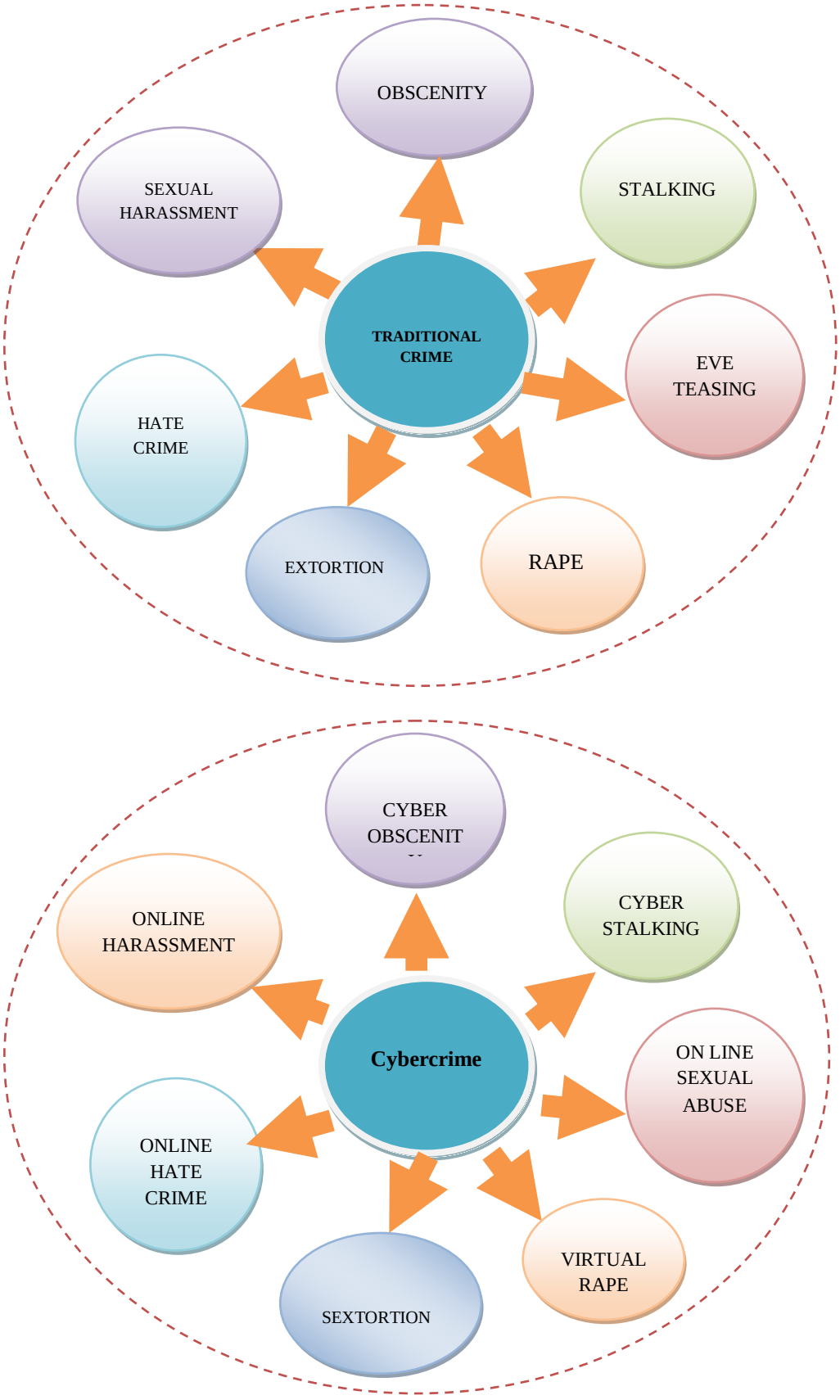

OBSCENITY
SEXUAL HARASSMENT
STALKING
TRADITIONAL CRIME
EVE TEASING
HATE CRIME
EXTORTION
RAPE
CYBER OBSCENIT
ONLINE HARASSMENT
CYBER STALKING
Cybercrime
ON LINE SEXUAL ABUSE
ONLINE HATE CRIME
VIRTUAL RAPE
SEXTORTION

Figure No. 3.1

Traditional crime against women includes obscenity, stalking, eve teasing, rape, sexual harassment, hate crime and extortion. Such crimes are duly codified in Indian Panel Code, 1860 and other respective statutes passed by legitimate authority. The scope of traditional crimes against women is changing due to advancement of new-age technologies. These sophisticated technologies have given a new way of doing such crimes (now termed as cybercrime) against women where women are becoming victims in cyber space. In Cyber space, offenders are misusing the cyber tools and adopt new methods for committing cyber crime. Cybercrime against women cyber obscenity, cyber stalking, online harassment, virtual rape, on line sexual abuse, online hate crime, trolling, cyber bulling, sextortion.

3.2.3. Kinds of Cybercrime against Women

There are various categories of cybercrime which affect the individual, property, society and Government. They are categorized as "Cybercrime against Individual", "Cybercrime against Society", "Cybercrime against Property" and "Cybercrime against Government". Here the researcher has defined the various form of cybercrime against individuals which especially target women. Following are the kinds of cybercrime against women which target women especially.

(i) Hatred is Expressed Through Cyber Verbal Abuse By Groups of Perpetrators: This can be described as "cyber mob attack" where a female member of the social network (SNW) may be attacked by a group of perpetrators both in the community or social media platform and also in her own message box.[10] There are several other platforms which can be considered today in the form of social networking sites. It can be understood also as "trolling" or "mass criticism" of a person on social platforms for the social execution, forcefully shaping of opinion and restricting the liberty to express any opinion on general platforms.

(ii) Cyber Defamation Targeting the Individual: This crime is an extension of defamation in general, in which any electronic medium or platform is used to

[10] Danielle K. Citron, "Cyber Mobs, Disinformation, and Death Videos: The Internet As It Is (And As It Should Be)" 118 *Michigan Law Review* 1073 (2020).

publish or disseminate information about the victim, information may true or not, with the intent of harming the victim's reputation in society. The intention and the reason for the same is not necessary to constitute this crime as emotional breakups may lead the male member to spread lies about the female member to other members through his own posts on community walls, social media etc.[11]

(iii) Cyber Stalking: The female member is stalked in all the groups she joins, her friends' walls are constantly watched for seeing her posts, her own write ups and her activities online. It is related to the "behavioral misconduct" in the cyber space to harass an individual but may not limit to transmission of threats and false acquisition or constant follow-up at different platforms. Indian Penal Code,1860 also defines cyber staking under section 354D[12] which explains that whoever pursuing digitally by shadowing any women/girl for foster personal interaction, repeatedly, despite a clear indication of disinterest by such women which also communicates digitally the fear of violence and threat in case on non-compliance of the side request or proposition.

(iv) Cyber Morphing: This kind of crime is editing, cropping and shadowing any image or videos of a women/girl where photographs of the female members are taken from the personal albums or through any other platforms in cyber space and they are morphed for pornographic purposes by using parts of the pictures, for instance, the head or up to breast. Any other form of insult or disrespect can be used in the text if the subject matter is connected to women. It's also very close for

[11] Law Commission of Ontario, "Defamation Law in the Age of the Internet: Young People's Perspectives" 14(2017).

[12] Indian Penal Code,1860 (Act 45 of 1860), s.354D says that "(1) Any man who,
follows a woman and contacts, or attempts to contact such woman to foster personal interaction repeatedly despite a clear indication of disinterest by such woman; or monitors the use by a woman of the internet, email or any other form of electronic communication, commits the offence of stalking; Provided that such conduct shall not amount to stalking if the man who pursued it proves that:
a) it was pursued for the purpose of preventing or detecting crime and the man accused of stalking had been entrusted with the responsibility of prevention and detection of crime by the State; or
b) it was pursued under any law or to comply with any condition or requirement imposed by any person under any law; or
c) in the particular circumstances such conduct was reasonable and justified.
(2) Whoever commits the offence of stalking shall be punished on first conviction with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine; and be punished on a second or subsequent conviction, with imprisonment of either description for a term which may extend to five years, and shall also be liable to fine."

entertainment purposes, but it's causing women victim distress and harming their mental health.

(v) Cyber Cloning: Cloning also known as "Fake Avatar" is a kind of crime where duplicate profiles or fake profiles of female victims are created by stealing the personal information of the female member. The cloned profile presents the original profile in such a manner that people are duped. The cloned profile then asks the friends of the original member to become his/ her friend and breach the privacy of other members besides using the original member's information for malevolence purposes. Female members of social media site like Facebook, Instagram and Myspace often face this kind of problem.

(vi) Cyber Obscenity: This kind of crime consists of proliferation and dissemination and sexual or erotic content over the internet bringing the glut of such material for the common vision. This includes pornographic web sites, pornographic magazine produced using computer to publish and print the material and the internet to download and transmit pornographic images, videos and writings etc. Such wise dissemination created first "moral panic" in the society at large whereas these contents are created with mainly the consent of the objective and characters used in such content. [13]

(vii) Cyber Harassment: This may include constant messaging to the profile's wall or personal email id which is shown in the profile, regular peeping in as a visitor and leaving messages in her wall, continuously sending request for friendship, joining groups where she is member and constantly posting messages disagreeing with her, etc. This is a form of harassment, including blackmailing. Threatening and continuous sending of love letters by fake names or constant sending of embarrassing e-mails to the mail box of some other user. This behavior is intended to disturb a person through the usage of internet.[14] Sexual harassment is a specific type of harassment which is particularly sexual in nature, among several other

[13] Jacob Rowbottom, *Obscenity Laws and the Internet: Targeting the Supply and Demand* 100 (Criminal Law Review, Sweet & Maxwell, London, 2006).

[14] U. Mayura and Archana Sakure, "Cyberspace and women", 8 *International Journal of Engineering and Advance Technology"* 1671 (2019).

types of them; it vitally takes into consideration constant and undesirable sexual activities.

(viii) Virtual Rape: This is a violent type of cyber victimization where the targeted woman is taken up by a harasser. He either posts constant messages like "I will rape you" or "I will tear you up" etc, or particular community members may "mob attack" the targeted female with such words which successfully generates more enthusiasm among other unrelated members to comment on the victim's sexuality. The profile owner then becomes a hot topic for erotic discussions, vulgar name calling etc. [15]

(ix) Banning A Female Member and Restraining Her From Expressing Her Views: This generally happens in a male dominated group or community where the moderator or owner or group members may victimize the targeted female member by banning her for her own feminist ideologies even through the group or the community could have been created for letting people express their own ideologies. The reason could be that the majority of the group may be pro feminist or some individual members may dislike the straight forwardness of the female members in discussing the problems of women in everyday world.

(x) Cyber Bullying and Name Calling: The harasser may constantly bully the target on social media, both in her wall and in the groups or communities where either he or she is member. Even though this is a gender-neutral cyber offence, but women are most chosen targets for their sexuality, emotional breakups or even domestic violence. The ex-spouse or the ex-lover constantly bully the woman to vent out his anger in public.

(xi) Domestic Violence and Cyber Flame: As mentioned above, separated partners may take up Social networks to vent out their rage against the female member. In such cases the ex-partner starts bullying the woman first and then provokes her to have "online fights".

(xii) Impersonation and Cheating: Social networks give wide options for creating profiles under pseudo names, hiding one's real age, sex and other information.

[15] Wendy Kaminer, Virtual Rape, *Newyork Times Magzine*, 25th Nov, 2001, *available at*: https://www.nytimes.com/2001/11/25/magazine/virtual-rape.html. (last visited on 7th July, 2021).

Further, the creation of multiple profiles of the same individual using different email ids is also possible in the social networking sites. This gives the opportunity for mischief mongers to impersonate and flirt with female members. The harasser drags the victim in an emotional relationship and she is encouraged to share her secrets, and even have erotic chats with the harasser. When the victim finally pressurizes to meet him in person, either he blackmails the victim or cheats the victim. However, impersonation and cheating can even happen for financial issues in the social networks as well. The harasser may promise the victim some online or offline monetary gain by showing his fake credentials and there by later on dupe the victim.

(xiii) Blackmailing and Threatening: This happens due to the easy availability of the personal information of the women members in the social networks. Ex-spouses, mischief mongers and stalkers may threaten and blackmail the woman for various reasons which may even lead to the shutting down of the profile of the female member. This can even have an offline effect where miscreants may physically threat and blackmail the woman with her secrets that she may have shared with her friends in groups or communities.[16]

(xiv) Cyber Flirting: Generally cyber flirting may be considered a very minimal and petty offence that starts when the perpetrator forces the victim to hear the obscene songs, messages and it may consequently result in sexual defamation and breach of trust.[17]

3.3. Conceptual Understanding of Revenge Porn and Blackmailing

While the Internet has opened many doors by facilitating communications around the world, it has revealed a dark side that creates fear, danger, and terror among the women when used for the wrong purposes.[18] Specifically, the Internet has allowed new

[16] Lenore Manderson and Linda Rae Bennett (eds.), *Violence against Women in Asian Societies: Gender Inequality and Technologies of Violence* 118 (Taylor and Francis, 2013).

[17] Shobhna Jeet, "Cyber-crimes against women in India: Information Technology Act, 2000", 47 *Elixir Criminal Law* 8891-8895 (2012).

[18] Cassie Cox, "Protecting Victims of Cyber stalking, Cyber harassment, and Online Impersonation Through Prosecutions and Effective Laws", 54(3) *SPRING* 277-302 (2014), *available at:* https://www.jstor.org/stable/24395601. (last visited on 21st December, 2021).

crimes to emerge i.e., revenge porn and blackmailing. In recent year, several cases such as Delhi DPS case, Global Jindal University case, Madhukar Trisha and other cases of pornography and revenge porn cases gain a widespread media attention in India.

Revenge pornography is a form of Technology-Facilitated violence against women that has attracted significant attention from the public, the media, and governments in recent years. It is perpetrated primarily by men against women, with significant repercussions for female victims' social, professional, and psychological well-being.[19]

Digital-age revenge porn cybercrime first gained unsavory reputation in 2010, when one of the first websites to exclusively host this kind of material, *Is Anyone Up?,* featured thousands of nude images of non-consenting men and women alongside links to their social media profiles and accompanying derogatory commentary.[20] Named 'revenge porn' by the media, this term has now become synonymous with the practice of nonconsensually distributing individuals' private, sexually graphic images online.[21]

American founder of the site's Hunter Moore, made various claims about his motivations, including a wish for his friends to see photos of the woman with whom he was sleeping at the time, and assertions that he wished to establish a means by which he and his friends could 'get back' at their ex-girlfriends. Moore was notoriously unresponsive to requests from victims to remove their images, earning him the reputation of being 'the most hated man on the Internet.' [22]

The revenge porn and blackmailing crime is not a gendered based cybercrime. Male and female both may become the victims of revenge porn and blackmailing cybercrime. But due to the vulnerability of the women in cyberspace women are much more victimized in this form of cybercrime as compared to the male victims. Therefore, most of the cases are recorded against the male perpetrators.

---

[19] M. Aikenhead, "Revenge Pornography and Rape Culture in Canada's Nonconsensual Distribution Case Law", in Bailey, J., Flynn, A. and Henry, N. (ed.) *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*, 533-553 (Emerald Publishing Limited, Bingley, 2021).

[20] Alex Morris, 'Hunter Moore: The Most Hated Man on the Internet,' Rolling Stone (13th November 2012) *available at:* http://www.rollingstone.com/culture/news/the-most-hated-man-on-the-internet-20121113#ixzz3v3DNTckW. (last visited on 15th January, 2019).

[21] *Ibid.*

[22] *Id.* at 19.

The term "revenge porn" is often misused in the media to indicate acts that are not necessarily cases of revenge porn. There was the case of I-cloud hacking scandal in 2014, when hundreds of celebrities' saw their intimate, private and sexual image being disclosed by the hackers without their consent.[23] The recent case of Trishakar madhu leaked mms case in India.

There is a sparkling debate in the academic world revolving around the issue of whether the term "revenge pornography" is appropriate at all. The term that seems synonymous are "involuntarily"[24] pornography; "non-consensual" pornography; "image based sexual exploitation and "image based sexual abuse". All these terms refer to the non-consensual distribution of sexually explicit or intimate image created with or without the consent of the person in the image; images created by the victim himself or herself (selfie) or image that have been stolen from a hacked computer or other digital device of the victim.

3.3.1. Brief History of Revenge Porn

The concept of "revenge porn" entered the mainstream in 2012, when an FBI investigation against Hunter Moore, the founder of the website *IsAnyoneUp.com*, exposed the site's posting of sexual images/ photos and videos of individuals, often accompanied by identifying information, obtained without their consent.[25]

Moore the founder of the site had used his website *IsAnyoneUp.com* as a way to share nude images of his girlfriend among his circle of friends. After the images garnered more than 14,000 hits in a single day, Moore switched the focus of his website to nonconsensual pornography with identifying information about the individuals in the images. Despite the discovery that a majority of the images had been illegally hacked by

[23] Paul Farrel, "Nude photos of Jennifer Lawrence and other posted online by the hacker". *The Guardian,* September1, 2014.

[24] The Indian Penal Code,1860(Act 45 of 1860), s.39 state that: "A person is said to cause an effect "voluntarily" when he causes it by means whereby he intended to cause it, or by means which, at the time of employing those means, he knew or had reason to believe to be likely to cause it. Illustration A sets fire, by night, to an inhabited house in a large town, for the purpose of facilitating a robbery and thus causes the death of a person. Here, A may not have intended to cause death; and may even be sorry that death has been caused by his act; yet, if he knew that he was likely to cause death, he has caused death voluntarily".

[25] A. Levendowski, "Using Copyright to combat Revenge porn" 3*NYU Journal of Intellectual Property and Law* 422-446 (2014).

Moore's associate and not uploaded by angry exes, the vengeful nature of many of the website's posts and Moore's own admissions of revenge on women as a primary motivation for the site established the term "revenge porn".[26] Its shows that, the site was developed for the business model but not for any revenge motive.

While the now this site is defunct *IsAnyoneUp.com* is reputed to be the first revenge porn website, the practice of posting sexual images of someone without their consent was not a new practice. In the 1980s, Hustler magazine was the subject of controversy when a lawsuit revealed that many images of women in the magazine's monthly "Beaver Hunt" feature had been submitted without the women's consent.[27] With the advent of the internet, Italian researcher *Sergio Messina* began noticing a trend of what he dubbed "real core pornography"[28] where men were sharing sexual images of their ex-girlfriends in internet bulletin boards[29], because revenge porn has emerged as a computer mediated phenomenon, one can also use computer mediated methods to track its history.

According to Google Trends, since the major search engine went public in 2004, a significant peak for the term "revenge porn" in Google searches occurred in October 2008. This correlates with the timeline when in 2008 several internet porn sites announced they had received complaints about nonconsensual pornography hosted on the sites, but due to its rising popularity, several sites also emerged around this time focusing specifically on authentic and simulated revenge porn.[30]

Again in June 2015 and August 2015, Google searches for "revenge porn" peaked at their second most and highest peaks, respectively, following the June 2015 announcement by Google he pledging to remove revenge porn links upon victim's request[31] and the August 2015 announcement that lawmakers were working on the

---

[26] *Ibid.*

[27] Alexa Tsoulis Rray, "brief history of revenge porn" *New York Magazine*, 21st July, 2013, *available at:* https://nymag.com/news/features/sex/revenge-porn-2013-7/. (last visited on 7th August 2021).

[28] Real core pornography is amateur pornography distributed online, and such was first described with this name in 2000 by Sergio Messina.

[29] Alexa Tsoulis Rray, "Brief History of Revenge Porn" *New York Magazine*, 21st July, 2013, *available at:* https://nymag.com/news/features/sex/revenge-porn-2013-7/. (last visited on 7th August, 2021).

[30] *Ibid.*

[31] Emma Cueto, *Google Tackle Revenge Porn by Pledging To Remove It from Search Result.* Bustle (2015). *available at: https://www.bustle.com/articles/91760-google-tackles-revenge-porn-by-pledging-to-remove-it-from-search-results-hooray* (last visited on 3rd November, 2020).

introduction of the Intimate Privacy Protection Act, a proposed amendment to the Title 18 of the Code of Laws of the United States, that would make revenge porn and nonconsensual pornography a federal crime.[32] The Intimate Privacy Protection Act was formally proposed to the U.S. Congress by Representative *Jackie Spier* in the summer of 2016 and is pending congressional approval. 2016 presidential candidate Hillary Clinton had promised to make revenge porn illegal as part of her platform.[33]

By 2016, 'revenge pornography' had been added to both the Merriam Webster and Oxford English Dictionaries. Its translations had also come to predominate in many other languages, including French (vengeance pornographique), Spanish (pornovenganza), Chinese (色情复仇) and Japanese (リベンジポルノ). While it is most commonly associated with the leaking of private images by a vengeful ex-partner, 'revenge pornography' also communicates a wider set of harms. It is used to convey the habitual abuse of images by intimate partners, child sex abusers, rapists and sex traffickers. For them it is a valuable tool to blackmail, control and humiliate victims. 'Revenge porn' is also used to describe the actions of hackers who break into image storage accounts, scammers who extort victims for money, and voyeurs who covertly capture images in private and public. According to the data gathered by the Cyber Civil Rights Initiative, victims often have their personal details published alongside their intimate content (known as doxing), and the vast majority of victims experience severe emotional distress. In some cases, this has led to the exile, murder or suicide of victims and perpetrators.[34]

The term 'revenge pornography' reduces these severe harms to a simple 'scorned ex-boyfriend' narrative. It suggests that perpetrators are motivated only by personal vengeance and implies that victims are to blame for causing perpetrators to seek revenge.

---

[32] S. Nelson, Lawmakers unveil proposal to take nip out of revenge porn. *US News*, 14th July 2016, *available at*: http://www.usnews.com/news/articles/2016-07- 14/lawmakers-lay-bare-proposal-to-take-nip-out-of-revenge-porn.(last visited on 15th July, 2021).

[33] T. Avila, "You Tube star ask Hillary Clinton How She shall help stop Revenge Porn" *NYMag.com. available at*: https://www.thecut.com/2016/06/hillary-asked-how-shell-help-stop-revenge-porn.html#_ga= 2.56867882.1811959676.1645281638-1339713292.1645281637.(last visited on 20th December, 2020).

[34] Sophie Maddocks, From Non-consensual Pornography to Image-based Sexual Abuse: Charting the Course of a Problem with Many Names, 33(97) *Australian Feminist Studies* 345-361(2018), *available at:* https://doi.org/10.1080/08164649.2018.1542592. (last visited on 30th December, 2020).

3.3.2. Definition of Revenge Porn

For a long time, the unauthorized disclosure of intimate images has been colloquially referred to as 'revenge porn'. In recent times, however, a wave of criticisms have been directed at the use of this 'anachronistic' concept, with leading scholars in the field arguing for the adoption of more apt terminological references, including 'non-consensual pornography' [35] and 'image-based sexual abuse',[36] among others. The central argument advanced by these scholars has been that the term 'revenge porn' is both too narrow and misleading.[37] More specifically, other scholars argue that the traditional reference to 'revenge porn' does not take account of the fact that intimate images may not only be distributed as a result of a relationship coming to an end, but also in circumstances where a victim's computer has been hacked and their images have been disclosed to the public without consent. [38] Even further, it has been argued that the notion of 'revenge' somewhat suggests that the perpetrator's vengeful act can in some ways be justified as it is a response to something wrong which the victim has done. The truth, however, is that the phenomenon, in most cases, involves a malevolent response to victims exercising their autonomy to move on from or out of a relationship that might not be in their best interest.[39] As such, the 'revenge' exacted cannot, from any moral standpoint, ever be justified. Yet, still, other scholars contend that language matters and that, in this regard, it is vital to frame the phenomenon using clear, non-emotive terms that are focused on behaviour and not motivations or intentions. The researcher argued that, 'revenge' is not always the only motive behind the disclosure of intimate images; in many instances, perpetrators seek financial gain or notoriety or simply entertainment

[35] E Poole "Fighting Back against Non-Consensual Pornography" 49 *USF Law Review* 181-184(2015).
[36] *Ibid.*
[37] M. A. Franks, *Criminalizing Revenge Porn: Frequently Asked Questions* (University of Miami School of Law, Working Article,9 October 2013), *available at:* https://articles.ssrn.com/sol3/articles. cfm? abstract_id=2337998. (last visited on 10th February, 2021).
[38] M. Salter 'Responding to Revenge Porn: Gender, Justice and Online Legal Impunity', Article delivered at: *Whose Justice? Conflicted Approaches to Crime and Conflict* (University of Western Sydney, Sydney, 2013).
[39] S Bloom 'No Vengeance for 'Revenge Porn' Victims: Unravelling Why This Latest Female-Centric, Intimate-Partner Offense Is Still Legal, and Why We Should Criminalize It' 42 *Fordham Urban Law Journal* 234-237(2016).

when disclosing the intimate images of victims without their consent.[40] Moreover, the colloquial concept, it is argued, may encourage victim blaming, as it (in)advertently categorizes the victims' actions as 'pornography' when, in reality, it is anything but. In short, the term 'revenge porn' reinforces the view that victims are somehow responsible for the misuse of their intimate images because they supposedly consented to the creation of these images in the first place.

The challenge with this approach, however, is that it misrepresents victims' sexual autonomy and mischaracterizes consent when given in the context of a relationship built on confidence, with consent to the subsequent disclosure of said images to third parties. This has serious adverse implications for victims, and, in particular, the way in which these victims are treated by the law, law enforcement officials, victim support personnel, and the public at large. Given the countless objections associated with the term 'revenge porn', in this research work, researcher has used the term revenge porn.

"Revenge porn" as it is commonly understood, involves a person posting nude or sexual images of a former romantic partner online in an effort to punish that person for infidelity, terminating the relationship, or some other perceived wrongdoing. The images may have been created with the consent or active participation of the victim, or they may have been obtained via coercion or secret recording.[41]

Revenge porn has been defined as "sexually explicit image of a person posted online without that person's consent especially as a form of revenge or harassment"[42], revealing or sexually explicit images or videos of a person posted on internet, typically by a former sexual partner, without the consent of the subject and in order to cause them distress or embarrassment. Both definitions have lack clarity with regard to action that has been consent and focused on the aspect of revenge.

[40] M. A. Franks 'Drafting an Effective "Revenge Porn" Law: A Guide for Legislators' (Cyber Civil Rights, Initiative) 1.

[41] M. Aikenhead. "Revenge Pornography and Rape Culture in Canada's Nonconsensual Distribution Case Law", in J. Bailey and Henry, N. et.al. (ed). *The Emerald International Handbook of Technology-Facilitated Violence and Abuse* 533-553 (Emerald Publishing Limited, Bingley, 2021).

[42] Revenge Porn (2016) in Marriam Webster Dictionary, Online Resource.

'Revenge porn' is a media-generated term typically used to describe the online distribution of nude or sexual intimate images or videos by a jilted ex-lover without the consent of the person depicted in the image.[43]

Henry & Powell define "revenge pornography as the non-consensual distribution of sexually explicit or intimate image of another person without their consent." Although a very sensible definition, but it has two drawbacks. First is the over usage of the term consent in the definition. If the distribution is non-consensual there is no need to add "without their consent" at the end of the definition.[44]

The second, much more problematic drawback is the addition of the phrase "intimate images" in the definition. Intimate is defined as private, personal, and therefore intimate images refer to very personal or private images.

One can think of many examples of situations in which private images can have absolutely nothing to do with sexual exploitation or sexual abuse, and only affect the personal integrity, good name and honour of an individual e.g., picture of a private moment when a person is Sitting on the toilet in the bathroom, however no intimate body parts are revealed.

Another deficiency in this definition rests with the use of the term "distribution", which has a more industrial meaning as a process of marketing and supplying goods; and in law often refers to the transmission of inherited property to its heirs after taxes, debts, and costs of the estate have been paid. The term "dissemination" is therefore preferred.

It is also preferred to use the singular instead of plural in definitions since a non-consensual distribution of one image or a singular movie clip can have just as serious psychological effects on the victim as the distribution of multiple images.[45]Therefore, the definition "non consensual definition of sexually explicit image of another person" seems from the criminal law perspective better. A detailed analysis of each part of the definition is needed for further study.

---

[43] Nicola Henry and Asher Flynn Anastasia Powell "Responding to 'revenge pornography': Prevalence, nature and impacts Report to the Criminology Research Advisory Council Grant: CRG 08/15-16 March 2019.

[44] Samantha Brunick, "Revenge Porn: Can Victims Get Images off the Internet" *United States Attorneys' Bulletin* (May 2016).

[45] M. Kamal, and W. J. Newman, "Revenge Pornography: Mental Health Implications and Related Legislation, 44 *Journal of the American Academy of Psychiatry and the Law* 359-367 (2016).

Some legislation, for example the California Penal Code goes as far as demanding that the perpetrator has the criminal intent i.e., *mens rea*, to actually cause serious emotional distress, and that the depicted person suffers serious emotional distress. Other counties legislations explicitly demand that the dissemination of images seriously affects a person's privacy. This is problematic from two aspects. Firstly, perpetrators often disseminate revenge pornography for profit motive or simply for fun and have no intent to cause serious emotional distress to the victim or to negatively affect his or her privacy interests. Secondly, it opens the door to secondary victimization in the courtroom, where the victim must be examined on the question of whether he or she actually suffered serious emotional distress.

Therefore, it is the researcher is opinion of that the "ideal" legal definition does not include serious invasion of a victim's privacy. Nor does it include the perpetrator's *mens rea* to cause serious emotional distress and proof that the victims suffered serious emotional distress. Rather, the intent (*mens rea*) of the perpetrator should only cover the willful dissemination of sexually explicit content. That is to say, where the perpetrator is aware that the individual depicted in the content did not consent to such dissemination of the images/ videos, nevertheless he shares it intentionally. Conclusively, said that, 'revenge porn' is about power and powerlessness. The perpetrator seeks to exert dominance and control over his disempowered victim.

A victim who can do very little to negate the damage, especially if the images have been distributed using near instant forms of communication, such as being Emailed, uploaded to websites such as Facebook or YouTube, or sent via mobile telephone text message. However, the term 'revenge porn' connotes some sort of wrongdoing or blame attributable to the victim[46]

3.3.3. Definition of Blackmailing in Reference to Revenge Porn

The act of "blackmailing" is defined as threatening to publish personal data and then exploiting the material for public dissemination to the public, friends, and family

[46] Michelle Evans, "Regulating the Non-Consensual Sharing of Intimate Images ('Revenge Pornography') *Via* A Civil Penalty Regime: A Sex Equality Analysis, *available at:* https://www.monash.edu/__data/assets/pdf_file/0006/1981455/04_Evans.pdf. (last visited on 6th November 2021).

members. It uses photographs, videos, and other private information to intimidate others, get certain benefits, or restrict the victim's freedom to use her liberty, and exploits them sexually and emotionally in favor of the perpetrator.

It may occur to any internet platform including the Apps and social media and emails. The nature of threat and act of using coercion or arbitrary force to influence the decision of the victim for the undue favor or sexually explicit nature amounts to revenge porn when it is done after the break-up of the partner or by any friend or acquaintance, particularly this form of crime when committed by the jilted lovers, brings the definition near to revenge porn. Otherwise, the general act of threatening or blackmailing for the sexual favor is sextortion and other benefits are coving the meaning of blackmailing. It also includes a photo that has been released by the outsiders who have hacked your phone, laptops and cloud storage accounts.[47]

During the recent decades, India has increased in the cybercrime and sextortion crimes, which is basically blackmailing for sexual benefits. Although the blackmailing and sextortion used often interchangeably the meaning of the same is different with each other. Whereas the *actus res* is the same in the both forms of crime but the motive behind them are different. In terms of blackmailing the benefit, which culprit want to deduce is not always of the sexual nature whereas in terms of sextortion it is always for the sexual favor.

3.4. Difference between Consensual Pornography and Non Consentual Pornography

3.4.1. Consensual Pornography

Consensual pornography, although often faced with the criticism that it is degrading, nevertheless has consenting adults at its focus. The same cannot be said for non-consensual pornography. As non-consensual objectification affects the level to which non-consensual pornography is degrading, consensual pornography and non-consensual pornography should not be confused. The extent to which both concepts are degrading and individuals are objectified is discussed in the following.

The Oxford Dictionaries define pornography as "Printed or visual material containing the explicit description or display of sexual organs or activity, intended to

[47] Al Habsi, and A. Butler, "Blackmailon Social media: what do we know and what remain unknown?" 34(3) *Security Journal* 525-540 (2021).

stimulate sexual excitement".[48] Although this provides some clarification, the definition lacks specificity. From this definition it is clear that pornography is "material intended to stimulate sexual excitement" in the viewer. Sexual excitement in this context does not refer to the sexual excitement of the person depicted in the pornographic material nor of the producer of the material, but rather to the sexual excitement of the person watching the pornographic material. The object of production of pornography is that it is intended to sexually arouse the viewer, indicating that pornography is made with an unknown audience in mind, and therefore it is meant to be public: it is meant to be accessible to third parties not participating in the acts recorded.[49] The intended audience would find the material arousing, although unintentional viewers would not necessarily feel that way. Materials produced for a particular niche market can still be pornography, even if the average viewer would not find it arousing. That the sexual arousal referred to in the definition of Pornography regards the audience, and not the depicted individuals at the time of the production, is clear from the lack of reference towards individuals depicted: pornography is not limited to Photographs or videos, but might as well be formed of text or drawings, eliminating the presence of depicted individuals without eliminating the intended sexual arousal. The possible use of pornography to stimulate sexual excitement must therefore be what is meant by the intent to stimulate sexual excitement; otherwise, the fact that a viewer would fail to be sexually aroused by the material would question the original intent to arouse.

The use of pornography for sexual arousal in a third person is necessarily objectifying towards the individuals appearing in the pornographic material. As no personal relationship exists between the audience and the depicted individuals, the audience is unable, even if they were willing, to see and experience the depicted individuals in any other way than as objects that the audience can use in the case of pornography for their sexual arousal. It should be noted that the intention of the distributor is key with regard to the applicability of the term 'pornography'. It is the

[48] Oxford Dictionary definition, 2016.

[49] Michelle Evans, "Regulating the Non-Consensual Sharing of Intimate Images ('Revenge Pornography') *Via* A Civil Penalty Regime: A Sex Equality Analysis, available at: https://www.monash.edu/_ _data/assets/pdf_file/0006/1981455/04_Evans.pdf. (last visited on 6th November, 2021).

original distributor of nonconsensual pornography who ensures disclosure of the material, which is pornographic.

3.4.2. Non Consensual Pornography

Non-consensual pornography [50] is an umbrella term: Revenge pornography, uninvolved revenge pornography, non-voluntary pornography and edited portrayals fall under its scope. However, some scholars use the term as an equivalent of revenge pornography, even when they recognize that the term 'non-consensual pornography' is broader than 'revenge pornography'.[51] Revenge pornography is sometimes taken to be the exact and full meaning of non-consensual pornography but both terms are used for same concept. The same holds true for non-consensual pornography and non-voluntary pornography. When one replaces a specific term with a general term, the nuances of the specific terms are lost. Although there may be good arguments to use the same term for all concepts, it is nevertheless important to be able to distinguish the different concepts. If the nuances are invisible, confusion about the subject matter will increase, as was shown by the vast differences in legislation regarding 'revenge porn'. If no one knows the differences between revenge porn and non-voluntary pornography, the latter may be criminalised while the former is not, even though it was the legislator's intention to criminalise both. Therefore, this thesis argues that it is important to call the different concepts by different names, even if those names may not be ideal in reflecting the content of the concepts.

What makes non-consensual pornography pornographic, as opposed to consensual pornography which is considered pornographic from the moment it is made even before distribution, is the act of publication. This is a defining characteristic of non-consensual pornography: before it has been published the materials used in non-consensual pornography do not in themselves constitute pornography, as pornography requires an

[50] Nonconsensual pornography is also sometimes referred to as "revenge porn, "cyber rape" or "involuntary porn".

[51] Danielle Keats Citron and Mary Anne Franks, "Criminalizing Revenge Porn," 49 *Wake Forest Law Review* 346 (2014).; Mary Anne Franks, "Drafting an effective revenge porn law: A guide for legislators, 2016," available at: https://www.cybercivilrights.org/wpcontent/uploads/2016/09/Guide-for-Legislators-().'16.pdf .; Mary Anne Franks, "Criminalising Revenge Porn: A Quick Guide" *Social Science Research Network*, 9th October,2013, available at: http://dxd0ix)rg/10.2139/ssrn.23379982013. (last visited on 5th September 2021).

audience. If an image or film was not taken or made to arouse an audience, then it is not pornographic in itself. It can still become pornographic after it has been disclosed, but this discloser is unlikely to have taken place with consent of the depicted individual.[52]

Researcher conclusively says that, Revenge pornography, as the term suggests, is considered to be a form of pornography. However, it is not a form of consensual pornography. Many differences between consensual pornography and non consensual pornography (revenge porn) exist. The differences between consensual pornography and non-consensual pornography will be demarcated from the definition of pornography so as to create a thorough understanding of both concepts.

3.5. Revenge Porn, Blackmailing and Sextortion[53]

The difference between revenge porn, blackmailing and extortion can be understood through a short story. A lady contacted a lawyer seeking legal help and professional advice on what she should do; her ex-boyfriend whom she used to send her nude pictures and videos to while they were dating started to extort money from her and always threatened to blackmail her with those pictures and videos if she ever refused to send him the money he requested. This has been going on for a long time and the ex keeps coming up with requests and the threat of releasing her nudes if she ever refuses to grant him his requests.

This kind of scenario falls into the Blackmail, Revenge porn and Sextortion category of the crime of sexual exploitation: Blackmail is an act of coercion using the threat of revealing or publicising either substantially true or false information about a person or people unless certain demands are met. In many jurisdictions of the world, including Nigeria, blackmail is a statutory criminal offence, carrying punitive sanctions of jail terms for the perpetrators. In Indian legislation no term such as 'blackmail' or 'blackmailing' has been used but it is used for interchange term for extortion.

---

[52] Marthe Goudsmit, "Revenge Pornography: A Conceptual Analysis Undressing A Crime of Disclosure" *available at:* https://www.researchgate.net/publication/324360144Revenge pornography_A_conceptual_analysis_Undressing_a_crime_of_disclosure. (last visited on 3rd November, 2021).

[53] Michael Salter, "Responding to Revenge Porn: Challenging to Online Legal Impunity" in L. Comella and S. Tarrant (eds.), *New Views on Pornography: Sexuality, Politics and the Law* (Westport, 2015).

Also, Revenge porn is the illegal distribution of sexually explicit images or videos of individuals without their consent. Though the intimate images or videos may have been made or taken with the knowledge and consent of the partner, its distribution without the consent of the partner is illegal and criminal and violation of the right to privacy.

On the other hand, Sextortion is a special crime that occurs when someone threatens to distribute your nudes and private videos if you don't grant them sexual favours, or pay them some money. The name was coined out to suit the act and it has long been a crime most criminal justice systems of the world are beginning to pay much attention to. It is a special category of sexual exploitation in which victims are threatened that their private pictures and videos will be released to the public if the victim fails to meet the demand of the blackmailer; the demand which is usually payment of some amount of money.[54]

The sad news is, blackmailers and sextortionists are a greedy set of people, they never stop. They always keep coming back with requests upon requests with the same threat of releasing their victims' private contents if their demands are not met. It is clear that revenge porn is the focus of strong but conflicting sentiments that have obstructed the development of a rational policing or legal response.[55]

Efforts to protect revenge porn victims from abuse and to hold perpetrators to account are in direct conflict with the view that the harms of revenge porn are the fault, primarily, of the woman who took the picture or allowed it to be taken. This is the view articulated by revenge porn operators such as Moore, who revealed in the evident a morality of his conduct while repudiating responsibility for it. Instead, he assigned ultimate culpability to those who take erotic or sexual images of themselves in the first place.

He articulates a sexual ethos that is a paradoxical mix of prurient conservativism and libertarian machismo, in which women who take sexual photos of themselves

[54] Saloni Agrawal, "Online Sextortion" 6(1) *Indian Journal of Health, Sexuality & Culture Volume* 18 (2020), *available at:* https://iisb.org/pdf/june2020/June_2020_Final.pdf. (last visited on 20th November, 2021).

[55] Stanley Alieke, The Offence of Sexual Blackmail, Sextortion and Revenge Porn: The Rights and Remedies of Victims, available at: http://saharareporters.com/2022/02/13/offence-sexual-blackmail-sextortion-and-revenge-porn-rights-and-remedies-victims-stanley. (last visited on 15th January 2021).

deserve to be publicly shamed and humiliated, and do not deserve the benefit of legal rights and protections but those that humiliate them do. However, the allegations against him suggest that this served as a rationale behind which a more complex set of calculations were at play, in which Moore allegedly sought to meet viewer demand for more images and thus maintain the profitability of his site by engaging a hacker.

3.6. Right to Privacy and Dignity *vis-a-vis* Revenge Porn and Blackmailing

❖ **Right to Privacy**

It is difficult to describe what "Privacy" is but an attempt was made by Warren and Brandeis in 1890,[56] the description of it as the 'right to be let alone'. The right to privacy includes protection of the individual's autonomy, wellbeing, and right to self-realization. This right considers privacy to be inherent within human dignity. Privacy allows individuals to protect their autonomous space and grants them the ability to control their lives by controlling the dissemination of information about them. In this sense, the right to privacy includes an individual's decisions regarding his own body and establishes an individual's right to disengage from society and to be left alone.[57] The justification of the right to privacy in terms of human dignity is a classic liberal position that regards disengagement as a human need.[58] This is based on a Kantian conception according to which human beings are ends in themselves and should not be treated as a means to other ends.[59] Privacy is the core of one's personal autonomy, and its infringement, irrespective of the consequences, is prohibited.

Another type of justification regards privacy as a means of achieving other important ends. Thus, there are those who regard the right to privacy as a means of satisfying an individual's psychological needs.[60] Without the right to privacy, one cannot fulfill oneself in the best possible way. People need privacy in order to have experiences,

[56] S. Warren and L. Brandeis, "The Right to Privacy" 4 *Harvard Law Review* 193(1890), *available at:* http://links.jstor.org/sici?sici=0017811X%2818901215%294%3A5%3C193%3ATRTP%3E2.0.CO%3B2-C (last visited on 15th July, 2021).

[57] Thomas P Crocker, "From Privacy to Liberty: the Fourth Amendment after Lawrence" 57 *UCLA Law Review1*, 23(2009).

[58] Randy K. Lippert and Kevin Walby, "Governing through Privacy: Authoritarian Liberalism, Law and Privacy knowledge" 12 *Law Culture & Human* 329-333 (2013).

[59] Immanuel Kant, *The Philosophy of Law* (W. Hastie Trans., 1887).

[60] Sidney M. Jourard, "Some Psychological aspect of Privacy" 31 *Law and Contemporary Problems* 307 (1966), *available at:* https://lcp.law.duke.edu/. (last visited on 3rd September, 2021).

to learn, to make mistakes, and to think. Without personal space, people cannot develop themselves and control their lives as they wish.[61] Furthermore, the right to privacy is essential in ensuring trust between people and creating conditions of mutual respect, love, and friendship.

Privacy is also viewed as the basis for a democratic regime. This justification falls outside the realm of individual rights and emphasizes the general good. Being able to live without having one's activities monitored is a freedom granted to individuals in a democracy, which makes trust possible between a country and its citizens. [62]

A private space that is not under observation by the state is essential in a pluralistic society that allows for a variety of voices. Privacy also enables criticism of the government and is vital in the development of views that eventually make their way into the political sphere.

Researcher has no dispute with the fact that revenge porn violates the privacy of the victims. However, in researcher opinion's, the infringement of privacy does not reflect the full impact of the violation and its essence. Unlike a trivial violation of a person's privacy that harms the aforementioned interests, revenge porn amounts to sexual abuse for the following reasons. First, the mental, emotional, and physical harm inflicted on many revenge porn victims is similar in nature to that caused to victims of classic sexual assault, as noted earlier, studies indicate that depression, anorexia, anxiety, and sometimes even suicidal tendency. In the cases of sexual assault, consistent with a subset of harms experienced following rape.[63] This fact can provide support for categorizing the offense as sexual rather than as a violation of privacy. Second, and more importantly, the protected values in the context of revenge porn are similar in nature to those that underlie classic sexual offenses. Indian Supreme courts have determined that the protected values underlying rape include sexual privacy, sexual autonomy, and human dignity.[64] Although the values of human dignity and human autonomy are also infringed on in the case of a

[61] Ruth Gavison, "Privacy and Limits of Law" 89 *Yale law Journal* 421-435(1980), *available at:* https://www.jstor.org/stable/pdf/795891.pdf?refreqid=excelsior%3Aa69621708b426c3274a05ea64b89984d&ab_segments=&origin. (last visited on 20th September 2021).

[62] Paul Bernal, Data gathering, Surveillance and Human Rights: Recasting the Debate, 1 *International Journal of Cyber Policy* 249 (2016).

[63] Rebecca Campbell, The Psychological Impact of Rape Victims Experiences with Legal, Medical and Mental Health Systems" 63 *Americal Psychological Journal* 702 (2008).

[64] *Navtej Singh Johar* v. *Union of India,* AIR 2018 SC 432.

classic violation of privacy, the nature of a violation of human dignity and human autonomy in the case of revenge porn is completely different and justifies the categorization of revenge porn as a sexual offense and not just as a privacy offense.

Right to privacy may be looked through the lenses of the European Commission on Human Right (ECHR) Jurisprudence. When images of individuals are involved, there are sensitivities surrounding the taking and publication of such images. ECHR jurisprudence clearly includes the right to protection of one's image, as set out in ***Von Hannover Case***:

"*Freedom of expression includes the publication of photos ... This is nonetheless an area in which the protection of the rights and reputation of others takes on particular importance, as the photos may contain very personal or even intimate information about an individual or his or her family*."[65]

Further clarity is provided through the ***Von Hannover cases*** and, following **Von *Hannover* v. *Germany No. 2***, the Court laid down criteria to be applied when balancing Art. 8 and 1025 of the ECHR. Under the laws of England and Wales, privacy protection is reliant upon the concept of the claimant having a 'reasonable expectation of privacy', with two related questions asked:

(i) Essentially the touchstone of private life is whether in respect of the disclosed facts the person in question had a reasonable expectation of privacy, e.g. Is Article 8 ECHR (the right to respect for private and family life) engaged?[66]

(ii) If so, does this expectation of privacy outweigh the publisher's Article 10 ECHR rights to freedom of expression?

Although it has been emphasized how establishing a reasonable expectation of privacy takes into account all the circumstances of the case, the need and sensibility of such a test has been questioned, particularly in circumstances where information is obviously private.[67]

---

[65] *Von Hannover* v. *Germany (No 2)* 15EHRR 103(2012).

[66] Eric Barendt, "Problems with the "Reasonable Expectation of Privacy" Test' 8(2*) Journal of Media Law* 129–37 (2016), *available at:* https://doi.org/10.1080/17577632.2021.1933704. (last visited on 7th July, 2019).

[67] Holly Hancock, "The Impact of The Image on Personal Life: Is Current Law out of Focus?" 13(1) *Journal of Media Law*, 54-80(2021), *available at:* https://doi.org/10.1080/ 17577632.2021.1933704.(last visited on 7th July, 2019).

❖ **Human Dignity *vis-a-vis* Women's Dignity**

To live is to live with dignity. The draftsmen of the Constitution defined their vision of the society in which constitutional values would be attained by emphasising, among other freedoms, liberty and dignity. So, fundamental is dignity that it permeates the core of the rights guaranteed to the individual by Part III of Constitution India. Dignity is the core which unites the fundamental rights because the fundamental rights seek to achieve for each individual the dignity of existence. Privacy with its attendant values assures dignity to the individual and it is only when life can be enjoyed with dignity can liberty be of true substance. Privacy ensures the fulfilment of dignity and is a core value which the protection of life and liberty is intended to achieve."[68]

Revenge porn violates the dignity of the victim, humiliates her sexually, and degrades her. Some victims avoid leaving their homes, fearing that any one they meet may have seen the disseminated image. In this sense, the sexual humiliation produced by revenge porn may be much more severe than that caused by an indecent act, which is a one-time, isolated experience. As previously stated, victims of revenge porn describe an experience that is akin to being raped. In other words, the victim also experiences desecration of her body in the case of revenge porn.

Another feature of revenge porn is that it reduces the victim's identity to her intimate organs, degrading her moral status and dignity. This isn't to argue that a person's sexuality is the only aspect of his or her identity. Intellectual and creative qualities, for example, are also aspects of a person's personality, and their privacy must be respected in order to avoid intellectual uniformity. However, a violation of privacy in the intellectual context, for example, does not restrict a person's identity to his or her intellectual capacities alone, and hence the injury to dignity in this scenario is little compared to the loss to dignity in the case of a violation of sexual privacy.

Furthermore, and more than other types of privacy, sexual privacy allows a person to feel autonomous as an individual rather than as a person belonging to the collective. As *Samuel Warren* and *Louis Brandeis* emphasized the psychological need for people to disengage themselves from society and to create an inviolate personality for themselves. Every person is a different entity, and when one's sexual privacy is infringed, one's

[68] *Saumya Tiwari* v. *State of U.P*, Date of Decision 16th December, 2021.

dignity is also violated. Revenge porn humiliates and degrades a woman, transforming her body into an object and she no longer belongs to herself.[69]

The fact that human dignity is violated in the case of both nonsexual infringement of privacy and revenge porn does not mean that they should both be included under the rubric of infringement of privacy. It should distinguish between the nonconsensual publication of a non-intimate image of a person and the nonconsensual publication of a nude image of a woman in terms of human dignity breaches. The degradation and humiliation in the second case are concrete, evident, and violate the women's dignity. Not only is the women's privacy infringed on in the sense that her right to be left alone is violated, but also desecrates her body and compromises her sexual dignity, in contrast, the effect on human dignity in the capture of a non-intimate picture in a private domain is not likely to cause any serious humiliation and does not have consequences beyond that situation.[70]

❖ Right To Privacy Under Constitution Of India

Privacy is a complex concept that has been difficult to define. In many circumstances, the harms that arise from violations of privacy are difficult to identify because very often they are intangible. Despite its amorphous nature, there are a number of reasons why protecting privacy is considered valuable. The protection of privacy permits individuals to plan and carry out their lives without unnecessary intrusion.[71] Informational privacy is often understood as the freedom of individuals "to determine for themselves when, how, and to what extent information about them is communicated to others"[72] and this freedom allows for individuals to protect themselves from harm. However, not all information about an individual is necessarily private and deserving of protection. It is for a legal framework to determine where affording such freedom is appropriate and where it is not.

---

[69] S. Warren and L. Brandeis, "The Right to Privacy" 4 *Harvard Law Review* 193(1890), *available at:* http://links.jstor.org/sici?sici=0017811X%2818901215%294%3A5%3C193%3ATRTP%3E2.0.CO%3B2-C. (last visited on 4th August 2019).

[70] Roni Rosenberg And Hadar Dancig Rosenberg, Reconceptualizing Revenge Porn, 63(199) *Arizona Law Review* 199-228(2021).

[71] Our data, worth a water bottle? *The Hindu*, 21st January, 2018.

[72] Alan Westin, 'Privacy and Freedom', 7 (Atheneum, 1967), *available at:* https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20. (last visited on 5th November, 2019).

Privacy, in its simplest sense, allows each human being to be left alone in a core which is inviolable. Yet the autonomy of the individual is conditioned by her relationships with the rest of society. Those relationships may and do often pose questions to autonomy and free choice. The overarching presence of state and nonstate entities regulates aspects of social existence which bear upon the freedom of the individual. The preservation of constitutional liberty is, so to speak, work in progress. Challenges have to be addressed to existing problems. Equally, new challenges have to be dealt with in terms of a constitutional understanding of where liberty places an individual in the context of a social order. The emergence of new challenges is exemplified by this case, where the debate on privacy is being analysed in the context of global information based society. In an age where information technology governs virtually every aspect of our lives, the task before the Court is to impart constitutional meaning to individual liberty in an interconnected world. While we revisit the question whether our constitution protects privacy as an elemental principle, the Court has to be sensitive to the needs of and the opportunities and dangers posed to liberty in a digital world. While discussing the right to privacy in Indian perspective**,** both men and women are vulnerable to unwelcome privacy invasions in cyberspace. Indeed, in major respects, men and women sail through cyberspace in the same leaky boat. We can analogize cyberspace to a vast sea into which spills the private data of those who navigate its swelling waters.[73]

The right to privacy by itself has not been identified under Constitution of India. As a concept it may be too broad and moralistic to define it judicially. The Constitution of India has not guaranteed the right to privacy as a fundamental right to the citizens but nevertheless, the Supreme Court has come to the rescue of common citizen, time and again by construing "right to privacy" as a part of the right to "protection of life and personal liberty".

Even the fundamental right "to freedom of speech and expression" as enumerated in Art. 19(1)(a) comes with reasonable restrictions imposed by the state relating to: defamation; contempt of court; decency or morality; security of the state; friendly

[73] Allen,and L. Anita, "Gender and Privacy in Cyberspace" *Faculty Scholarship at Penn Law* 789 (2000). *available at:* https://scholarship.law.upenn.edu/faculty_scholarship/789. (last visited on 6th November 2021).

relations with foreign states; incitement to an offence; public order; maintenance of the sovereignty and integrity of India. Thus, the right to privacy is limited against defamation, decency or morality.

Moreover, the right to privacy could also be read into Art. 21 of the Constitution which states that "*No person shall be deprived of his life or personal liberty except according to procedures established by law*". In the context of personal liberty, the Supreme Court has observed [74] that "*those who feel called upon to deprive other persons of their personal liberty in the discharge of what they conceive to be their duty must strictly and scrupulously observe the forms and rules of the law*".

Keeping in view the scope of 'personal liberty', Art. 21 has been turned into a safeguard against arbitrary legislation. ***Kharak Singh* v. *State of Uttar Pradesh***,[75] where the appellant was being harassed by police under regulation 236(b) of UP Police Regulation, which permits for the domicillary, visits at night. The Supreme Court held that the regulation 236 is unconstitutional and it is violation of Art. 21 of the Constitution. It concluded that the Art. 21 of the Constitution to include "right to privacy" as a part of the right to "protection of life and personal liberty". In fact, it was the minority view expressed by *Justice Subba Rao* that equated 'personal liberty' with 'privacy', that "the concept of liberty in Art. 21 was comprehensive enough to include and that a person's house, where he lives with his family is his castle and that nothing deleterious to a man's physical happiness and health than a calculated interference with his privacy"

Similarly, in ***Gobind* v. *State of Madhya Pradesh***,[76] the Court observed that "domiciliary visits and picketing by the police should be reduced to the clearest cases of danger to community security and not routine follow up at the end of a conviction or release from prison or at the whim of a police officer. In truth, legality apart, this regulation ill accord with the essence of personal freedoms and the state will do well to revise these old police regulations verging perilously near unconstitutionality"
In fact, *Mathew J.* stated the law in the following words:

[74] *Ram Narain* v. *State of Bombay* (1952).
[75] AIR 1963 SC 1295.
[76] AIR 1975 SC 1378.

"*Privacy-dignity claims deserve to be examined with care and to be denied only when an important countervailing interest is shown to be superior. If the Court does find that a claimed right is entitled to protection as a fundamental privacy right, a law infringing it must satisfy the compelling State interest test".*

Privacy primarily concerns the individual. It therefore relates to and overlaps with the concept of liberty. The most serious advocate of privacy must confess that there are serious problems of defining the essence and scope of the right. Privacy interest in autonomy must also be placed in the context of other rights and values.

Any right to privacy must encompass and protect the personal intimacies of the home, the family, marriage, motherhood, procreation and child rearing...

Another dimension has been added to the recognition of privacy rights, when in ***State* v. *Charulata Joshi*** [77] the Supreme Court held that "the constitutional right to freedom of speech and expression conferred by Article 19(1) (a) of the Constitution which includes the freedom of the press is not an absolute right. The press must first obtain the willingness of the person sought to be interviewed and no court can pass any order if the person to be interviewed expresses his unwillingness".

Further in ***R. Rajagopal* v. *State of Tamil Nadu***,[78] where the question was:

(i) Whether a citizen of this country can prevent another person from writing his life-story or biography

(ii) Whether freedom of press guaranteed by Art. 19(1) (a) entitle the press to publish such unauthorised account of a citizen's life and activities and if so to what extent and in what circumstances? and

(iii) Whether the public officials, who apprehend that they or their colleagues may be defamed, can impose a prior restraint on the press to prevent such publication?

Justice B.P. Jeevan Reddy observed that:

"*The right to privacy is implicit in the right to life and liberty guaranteed to the citizens of this country by Article 21. It is a "right to be let alone" 'A citizen has a right to safeguard the privacy of his own, his family, marriage, procreation' motherhood, child bearing and education among other matters. None can publish anything concerning the*

[77] (1999) 4SCC 65.
[78] AIR 1995 SC 264.

above matters without his consent, whether truthful or otherwise and whether laudatory or critical. If he does so, he would be violating the right to privacy of the person concerned and would be liable in an action for damages".

The rule aforesaid is subject to the exception, that any publication concerning the aforesaid aspects becomes unobjectionable if such publication is based upon public records including Court records. This is for the reason that once a matter becomes a matter of public record, the right to privacy no longer subsists and it becomes a legitimate subject for comment by press and media among others...

In the case of public officials, it is obvious, right to privacy, or for that matter' the remedy of action for damages is simply not available with respect to their acts and conduct relevant to the discharge of their official duties. This is so even where publication is based upon and statements, which are not true unless the official establishes that the publication was (by the defendant) with reckless regard for truth. In such a case, it would be enough the defendant (member of the press or media) to prove that he acted after a reasonable fortification of the facts; it is not necessary for him to prove that what he has written is true.

The Court decided that the petitioners have the right to publish what they claim to be Auto Shankar's story/autobiography based on public sources, even without his consent or approval. However, if they go beyond that and publish his personal story, they may be infringing on his right to privacy, and they will be considered legally culpable for the repercussions. Similarly, the state or its authorities are powerless to restrict or restrain the publication in question.

In ***People's Union for Civil Liberties (PUCL)* v. *Union of India***,[79] the Supreme Court held that the telephone tapping by Government under section 5(2) of Telegraph Act amounts infraction of Art. 21. Right to privacy is a part of the right to "life" and "personal liberty" enshrined under Art. 21 of the Constitution. Once the facts in a given case constitute a right to privacy, Art. 21 is attracted. The said right cannot be curtailed "except according to procedure established by law"

The right to privacy by itself has not been identified under the Constitution. As a concept it may be too broad and moralistic to define it judicially. Whether right to

[79] AIR 1997 SC 568.

privacy can be claimed or has been infringed in a given case would depend on the facts of the said case. But the right to hold a telephone conversation in the privacy of one's home or office without interference can certainly be claimed as "right to privacy". Conversations on the telephone are often of an intimate and confidential character. Telephone conversation is a part of modern man's life. Telephone conversation is an important facet of a man's private life. Right to privacy would certainly include telephone conversation in the privacy of one's home or office. Telephone tapping would, thus, infract Article 21 of the Constitution of India unless it is permitted under the procedure established by law.

Yet another dimension to right to privacy was added in ***'X'* v. *Hospital 'Z'***,[80] where the appellant's blood was to be transfused to another but he was tested HIV (+) at the respondent's hospital. On the account of disclosure of this fact, the appellant's proposed marriage to one 'A' which had been accepted, was called off. Moreover, he was severally criticised and was also ostracised by the community. The appellant approached the National Consumer Disputes Redressal Commission (NCDRC) for damages against the respondents on the ground that the information required under medical ethics, to be kept secret, was disclosed illegally and that therefore, the respondents were liable to pay damages to the appellant. The Commission dismissed the Petition on the ground that the appellant could seek his remedy in the civil court.

Before the Supreme Court the appellant contended that the principle of "duty of care" applicable to persons in medical profession included the duty to maintain confidentiality and that the said duty had a correlative right vested in the patient that whatever came to the knowledge of the doctor would not be divulged. The appellant added that for violating that duty as well as for violating the appellant's right to privacy, the respondents were liable for damages to the appellant

Apex Court, while rejecting the appellant's contentions, held that the right to privacy has been culled out of the provisions of Art. 21 and other provisions of the Constitution relating to the Fundamental Rights read with the Directive Principles of State Policy. Right of privacy may, apart from contract, also arise out of a particular specific relationship, which may be commercial, matrimonial, or even political. Doctor-

[80] (2003) 1 SCC 500.

patient relationship, though basically commercial, is professionally, a matter of confidence and, therefore, doctors are morally and ethically bound to maintain confidentiality. In such a situation, public disclosure of even true private facts may amount to an invasion of the right of privacy which may sometimes lead to the clash of one person's "right to be let alone" with another person's right to be informed. This is also applicable in case of revenge porn and blackmailing.

The right, however, is not absolute and may be lawfully restricted for the prevention of crime, disorder or protection of health or morals or protection of rights and freedom of others.

Where there is a clash of two fundamental rights, as in this case, right of privacy of one party as part of right to life and right to lead a healthy life of another party which is also a fundamental right under Art. 21, the right which would advance the public morality or public interest, would alone be enforced through the process of court, for the reason that moral consideration cannot be kept at bay and the judges are not expected to sit as mute structures of clay in the hall known as the courtroom, but have to be sensitive, "in the sense that they must keep their fingers firmly upon the pulse of the accepted morality of the day".

Further in ***Sharda* v. *Dharmpal***,[81] it was held by the Supreme Court that "*the right to privacy in terms of Art. 21 of the Constitution is not an absolute right. If there were a conflict between fundamental rights of two parties, that right which advances public morality would prevail*."

In ***District Registrar and Collector* v. *Canara Bank***,[82] it was held by the Hon'ble Supreme Court that:

"*the exclusion of illegitimate intrusions into privacy depends on the nature of the right being asserted and the way in which it is brought into play; it is at this point that the context becomes crucial, to inform substantive judgment. If these factors are relevant for defining the right to privacy, they are quite relevant whenever there is invasion of that right by way of searches and seizures at the instance of the State*."

[81] AIR 2003 SC 3450.
[82] 2005 1 SCC 496.

Similarly, in ***State of Maharashtra* v. *Madhukar Narayan Mardikar***,[83] the Supreme Court protected the right to privacy of a prostitute. It was held that "even a woman of easy virtue is entitled to her privacy and no one can invade her privacy as and when he likes."

Also, in ***Malak Singh* v. *State of Punjab and Haryana***,[84] wherein an application was filed by the applicants seeking to remove their names from the surveillance register maintained by the police station of their jurisdiction under the Punjab Police Rules. Court while upholding the jurisdiction of Punjab Police made observations on the mode of surveillance and emphasised that surveillance must be conducted as per rules. However, in ***Bhavesh Jayanti Lakhani* v. *State of Maharashtra,***[85] the Court observed that "*no such guidelines, however, has been laid down in respect of surveillance conducted pursuant to a red corner or yellow corner notice (of Interpol). The Central Government and in particular the Ministry of External Affairs, in our opinion, should frame appropriate guidelines in this behalf*". Further in ***Ram Jethmalani* v. *Union of India,*** the Supreme Court has dealt with the right to privacy elaborately and held as under:

"*Right to privacy is an integral part of right to life, This is a cherished constitutional value, and it is important that human beings should be allowed domains of freedom that are free of public scrutiny unless they act in an unlawful manner...*"

The solution to the problem of one zone of constitutional values being abrogated cannot be the formation of another zone of constitutional values being abrogated... The concept of fundamental rights, such as the right to privacy as part of the right to life, involves more than just prohibiting the state from violating them. It also involves the state's responsibility to defend them against the activities of others in society, even while those persons are exercising fundamental rights.

Privacy debate has taken a different turn when during the "***Aadhaar case*"**[86] hearings before the Supreme Court, Union of India took a stand, whether privacy is a fundamental right, this needs to be examined by a larger Constitutional Bench as the previous judgments have failed to clear the confusion?

[83] AIR 1991 SC 207.
[84] AIR 1981 SC 760.
[85] (1991) 1 SCC 57.
[86] *K.S. Puttaswamy(Retd.)* v. *Union of India* , AIR 2017 SC 4161.

This confusion was decided in the case ***K.S. Puttaswamy (Retd.)* v. *Union of India***.[87] This case was decided by 9 Judge's Constitutional Bench, held that "*the right to privacy was integral to freedoms guaranteed across Fundamental Rights, and was an intrinsic aspect of dignity, autonomy and liberty*."

Justice *Chandrachud* in the ***Puttaswamy*** judgment, clearly addresses 'the woman question' by dedicating an entire section of his judgement, with reference to the feminist critique of the privacy doctrine. He incorporates this American white, middle class voice by placing privacy in the individual, enshrining decisional privacy as a constitutional right. It makes interest of women in intimate privacy inviolable.[88]

3.7. Impact of Revenge Porn and Blackmailing on Women Victim

Revenge porn impacts victim in ways that are very similar to those of sexual abuse or harassment. The impacts experienced by survivors of revenge porn including feelings of permanence and shame. The Researcher has recognised multiple other consequences that distribution can have on victims of the revenge porn and blackmailing.

There is no uniformity regarding the trauma and violence impacted upon the victim differently and in multitude of ways. But, it is important to recognise patterns of responses and impacts in order to understand the true effects that nonconsensual sexual image dissemination on online platforms. The Researcher discussed the instances of blackmailing, losing of jobs or being unable to find work, and regular stalking. It is also considered more psychological effects it means impacting mental health such as Post-traumatic Stress Disorder (PTSD), anxiety, a feeling of no control, depression, and suicide. With the above in mind the researcher has also considered the existence of a 'culture of fear' which extends beyond the immediate survivors of revenge porn and blackmailing.[89]

[87] *K.S. Puttaswamy(Retd.)* v. *Union of India* , AIR 2017 SC 4161.

[88] Devangana Kuthari , "Revisiting Puttaswamy: A Feminist Critique- The Woman Question and The Physiological Paradigm of Abortion in Privacy" 2 *Indian Journal Of Legal Theory* 6 (2020).

[89] Roshni D'souza, The dangerous rise of revenge porn in India. *available at:* https://madrascourier.com/opinion/the-dangerous-rise-of-revenge-porn-in-india/.(last visited on 21st December, 2021).

Victim's of revenge porn and blackmailing often experience severe reaction to the posting of the nonconsensual pornography. The victim feels shame and humiliation from material as well as anxiety, depression and suicidal thought.[90]

The use of blackmail as a tool in instances of revenge porn seems an almost common narrative; the shame aspect surrounding the images make the threat of their posting an effective tool for the blackmailer.[91] A case from Delhi was published on the 20th of December 2020, in which a man was arrested for blackmailing 100 women using fictitious nude photos. In this case, a 26-year-old accused of blackmailing at least 100 women was detained in Delhi for reportedly attempting to extort money from a woman in south Delhi by threatening to circulate her sexual images on social media.[92] The level of power that the abuser is able to exert over their victims with the threat of revenge porn is deeply unsettling. Being able to coerce unwilling partners into sex is nothing less than rape, and a further validation of the argument that nonconsensual sexual images or the threat of them is a violent abuse of power. Revenge over a partner is not the only reason for abusing the power that society imbues the possession of these sexual images; profit, coercion, and torment have all apparently been motivators with which to blackmail someone. Blackmail is a clear example of how the propagation of nonconsensual sexual images expands the potential for violations against an individual's right to privacy; the sharing of sexual images without consent is rarely the only impact that survivors have to contend with.

Another significant mass consequence of revenge porn is a victim of revenge porn was unable to find work or being terminated from their existing job/work. There have been reports of images or videos being sent directly to her colleagues or places of work, as well as the photos being available online.

There have been multiple examples of teachers and government employees being fired from their jobs after the intimate images were posted online, due to reputation of company and institution in other countries. Compounded with losing a job can be the inability of finding a new one; a 2009 study commissioned by Microsoft found that 80%

[90] *Ibid.*

[91] Sara Polak and Daniel Trottier(ed.), *Violence and Trolling on Social Media* 180 (Amsterdam University Press, Netherland, 2020).

[92] "Ghaziabad: Man held for morphing images of women, blackmailing them", *Times of India*, 20th Febuary, 2022.

of employers use search engines to find out more about job applicants and that 70% of the time they reject applicants because of these findings. Regardless of the arguments concerning the morality or fairness of this it's a fact that employers don't want to hire individuals whose search results they fear could impact negatively upon them.

Therefore, the economic ramifications can be huge for an individual who as a result of the violation itself is already in a vulnerable position. An inability to financially support themselves, and the stress, fear and uncertainty this would undoubtedly cause to further intensify the impact of nonconsensual sexual images.

There are high percentages of revenge porn that are accompanied by the victim's full name and contact information, but a further possible aspect of this violation of privacy is stalking. *Noah Berlatsky* states that, "the web has made it possible to crowd source misogyny and stalking"[93] and that statement certainly rings true of nonconsensual sexual images. When a survivor's phone number was included with the photos, she received calls every six minutes on average, while another received death threats directed at her and her family. Stalking has been linked to significant emotional and behavioural repercussions, as well as health issues and thoughts of suicide, according to studies. Because of the fear of physical harm and the unrelenting nature of the abuse, it can spread beyond the online realm. This is another method of perpetuating control over the victim and ensuring that they cannot escape from the abuse.[94]

Unauthorized disclosure of intimate images cause a great impact on the victim such as humiliation, distress, embarrassment, and shame, which could not be ignored. The effects of revenge porn and blackmailing offence are very severe upon victim, its causing chaos on their professions, families, and even their health and well-being.[95] Victims struggle with anxiety and panic attacks and can develop ailments such as anorexia nervosa and depression. Some victims have lost jobs, been forced to change

[93] Afroditi Pina, "The Malevolent Side of Revenge Porn Proclivity: Dark Personality Traits and Sexist Ideology" 8(1) *International Journal of Technoethics* 31(2017), *available at:* https://www.igiglobal.com/gateway/article/178531#pnlRecommendationForm. (last visited on 4th January, 2021).

[94] Francesca Coletti, Revenge Porn: The Concept and Practice of Combatting Nonconsensual Sexual Images in Europe (Published Dessertation in 2017), University of Latvia, European Master's Degree in Human Rights and Democratisation).

[95] Justine Mitchell "Censorship in Cyberspace: Closing the Net on Revenge Porn" 25(8) *Entertainment Law Review* 283- 283 (2014).

schools, move house or change their name after being subjected to stalking and harassment, suffering sometimes irreparable reputational damage and emotional harm. Consequently, some victims have committed suicide as a direct result of having their images distributed in this way. Victims can suffer 'loss of personal dignity, a lost sense of security, lowered respect from family and friends, and a greater difficulty in maintaining and securing future romantic relationships.' [96] *Citron and Franks* highlight the professional costs of revenge porn, explaining how victims are in danger of losing jobs or not getting a job at all, when an Internet search by a prospective employer prominently displays naked pictures or videos at the top of its results.[98] *Citron and Franks* also raise the issue of domestic abuse, observing how the threat of disclosing images is used by abusers to keep their partners 'under control, making good the threat once their partners find the courage to leave.'[97]

1.7. Recent Case of Cybercrime against Women in India

❖ Global Jindal Rape Case (2015)[98]

The fact of the case is that, victim and accused met on children day in 2013, victim is 18years old of management student, where as accused is 20 year old and a law student at O. P. Global Jindal University, Sonipat. Later on as their friendship grew, exchange of messages became frequent. Subject to the visiting hours of hostel, they made a point to meet after class and stay out till 10.00.P.M, the cut hours to return to hostel. But all became sour on 11th April, 2015, when the victim approached the university administration and narrated the whole incident to the administration. The victim alleged that accused Hardik Sikri had been blackmailing her for a year and half and had forced her to have sexual relation with him and two other his friend Vikas Garg and Karan Chabra.

---

[96] Zak Franklin, "Justice for Revenge Porn Victims: Legal Theories to Overcome Claims of Civil Immunity by Operators of Revenge Porn Websites" 102 *California Law Review* 1303-1307 (2014).

[97] *Available at:* https://law.yale.edu/sites/default/files/area/center/isp/documents/daniellecitron_-criminalizing_revenge_porn_-_fesc.pdf. (last visited on 21st December, 2021).

[98] "Hisar: Blackmail, rape, arrest of 3 law students has campus in turmoil" *Indian Express*, 28th May 2015, *available at:* www.Indianexpress.com/article/india/india-others/hisar-blackmail-rape-arrest-of-3-law-students-has-campus-in-turmoil/ (last visited on 1st December, 2021).

In her complaint registered with Rai Police Station in Sonipat the victim girl stated that "she met him in 2013 on children's day and befriended him. A month later our friendship grew and he began forcing me to send him explicit images of myself. Even when I refused he forced me that I will have to do so. Following this he began blackmailing me into having sexual relations with him and threatening that he will circulate the intimate pictures widely. According to the victim, Sikri soon began forcing her to have sexual relations with two of his roommates. "The accused (Sikri) would sexually harass me on campus only after 10 pm. While one of the accused established frequent sexual relations with me, I was forced to maintain this with the other two on three separate occasions," she told police. Police arrested the three accuse on the same day.

The three accused were convicted by trial court for raping a fellow student but Punjab and Haryana High Court had suspended their conviction on the ground that the women were "promiscuous" and had "casual sexual escapades". The victim approached the Supreme Court, challenging the high court order of suspension of their sentences. The victim alleged that the accused have been blackmailing her as they have her objectionable pictures and expressed apprehension of circulation of those photograph.[99]

❖ **Raj Kundra Case (2021)**

In July 2021 a celebrity and business man Raj kundra was arrested for production and broadcasting of pornographic content on some OTT platforms or App based platforms. Mumbai police linked this case with the racket of production and dissemination of pornography in Mumbai using android based apps or through transferable medium to which the accused denyied all charges. While the investigation was going on Kundra secured a Metropolitan magistrate's order to shift the remand into custody which Kundra claimed in high court for the interim bail order as the Cr.P.C. Sec. 41-A order is breached for which the investigation officer mentioned that I can't wait for the arrest when the evidence was destroyed before me, whereas the court is not taking any substantive decision for the starting of trail in the lack of evidences.

Raj Kundra and his associate have been booked under sections 420 (cheating), 34 (common intention), 292 and 293 (related to obscene and indecent advertisements and

[99] *Indian Express* 7th February, 2018.

displays) of Indian Penal Code, 1860 besides relevant sections of the Information Technology Act, 2000 and the Indecent Representation of Women (Prohibition) Act, 2006.[100]

Although such acts and sections are applied in this case however the picture of investigative challenges in these cases where finding any evidence is quite tough whereas destroying it is quite easy and can bring no legal action as it is not covered under the definitions of the crime because the procedural steps of arrest and investigation are also not clear to the police in such cases where the content production and tools of dissemination are considered to be in traditional scenes of tools or weapons of the crime whereas the technicality and operation of such modern tools are quite different than the traditional scenes where there is no law to make the owner of the platform liable for the same. Researcher has tried to pull the procedural complexity and challenges due to absence of the direct definition of such crime and procedural law and expertise for the fair investigation of the case. As the matter is still considered to be just an indecent representation of women and cheating the bail of such victim is quite easy giving lot of time to destroy the evidences and influence the witnesses as in this case too no one is pressing against the accused Raj Kundra for any indecent representation or breach of privacy or dignity or any other crime of indecent representation. The trial is pending before the court of law for any substantive judicial activism.

- **Trisha Kar Madhu MMS Leaked Case (2021)**

This case is related to the Bhojpuri Actress Trishkar Madhu, as her intimate video was leaked on various social media platform. Thereafter, she was trolled and bullied by the fans. Trisha kar madhu has been trolled repeatedly after her MMS went viral in August 2021, in which she was shown in an objectionable intimate position with an unidentified man. In a 22-minute leaked film that was widely shared on social media sites, the actress was shown in a compromising position. Trisha has now apologised for her actions and provided clarifications through her social media platform. There was no FIR registered by the actress. Every case is not only for revenge, harassment or for

[100] "Pornography Case: Supreme Court relief from arrest to Raj Kundra", *Times of India*, 16th December 2021.

embarrassment some time the celebrities leaked their intimate images / videos online for gaining popularity.

❖ **Bulli Bai App and Sulli Deal App Case(2022)**

Two recent cases of online sexual harassment against Muslim women have managed to hit the headlines with alleged perpetrators being arrested, legal experts stressed fighting these cases is often an uphill battle for victims.

"Sulli Deals" was an open-source app created by a Trads group which posted photographs and personal information of some 100 Muslim women online. Thereafter an FIR was filed by the Delhi Police with National Commission for Women India for taking suo moto cognisance of the matter on 8th July The identity of the creator was revealed to be Aumkareshwar Thakur, a BCA Student from Indore, Madhya Pradesh. On 9th January 2022, Thakur, who created the app to "defame" Muslim women, was arrested by the Delhi Police.[101]

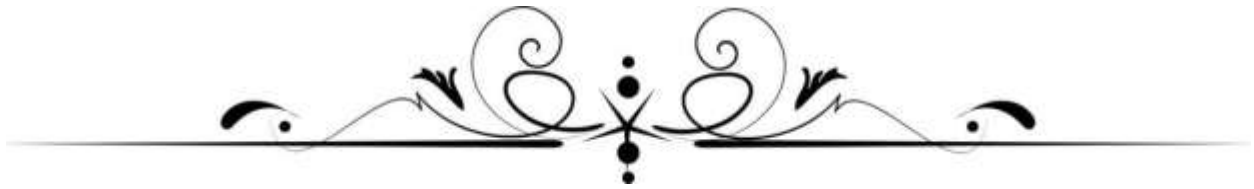
In this incident of the 'Bulli Bai' app, where images of Muslim women were being taken from their social media and uploaded onto app. The main motive of his app was to humiliate the women by auctioning them and writing obscene derogatory comments against them. Most of the women belong to the minority community that is muslim community. This isn't the first time such an incident has been occurred. Neeraj Bishnoi the mastermind behind the app, arrested by the police had contacts with the person who made the 'Sulli deal app'. In both instances, images of the women were taken from their public domain and uploaded without their consent. A law regarding revenge porn could also address the uploading of images or video on any platform without the consent of the victim with a malicious motive. The 'Sulli deal' and Bulli Bai deal' apps are only small drop in the vast ocean of the cybercrime against women.

There are many incidents of revenge pornography happening across the country in which criminals misuse digital platforms and commit such crimes out of vengeance. Although very few cases are recorded by the police or complaint by victims because in such matters people take a lot of time to file a report and when they do, they are often discouraged by the authorities.

[101] Delhi Police Files FIR on 'Sulli Deals' App That 'Auctioned' Photos of Muslim Women, *Wire* 8th July, 2021, *available at:* https://thewire.in/women/sulli-deals-github-delhi-police-fir (last visited on 16th December, 2021).

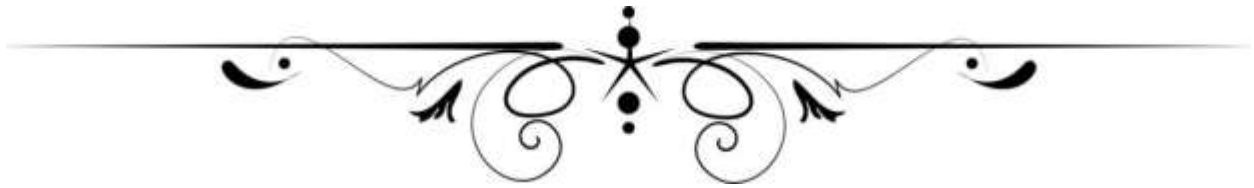
Conclusion

This research finds that victims of intimate image abuse are disproportionately female and that the impacts of intimate image abuse are highly gendered. It also finds that two types of perpetrators of intimate image abuse exist. Type one perpetrators share images anonymously on large pornography sites, with motivations largely unknown, and type two perpetrators use threats to share images as part of a broader pattern of coercive and controlling behaviour. Privacy is considered to be the extension of liberty of human beings. The protection of privacy requires the attention of state and non-state actors, where the 'informational confidentiality' is linked with the private matters like sexual integrity, autonomy on the person's body. The revenge porn and blackmailing is an offence under infringement of privacy. There is need of focused law to establish breach of privacy in cyberspace as violation of Fundamental Right to privacy. Conclusively said that any sort of privacy infringement by way of electronic media may also prove extremely dangerous for women, where women have undergone serious mental trauma in anticipation of damage of reputation, especially for marriage market, due to digital breach of privacy. Breach of privacy has developed suicidal tendency among the large number of women victim of revenge porn and blackmailing.



CHAPTER-IV

CYBERCRIME AGAINST WOMEN: NATIONAL LEGAL PERSPECTIVE



CHAPTER-IV
CYBERCRIME AGAINST WOMEN: NATIONAL LEGAL PERSPECTIVE

4.1. Introduction

As now, it is clear from the preceding chapters that Cybercrimes are distinctly different from the traditional crimes, are often more difficult to detect and prosecute. Cybercrimes are perpetrated by perpetrators through small, targeted cyber threats, and large networks of commercial purposes leased, hijacked computers are used to launch significant attacks. Such crimes are much more widespread unlike traditional crimes and these are increasing at a faster rate. In addition, cybercrime harms society more than traditional crime, and is much more difficult to investigate. Cybercrime contains any computer and network-related criminal act.

In this chapter, researcher has made a detailed study of Indian laws dealing the issue of cybercrimes especially related to women. For that purpose researcher first provided the provisions available under the traditional laws and then tried to evaluate the remedies available in the specific law dealing with the problem of Cybercrime.

Further researcher, analysed the Information and Technology Act, 2000 and other statutes while dealing with revenge porn and blackmailing under cybercrime against women to find out the solution for persecution of revenge porn and blackmailing cybercrime criminals.

4.2. Traditional Laws for the Protection of Crime against Women

India has an extremely detailed and well defined legal system in place. Numerous laws have been enacted and implemented and the foremost amongst them, the Constitution of India. However, the arrival of Internet signaled the beginning of the rise of new and complex legal issues. It may be pertinent to mention that all the existing laws in place in India were enacted way back keeping in mind the relevant political, social, economic, and cultural scenario of that relevant time. Nobody then could really visualize about the Internet and cybercrime. Despite the brilliant acumen of our master draftsmen,

the requirements of cyberspace could hardly ever be anticipated. As such, the coming of the Internet led to the emergence of numerous ticklish legal issues and problems which necessitated the enactment of cyber laws.

4.2.1. Constitutional Provisions for Protection of Women's Rights

The Constitution of India not only grants equality to women but also empowers the State to adopt measures of positive discrimination in favour of women for neutralizing the cumulative socio economic, education and political disadvantages faced by them. Fundamental Rights, among others, ensure equality before the law and equal protection of law; prohibits discrimination against any citizen on grounds of religion, race, caste, sex or place of birth, and guarantee equality of opportunity to all citizens in matters relating to employment. Articles 14, 15, 15(3), 16, 19, 21, 24, 39(a), (b), (c) and 42 of the Constitution are of specific importance in this regard.

The Constitution of India has certain provisions relating to women. It makes special provisions relating to women for treatment and development of women in every sphere of life. The preamble[1] states with the word *"We, the people of India, having solemnly resolved to constitute India into a Sovereign, Socialist, Secular, Democratic, Republic and to secure to all its citizens Justice[2], Liberty[3], Equality[4], Fraternity[5] in our Constituent Assembly on this twenty-sixth day of November, 1949, do hereby, adopt, enact and give to ourselves this Constitution."*

The preamble is the explanation to the Constitution which does not discriminate between men and women but it treats them equally. The framers of the Constitution were all aware of unequal treatment meted out to the fair sex, from the time immemorial. In India, the history of suppression of women is very old and long which is responsible for including general and special provisions for upliftment of status of women; certain provisions are specifically designed for the benefit of women.

[1] Constitution of India, Preamble, P.M Baxi, *Constitution of India, 1950* (Universal Law Publication, New Delhi, 2019).
[2] Social, Economic and Political.
[3] of thought, expression, belief, faith and worship.
[4] of status and opportunity.
[5] Assuring the dignity of the individual and the unity and integrity of the nation.

The preamble appended to the Constitution of India, contains various objectives including 'the equality of status and of opportunity' to all the citizens. This objective has been inserted with a view to giving equal status to men and women in terms of the opportunity.

Art. 51(c) has been relied upon to introduce and implement various international instruments, particularly the Universal Declaration of Human Rights and the two Covenants on the Political and Civil Rights and the Economic, Social and Cultural Rights in the interpretation of fundamental rights. The courts have held that by virtue of this article[6] international instrument, particularly those to which India is a party; become part of the Indian law so long as they are not inconsistent with it. Therefore, they can be very well relied upon and enforced.[7]

Art. 253 have been invoked from time to time.[8] Almost all legislations on women since mid-1970s have been enacted under this provision. Mere showing respect is not enough; it would only serve the purpose if we imbibe it. Otherwise inequalities and discrimination would be perpetuated instead of recognising their nobility like self-sacrifice and self-denial.

Art. 15 of the Constitution of India has explicitly prohibited discrimination against women.[9] This was the Draft Art. 9 (Art. 15) debated on 29th November, 1948. It

---

[6] The Constitution of India, art. 51(c) state that "The State shall endeavour to foster respect for the international law and treaty obligations in the dealings of organised peoples with one another".

[7] *Sheela Barse* v. *Secy, Children's Aid Society* (1987) 3SCC 50, 54; *Vishaka* v. *State of Rajasthan*, (1977) 6 SCC 241.

[8] The Constitution of India, art. 253 state that "Notwithstanding anything the parliament has power to make any law for the whole or any part of the territory of India for implementing any treaty agreement or convention with any other country or countries or any decision made at any international conference, association or other body".

[9] The Constitution of India, art. 15 states that "1.The state shall not discriminate against any citizen on grounds only of religion, race, caste, sex, place of birth or any of them.

2. No citizen shall, on grounds only of religion, race, caste, sex, place of birth or any of them, be subject to any disability, liability, restriction or condition with regards to-
(a) Access to shops, public restaurants, hotels and place of public entertainment, or
(b) The use of wells, tanks, bathing ghats, roads, and places of public resort maintained locally or partly out of the state funds or dedicated to the use of general public.

3. Nothing in this Article shall prevent the state from making any special provision for women and children.

4. Nothing in this Article or in clause (2) of the Article 29 shall prevent the state from making any special provision for the advancement of any socially and educationally backward classes of citizen or for the Scheduled Castes and Scheduled Tribes."

prohibited discrimination on five (5) grounds: religion, race, caste, sex or place of birth. It was adopted by the members of the constituent assembly without any more debate. It's clearly mentioned that no one shall be discriminated on the basis of the sex. Therefore, women enjoy the special status under this Art. 15(3) of the Constitution of India. The Constitution of India explicitly mentions equality of opportunities for all and prohibits the discrimination against women.[10]

It clearly states that there should not be any negative discrimination; but a protective discrimination with the distinct aim of achieving the goal of equality. There are some important provisions in the Constitution of India that provide equal opportunities for women implicitly as they are applicable to all people of both sexes. To be compatible to the commands of the Constitution, the State is obligated not to deny to any person equality before the law or the equal protection of the laws within the territory of India.[11]

Under Art. 19(1), it guarantees a freedom of speech and expression. It provides that all citizens have the right to freedom of speech and expression. Art. 19 (2) provides that in the interest of decency and morality, reasonable restrictions may be imposed by law upon this freedom.[12]

---

[10] The Constitution of India, art.16 State that "1.There shall be equality of opportunity for all citizen in matters relating to employment or appointment to any office under the state.
2. No citizen shall, on the ground only of religion, race, caste sex, descent place of birth, residence or any of them, be ineligible for, or discriminated against in respect of, any employment or office under the state.
3. Nothing in this Article shall prevent parliament from making any law prescribing, in regard to a class or classes of employment or appointment to an office/under the government or any local or other authority within, a state or union territory, any requirement as to residence within the state or union territory prior to such employment or appointment.
4. Nothing in the Article shall prevent the state from making any provision for the reservation of appointments or posts in favour of any backward class of citizens which, in opinion of the state, is not adequately represented in service under the state (a) Nothing in this Article shall prevent the state from making any provision for reservation in matters of promotion of any class or classes of posts into the services under the state in favour of scheduled castes or scheduled tribes which, in the opinion of the state are not adequately represented in the service under the state.
5. Nothing in this Article shall effect the operation of any law which provides that the incumbent of an office in connection with affairs of any religious or denominational institution or any member of the government body thereof shall be a person professing a particular religion or belonging to a particular denomination."

[11] The Constitution of India, art. 14 state that "The State shall not deny to any person equality before the law or the equal protection of the laws within the territory of India."

[12] The Constitution of India, art. 19(1) state that "All citizens shall have the right -
(a) To freedom of speech and expression.

The freedoms have been given under this Article, however are not absolute. These freedoms are restricted by the Constitution in clauses (2) to (6) of Art. 19. The restriction which may be imposed by the state under any clauses must be reasonable restrictions and not arbitrary. There was debate regarding the restriction imposing against the freedom of speech and expression in Constituent Assembly, many members argued that the restriction will negate the enforcement of the freedom guaranteed. But with amendment to 'reasonable restriction' it has been adopted.

The rights to life and personal liberty in India have been guaranteed by the constitutional provision,[13] Art. 21 spell that no person shall be deprived of life or personal liberty. The Art. 21 has received the widest possible interpretation. Under the heaven of Art. 21 of the Constitution, so many rights have found shelter, which grow and get nourishment. Right to privacy became the fundamental right under the shelter of the person right to privacy now protected under Art. 21 of the Constitution of India. This Article if read literally is a colorless article and would satisfy, at the moment, established by the state that there is a law which provides a procedure which has been followed by the impugned action. But the expression "procedure established by law" in article has been judicially construed as a procedure which is just, fair, reasonable.[14] This Article 21 gives a positive effect by judicial interpretation.

Art. 21-A guarantees compulsory education to all children of the age 6-14 irrespective of gender.[15]

Art. 23 of the Constitution of India prohibit traffic in human beings and forced labour. Employment of children below the age of fourteen years in factory or mine or engaged in any other hazardous employment is also prohibited.[16]

(b) To assemble peacefully and without arms.
(c) To form association or union.
(d) To move out freely throughout the territory of India.
(e) To reside and settle in any parts of the territory of India and
(g) To practice any profession, or to carry on any occupation, trade or business.

[13] The Constitution of India, art.21 state "no person shall be deprived of his life and personal liberty except according to procedure established by law".

[14] A. Singh, *Constitution and Women's Rights* 47(Axis Book, New Delhi, 2013).

[15] The Constitution of India, art. 21-A state that "The state shall provide free and compulsory education to all children of the age of six to fourteen years in such manner as the state may, by law determine".

In Art. 25, all the persons are equally entitled to freedom of conscience and the right to freely profess, practice and propagate religion.[17]

It also provides that no person shall be compelled to pay any taxes, the proceeds of which are specifically appropriated in payment of expenses for the promotion or maintenance of any particular religion or religious denomination.[18]

The Constitution further warrants that no person attending any educational institution recognised by the state or receiving aid out of the state funds shall be required to take part in any religious instruction to attend any religious workshop that may be conducted in such institution.[19] The words 'citizen' 'person' means both 'male' person and 'female' person. Hence, women are equally entitled for the protection of all fundamental rights along with men. There is no discrimination of women relating to the fundamental rights guaranteed in the Constitution of India.

Under the Constitution of India, the Directive Principles of State Policy is the manifestation of governance that India is a welfare democratic State. This policy envisaged equal rights to work, equal pay for equal work, adequate means of decent and dignified livelihood to both men and women, these are guaranteed under the Directive Principle of State Policy *viz*. Part IV of the Constitution to deal with the welfare and development of women as well.[20]

The Directive Principles of State of Policy have two characteristics.[21] Firstly they are not enforceable in any court of law and therefore, if a directive is not obeyed or

[16] The Constitution of India, art. 24 state that "No child below the age of fourteen years shall be employed to work in any factory or mine or engaged in any other hazardous employment".

[17] The Constitution of India, art. 25(1) says that "Subject to public order, morality and health and to the other provisions of this Part, all persons are equally entitled to freedom of conscience and the right freely to profess, practice and propagate religion".

[18] The Constitution of India, art. 27 state that "No person shall be compelled to pay any taxes, the proceeds of which are specifically appropriated in payment of expenses for the promotion or maintenance of any particular religion or religious denomination".

[19] The Constitution of India, art. 28(3) say that "No person attending any educational institution recognised by the State or receiving aid out of State funds shall be required to take part in any religious instruction that may be imparted in such institution or to attend any religious worship that may be conducted in such institution or in any premises attached thereto unless such person or, if such person is a minor, his guardian has given his consent thereto Cultural and Educational Rights".

[20] The Constitution of India, art. 38, 39 (a), (d) and (e), 42, 44 and 45.

[21] Mahendra Pal Singh , *V.N. Shukla's, Constitution of India* 342 (Eastern Book Company, Lucknow, 11th ed., 2019).

implemented by the state, its obedience or implementation cannot be secured through judicial proceeding. This characteristic has been weak in practice by court decisions, which have enforced some of the directive principles in support of the fundamental rights. Secondly, they are fundamental in the governance of the country and it shall be the obligation of the state to apply their principles in making laws. The expression 'laws' must be construed in a generic sense and should include all normative exercise of power including in the decision making.

Thus, in ***Minerva Mills Ltd.* v. *Union of India***[22], the appellate court observed that harmony and balance between fundamental rights and directive principle is an essential feature of the basic structure of the Constitution. Therefore, the directive Principle of State Policy has the same status as Fundamental Rights but without justifiability.

Further, Art. 31C speaks of saving of laws giving effect to the policy of the state towards securing[23] all or any of the principles laid down in Part (IV) shall be deemed to be void on the ground that it is inconsistent with or takes away or abridges any of the rights conferred by Art. 14 or 19 shall be called in question in any court on the ground that it does not give effect to.[24]

The state shall, in particular, direct its policy towards securing;

(a) That the citizens, men and women equally, have the right to an adequate means of livelihood.

(b) That the ownership and control of the material resources of the community are so distributed as best to sub serve the common good;

(c) That the operation of the economic system does not result in the concentration of wealth and means of production to the common detriment;

(d) That there is equal pay for equal work for both men and women;

(e) That the wealth and strength of the workers, men and women and the tender age of the children are not abused and that the citizens are not forced by economic necessity to enter avocations unsuited to their age or strength; and

[22] *Minerva Mills Ltd.* v. *Union of India,* AIR 1980 SC 1789, 1806.
[23] The Constitution of India.art. 39.
[24] Substituted by The Constitution (Forty-Second Amendment) Act, 1976.

(f) That children are given opportunities and facilities to develop in a healthy manner and conditions of freedom and dignity and the childhood and youth are protected against moral and material abandonment.[25]

Art. 42 of the Constitution has incorporate provision for the benefit of the women. It directs, that the state shall make provision for securing just and humane conditions to work and for maternity relief.[26]

The state shall within the limits of its economic capacity and development, make effective provision for securing the right to work, to educate and to public assistance in cases of unemployment, old age, sickness and disablement, and in other cases of un-deserved want and there is no compartmentalisation between men and women.[27]

The state shall endeavour to secure for the citizens a uniform civil code throughout the territory of India.[28]

The state shall regard the raising of the level of nutrition and the standard of living of its people and the improvement of public health as among its primary duties and, in particular, the state shall endeavour to bring about prohibition of the consumption, except for medical purposes, of drinks, which are injurious to health.[29]

The state shall take steps to organise village panchyats and endow them with such powers and authority as may be necessary to enable them to function as units of self-government. Reservation of seats for women in panchayats and municipalities has been provided in Art. 243D and 243T of the Constitution of India. Part (ix) and (ix A) have been added to the Constitution by Constitution (73rd Amendment) Act, 1992 and the Constitution (74th Amendment) Act, 1992 popularly known as the Panchayati Raj and

[25] Substituted by The Constitution (Forty-Fourh Amendment) Act, 1976

[26] The Constitution of India, art. 42 says that "The State shall make provision for securing just and humane conditions of work and for maternity relief".

[27] The Constitution of India, art.45 state that "The State shall endeavour to provide, within a period of ten years from the commencement of this Constitution, for free and compulsory education for all children until they complete the age of fourteen years".

[28] The Constitution of India, art. 44 say that "The State shall endeavour to secure for the citizens a uniform civil code throughout the territory of India".

[29] The Constitution of India, art. 47 state that "The State shall promote with special care the educational and economic interests of the weaker sections of the people, and, in particular, of the Scheduled Castes and the Scheduled Tribes, and shall protect them from social injustice and all forms of exploitation".

Nagarpalika Constitution Amendment Acts with Arts. 243, 243A to 243D and Art. 243P to 243ZG.

Art. 51-A was newly added to the Constitution by the 42nd Amendment, 1976. This Article for the first time specified a code of eleven Fundamental Duties for the citizens. Art. 51A (e) is related to women[30] & imposed the duty to remove the practices derogatory to the dignity of women.

All laws in force in the territory of India immediately before the commencement of the Constitution, in so far as they are inconsistent with the provisions of this part, shall to the extent of such inconsistency, be void.[31] This means that the ex-post facto laws, which are consistent with the provisions of the Constitution, can be adapted under Art. 372 to the Indian legal system unless altered or repealed or amended by competent legislature or other competent authority. Further state shall not make any law, which takes away or abridges the rights conferred by this part or any law made in contravention of this clause shall, to the extent of the contravention be void.[32] Thus, it prohibits the state from making any law, which either takes away totally or abrogates in part a fundamental right. Unless the context otherwise requires, law includes any ordinance, order, bye laws, rule, regulation, notification, custom or usage having in the territory of India the force of law.[33]

All these are fundamental rights. Therefore, women can go to the court if one is subjected to any discrimination.[34] All are the protective provision envisaged in the Constitution of India to protect the women from any kind of discrimination and violation

[30] The Constitution of India, art. 51-A (e) states that "it shall be the duty of every citizen of India to promote harmony and the spirit of common brotherhood amongst all the people of India transcending religious, linguistic and regional or sectional diversities; to renounce practices derogatory to the dignity of women".

[31] The Constitution of India, art. 13(1) state that "All laws in force in the territory of India immediately before the commencement of this Constitution, in so far as they are inconsistent with the provisions of this Part, shall, to the extent of such inconsistency, be void."

[32] The Constitution of India, art. 13(2) state that "The State shall not make any law which takes away or abridges the rights conferred by this Part and any law made in contravention of this clause shall, to the extent of the contravention, be void."

[33] The Constitution of India, art. 13(3) (a) provide that "In this article, unless the context otherwise requires, (a) "law" includes any Ordinance, order, bye-law, rule, regulation, notification, custom or usage having in the territory of India the force of law;"

[34] Sunita Sharma, *Women and Crime* 9 (Crescent Publishing Corporation, New Delhi, 2017).

of fundamental rights. Constitution of India is Grundnorm for all statues which are enacted by the Parliament; they should keep in mind that foremost duty of the state is to protect the women who are much vulnerable to violence and crime. Thus, our Constitution assures that no one will be discriminated on the basis of sex.[35]

4.3. Existing Legislative Provisions Related to Crime against Women's

To uphold the constitutional mandate, the state has enacted various legislative measures intended to ensure equal rights, to counter social discrimination and various form of violence and atrocities against women.

4.3.1. Crime against Women under Penal Law

The women may be victim of various offences given under Indian Penal Code such as murder, robbery, cheating, etc., but those crime which are commited specifically against women, are considered as "crime against women". In order to curb ever growing crimes relating to women a numbers of laws have been enacted and amendments are made in existing laws from time to time to curb such crime effectively.

Crimes against women under the Indian Penal Code are as follows:

A. Rape (Sections 375, 376, 376A, 376B, 376C, 376D, and 376E the Indian Penal Code)[36]

Protection from sexual offence related to rape, the relevant statutory provisions give under Sections 375, 376, 376 A, 376 B, 376C, 376D and 376 E. According to Section 375 clauses (a), (b), (c) and (d):-[37]

---

[35] Nitu Nawal, *Human Rights and Women justice: International and National* Perspective (Regal Publication, New Delhi, 2015); Tanuja Trivedi, *Women Rights and Duties* 150 (Jnanada Prakashan, Arunachal Pradesh, 2017).

[36] Inserted by the Criminal (Amendment) Act, 2013.

[37] Indian Penal Code, 1860 (Act 45 of 1860), s.375 state that "A man is said to commit "rape" if he-
(a) penetrates his penis, to any extent, into the vagina, mouth, urethra or anus of a woman or makes her to do so with him or any other person; or
(b) inserts, to any extent, any object or a part of the body, not being the penis, into the vagina, the urethra or anus of a woman or makes her to do so with him or any other person; or
(c) manipulates any part of the body of a woman so as to cause penetration into the vagina, urethra, anus or any part of body of such woman or makes her to do so with him or any other person; or
(d) applies his mouth to the vagina, anus, urethra of a woman or makes her to do so with him or any other person,

A man is said to commit rape if he-

(a) Penetrate his penis, into the vagina, mouth, urethra or anus of a women or make her to do so with him or any other person; or

(b) Insert any object or a part of body, into vagina, the urethra or anus of a women or make her to do so with him or any other person; or

(c) Manipulates any part of the body of a women so as to cause penetration into the vagina, urethra or anus of a women or make her to do so with him or any other person

(d) Applies his mouth to the vagina, urethra or anus of women or make her to do so with him or any other person.

As stated above the act to constitute rape must be committed by man with women against her will and without her consent.

There are two explanations I and II have been appended with the section and Section 375 also provides two exceptions when the act will not be considered rape. Namely, a medical procedure or intervention and sexual intercourse by a man with his own wife when she is not below 15 years of age.

---

under the circumstances falling under any of the following seven descriptions:
First. Against her will
Secondly. Without her consent
Thirdly. With her consent, when her consent has been obtained by putting her or any person in whom she is interested, in fear of death or of hurt
Fourthly. With her consent, when the man knows that he is not her husband and that her consent is given because she believes that he is another man to whom she is or believes herself to be lawfully married
Fifthly. With her consent when, at the time of giving such consent, by reason of unsoundness of mind or intoxication or the administration by him personally or through another of any stupefying or unwholesome substance, she is unable to understand the nature and consequences of that to which she gives consent
Sixthly. With or without her consent, when she is under eighteen years of age
Seventhly. When she is unable to communicate consent
Explanation 1.For the purposes of this section, "vagina" shall also include labia majora.
Explanation 2.Consent means an unequivocal voluntary agreement when the woman by words, gestures or any form of verbal or non-verbal communication, communicates willingness to participate in the specific sexual act:
Provided that a woman who does not physically resist to the act of penetration shall not by the reason only of that fact, be regarded as consenting to the sexual activity.
Exception 1. A medical procedure or intervention shall not constitute rape.
Exception 2.Sexual intercourse or sexual acts by a man with his own wife, the wife not being under fifteen years of age, is not rape.

Further, a drastic change has been made in case of punishment for rape *vides* Criminal Law (Amendment) Act, 2013 to deter people from committing such heinous crime against women.[38]Section 376 provides punishment for whoever commits offence of rape against women. It enumerates 14 situations in which punishment shall not be less than 10 years but which may be extended to imprisonment for the remainder of that person natural life or death.[39]

---

[38] *Ibid.*

[39] Indian Penal Code, 1860 (Act 45 of 1860), s.376 state that "(1) Whoever, except in the cases provided for in sub-section (2), commits rape, shall be punished with rigorous imprisonment of either description for a term which shall not be less than ten years, but which may extend to imprisonment for life, and shall also be liable to fine.

(2) Whoever,

(a) being a police officer, commits rape
  (i) within the limits of the police station to which such police officer is appointed; or
  (ii) in the premises of any station house; or
  (iii) on a woman in such police officer's custody or in the custody of a police officer subordinate to such police officer; or

(b) being a public servant, commits rape on a woman in such public servant's custody or in the custody of a public servant subordinate to such public servant; or

(c) being a member of the armed forces deployed in an area by the Central or a State Government commits rape in such area; or

(d) being on the management or on the staff of a jail, remand home or other place of custody established by or under any law for the time being in force or of a women's or children's institution, commits rape on any inmate of such jail, remand home, place or institution; or

(e) being on the management or on the staff of a hospital, commits rape on a woman in that hospital; or

(f) being a relative, guardian or teacher of, or a person in a position of trust or authority towards the woman, commits rape on such woman; or

(g) commits rape during communal or sectarian violence; or

(h) commits rape on a woman knowing her to be pregnant; or

(j) commits rape, on a woman incapable of giving consent; or

(k) being in a position of control or dominance over a woman, commits rape on such woman; or

(l) commits rape on a woman suffering from mental or physical disability; or

(m) while committing rape causes grievous bodily harm or maims or disfigures or endangers the life of a woman; or

(n) commits rape repeatedly on the same woman,

shall be punished with rigorous imprisonment for a term which shall not be less than ten years, but which may extend to imprisonment for life, which shall mean imprisonment for the remainder of that person's natural life, and shall also be liable to fine.

Explanation.-For the purposes of this sub-section,-

(a) "armed forces" means the naval, military and air forces and includes any member of the Armed Forces constituted under any law for the time being in force, including the paramilitary forces and any auxiliary forces that are under the control of the Central Government or the State Government;

(b) "hospital" means the precincts of the hospital and includes the precincts of any institution for the reception and treatment of persons during convalescence or of persons requiring medical attention or rehabilitation;

(c) "police officer" shall have the same meaning as assigned to the expression "police" under the Police Act, 1861 (5 of 1861);

A group of five Sections 376A, 376B, 376C, 376D, and376E have been added in Indian Penal code *vide* Criminal Law (Amendment) Act, 2013 with a view to provide severe punishment to deter criminal from indulging into different types of aggravated crimes against women. These are:

(i) Death or Resulting in Vegetative State

In case of causing death of the victim or resulting her being in a persistent vegetative state as result of inflicting injury during the cause of rape the accused shall be punished with minimum of 20 years of rigorous imprisonment that may be extended to life imprisonment.[40]

(ii) Marital Rape

The Indian law on marital rape has been extensively amended keeping in view that marriage is regarded as a partnership of equals. The Section 376B IPC makes husband liable to punishment with imprisonment and fine in case of intercourse with his wife during the period of separation without her consent.[41]

(d) "women's or children's institution" means an institution, whether called an orphanage or a home for neglected women or children or a widow's home or an institution called by any other name, which is established and maintained for the reception and care of women or children.

(3) Whoever, commits rape on a woman under sixteen years of age shall be punished with rigorous imprisonment for a term which shall not be less than twenty years, but which may extend to imprisonment for life, which shall mean imprisonment for the remainder of that person's natural life, and shall also be liable to fine:

Provided that such fine shall be just and reasonable to meet the medical expenses and rehabilitation of the victim:

Provided further that any fine imposed under this sub-section shall be paid to the victim."

[40] Indian Penal Code, 1860 (Act 45 of 1860), s.376A state that Punishment for causing death or resulting in persistent vegetative state of victim. "Whoever, commits an offence punishable under sub-section (1) or sub-section (2) of section 376 and in the course of such commission inflicts an injury which causes the death of the woman or causes the woman to be in a persistent vegetative state, shall be punished with rigorous imprisonment for a term which shall not be less than twenty years, but which may extend to imprisonment for life, which shall mean imprisonment for the remainder of that person's natural life, or with death."

[41] Indian Penal Code, 1860 (Act 45 of 1860), s.376B provide punishment for rape on woman under twelve years of age. "Whoever, commits rape on a woman under twelve years of age shall be punished with rigorous imprisonment for a term which shall not be less than twenty years, but which may extend to imprisonment for life, which shall mean imprisonment for the remainder of that person's natural life, and with fine or with death:

Provided that such fine shall be just and reasonable to meet the medical expenses and rehabilitation of the victim:

Provided further that any fine imposed under this section shall be paid to the victim."

(iii) Custodial Rape: Sexual Intercourse by a Person in Authority

Section 376C has created a new category of sexual offences which do not amount to rape, because the consent of the victim is given in such cases, but under compelling circumstances. This section 376C has provided punishment for custodial rape.[42]

(iv) Gang Rape

Section 376D makes punishment very severe in case of the gang rape that may be imprisonment till the natural life of the person.[43] Further, section 376DA[44] and Section 376DB [45] inserted by Criminal Law (Amendment) Act, 2018 which provides the punishment for gang rape of woman below the age of 16 years and below the age of 12 years respectively. These sections seek to protect the teen girls from such heinous crime.

[42] Indian Penal Code, 1860 (Act 45 of 1860), s.376C state that "Sexual intercourse by husband upon his wife during separation- Whoever has sexual intercourse with his own wife, who is living separately, whether under a decree of separation or otherwise, without her consent, shall be punished with imprisonment of either description for a term which shall not be less than two years but which may extend to seven years, and shall also be liable to fine.
Explanation- In this section, "sexual intercourse" shall mean any of the acts mentioned in clauses (a) to (d) of section 375".

[43] Indian Penal Code, 1860 (Act 45 of 1860), s.376D state that "Gang Rape-Where a woman is raped by one or more persons constituting a group or acting in furtherance of a common intention, each of those persons shall be deemed to have committed the offence of rape and shall be punished with rigorous imprisonment for a term which shall not be less than twenty years, but which may extend to life which shall mean imprisonment for the remainder of that person's natural life, and with fine:
Provided that such fine shall be just and reasonable to meet the medical expenses and rehabilitation of the victim:
Provided further that any fine imposed under this section shall be paid to the victim."

[44] Indian Penal Code, 1860 (Act 45 of 1860), s.376DA state that "Punishment for gang rape on woman under sixteen years of age- Where a woman under sixteen years of age is raped by one or more persons constituting a group or acting in furtherance of a common intention, each of those persons shall be deemed to have committed the offence of rape and shall be punished with imprisonment for life, which shall mean imprisonment for the remainder of that person's natural life, and with fine:
Provided that such fine shall be just and reasonable to meet the medical expenses and rehabilitation of the victim:
Provided further that any fine imposed under this section shall be paid to the victim."

[45] Indian Penal Code, 1860 (Act 45 of 1860), s.376DB state that "Punishment for gang rape on woman under twelve years of age- Where a woman under twelve years of age is raped by one or more persons constituting a group or acting in furtherance of a common intention, each of those persons shall be deemed to have committed the offence of rape and shall be punished with imprisonment for life, which shall mean imprisonment for the remainder of that person's natural life, and with fine, or with death:
Provided that such fine shall be just and reasonable to meet the medical expenses and rehabilitation of the victim:
Provided further that any fine imposed under this section shall be paid to the victim."

(v) Punishment for Repeat Offender

Section 376E provides punishment for the repeat offenders.[46]

B. Kidnapping and Abduction of Women for Different Purposes (Section 363-369, The Indian Penal Code)

From Section 359 to 369 of the Indian Penal Code, 1860 have made kidnapping and abduction punishable with varying degree of sternness according to nature and severity of the offence. The principal object of enacting these provisions is to secure the personal liberty of every citizen and to give legal protection to children of tender age and women from being abducted or seduced for improper purposes. Section 359 says that there are two kinds of kidnapping, kidnapping from India[47] and kidnapping from lawful guardianship.[48] The term kidnapping from India has been defined under Section 360 and kidnapping from lawful guardianship under Section 361.

Section 362 of the Code defines the abduction.[49] It's means that, if any women taken without her consent, taken forcefully the person shall be liable for punishment under Section 363 of the Code. Section 363 provides punishment for kidnapping and abduction upto three years of imprisonment.[50] Other forth going, sections provide the punishment for kidnapping for various purposes.

---

[46] Indian Penal Code, 1860 (Act 45 of 1860), s.376E state that "Whoever has been previously convicted of an offence punishable under section 376 or section 376A or section 376AB or section 376D or section 376DA or section 376DB, and is subsequently convicted of an offence punishable under any of the said sections shall be punished with imprisonment for life which shall mean imprisonment for the remainder of that person's natural life, or with death".

[47] Indian Penal Code, 1860 (Act 45 of 1860), s.360 state that "Whoever conveys any person beyond the limits of [India] without the consent of that person, or of some person legally authorised to consent on behalf of that person, is said to kidnap that person from [India]".

[48] Indian Penal Code, 1860 (Act 45 of 1860), s.361 state that "Whoever takes or entices any minor under [sixteen] years of age if a male, or under [eighteen] years of age if a female, or any person of unsound mind, out of the keeping of the lawful guardian of such minor or person of unsound mind, without the consent of such guardian, is said to kidnap such minor or person from lawful guardianship.
Explanation-The words "lawful guardian" in this section include any person lawfully entrusted with the care or custody of such minor or other person.
Exception- This section does not extend to the act of any person who in good faith believes himself to be the father of an illegitimate child, or who in good faith believes himself to be entitled to the lawful custody of such child, unless such act is committed for an immoral or unlawful purpose."

[49] Indian Penal Code, 1860 (Act 45 of 1860), s.362 state that "Whoever by force compels, or by any deceitful means induces, any person to go from any place, is said to abduct that person".

[50] Indian Penal Code, 1860 (Act 45 of 1860), s.363 state that "Whoever kidnaps any person from [India] or from lawful guardianship, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine".

Section 364 provides the punishment for kidnapping or abduction in order of murder.[51]Section 364A provides punishment for kidnapping or abduction for ransom.[52] Section 365 states the punishment for kidnapping or abduction with intent to wrongful confinement.[53] Section 366 provides the protection to the women victim. This Section says that kidnapping or abducting or inducing any women to compel her to marry against her will is offence against women.[54]

C. Murder, Dowry Death, Abetment of Suicide, etc., (Sections 302, 304B and 306, The Indian Penal Code)

Section 302 provides punishment for murder. If any person murders any women, he will be liable to punishment under this section. Further, Dowry death is punishable under Section 304B of Indian Penal Code. This Section was inserted in the year 1986 *vide* Criminal Law (Amendment) Act, 1986 with a view to curb the dowry death, suicide, bride burning etc, rampant in the country. Section 304B (1) defines "dowry death" and sub section (2) prescribes the punishment for such cases.[55] Section 306 punishes

[51] Indian Penal Code, 1860 (Act 45 of 1860), s.364 state that "Whoever kidnaps or abducts any person in order that such person may be murdered or may be so disposed of as to be put in danger of being murdered, shall be punished with [imprisonment for life] or rigorous imprisonment for a term which may extend to ten years, and shall also be liable to fine".

[52] Indian Penal Code, 1860 (Act 45 of 1860), s.364A state that "Whoever kidnaps or abducts any person or keeps a person in detention after such kidnapping or abduction and threatens to cause death or hurt to such person, or by his conduct gives rise to a reasonable apprehension that such person may be put to death or hurt, or causes hurt or death to such person in order to compel the Government or [any foreign State or international inter-governmental organization or any other person] to do or abstain from doing any act or to pay a ransom, shall be punishable with death, or imprisonment for life, and shall also be liable to fine]".

[53] Indian Penal Code, 1860 (Act 45 of 1860), s.365 state that "Whoever kidnaps or abducts any person with intent to cause that person to be secretly and wrongfully confined, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine".

[54] Indian Penal Code, 1860 (Act 45 of 1860), s.366 state that "Whoever kidnaps or abducts any woman with intent that she may be compelled, or knowing it to be likely that she will be compelled, to marry any person against her will, or in order that she may be forced or seduced to illicit intercourse, or knowing it to be likely that she will be forced or seduced to illicit intercourse, shall be punished with imprisonment of either description for a term which may extend to ten years, and shall also be liable to fine;[and whoever, by means of criminal intimidation as defined in this Code or of abuse of authority or any other method of compulsion, induces any woman to go from any place with intent that she may be, or knowing that it is likely that she will be, forced or seduced to illicit intercourse with another person shall also be punishable as aforesaid]".

[55] Indian Penal Code, 1860 (Act 45 of 1860), s.304B state that "(1) Where the death of a woman is caused by any burns or bodily injury or occurs otherwise than under normal circumstances within seven years of her marriage and it is shown that soon before her death she was subjected to cruelty or harassment by her

abetment of suicide i.e.,[56] the punishment in such a case may extend up to 10 years of imprisonment. A man encourages a women to commit suicide is liable and his act is punishable under law.

D. Cruelty by Husband or Relatives of Husband (Section 498A of The Indian Penal Code)

Section 498A of Indian Penal Code 1860[57] was introduced in the year 1983 to protect married women from being subjected to cruelty by the husband or his relatives. A punishment extending to 3 years and fine has been prescribed. The expression "Cruelty" has been defined under this section in wide terms, so as to include inflicting physical or mental harm to the body or health of the woman and indulging in acts of harassment with a view to coerce her or her relatives to meet any unlawful demand for any property or valuable security. Harassment for dowry falls within the sweep of latter limb of the section. Creating a situation driving the woman to commit suicide is also one of the ingredients of "Cruelty". This Section 498A provided punishment to protect the women from the cruelty from near and dear one.

E. Out Raging The Modesty of a Woman (Molestation) (Sections 354, 354A, 354B, 354C and, 354D of The Indian Penal Code)

The object of the provisions as contained in Sections 354, 354A, 354B, 354C and, 354D are to protect women against indecent behaviour of others, which is offensive to

husband or any relative of her husband for, or in connection with, any demand for dowry, such death shall be called 'dowry death', and such husband or relative shall be deemed to have caused her death.
Explanation: For the purposes of this sub-section, "dowry" shall have the same meaning as in section 2 of the Dowry Prohibition Act, 1961 (28 of 1961).
(2) Whoever commits dowry death shall be punished with imprisonment for a term which shall not be less than seven years but which may extend to imprisonment for life."

[56] Indian Penal Code, 1860 (Act 45 of 1860), s.306 state that "Abetment of suicide. "If any person commits suicide, whoever abets the commission of such suicide, shall be punished with imprisonment of either description for a term which may extend to ten years, and shall also be liable to fine."

[57] Indian Penal Code, 1860 (Act 45 of 1860), s.498A says that "Husband or relative of husband of a woman subjecting her to cruelty- Whoever, being the husband or the relative of the husband of a woman, subjects such woman to cruelty shall be punished with imprisonment for a term which may extend to three years and shall also be liable to fine.
Explanation: For the purposes of this section, "cruelty" means
(*a*) any wilful conduct which is of such a nature as is likely to drive the woman to commit suicide or to cause grave injury or danger to life, limb or health (whether mental or physical) of the woman; or
(*b*) harassment of the woman where such harassment is with a view to coercing her or any person related to her to meet any unlawful demand for any property or valuable security or is on account of failure by her or any person related to her to meet such demand."

morality.[58] In fact, these offences are as much in the interest of the women as in the interest of public morality and decent behaviour. With a view to curb the growing menace of criminal assault and harassment against women in recent years, four new type of offence introduced in Indian Penal Code *vide* Criminal Law (Amendment) Act, 2013. They are follows:

(i) Sexual Harassment: Section 354A

Section 354A defines sexual harassment and provides punishment for such crime which may be extended upto one or three years of imprisonment or fine depending upon the gravity of the crime.[59]

(ii) Assault to Disrobe Women: Section 354B

If man assaults or uses criminal force to disrobe a woman, then Section 354B provides punishment which shall not be less than three years, but may extend upto seven years of imprisonment and fine.[60]

(iii) Voyeurism: Section 354C

Section 354C has made voyeurism an offence.[61] If any person watches or captures the image of women engaged in private act, he may be punished with a minimum of three years of imprisonment which may extend upto seven years and fine.

---

[58] Indian Penal Code, 1860 (Act 45 of 1860), ss. 354A, 354B, 354C,354D has been inserted and s. 354 has been substituted for old s. 354 by The Criminal Law (Amendment) Act, 2013.

[59] Indian Penal Code, 1860 (Act 45 of 1860), s.354A state that "Sexual harassment and punishment for sexual harassment -(1) A man committing any of the following acts-
(i) physical contact and advances involving unwelcome and explicit sexual overtures; or
(ii) a demand or request for sexual favours; or
(iii) showing pornography against the will of a woman; or
(iv) making sexually coloured remarks,
shall be guilty of the offence of sexual harassment.
(2) Any man who commits the offence specified in clause (i) or clause (ii) or clause (iii) of sub-section (1) shall be punished with rigorous imprisonment for a term which may extend to three years, or with fine, or with both.
(3) Any man who commits the offence specified in clause (iv) of sub-section (1) shall be punished with imprisonment of either description for a term which may extend to one year, or with fine, or with both."

[60] Indian Penal Code, 1860 (Act 45 of 1860), s.354B state that "Assault or use of criminal force to woman with intent to disrobe- Any man who assaults or uses criminal force to any woman or abets such act with the intention of disrobing or compelling her to be naked, shall be punished with imprisonment of either description for a term which shall not be less than three years but which may extend to seven years, and shall also be liable to fine."

[61] Indian Penal Code, 1860 (Act 45 of 1860), s.354C state that "Voyeurism- Any man who watches, or captures the image of a woman engaging in a private act in circumstances where she would usually have the expectation of not being observed either by the perpetrator or by any other person at the behest of the

(iv) Stalking: Section 354D

Section 354D has make stalking an offence under Indian Penal Code[62] and provides punishment for same. This section also punishes the offender who stalks online by using the computer network.

F. Importation of Girls up to 21 Years of Age (Section 366B of The Indian Penal Code)

Section 366 B provide for punishment for importation of girl under age of 21 years for illicit intercourse with another person. This Section protects the women who were imported into the foreign countries for prostitution. This Section seeks to prevent the prostitution running in India.[63]

---

perpetrator or disseminates such image shall be punished on first conviction with imprisonment of either description for a term which shall not be less than one year, but which may extend to three years, and shall also be liable to fine, and be punished on a second or subsequent conviction, with imprisonment of either description for a term which shall not be less than three years, but which may extend to seven years, and shall also be liable to fine.

Explanation 1- For the purpose of this section, "private act" includes an act of watching carried out in a place which, in the circumstances, would reasonably be expected to provide privacy and where the victim's genitals, posterior or breasts are exposed or covered only in underwear; or the victim is using a lavatory; or the victim is doing a sexual act that is not of a kind ordinarily done in public.

Explanation 2- Where the victim consents to the capture of the images or any act, but not to their dissemination to third persons and where such image or act is disseminated, such dissemination shall be considered an offence under this section."

[62] Indian Penal Code, 1860 (Act 45 of 1860), s.354D state that "Stalking- (1) Any man who-

(i) follows a woman and contacts, or attempts to contact such woman to foster personal interaction repeatedly despite a clear indication of disinterest by such woman; or

(ii) monitors the use by a woman of the internet, email or any other form of electronic communication, commits the offence of stalking:

Provided that such conduct shall not amount to stalking if the man who pursued it proves that--

(i) it was pursued for the purpose of preventing or detecting crime and the man accused of stalking had been entrusted with the responsibility of prevention and detection of crime by the State; or

(ii) it was pursued under any law or to comply with any condition or requirement imposed by any person under any law; or

(iii) in the particular circumstances such conduct was reasonable and justified.

(2) Whoever commits the offence of stalking shall be punished on first conviction with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine; and be punished on a second or subsequent conviction, with imprisonment of either description for a term which may extend to five years, and shall also be liable to fine."

[63] Indian Penal Code, 1860 (Act 45 of 1860), s.366B state that "Whoever imports into India from any country outside India or from the State of Jammu and Kashmir, any girl under the age of twenty-one years with intent that she may be, or knowing it to be likely that she will be, forced or seduced to illicit intercourse with another person, shall be punishable with imprisonment which may extend to ten years and shall also be liable to fine."

G. Insult to the Modesty of a Women (Eve Teasing) (Section 509 or 294 The Indian Penal Code)[64]

Although, Indian Penal Code does not use term 'eve teasing' or 'street sexual harassment' but the women victim can take recourse through Section 294[65] and Section 509. It is a form of sexual harassment or aggression that range in severity. Section 509 specifically talks about the insult and modesty of women,[66] whereas, Section 354 says about the outrage the modesty of the women. Section 509 was amended *vide* Criminal Law (Amendment) Act, 2013 to enhance the punishment from one year imprisonment to three years imprisonment.

H. Of Voluntarily Causing Grievous Hurt by Throwing Acid (Sections 326A & Section 326B the Indian Penal Code)[67]

Section 326A and Section 326B was introduced by The Criminal Law (Amendment) Act, 2013 in pursuance to the recommendation of J. S. Verma Committee Report. Section 326A says that voluntarily causing grievous hurt by use of acid[68] and Section 326B says voluntarily throwing or attempting to throw acid.[69] Both sections seek to protect the women from an acid attack which is very rampant in the society.

---

[64] The Indian Penal Code, 1860, s. 509 has been substituted for s. 509 the Indian Penal Code by The Criminal Law Amendment Act, 2013.

[65] Indian Penal Code, 1860 (Act 45 of 1860), s.294 state that "Whoever, to the annoyance of others:
Does any obscene act in any public place, or sings, recites or utters any obscene song, ballad or words, in or near any public place, shall be punished with imprisonment of either description for a term which may extend to three months, or with fine, or with both".

[66] Indian Penal Code, 1860 (Act 45 of 1860), s.509 says that "Whoever, intending to insult the modesty of any woman, utters any words, makes any sound or gesture, or exhibits any object, intending that such word or sound shall be heard, or that such gesture or object shall be seen, by such woman, or intrudes upon the privacy of such woman, [shall be punished with simple imprisonment for a term which may extend to three years, and also with fine]".

[67] The Indian Penal Code, 1860, ss. 326A and 326B has been inserted by The Criminal Law Amendment Act, 2013.

[68] Indian Penal Code, 1860 (Act 45 of 1860), s.326A state that "Whoever causes permanent or partial damage or deformity to, or burns or maims or disfigures or disables, any part or parts of the body of a person or causes grievous hurt by throwing acid on or by administering acid to that person, or by using any other means with the intention of causing or with the knowledge that he is likely to cause such injury or hurt, shall be punished with imprisonment of either description for a term which shall not be less than ten years but which may extend to imprisonment for life, and with fine:
Provided that such fine shall be just and reasonable to meet the medical expenses of the treatment of the victim: Provided further that any fine imposed under this section shall be paid to the victim".

[69] Indian Penal Code, 1860 (Act 45 of 1860), s.326B state that "Whoever throws or attempts to throw acid on any person or attempts to administer acid to any person, or attempts to use any other means, with the

I. Of Offences Relating to Marriage (Sections 493 to 498 the Indian Penal Code)[70]

Section 493 of Indian Penal Code penalises cohabitation caused by man deceitfully inducing a belief of lawful marriage.[71]

Section 494 deals with the offence relating to bigamy, it means marrying in lifetime of husband or wife. It is gender neutral provision; it's also applicable irrespective of gender. Bigamy has been made a punishable offence under this section.[72]

Further, Section 497 of Indian Penal Code defines and punishes the offence of adultery.[73]

Section 498 of Indian Penal Code states that whoever either takes or entices away any woman who is and who he knows to be or has reason to believe to be the wife of any person, with intention that she may have illicit intercourse with him or any person.[74]

---

intention of causing permanent or partial damage or deformity or burns or maiming or disfigurement or disability or grievous hurt to that person, shall be punished with imprisonment of either description for a term which shall not be less than five years but which may extend to seven years, and shall also be liable to fine".

[70] Suman Soni, *Women in 21st Centuary* 148-153 (DND Publications, Jaipur, 2012).

[71] Indian Penal Code, 1860 (Act 45 of 1860), s.493 state that "Every man who by deceit causes any woman who is not lawfully married to him to believe that she is lawfully married to him and to cohabit or have sexual intercourse with him in that belief, shall be punished with imprisonment of either description for a term which may extend to ten years, and shall also be liable to fine."

[72] Indian Penal Code, 1860 (Act 45 of 1860), s.494 state that "Whoever, having a husband or wife living, marries in any case in which such marriage is void by reason of its taking place during the life of such husband or wife, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.

Exception: This section does not extend to any person whose marriage with such husband or wife has been declared void by a Court of competent jurisdiction,

nor to any person who contracts a marriage during the life of a former husband or wife, if such husband or wife, at the time of the subsequent marriage, shall have been continually absent from such person for the space of seven years, and shall not have been heard of by such person as being alive within that time provided the person contracting such subsequent marriage shall, before such marriage takes place, inform the person with whom such marriage is contracted of the real state of facts so far as the same are within his or her knowledge."

[73] Indian Penal Code, 1860 (Act 45 of 1860), s.497 state that "Whoever, dishonestly or with a fraudulent intention, goes through the ceremony of being married, knowing that he is not thereby lawfully married, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine".

[74] Indian Penal Code, 1860 (Act 45 of 1860), s.498 state that "Whoever takes or entices away any woman who is and whom he knows or has reason to believe to be the wife of any other man, from that man, or from any person having the care of her on behalf of that man, with intent that she may have illicit intercourse with any person, or conceals or detains with that intent any such woman, shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both".

J. Causing of Miscarriage, Injuries to Unborn Child etc. (Sections 312 To 318 of Indian Penal Code)

Section 312 of Indian Penal Code punishes the offence of causing miscarriage. According to this section whoever voluntarily causes a women to miscarry is liable to be punished. The offence under this section is non cognizable, bailable and non-compoundable.[75] Section 313 says that whoever commit the offence as defined under Section 312 without the consent of women whether the women is quick with child or not, shall be punished.[76]

Section 314 of Indian Penal Code penalises causing death by an act done with intention of causing miscarriage.[77] Section 315 says that whoever before the birth of any child does any act with the intention of thereby preventing that child from being born alive or causing it to die after its birth, such person shall be liable for punishment provided under this section.[78] Section 316 section states that whoever does any act, under such circumstances that if he thereby caused death he would be liable.[79] Section 317

[75] Indian Penal Code, 1860 (Act 45 of 1860), s.312 state that "Whoever voluntarily causes a woman with child to miscarry, shall, if such miscarriage be not caused in good faith for the purpose of saving the life of the woman, be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both; and, if the woman be quick with child, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.
Explanation- A woman who causes herself to miscarry, is within the meaning of this section."

[76] Indian Penal Code, 1860 (Act 45 of 1860), s.313 state that "Whoever commits the offence defined in the last preceding section without the consent of the woman, whether the woman is quick with child or not, shall be punished with [imprisonment for life], or with imprisonment of either description for a term which may extend to ten years, and shall also be liable to fine."

[77] Indian Penal Code, 1860 (Act 45 of 1860), s.314 state that "Whoever, with intent to cause the miscarriage of a woman with child, does any act which causes the death of such woman, shall be punished with imprisonment of either description for a term which may extend to ten years, and shall also be liable to fine;
If act done without woman's consent and if the act is done without the consent of the woman, shall be punished either with [imprisonment for life], or with the punishment above mentioned.
Explanation: It is not essential to this offence that the offender should know that the act is likely to cause death."

[78] Indian Penal Code, 1860 (Act 45 of 1860), s.315 state that "Whoever before the birth of any child does any act with the intention of thereby preventing that child from being born alive or causing it to die after its birth, and does by such act prevent that child from being born alive, or causes it to die after its birth, shall, if such act be not caused in good faith for the purpose of saving the life of the mother, be punished with imprisonment of either description for a term which may extend to ten years, or with fine, or with both."

[79] Indian Penal Code, 1860 (Act 45 of 1860), s.316 state that "Whoever does any act under such circumstances, that if he thereby caused death he would be guilty of culpable homicide, and does by

penalised exposure and abandonment of child under 12 years by parents or person having care of it. This Section deals with liability of the father or mother of the child or any person who has the care of the child.[80] Section 318 of the IPC punishes the concealment of the birth by secret disposal of dead body of child.[81]

Conclusively, despite the various protective legal provisions as mentioned above, the plight of the women has not changed till today, still women suffer the menace of crime.

4.3.2. Other Statutory Provisions Related to Crime against Women

Various provisions of law relating to women have been reviewed periodically and amendments carried out to keep pace with the emerging needs. Some of the acts which have special provisions to safeguard women and their interest are as follows:

4.3.2.1. The Immoral Trafficking(Prevention) Act, 1956

In 1950, the Government of India ratified the International Convention for the suppression of immoral traffic in person and the exploitation of the prostitution of others. In 1956, India passed the Suppression of Immoral Traffic in Women and Girls Act, 1956 (SITA). The Act was further amended and changed in 1986, resulting in the Immoral Traffic Prevention Act also known as PITA. PITA only discusses trafficking in relation to prostitution and not in relation to other purposes of trafficking such as domestic worker, child labour, organ harvesting, etc.[82] Trafficking of the women generally starts on the

such act cause the death of a quick unborn child, shall be punished with imprisonment of either description for a term which may extend to ten years, and shall also be liable to fine".

[80] Indian Penal Code, 1860 (Act 45 of 1860), s.317 state that "Whoever being the father or mother of a child under the age of twelve years, or having the care of such child, shall expose or leave such child in any place with the intention of wholly abandoning such child, shall be punished with imprisonment of either description for a term which may extend to seven years, or with fine, or with both.
Explanation: This section is not intended to prevent the trial of the offender for murder or culpable homicide, as the case may be, if the child dies in consequence of the exposure".

[81] Indian Penal Code, 1860 (Act 45 of 1860), s.318 state that "Whoever, by secretly burying or otherwise disposing of the dead body of a child whether such child die before or after or during its birth, intentionally conceals or endeavors to conceal the birth of such child, shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both".

[82] N. B. Chandrakala, and G. Indira Priyadarsini (ed.), *Women Rights and Gender Justice* 95 (Regal Publication, New Delhi, 2015).

promise of job or marriage by which recruiters entice the victims to leave home. Further, the village girls and their families are often deceived by the agents.

The following is an outline of the provisions in this law that pertains to children below the age of 18.

Section 5 of the Act states that if a person procures, induces or takes a child for the purpose of prostitution then the prison sentence is a minimum of seven years but can be extended to life.[83] If a person if found with a child it is assumed that he has detained that child there for the purpose of sexual intercourse or any person committing prostitution in public extend with a child and hence shall be punishable to seven years in prison up to life imprisonment, or a term which may extend to ten years and also a maximum fine of one lakh rupees.

In 2006, the Ministry of Women and Child Development proposed an amendment bill that is yet to be passed. The amendment does not really concern any of the provisions related to the child but has many important consequences for the right of women sex workers.

4.3.2.2. The Dowry Prohibition Act, 1961

The Dowry Prohibition Act, 1961 was enacted by Parliament in 1961 to promote marital and family harmony. The dowry legislation have also been criticised by the women's organisations. Among the most important criticism is confusion of meaning between "dowry" and "gift". Section 2 of the Dowry Prohibition Act, 1961 defines the "dowry".[84] The law disallowed giving and receiving dowry but allowed one to receive gifts. Demand for cash, gold, car or any other type of property also constitutes dowry. Giving taking or demanding or even advertising for dowry is an offence. Despite the legislation protecting the rights of women, most importantly the prohibition of giving and taking of dowry under the Dowry Prohibition Act, 1961, women in India are

[83] Immoral Traffic Prevention Act, 1956(Act 104 of 1956) s.5.

[84] The Dowry Prohibition Act, 1961(Act 28 of 1961), s.2 state that, "Dowry" means any property or valuable security given or agreed to be given either directly or indirectly by one party to the other at or before or at any time after marriage.

tortured physically and mentally, even killed for bringing insufficient dowry.[85] This enactment is for the protection of women from such harassments.

4.3.2.3. The Indecent Representation of Women (Prohibition) Act, 1986

The Indecent Representation of Women (Prohibition) Act was enacted in 1986 by Indian Parliament in response to demands from the women's movement to prevent the offensive depiction of women in the media. They believed that the media was perpetrating a social norm that further objectified the women. The Indecent Representation of Women (Prohibition) Act explicitly prohibitss "the Indecent Representation of Women through advertisement or in publications, writing, paintings, and figures or in any other manner." It defines "Indecent Representation" as follows:

"The depiction in any manner of the figure of a women; her form body or any part thereof in such way as to have the effect of being indecent, or derogatory to, or denigrating women, or is likely to deprave, corrupt or injure the public morality or morals."[86]

This Act provides punishment for the indecent representation of women. This Act prohibits the publication of any advertisement which contains indecent representation of women in any form.[87] Despite the provision in the law to punish violator, the law has not been effectively enacted. If the offence is committed by the company then Section 7 will be apply. Its further states that companies where any kind of "Indecent Representation of Women" (such as the display of pornography) takes place in the premises shall be deemed guilty of offence and shall be liable to be proceeded against and punished

[85] Babita Chaugh, *Women and Crime* 13(Rajat Publication, New Delhi, 2015).
[86] The Indecent Representation of Women (Prohibition) Act, 1986 (Act 60 of 1986), s. 2(c).
[87] The Indecent Representation of Women (Prohibition) Act, 1986 (Act 60 of 1986), s. 6 state that "Any person who contravenes the provisions of section 3 (Prohibition of advertisements containing indecent representation of Women) or section 4 (Prohibition of publication or sending by post of books, pamphlets, etc. containing indecent representation of women) shall be punishable on the first conviction with imprisonment of either description for a term which may extend to two years, and with fine which may extend to two thousand rupees, and in the event of a second or subsequent conviction with imprisonment for term of not less than six months but which may extend to five years and also with a fine not less than ten thousand rupees but which may extend to rupees one lakh.

accordingly.[88] This Act not amended even technological development and crime through use of technology. Procedure for remedy under this Act is that a person has to file a complaint in the nearest police station if any such offence occurs. The rest of the procedure shall be carried out in accordance with law.

4.3.2.4. The Protection of Women from Domestic Violence Act, 2005

The Protection of Women from Domestic Violence Act (43 of 2005) of 2005 was enacted to provide for more effective protection of the rights of women guaranteed under the Constitution of India who are victims of "domestic violence". This Act was enacted in 2005, the very first time in the history of Indian Laws recognised physical and sexual abuse, and it was implemented from October, 2006. The Act broadens the Definition of "Domestic Violence" is under Section 3 of the Act[89] and its cover the following kinds of abuses;

[88] Chanchal Sinha and Prateeksha Tyagi, "Women's Indecent Portrayal in Media" in Vidya Jain and Rashmi Jain, *Women Media and Violence* 100 (Rawat Publication, New Delhi, 2016).

[89] The Domestic Violence Act, 2005, s. 3 define "domestic violence" it includes, "any act, omission or commission or conduct of the respondent shall constitute domestic violence in case it-
(a) harms or injures or endangers the health, safety, life, limb or well-being, whether mental or physical, of the aggrieved person or tends to do so and includes causing physical abuse, sexual abuse, verbal and emotional abuse and economic abuse; or
(b) harasses, harms, injures or endangers the aggrieved person with a view to coerce her or any other person related to her to meet any unlawful demand for any dowry or other property or valuable security; or
(c) has the effect of threatening the aggrieved person or any person related to her by any conduct mentioned in clause (a) or clause (b); or
(d) otherwise injures or causes harm, whether physical or mental, to the aggrieved person. Explanation I. For the purposes of this section,
(i) "physical abuse" means any act or conduct which is of such a nature as to cause bodily pain, harm, or danger to life, limb, or health or impair the health or development of the aggrieved person and includes assault, criminal intimidation and criminal force;
(ii) "sexual abuse" includes any conduct of a sexual nature that abuses, humiliates, degrades or otherwise violates the dignity of woman;
(iii) "verbal and emotional abuse" includes
(a) insults, ridicule, humiliation, name calling and insults or ridicule specially with regard to not having a child or a male child; and
(b) repeated threats to cause physical pain to any person in whom the aggrieved person is interested.
(iv) "economic abuse" includes
(a) deprivation of all or any economic or financial resources to which the aggrieved person is entitled under any law or custom whether payable under an order of a court or otherwise or which the aggrieved person requires out of necessity including, but not limited to, household necessities for the aggrieved person and her children, if any, stridhan, property, jointly or separately owned by the aggrieved person, payment of rental related to the shared household and maintenance;

- *Physical abuse,*
- *Sexual abuse*
- *Verbal and emotional abuse and*
- *Economic abuse*

The Act further broadens the definition of domestic relationships by including mothers, wives, sister-in-laws, daughters, and daughter-in-laws. Beneficiaries under the Act are: Women, Children and Respondent. It is important to note, at this stage, that domestic violence constitute a wide range of conduct and affect an array as relationship.[90]

The Act recognizes a life free of violence and fear and makes the state responsible for extending protection against domestic violence to women. This Act was enacted to seek to protect women from all forms of domestic violence and check harassment and exploitation by family members or relatives. This Act also provides the civil remedies to the victim who facing the domestic violence.

- **Procedure of filing complaint and the Court's Duty (Sections 12-29)**

The aggrieved person or any other witness of the offence can approach a Police officer, Protection Officers or Service Provider or Magistrate. The Magistrate shall give a notice of the date of hearing to the Protection officers within a maximum period of 2 days or such further reasonable time as allowed by the Magistrate. The court is required to dispose the case within 60 days of the first hearing. Upon finding the complaint to be genuine, the Magistrate may, direct the respondent or the aggrieved person, either singly or jointly, to undergo counseling; direct that the women shall not be evicted or excluded

(b) disposal of household effects, any alienation of assets whether movable or immovable, valuables, shares, securities, bonds and the like or other property in which the aggrieved person has an interest or is entitled to use by virtue of the domestic relationship or which may be reasonably required by the aggrieved person or her children or her stridhan or any other property jointly or separately held by the aggrieved person; and

(c) Prohibition or restriction to continued access to resources or facilities which the aggrieved person is entitled to use or enjoy by virtue of the domestic relationship including access to the shared household. Explanation II.—For the purpose of determining whether any act, omission, commission or conduct of the respondent constitutes "domestic violence" under this section, the overall facts and circumstances of the case shall be taken into consideration."

[90] Nitu Narwal and R.K. Sharma, *Domestic Violence against Women: Legal Protection, Legislative and Judicial Aspect* 11(Regal Publication, New Delhi, 2013).

from the household or any part of it; pass a protection order, providing protection to the women which shall remain in force till the aggrieved person applies for discharge; grant monetary relief to meet the expenses incurred and losses suffered by the aggrieved person and any child of the aggrieved person due to domestic violence; grant custody orders of any child or children of aggrieved person; compensation/damages for the injuries including mental torture and emotional distress caused by domestic violence. If upon receipt of an application from the aggrieved person, the Magistrate is satisfied that the circumstances so require, he may alter, modify or revoke an order after recording the reasons in writing. A complaint can also be filed under Section 498-A of the Indian Penal Code.

4.3.2.5. The Protection of Children from Sexual Offences (POCSO) Act, 2012

Prior to 2012, India had a very limited legal understanding about crime against children. The Protection of Children from Sexual Offence Act, 2012 introduced new arenas of child rights whereby the law meant for prevention of sexual offence also recognized a child's rights for gender orientation. The Protection of Children from Sexual Offence Act, 2012 thereby recognised rights of all children irrespective of gender and gender orientation to be protected against sexual abuse from perpetrator be any one including adult and children, irrespective of gender and gender orientation.[91] The Act came into force on 14th November, 2012. The Act was enacted to provide a vigorous legal framework for the protection of children from offences of sexual assault, sexual harassment and pornography, while safeguarding the interest of the child at every stage of the judicial process. The framing of the Act seeks to put children first by making it easy to use by including mechanisms for child friendly reporting, recording of evidence, investigation and speedy trial of offences through designated Special Courts. The Act makes abetment of child sexual abuse an offence.

[91] Debrati Halder, *Child Sexual Abuse and Protection Laws in India* 57 (Sage Publication, New Delhi, 2018).

Offences under the Act includes

- **Penetrative Sexual Assault:** When any person penetrates his penis, inserts or manipulates any part of the body of the child so as to cause penetration into the vagina, urethra, anus or any part of body of the child or makes the child to do so with him or any other person; or he applies his mouth to the penis, vagina, anus, urethra of the child or makes the child to do so to such person or any other person is said that he has committed the offence of "penetrative sexual assault".[92] The person shall be punished with imprisonment not less than seven years but which may extend to life imprisonment.[93]
- **Aggravated Penetrative Sexual Assault:** Whoever being a police officer, member of armed forces or security forces, public servant, management or staff of jail/remand home/protection home/ observation home or any other place of custody, management or staff of a hospital whether Government or Private, management or staff of educational institution or religious institution commit penetrative sexual assault on child is said to commit aggravated penetrative sexual assault.[94] The person who

[92] The Protection of Children from Sexual Offence Act, 2012 (Act 32 of 2012), s.3 state that "A person is said to commit "penetrative sexual assault" if-
(a) he penetrates his penis, to any extent, into the vagina, mouth, urethra or anus of a child or makes the child to do so with him or any other person; or
(b) he inserts, to any extent, any object or a part of the body, not being the penis, into the vagina, the urethra or anus of the child or makes the child to do so with him or any other person; or
(c) he manipulates any part of the body of the child so as to cause penetration into the vagina, urethra, anus or any part of body of the child or makes the child to do so with him or any other person; or
(d) he applies his mouth to the penis, vagina, anus, urethra of the child or makes the child to do so to such person or any other person."

[93] The Protection of Children from Sexual Offence Act, 2012 (Act 32 of 2012), s.4 provides punishment for penetrative sexual assault.

[94] The Protection of Children from Sexual Offence Act, 2012 (Act 32 of 2012), s.5 state that " (a) Whoever, being a police officer, commits penetrative sexual assault on a child-
(i) within the limits of the police station or premises at which he is appointed; or
(ii) in the premises of any station house, whether or not situated in the police station, to which he is appointed; or
(iii) in the course of his duties or otherwise; or
(iv) where he is known as, or identified as, a police officer; or
(b) whoever being a member of the armed forces or security forces commits penetrative sexual assault on a child-
(i) within the limits of the area to which the person is deployed; or
(ii) in any areas under the command of the forces or armed forces; or
(iii) in the course of his duties or otherwise; or
(iv) where the said person is known or identified as a member of the security or armed forces; or

commits such offence shall be liable to be punished with rigorous imprisonment for a tem not less than 10 years but which may extend to life imprisonment.[95]

(c) whoever being a public servant commits penetrative sexual assault on a child; or
(d) whoever being on the management or on the staff of a jail, remand home, protection home, observation home, or other place of custody or care and protection established by or under any law for the time being in force, commits penetrative sexual assault on a child, being inmate of such jail, remand home, protection home, observation home, or other place of custody or care and protection; or
(e) whoever being on the management or staff of a hospital, whether Government or private, commits penetrative sexual assault on a child in that hospital; or
(f) whoever being on the management or staff of an educational institution or religious institution, commits penetrative sexual assault on a child in that institution; or
(g) whoever commits gang penetrative sexual assault on a child.
Explanation.-When a child is subjected to sexual assault by one or more persons of a group in furtherance of their common intention, each of such persons shall be deemed to have committed gang penetrative sexual assault within the meaning of this clause and each of such person shall be liable for that act in the same manner as if it were done by him alone; or
(h) whoever commits penetrative sexual assault on a child using deadly weapons, fire, heated substance or corrosive substance; or
(i) whoever commits penetrative sexual assault causing grievous hurt or causing bodily harm and injury or injury to the sexual organs of the child; or
(j) whoever commits penetrative sexual assault on a child, which-
(i) physically incapacitates the child or causes the child to become mentally ill as defined under clause (l) of section 2 of the Mental Health Act, 1987 (14 of 1987) or causes impairment of any kind so as to render the child unable to perform regular tasks, temporarily or permanently;
(ii) in the case of female child, makes the child pregnant as a consequence of sexual assault;
(iii) inflicts the child with Human Immunodeficiency Virus or any other life threatening disease or Infection which may either temporarily or permanently impair the child by rendering him physically incapacitated, or mentally ill to perform regular tasks;
[(iv) causes death of the child; or]
(k) whoever, taking advantage of a child's mental or physical disability, commits penetrative sexual assault on the child; or
(l) whoever commits penetrative sexual assault on the child more than once or repeatedly; or
(m) whoever commits penetrative sexual assault on a child below twelve years; or
(n) whoever being a relative of the child through blood or adoption or marriage or guardianship or in foster care or having a domestic relationship with a parent of the child or who is living in the same or shared household with the child, commits penetrative sexual assault on such child; or
(o) whoever being, in the ownership, or management, or staff, of any institution providing services to the child, commits penetrative sexual assault on the child; or
(p) whoever being in a position of trust or authority of a child commits penetrative sexual assault on the child in an institution or home of the child or anywhere else; or
(q) whoever commits penetrative sexual assault on a child knowing the child is pregnant; or
(r) whoever commits penetrative sexual assault on a child and attempts to murder the child; or
(s) whoever commits penetrative sexual assault on a child in the course of [communal or sectarian violence or during any natural calamity or in similar situations]; or
(t) whoever commits penetrative sexual assault on a child and who has been previously convicted of having committed any offence under this Act or any sexual offence punishable under any other law for the time being in force; or
(u) whoever commits penetrative sexual assault on a child and makes the child to strip or parade naked in public, is said to commit aggravated penetrative sexual assault.

[95] The Protection of Children from Sexual Offence Act, 2012 (Act 32 of 2012), s.6 provides punishment for aggravated penetrative sexual assault.

- **Sexual Assault:** Whoever, with sexual intent touches the vagina, penis, anus or breast of the child or makes the child touch the vagina, penis, anus or breast of such person or any other person, or does any other act with sexual intent which involves physical contact without penetration is said to commit sexual assault.[96] Punishment for sexual assault provided under section 8 of the Act.
- **Sexual Harassment**: This Act also defines the sexual harassment and provide punishment for the same.
- **Child Pornography:** In this Act in respect of Pornography, the Act criminalise even watching or collection of pornographic material /content involving children.
- **Aggravated Sexual Assault.**

The Act is gender-neutral. It also provides for various procedural reforms, making the process of trial considerably easier for children.

Child Welfare Committee (CWC): Police officer is duty bound to inform the CWC about every case under the Act within 24 hours. CWC can appoint a support person for the child who will be responsible for psychosocial wellbeing of the child. This support person will also liaise with the police, and keep the child and child's family informed about progress in the case. Procedure for Remedy: Anyone including a child (anyone below 18 years of age) can report an offence to Special Juvenile Police Unit/Local police.

4.3.2.6. The Sexual Harassment at Workplace (Prevention, Prohibition and Redressal) Act, 2013

Indian law rejects sex based discrimination and bias in all forms. The Supreme Court of India pronounced a momentous judgment in ***Vishaka* v. *State of Rajasthan***[97] in 1997, categorically recognizing the menace of sexual harassment at workplace and constitutionally rendering it as being in violation of fundamental rights guaranteed by Articles 15, 19, and 21 of the Constitution of India. The Court also provided a mechanism

[96] The Protection of Children from Sexual Offence Act, 2012 (Act 32 of 2012), s.7.

[97] *Vishaka* v. *State of Rajasthan*, AIR 1997 SC 3011. The petition was brought by as a class action by certain social activists with the aim of focusing attention towards the societal aberration with a view to find out solutions to prevent sexual harassment in the absence of legislative measures. The petition relates to an incident of an alleged brutal gang rape of a social worker in a village of Rajasthan

for redressal against sexual harassment which was ultimately reinforced by Parliament with the enactment of Sexual Harassment at Workplace (Prevention, Prohibition and Redressal) Act, 2013 (POSH Act).[98] It has promulgated a very stringent regulation for the sexual harassment of women at the workplace.

This Act prohibits all kinds of sexist behavior, including unwelcome acts or deeds (directly or by implication), physical contact or advances; demand or request for sexual favors, sexual innuendo, showing pornography; or any other unwelcome physical, verbal or non-verbal conduct of sexual nature. Under the law, it is obligatory for employers to set up Sexual Harassment Committees at workplaces, with a majority of women and an external non-governmental organization representative. Any violation of the law is liable for strict penal action.[99]

Although all laws are not gender specific, the provisions of law affecting women significantly have been reviewed periodically and amendments carried out to keep pace with the emerging requirements. Some acts which have special provisions to safeguard women and their interests are:

1. *The Employees State Insurance Act, 1948*
2. *The Plantation Labour Act, 1951*
3. *The Family Courts Act, 1954*
4. *The Special Marriage Act, 1954*
5. *The Hindu Marriage Act, 1955*
6. *The Hindu Succession Act, 1956 with amendment in 2005*
7. *Immoral Traffic (Prevention) Act, 1956*
8. *The Maternity Benefit Act, 1961 with Amended in 1995*
9. *Dowry Prohibition Act, 1961*
10. *The Medical Termination of Pregnancy Act, 1971*
11. *The Contract Labour (Regulation and Abolition) Act, 1976*

[98] Sanjay Jain and Saranya Mishra, "Scandalizing the Judiciary: An Analysis of the Uneven Response of the Supreme Court of India to Sexual Harassment Allegations against Judges", 18(2) *International Journal of Constitutional Law* 563-590 (2020).

[99] Sangeeta Goel, "Third Generation Sexism in Workplaces: Evidence from India" 24(3) *Asian Journal of Women's Studies*, 368-387(2018).

12. *The Equal Remuneration Act, 1976*
13. *The Prohibition of Child Marriage Act, 2006*
14. *The Criminal Law (Amendment) Act, 1983*
15. *The Factories (Amendment) Act, 1986*
16. *Indecent Representation of Women (Prohibition) Act, 1986*
17. *Commission of Sati (Prevention) Act, 1987*
18. *The Protection of Women from Domestic Violence Act, 2005*

4.4. Cybercrime and Women: A Legislative Overview

Under this technological development era the most effected victim is women. Every sphere of life now a day, starts and ends with digital intervention i.e. computer technological interferences. In the light of this, the positive as well as negative sides also come out. Cybercrime is a global phenomenon. The advancement of technology, cybercrime and victimization of women are on the high and it poses as a major threat to the security of a person as a whole.[100] The privacy and personal security of the individual are under threat with this growing issue of cybercrime in the cyberspace.[101] Internet is world's largest information system and giant network. As telecom infrastructure developments continue to penetrate into smaller towns, Internet usage numbers showcase the effects with its ever increasing base of users. The Internet is now a part of the globalization process that is evidently sweeping away old realities and certainties, creating new opportunities and challenges associated with living in a compact world.[102] The cyberspace has been a blessing to human civilization. Internet has connected people around the globe. The desire to know what is unknown is indispensable of human nature. It is the desire to know about the people, who inhabit the earth, has aggravated the urge of discovering the untrodden path. This has led to the unearthing of the cyber world.[103]

[100] Vakul Sharma, "Information Technology-Law & Practice" 135 (Universal LexisNexis, 5th ed. 2016).
[101] *Available at*: http://www.legalserviceindia.com/artic les/etea.htm. (last visited on 2nd November, 2019).
[102] Vakul Sharma, *Information Technology-Law & Practice* 135 (Universal LexisNexis, 5th ed. 2016).
[103] Fabio Marturana, Simone Tacconi and Giuseppe F. Italiano, "Cybercrime and Cloud Forensics: Applications for Investigation Processes" 313-330 (2013).

In a cybercrime, computer or the data itself 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 cybercrime.

4.4.1. The Information Technology Act, 2000

Let us now discuss in detail, the Information Technology Act, 2000 and the Information Technology (Amendment) Act, 2008 in general and particularly search provision for the protection of women from cybercrime. Before going into the section-wise or chapter-wise description of various provisions of the Act, let us discuss the history behind such a legislation in India, the circumstances under which the Act was passed and the purpose or objectives in passing it.[104]

The Genesis of Information Technology legislation in India: Mid 90's saw an growing thrust of globalization and computerisation, with more and more nations computerizing their governance, and e-commerce seeing an enormous growth. Until then, most of international trade and transactions were done through documents being transmitted through post and by telex only. Evidences and records, until then, were predominantly paper evidences and paper records or other forms of hard-copies only. With much of international trade being done through electronic communication and with email gaining momentum, a dire need was felt for recognizing electronic records i.e. the data what is stored in a computer or an external storage attached thereto.[105]

The United Nations Commission on International Trade Law (UNCITRAL)[106] adopted the Model Law on e-commerce in 1996.[107] The General Assembly of United

[104] S. C. Sharma, *Study of Techno-Legal Aspects of Cybercrime and Cyber Law Legislations* 86 (2nd ed., 2008).

[105] Anirudh Rastogi, *Cyber Law-Law of Information Technology and Internet* 2 (2nd ed. 2014).

[106] There was an international impetus also. The General Assembly created UNICITRAL in the year 1996 and its aim was to harmonize and unify international trade law so as to save the interest of developing countries. The United Nations Commission on International Trade Law (UNCITRAL} adopted Model Law on E-commerce in 1996. The United Nations General Assembly accepted the model and on 30 January 1997 recommended and requested all the States to adopt the model to create a suitable infrastructure through law. India honoured the request of the General Assembly by enacting the Information Technology Act, 2000.

[107] *Available at*: https://www.uncitral.org/pdf/engl ish/texts/electcom/05 -89450_Ebook.pdf. (last visited on 10th November 2019).

Nations passed a resolution in January 1997 inter alia, recommending all States in the UN to give favourable considerations to the said Model Law, which provides for recognition to electronic records and according it the same treatment like a paper communication and record.[108]

Being the member, under this background the Government of India enacted its Information Technology Act, 2000 with the objectives as follows, stated in the preface to the Act itself.

"to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto." [109]

The Information Technology Act, 2000, was thus passed as the Act No. 21 of 2000, got President Assent on 9thJune and was made effective from 17th October 2000. The Act essentially deals with the following issues:

- Legal Recognition of Electronic Documents
- Legal Recognition of Digital Signatures
- Offenses and Contraventions
- Justice Dispensation Systems for cybercrimes.

Thus from the objective of the act it is very clear that it was enacted for very purpose of facilitating e-commerce and once e-commerce has been given the recognition by the government , it ought to provide prosecution and penalties for violation of crime. This was the reason to include Chapter XI, 'Offence and Penalties' in the Information and Technology Act, 2000.

[108] *Available at*: https://www.uncitral.org/pdf/engl ish/texts/electcom/05 -89450_Ebook.pdf. (last visited on 10th November 2019).
[109] The Information Technology Act, 2000 (Act 21 of 2000), Preamble.

But due to increasing cybercrime against individuals and society at large, a dire need was felt to remove the lacunas in Information Technology Act, 2000 and then amend it in 2008.

Researcher analysed the various provisions of the Information Technology Act, 2000 for the protection from cybercrime, specifically targeting the women. Presently, women's are much vulnerable to cyber victimization. The Chapter XI 'Offence and Penalties' in the Information and Technology Act, 2000, deals with the following Cybercrime. They are as follows:

Section 65 deals with tampering with source documents its provide that Concealing, destroying, altering any computer source code when the same is required to be kept or maintained by law is a punishable offence with imprisonment for three years or 2 lakh rupees or with both.[110] Fabrication of an electronic record or committing forgery by way of interpolations in CD produced as evidence in a court which attract punishment under this Section.[111]

Computer source code under this Section refers to the listing of programmes, computer commands, design and layout etc., in any form.

Under this Section 66 dealt with Computer related offences such as Data theft stated in Section 43 is referred to in this Section. Whereas it was a simple civil offence with the remedy of compensation and damages only, in that Section, here it is the same act but with a criminal intention thus making it a criminal offence. The act of data theft or the offence stated in Section 43 if done dishonestly or fraudulently, becomes a punishable offence under this Section and attracts imprisonment upto three years or a fine of five lakh rupees or both. Earlier hacking was defined in Section 66 and it was an offence.[112]

---

[110] The Information Technology Act, 2000 (Act 21 of 2000), s. 65 state that "Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.
Explanation. For the purposes of this section, "computer source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form."

[111] *Bhim Sen Garg* v. *State of Rajasthan and Ors.*, 2006, Cri LJ, 3463, Raj 2411.

[112] The Information Technology Act, 2000 (Act 21 of 2000), s. 66 state that "(1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person

Section 66A provide for Sending offensive messages through communication service, causing annoyance etc., through an electronic communication or sending an email to mislead or deceive the recipient about the origin of such messages (commonly known as IP or email spoofing) are all covered here. Punishment for these acts is imprisonment upto three years or fine.[113]

Section 66B deals with dishonestly receiving stolen computer resource or communication device which attracts punishment for upto three years or fine of rupees one lakh or both.[114]

Section 66C deals with punishment for Electronic signature or other identity theft like using other's password or electronic signature etc., this offence is punishable for three years of imprisonment or fine rupees one lakh or both.[115]

---

destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack:

(2) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend upto two lakh rupees, or with both."

[113] The Information Technology Act, 2000, s.66A state that "Punishment for sending offensive messages through communication service, etc.,- Any person who sends, by means of a computer resource or a communication device,

(a) any information that is grossly offensive or has menacing character; or

(b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device;

(c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages,

shall be punishable with imprisonment for a term which may extend to three years and with fine.

Explanation: For the purposes of this section, terms "electronic mail" and "electronic mail message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.] Substituted by the Information Technology (Amendment) Act, 2008; Section 66A has been struck down by Supreme Court's Order dated 24th March, 2015 in the *Shreya Singhal* v. *Union of India*, AIR 2015 SC. 1523.

[114] The Information Technology Act, 2000 (Act 21 of 2000), s.66B state that "Whoever dishonestly receive or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both."

[115] The Information Technology Act, 2000 (Act 21 of 2000), s.66C state that "Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh."

Section 66D provides punishment for cheating by personation using computer resource or a communication device which shall be punished with imprisonment extend to three years and also he shall be liable to fine for rupees one lakh.[116]

Section 66E provides punishment for Privacy violation whoever publishing or transmitting private area of any person without his or her consent etc. who will be punished with three years imprisonment or two lakh rupees fine or both.[117]

Section 66F deals with Cyber terrorism means whoever intends to threaten the unity, integrity, security or sovereignty of the nation and denying access to any person authorized to access the computer resource or attempting to penetrate or access a computer resource without authorization. Acts of causing a computer contaminant (like virus or *Trojan Horse* or other spyware or malware) likely to cause death or injuries to persons or damage to or destruction of property etc. comes under this Section. Maximum punishment under this section is life imprisonment.[118] It may be observed that all acts

[116] The Information Technology Act, 2000(Act 21 of 2000), s.66D state that "Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

[117] The Information Technology Act, 2000 (Act 21 of 2000), s.66E state that "Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.
Explanation: For the purposes of this section:
(a) transmit means to electronically send a visual image with the intent that it be viewed by a person or persons;
(b) capture, with respect to an image, means to videotape, photograph, film or record by any means;
(c) private area means the naked or undergarment clad genitals, [pubic area], buttocks or female breast:
(d) publishes means reproduction in the printed or electronic form and making it available for public;
(e) under circumstances violating privacy means circumstances in which a person can have a reasonable expectation that:
(i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or
(ii) Any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

[118] The Information Technology Act, 2000(Act 21 of 2000), s.66 F state that: "(1) Whoever,
(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by--
(i) denying or cause the denial of access to any person authorised to access computer resource; or
(ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorised access; or
(iii) introducing or causing to introduce any computer contaminant,
and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies

under Section 66F are cognizable and non-bailable offences.[119] Intention or the knowledge to cause wrongful loss to others i.e. the existence of criminal intention and the evil mind i.e. concept of *Mens Rea*, destruction, deletion, alteration or diminishing in value or utility of data are all the major ingredients to bring any act under this Section.

Section 67 deals with publishing or transmitting obscene material in electronic form.[120] The earlier Section in Information Technology Act, 2000 was later widened as per Information Technology (Amendment) Act, 2008 in which child pornography and retention of records by intermediaries were all included. Publishing or transmitting obscene material in electronic form is dealt with here. Whoever publishes or transmits any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely to read the matter contained in it, shall be punished with first conviction for a term upto three years and fine of five lakh rupees and in second conviction for a term of five years and fine of ten lakh rupees or both.

Section 67A of the Act deals with publishing or transmitting of material containing sexually explicit act in electronic form. Contents of Section 67 when

---

or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70; or

(B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer data base that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer data base, with reasons to believe that such information, data or computer data base so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise,

Commits the offence of cyber terrorism.

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life."; Substituted by the Information Technology (Amendment) Act, 2008,

[119] Jyoti Ratan, *Cyber Laws & Information Technology*, 48 (Bharat Law House, Delhi, 3rd ed., 2017).

[120] The Information Technology Act, 2000 (Act 21 of 2000), s.67 state that " Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees".

combined with the material containing sexually explicit material attract penalty under this Section.[121]

Section 67B related to Child Pornography which is exclusively dealt with under this section. Depicting children engaged in sexually explicit act, creating text or digital images or advertising or promoting such material depicting children in obscene or indecent manner etc., or facilitating abusing children online or inducing children to online relationship with one or more children etc., come under this Section and constitute a penal offence.[122]

Exception of this section is bonafide heritage material being printed or distributed for the purpose of education or literature etc., are specifically excluded from the coverage of this Section, to ensure that printing and distribution of ancient epics or heritage material or pure academic books on education and medicine are not unduly affected.

---

[121] The Information Technology Act, 2000 (Act 21 of 2000), s.67A state that "Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees" ; Substituted by the Information Technology (Amendment) Act, 2008.

[122] The Information Technology Act, 2000(Act 21 of 2000), s.67B state that: "Whoever,
(a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct; or
(b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or
(c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or
(d) facilitates abusing children online, or
(e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children,
shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees:
Provided that provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting representation or figure in electronic form
(i) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting representation or figure is the interest of science, literature, art or learning or other objects of general concern; or
(ii) Which is kept or used for bona fide heritage or religious purposes.
Explanation--For the purposes of this section, "children" means a person who has not completed the age of 18 years"; Substituted by the Information Technology (Amendment) Act, 2008.

Screening video graphs and photographs of illegal activities through Internet all come under this category, making pornographic video or MMS clippings or distributing such clippings through mobile or other forms of communication through the Internet fall under this category.

Section 67C fixes the responsibility to intermediaries that they shall preserve and retain such information as may be specified for such duration and in such manner as the Central Government may prescribe. Non-compliance is an offence with imprisonment upto three years or fine.[123]

This Section 69[124] empowers the Government or agencies as stipulated in the Section, to intercept, monitor or decrypt any information generated, transmitted, received or stored in any computer resource, subject to compliance of procedure as laid down here. This power can be exercised if the Central Government or the State Government, as the case may be, is satisfied that it is necessary or expedient in the interest of sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign

[123] The Information Technology Act, 2000(Act 21 of 2000), s.67C state that: "(1) Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe.
(2) any intermediary who intentionally or knowingly contravenes the provisions of sub-section (1) shall be punished with an imprisonment for a term which may extend to three years and also be liable to fine";Substituted by the Information Technology (Amendment) Act, 2008.

[124] The Information Technology Act, 2000 (Act 21 of 2000), s.69 state that "(1) Where the Central Government or a State Government or any of its officers specially authorised by the Central Government or the State Government, as the case may be, in this behalf may, if satisfied that it is necessary or expedient so to do, in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource.
(2) The procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed.
(3) The subscriber or intermediary or any person in-charge of the computer resource shall, when called upon by any agency referred to in sub-section (1), extend all facilities and technical assistance to
(a) provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or
(b) intercept, monitor, or decrypt the information, as the case may be; or
(c) provide information stored in computer resource.
(4) The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with imprisonment for a term which may extend to seven years and shall also be liable to fine."

States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence. In any such case too, the necessary procedure as may be prescribed, is to be followed and the reasons for taking such action are to be recorded in writing, by order, directing any agency of the appropriate Government. The subscriber or intermediary shall extend all facilities and technical assistance when called upon to do so.

Section 69A inserted by the Information Technology (Amendment) Act, 2008 vests with the Central Government or any of its officers with the powers to issue directions for blocking for public access of any information through any computer resource, under the same circumstances as mentioned above.[125]

Section 69B discusses the power to authorise to monitor and collect traffic data or information through any computer resource.[126]

Section 71 deals with the Penalty for misrepresentation. If anyone makes any misrepresentation to, or suppresses any fact from the Controller or the Certifying Authority for obtaining licence or electronic signature certificate, then he shall be punished with imprisonment up to two years or fine.

Section 72 of this act provides Penalty for Breach of confidentiality and privacy.[127] If any person who, in pursuance of any of the powers conferred under this

[125] The Information Technology Act, 2000(Act 21 of 2000), s.69A state that: "(1) Where the Central Government or any of its officers specially authorised by it in this behalf is satisfied that it is necessary or expedient so to do, in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the Government or intermediary to block for access by the public or cause to be blocked for access by the public any information generated, transmitted, received, stored or hosted in any computer resource.
(2) The procedure and safeguards subject to which such blocking for access by the public may be carried out, shall be such as may be prescribed.
(3) The intermediary who fails to comply with the direction issued under sub-section (1) shall be punished with an imprisonment for a term which may extend to seven years and also be liable to fine".; Substituted by the Information Technology (Amendment) Act, 2008,

[126] Substituted by the Information Technology (Amendment) Act, 2008,

[127] The Information Technology Act, 2000 (Act 21 of 2000), s.69A state that "Penalty for Breach of confidentiality and privacy- "Save as otherwise provided in this Act or any other law for the time being in force, if any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other

Act, rules or regulations made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

4.4.2. The Information Technology (Amendment) Act, 2008

Being the first legislation in the nation on technology, computers and e-commerce and e-communication, the Act was the subject of extensive debates, elaborate reviews and detailed criticisms, with one arm of the industry criticizing some sections of the Act to be draconian and other stating it is too diluted and lenient. There were some conspicuous omissions too resulting in the investigators relying more and more on the time-tested (one and half century-old) Indian Penal Code even in technology based cases with the Information Technology Act also being referred in the process and the reliance more on Indian Penal Code rather on the Information Technology Act.[128]

Thus, the dire need for an amendment, a detailed one was felt for the Information Technology Act, almost from the year 2003-04 itself. Major industry bodies were consulted and advisory groups were formed to go into the perceived lacunae in the Information Technology Act and comparing it with similar legislations in other nations and to suggest recommendations. Such recommendations were analysed and subsequently taken up as a comprehensive Amendment Act and after considerable administrative procedures, the consolidated amendment called the Information Technology (Amendment) Act, 2008 was placed in the Parliament and passed without much debate, towards the end of 2008 (by which time the Mumbai terrorist attack of 26th November, 2008 had taken place). This Amendment Act got the President assent on 5th Feb, 2009 and was made effective from 27th October, 2009.

material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both".

[128] Substituted by the Information Technology (Amendment) Act, 2008.

Features of the Information Technology (Amendment) Act, 2008 are as follows:

- ❖ Focussing on data privacy
- ❖ Focussing on Information Security
- ❖ Defining cyber café
- ❖ Making digital signature technology neutral
- ❖ Defining reasonable security practices to be followed by corporate
- ❖ Redefining the role of intermediaries
- ❖ Recognising the role of Indian Computer Emergency Response Team
- ❖ Inclusion of some additional cybercrimes like child pornography and
- ❖ cyber terrorism authorizing an Inspector to investigate cyber offences (as against the DSP earlier)

The Information Technology Act, 2000 has no mention of cybercrime in an effective manner until the Amendment in 2008; when some separate offence committed through the medium of information technology are included. However, regretfully enough the response is yet not all pervasive. One such area is in respect of newly born revenge porn and blackmailing under cybercrime against women.

4.5. Women Targeted Cybercrimes: A Critical Evaluation of Information Technology Act, 2000

There cannot be any debate that Information Technology Act, 2000, offers different types of safety and securities. Thus, it includes the different types of aspects of the Information Technology and rules passed by the laws should be given to cover the uncharted field in such respect.

(i) Problems Underlying Tracking of Offence

It has been noticed that most of the times it become difficult to trace the person involved in the offence. It gets very hard to track them because it requires a suitable law that states the enforcing mechanism through cyber border co-operation of governments, businesses and institutions of other countries.[129] Unlike India, there are several countries

[129] Vimlendu Tayal, Cyber *Law Cybercrime Internet and E-commerce* 65 (Bharat Law Publication, Jaipur, 2011).

that do not have strict laws to tackle the crimes related with computer. Thus, due to the deficiency of appropriate laws available in india a lot of investigation is to be done while handling such cybercrime cases against women.[130] This might take a lot of time. Hence, just because of such leniency the offender become more confident and commits the crime without any fear. Therefore, the cybercrime against women are day by day increasing and accused are far away from the clutches of the criminal administrative authority.

(ii) Liability of Internet Service Provider

The Section 79 of the Information Technology Act, 2000 that deals with the liability of the Internet Service Provider (ISP) transfer the data that is related to some of the third party; without any interaction of the humans. Thus, it is not useful until the crime had occurred within his knowledge and in fact, it is not easy to prove it. A person can very easily escape under the exemption clause only if he is able to prove that it was done unknowingly i.e. without his knowledge. Other way is that he did it due to alertness for preventing the crime. It is hard to prove the commission of offence as the terms "due diligence" and "lack of knowledge" have not been defined anywhere in the Act.

(iii) No Specific Mention of Extra-Territoriality

Section 75 in the Act reflects the relation to the extra-territorial application of the Act.[131] It has been seen that the cybercrime is committed by the offenders belonging to different countries and operated from diverse part of the world. Hence, it is also known as an international crime. Hence, the Act does not explain how the extraterritoriality would be imposed. This condition is completely avoided by the Act, while it had come into existence to look into cybercrime which is on the face of it an international problem with no territorial boundaries.

In the current scenario the operation of the Information Technology Act in terms of protecting the data and maintains the privacy of the data, in relation to the legal agreements amongst the parties, the actual boards have been visited again and few of the amendments binds the provisions have been provided for. The things which are to be considered are: a new section should be introduced that deals with the personal data or

[130] *Ibid.*
[131] The Information Technology Act, 2000 (Act 21 of 2000), s. 75.

information. It must provide the classification of the asperity of the computer in relation with the offences related with the unfaithful subscriber.[132] Therefore, a new section has been included to the address revenge porn cybercrime with higher punishment[133] emergence of electronic evidence as a new discipline for handling computer related offences and uses thereof in the judiciary has been recognized and a provision of examiner of electronic evidence has been introduced.[134]

There are many laws that deal with the subject due to which there is a confusion related to their applicability. And, there is no law that is concerned with the subject especially into it. While the applicability of the legislation picked out from various laws is to handle the issues and no confusion should be created.[135] Therefore, several recommendations were given in this concern. It is important to consider all the laws related to internet so that the integration of the laws can be done by taking all the internet laws to arrive at a Code which is efficient enough to deal with all the problems related to internet crimes.

The current legislations only highlight the issues and problems which are coming across but it does not provide long run outcomes and solutions of such problems. The requirement for the single cyber legislation grows up which is co-ordinated to look after cybercrimes in all respects.

It is said that the Information Technology Act, 2000 is an initiative to overcome the offences relating to information technology, e.g., software piracy, software theft, data theft, misuse of data, making contracts with no intention to perform them or pornography or the commission of sexual offences, e.g., client soliciting. Indian Government Initiatives to deal with cybercrime issues. The main aim of the Indian government's security is to provide a safe cyber ecosystem to the people by building a trust and loyalty. It also focuses upon providing the assurance in the IT organization and communications

[132] The Information Technology Act, 2000 (Act 21 of 2000), s.72A as introduced by the Information Technology (Amendment) Act, 2008.
[133] The Information Technology Act, 2000 (Act 21 of 2000), ss. 67, and new 67 A.
[134] The Information Technology Act, 2000 (Act 21 of 2000), s.79A.
[135] Vimlendu Tayal, *Cyber Law Cybercrime Internet and E-commerce* 67 (Bharat Law Publication, Jaipur, 2011).

in the cyber ecosystem.[136] It even empowers the legal frameworks, maintains a 24X7 set of instruments that helps in identifying the cyber threats, and also to improve the clarity of the ICT products and their services by test and validation of their products. The government of India also intends to build a workforce of 5 lakh skilled professionals. They can do that by providing them proper training and enabling a cyber-safe space through suitable legislative involvement.[137]

The number of rising cyber-crime rates have been increased due to adopting the Digital India initiative. Many government and the Indian enterprises have been set to tackle with the rising crime rates. However, the NCSP (National Cyber Security Policy) is a confirmatory footstep taken on the right track. With the usage of this policy it becomes easy to combine all the old and new agendas under a common framework with a unified objective.[138]

4.6. Revenge Porn and Blackmailing under Indian Law

In India, there is no specific law which criminalising the revenge porn and blackmailing under cybercrime against women. But the law that covers the crime of revenge porn and blackmailing can be read into the provisions of the Information Technology Act, 2000, the Indian Penal Code, 1860.

4.6.1. Under Indian Penal Code, 1860

Section 292 and 293 were added in accordance with the resolution passed by the International Convention for the suppression and circulation of, and traffic in, Obscene Publications, signed at Geneva on 12th September, 1923. Section 292 and 293 were amended by the Indian Penal Code (Amendment) Act 1969. With a view to making the then existing law more definite and clear.[139] In The Indian Penal Code 1860, under Sections 292, 293 and 294 provide for limitations and prohibitions of certain things

[136] R.C. Nigam, *Law of Crimes in India, Principles of Criminal Law* 3 (Asia Pub. House, London, 1st ed. 1965).
[137] Talat Fatima, *Cybercrimes*, 61 (Eastern Book Company, Lucknow, 2nd ed. 2016).
[138] *Ibid* at 69.
[139] K. I. Vibhute, *PSA Pillai's Criminal Law* 700 (Lexis Nexis Butterworth Wadhwa, Nagpur, 10th edn., 2008).

which are obscene with some exception. Section 292 prohibits sale, distribution, publication, export, import etc., of obscene books, pamphlets, papers, writings, drawings, paintings, representations and the like except justifications under this section e.g., literature, art, learning, monuments, etc. and prescribes punishments on first conviction with imprisonment for a term which may extend to two years and with fine which may extend to two thousand rupees, and on second conviction with imprisonment for a term which may extend to five years and also with fine which may extend to five thousand rupees.[140]

[140] The Indian Penal Code, 1860 (Act 45 of 1860), s. 292 state that "(1) For the purposes of sub-section (2), a book, pamphlet, paper, writing, drawing, painting, representation, figure or any other object, shall be deemed to be obscene if it is lascivious or appeals to the prurient interest or if its effect, or (where it comprises two or more distinct items) the effect of any one of its items, is, if taken as a whole, such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.

(2) Whoever,

(a) sells, lets to hire, distributes, publicity exhibits or in any manner puts into circulation, or for purposes of sale, hire, distribution, public exhibition or circulation, makes, produces or has in his possession any obscene book, pamphlet, paper, drawing, painting, representation or figure or any other obscene object whatsoever, or

(b) imports, exports or conveys any obscene object for any of the purposes aforesaid, or knowing or having reason to believe that such object will be sold, let to hire, distributed or publicly exhibited or in any manner put into circulation, or

(c) takes part in or receives profits from any business in the course of which he knows or has reason to believe that any such obscene objects are, for any of the purposes aforesaid, made, produced, purchased, kept, imported, exported, conveyed, publicly exhibited or in any manner put into circulation, or

(d) advertises or makes known by any means whatsoever that any person is engaged or is ready to engage in any act which is an offence under this section, or that any such obscene object can be procured from or through any person, or

(e) offers or attempts to do any act which is an offence under this section,

shall be punished 4[on first conviction with imprisonment of either description for a term which may extend to two years, and with fine which may extend to two thousand rupees, and, in the event of a second or subsequent conviction, with imprisonment of either description for a term which may extend to five years, and also with fine which may extend to five thousand rupees.

Exception.-This section does not extend to

(a) any book, pamphlet, paper, writing, drawing, painting, representation or figure

(i) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting, representation or figure is in the interest of science, literature, art or learning or other objects of general concern, or

(ii) which is kept or used bona fide for religious purposes;

(b) any representation sculptured, engraved, painted or otherwise represented on or in--

(i) any ancient monument within the meaning of the Ancient Monuments and Archaeological Sites and Remains Act, 1958 (24 of 1958), or

(ii) any temple, or on any car used for the conveyance of idols, or kept or used for any religious purpose."

The Section 293 prohibits sale, etc., of obscene objects to young persons and prescribes punishments on first conviction with imprisonment for a term which may extend to three years and with fine which may extend to two thousand rupees, and on second conviction with imprisonment for a term which may extend to seven years and also with fine which may extend to five thousand rupees.[141] Section 294 prohibits obscene acts and songs to annoyance of others in or near any public place and prescribes punishments with imprisonment for a term which may extend to three months or with fine or with both.[142]

Further the revenge porn cybercrime against women looked through the lens of defamation. Thus, the Sections 499 to 502 invoked while dealing with such cases. Defamation is also attracting the civil matter; a person can file a civil suit in case of defamation. The Section 499 prohibit defamation with punishment except certain exceptional cases. This section provides definition of defamation in criminological aspect. [143]

---

[141] The Indian Penal Code, 1860 (Act 45 of 1860), s.293 state that "Whoever sells, lets to hire, distributes, exhibits or circulates to any person under the age of twenty years any such obscene object as is referred to in the last preceding section, or offers or attempts so to do, shall be punished [on first conviction with imprisonment of either description for a term which may extend to three years, and with fine which may extend to two thousand rupees, and, in the event of a second or subsequent conviction, with imprisonment of either description for a term which may extend to seven years, and also with fine which may extend to five thousand rupees].

[142] The Indian Penal Code, 1860 (Act 45 of 1860), s.294 state that "Whoever, to the annoyance of others,
(a) does any obscene act in any public place, or
(b) sings, recites or utters any obscene song, ballad or words, in or near any public place,
shall be punished with imprisonment of either description for a term which may extend to three months, or with fine, or with both.]

[143] The Indian Penal Code, 1860 (Act 45 of 1860), s.499 state that "Whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter excepted, to defame that person.
Explanation 1- It may amount to defamation to impute anything to a deceased person, if the imputation would harm the reputation of that person if living, and is intended to be hurtful to the fellings of his family or other near relatives.
Explanation 2 - It may amount to defamation to make an imputation concerning a company or an association or collection of persons as such.
Explanation 3 - An imputation in the form of an alternative or expressed ironically, may amount to defamation.
Explanation 4 - No imputation is said to harm a person's reputation, unless that imputation directly or indirectly, in the estimation of others, lowers the moral or intellectual character of that person, or lowers the character of that person in respect of his caste or of his calling, or lowers the credit of that person, or

Section 502A has been proposed to be inserted by the Information Technology (Amendment) Bill, 2006 and Information Technology (Amendment) Act, 2008 to protect right to privacy. But this was not passed. Section 505 prohibits making, publishing or circulating any statement or report with intention to conduce public mischief and prescribes punishments with imprisonment for a term which may extend to

---

causes it to be believed that the body of that person is in a lothsome state, or in a state generally considered as disgraceful.

First Exception - Imputation of truth which public good requires to be made or published.—It is not defamation to impute anything which is true concerning any person, if it be for the public good that the imputation should be made or published. Whether or not it is for the public good is a question of fact.

Second Exception- Public conduct of public servants.—It is not defamation to express in good faith any opinion whatever respecting the conduct of a public servant in the discharge of his public functions, or respecting his character, so far as his character appears in that conduct, and no further.

Third Exception - Conduct of any person touching any public question.—It is not defamation to express in good faith any opinion whatever respecting the conduct of any person touching any public question, and respecting his character, so far as his character appears in that conduct, and no further.

Fourth Exception - Publication of reports of proceedings of courts.—It is not defamation to publish substantially true report of the proceedings of a Court of Justice, or of the result of any such proceedings.

Explanation - A Justice of the Peace or other officer holding an enquiry in open Court preliminary to a trial in a Court of Justice, is a Court within the meaning of the above section.

Fifth Exception - Merits of case decided in Court or conduct of witnesses and others concerned.—It is not defamation to express in good faith any opinion whatever respecting the merits of any case, civil or criminal, which has been decided by a Court of Justice, or respecting the conduct of any person as a party, witness or agent, in any such case, or respecting the character of such person, as far as his character appears in that conduct, and no further.

Sixth Exception - Merits of public performance.- It is not defamation to express in good faith any opinion respecting the merits of any performance which its author has submitted to the judgment of the public, or respecting the character of the author so far as his character appears in such performance, and no further.

Explanation- A performance may be submitted to the judgment of the public expressly or by acts on the part of the author which imply such submission to the judgment of the public.

Seventh Exception - Censure passed in good faith by person having lawful authority over another.- It is not defamation in a person having over another any authority, either conferred by law or arising out of a lawful contract made with that other, to pass in good faith any censure on the conduct of that other in matters to which such lawful authority relates.

Eighth Exception - Accusation preferred in good faith to authorised person.—It is not defamation to prefer in good faith an accusation against any person to any of those who have lawful authority over that person with respect to the subject-matter of accusation.

Ninth Exception.-Imputation made in good faith by person for protection of his or other's interests.—It is not defamation to make an imputation on the character of another provided that the imputation be made in good faith for the protection of the interests of the person making it, or of any other person, or for the public good.

Tenth Exception - Caution intended for good of person to whom conveyed or for public good.—It is not defamation to convey a caution, in good faith, to one person against another, provided that such caution be intended for the good of the person to whom it is conveyed, or of some person in whom that person is interested, or for the public good.

three years or with fine or with both.[144] Section 507 prohibits criminal intimidation by an anonymous communication and prescribes punishments with imprisonment for a term which may extend to two years and other punishments as prescribed in Section 506[145] and Section 509 prohibits word, gesture or act intended to insult the modesty of a woman and prescribes punishments with imprisonment for a term which may extend to one year or with fine or with both.[146]

Section 354C which was introduced in the Indian Penal Code, 1860, by the Criminal Law (Amendment) Act of 2013 in the aftermath of the protests following 16th December *Gang Rape Case*. Section 354C provides for the offence of voyeurism. It is a

[144] The Indian Penal Code, 1860 (Act 45 of 1860), s. 505 state that "(1)Whoever makes, publishes or circulates any statement, rumour or report,
(a) with intent to cause, or which is likely to cause, any officer, soldier, [sailor or airman] in the Army, [Navy or Air Force] [of India] to mutiny or otherwise disregard or fail in his duty as such; or
(b) with intent to cause, or which is likely to cause, fear or alarm to the public, or to any section of the public whereby any person may be induced to commit an offence against the State or against the public tranquility; or
(c) with intent to incite, or which is likely to incite, any class or community of persons to commit any offence against any other class or community,
shall be punished with imprisonment which may extend to [three years], or with fine, or with both.
(2) Statements creating or promoting enmity, hatred or ill-will between classes. Whoever makes, publishes or circulates any statement or report containing rumour or alarming news with intent to create or promote, or which is likely to create or promote, on grounds of religion, race, place of birth, residence, language, caste or community or any other ground whatsoever, feelings of enmity, hatred or ill will between different religious, racial, language or regional groups or castes or communities, shall be punished with imprisonment which may extend to three years, or with fine, or with both.
(3) Offence under sub-section (2) committed in place of worship, etc. Whoever commits an offence specified in sub-section (2) in any place of worship or in any assembly engaged in the performance of religious worship or religious ceremonies shall be punished with imprisonment which may extend to five years and shall also be liable to fine.
Exception It does not amount to an offence, within the meaning of this section, when the person making, publishing or circulating any such statement, rumour or report, has reasonable grounds for believing that such statement, rumour or report is true and makes, publishes or circulates it [in good faith and] without any such intent as aforesaid."

[145] The Indian Penal Code, 1860 (Act 45 of 1860), s.506 state that "Whoever commits the offence of criminal intimidation shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both; If threat be to cause death or grievous hurt, etc. and if the threat be to cause death or grievous hurt, or to cause the destruction of any property by fire, or to cause an offence punishable with death or [imprisonment for life], or with imprisonment for a term which may extend to seven years, or to impute unchastity to a woman, shall be punished with imprisonment of either description for a term which may extend to seven years, or with fine, or with both."

[146] The Indian Penal Code, 1860 (Act 45 of 1860), s.509 state that "Whoever, intending to insult the modesty of any woman, utters any words, makes any sound or gesture, or exhibits any object, intending that such word or sound shall be heard, or that such gesture or object shall be seen, by such woman, or intrudes upon the privacy of such woman, shall be punished with simple imprisonment for a term which may extend to three years, and also with fine."

gender specific in its construction. Only a man can commit this offence against a woman. If a man watches or captures the image of a woman engaging in a private act, where she has a reasonable expectation that she would not be observed by any person or there is a dissemination of such image, the perpetrator is to be held liable. The section provides for a gradation of punishment based on first and second conviction. While the punishment for the first conviction is imprisonment for the minimum period of one year which may extend to three years and the liability also includes fine, on the second conviction, the minimum punishment provided is for three years and the maximum extends to seven years.[147] The definition of 'private act' as provided by explanation 1 emphasizes on the expectation of privacy. It is Explanation 2 of the section that deals with the aspect of revenge porn implicitly by providing that if the victim consents to the capture of images or act but not for the purposes of dissemination of the same to any third persons, such dissemination is culpable. There is some overlap between both the aforementioned sections yet, there is a lack of focused law covering the issue of revenge porn in India.

4.6.2. Under The Information Technology Act, 2000

The Information Technology Act, 2000 of Section 67 provide for the penal sanction. This Section 67 does not mention possession of objectionable material and the charge under this section can be brought if a part of the material is proved to be obscene. Section 67 was amended *vide* the Information Technology (Amendment) Act, 2008. The header of this provision was changed from 'publishing of information which is obscene

[147] The Indian Penal Code, 1860 (Act 45 of 1860), s.354C state that "Any man who watches, or captures the image of a woman engaging in a private act in circumstances where she would usually have the expectation of not being observed either by the perpetrator or by any other person at the behest of the perpetrator or disseminates such image shall be punished on first conviction with imprisonment of either description for a term which shall not be less than one year, but which may extend to three years, and shall also be liable to fine, and be punished on a second or subsequent conviction, with imprisonment of either description for a term which shall not be less than three years, but which may extend to seven years, and shall also be liable to fine."
Explanation 1-For the purpose of this section, "private act" includes an act of watching carried out in a place which, in the circumstances, would reasonably be expected to provide privacy and where the victim's genitals, posterior or breasts are exposed or covered only in underwear; or the victim is using a lavatory; or the victim is doing a sexual act that is not of a kind ordinarily done in public.

in electronic form' to punishment for publishing or transmitting obscene material in electronic form'.

The section provide that "whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to rupees one lakh and in the event of a second or subsequent conviction, with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees."[148]

This section is similar to the draft Convention 2000 of the European Council to combat cybercrime problems. Chapter II of the Convention provides that measures to be taken at the national level to combat cyber pornography. Title 3 of the Convention deals with content related offences of which Art. 9 prohibit offences related to cyber pornography and child pornography in cyberspace. Section 67 of the Information Technology Act, 2000 was not enough because when any person uploads or provides pornographic materials then it must be treated as an offence. But Indian Penal Code provides that even possession of pornographic material in computer or devices are prohibited as offence. In jurisdictional issues under Section 75 of the Information Technology Act, 2000 there is need of only one link with computer activity in India to apply the Indian law in foreign country.

Nowadays, internet has entered into our drawing room and even pocket through new technology and communication convergence e.g., computer, pocket PC, wireless, mobile phone, television etc. with internet connection. The demerits of the technological revolution is growth of crime rate in society e.g., child abuse, sexual harassment, digital exploitation of child and women, video clips, use of smart camera or web camera for live sex or pornographic picture of girlfriend, school friend, actor, actress, teachers and other cyber-crimes as well as other abuse and misuse. Enumerations are not exhaustive in

[148] The Information Technology Act, 2000 (Act 21 of 2000), s.67.

Indian contemporary technological era. This problem is not only in India but rather the USA, the UK, Canada, Australia, Pakistan, China, Bangladesh and whole world is facing same problem. International concern in contemporary social phenomenon is how to prevent and control the situation. But the Information Technology Act, 2000 draftsman and legislature were reluctant to mention online child abuse and exploitation of child while drafting, enacting or passing the law. Section 67 only prohibits dissemination of obscene material, pornographic material which corrupts the young person's through indecent exposure. Therefore, we may say 'young person' means child. But it is not child pornography as such. It is suggested for the amendment of Section 67 to increase punishment, define pornography and child pornography under the Information Technology Act, 2000 after DPS-MMS-Clip controversy and to adopt security measures in several occasions before proposed amendments 2006 and 2008.

However, the proposed Information Technology (Amendment) Bill 2006 suggested amendment of Section 67, to introduce Section 67A and other sections (i) to include exceptions for the sake of arts, literature and so forth, (ii) to include pornography in cyberspace as offence. Therefore, by implementation of the Amendment Act drawbacks of our existing law can be repaired but not in totality.

However Sections 67 and 67A do not extend to any books, pamphlets, papers, writings, drawings, paintings, representation or figure in electronic form (i) the publication of which is proved to be justified as being for the public good on the ground that such books, pamphlets, papers, writings, drawings, paintings, representation or figure is in the interest of science, literature, art or learning or other objects of general concern; or (ii) which is kept or used bona fide for religious purposes.

On the other hand the proposed Amendment of 2006 reduced even minimal liability of internet service providers by inserting new Section 67A [149] and amending Section 79 of the Information Technology Act, 2000; and reduced punishment under

[149] The Information Technology Act, 2000 (Act 21 of 2000), s.67A state that "Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees."

Section 67 i.e., from five years it reduced the period of imprisonment to two years on first conviction.

But in the name of science, literature, art, learning and religion purposes any one is allowed to publish and transfer electronic material and documents containing sexually explicit act and conduct. This section is also not clear about the words "sexually explicit act or conduct". Section 67A does not mention the term pornography or obscenity rather uses the words 'sexually explicit act or conduct' which may be more dangerous than obscenity and pornography. Therefore, there is great need of specific definition of the words "sexually explicit act or conduct".

For the prevention and control of cyber pornography and other cybercrimes, the Information Technology Act adopted certain procedural measures. Under Section 68 the Act empowers the Controller to give directions, order to certified Authority or any employee to take necessary action to comply with the provisions of the said Act, rules or any regulations.[150]

Section 69 empowers issue of directions for interception or monitoring or decryption of any information through any computer resources. Interception, monitoring, decryption are very much required to prevent and control cybercrimes. But there is immediate need of suitable safeguards when, why, how and by whom this interception or decryption may be done so that right to privacy may also be preserved and protected to the possible extent which is also proposed to be inserted.[151]

---

[150] The Information Technology Act, 2000 (Act 21 of 2000), s.68 state that "(1) The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made there under.
[(2) Any person who intentionally or knowingly fails to comply with any order under sub-section (1) shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding two years or a fine not exceeding one lakh rupees or with both."

[151] The Information Technology Act, 2000 (Act 21 of 2000), s.69 state that "(1) Where the Central Government or a State Government or any of its officers specially authorised by the Central Government or the State Government, as the case may be, in this behalf may, if satisfied that it is necessary or expedient so to do, in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or

Section 72A of the Information Technology Act, 2000 and Section 502A proposed to be inserted of the Indian Penal Code 1860 after Section 502. Section 69 imposes liability upon subscriber or intermediary or in charge of computer resource to help law enforcement agencies by providing facilities and technical assistance for interception, monitoring and decryption. On the other hand it imposes no responsibility upon internet service providers under Section 67A. Under Section 67A (3) as proposed to be inserted by the Information Technology (Amendment) Bill 2006 empowers service providers to collect, retain and appropriate service charges though there is no express provision under this Act, rule, regulation or notification under which service providers can collect, retain and appropriate e-service charges.

Network service providers and material providers are not the same. Section 79 provides[152] that network service providers are not liable in certain cases if they can prove

monitored or decrypted any information generated, transmitted, received or stored in any computer resource.

(2) The procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed.

(3) The subscriber or intermediary or any person in-charge of the computer resource shall, when called upon by any agency referred to in sub-section (1), extend all facilities and technical assistance to--

(a) provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or

(b) intercept, monitor, or decrypt the information, as the case may be; or

(c) provide information stored in computer resource.

(4) The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with imprisonment for a term which may extend to seven years and shall also be liable to fine."

[152] The Information Technology Act, 2000 (Act 21 of 2000), s.79 state that "(1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him.

(2) The provisions of sub-section (1) shall apply if-

(a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; or

(b) the intermediary does not-

(i) initiate the transmission,

(ii) select the receiver of the transmission, and

(iii) select or modify the information contained in the transmission;

(c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.

(3) The provisions of sub-section (1) shall not apply if-

(a) the intermediary has conspired or abetted or aided or induced, whether by threats or promise or otherwise in the commission of the unlawful act;

(b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource

the data provided by them was without their knowledge in spite of taking reasonable caution to prevent this offence. Here burden of proof that ISPs are innocent is imposed upon service providers. Section 79 states that network service providers are not to be held liable in certain cases. For the removal of doubts, it is declared that no person providing any service as a network service provider shall be liable under this Act, rules or regulations made there under for any third party information or data made available by him if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention. Explanation (a) provides that 'network service' provided means an intermediary. Explanation (b) provides 'third party information' means any information dealt with by a network service provider in his capacity as an intermediary. Section 2(1)(w) of the said Act provides that 'intermediary' with respect to any particular electronic message means any person who on behalf of another person receives, stores or transmits that message or provides any service with respect to that message.

Therefore, we can say the very little or even no liability is imposed upon the service providers to prevent and control cyber pornography and other computer related crimes under the Information Technology Act, 2000. Section 79 has been substituted so that "(1) they shall not be liable for any third party information, data or communication link made available by them when:

a. the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or stored; or
b. the intermediary does not;
    i. initiate the transmission,
    ii. select the receiver of the transmission, and
    iii. select or modify the information contained in the transmission."

controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.
Explanation.- For the purposes of this section, the expression "third party information means any information dealt with by an intermediary in his capacity as an intermediary".

Section 79(3) provides for liability of the ISPs for abetment and conspiracy in the commission of the unlawful act.

The word 'computer' is defined in s. 2(1) of the Information Technology Act, 2000 and Section 2 of the Copyright Act, 1957. It includes entire old and new computer related device, mobile phone with internet connection, television with computer relation and internet connection and wireless network services in the era of communication convergence are to be treated as computer. The Information Technology (Amendment) Act, 2008 proposed certain changes to the existing Information Technology Act, 2000 relating to privacy and cyber pornography.[153]

Along with these amendments, Section 66E was introduced in the Information Technology Act, 2000 by the 2008 amendment in chapter containing offences. The Section provides for punishment on the ground of violation of privacy. It deals with publishing or transmitting the image of a person' private area, captured intentionally or knowingly, under circumstances that violate privacy of that person. The explanation that follows the section lays down definitions of the words 'transmit', 'capture', 'private area', 'publishes' and 'under circumstances violating privacy'. The offence is gender neutral in its language, both in terms of the perpetrator of the crime and in terms of the victim of such crime. The offence is punishable with imprisonment extending to three years or fine not extending beyond 2 lakh rupees or both.

[153] The Information Technology Act, 2000(Act 21 of 2000), s. 66E states that "whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent under circumstances violating the privacy of that persons shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees or with both.
Explanation. For the purposes of this section,
(a) 'transmit' means to electronically send a visual image with the intent that it be viewed by a person or persons;
(b) 'capture' with respect to an image, means to video tape, photograph, film or record by any means;
(c) 'private area' means the naked or undergarment clad genitals, public area, buttocks or female breast;
(d) 'publishes' means reproduction in the printed or electronic form and making it available to public;
(e) 'under circumstances violating privacy' means circumstances in which a person can have a reasonable expectation that
(i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured or
(ii) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place".

Revenge porn and blackmailing treated as the advance form violation of right to privacy. However, there was still no focused law on sexual offence targeting women in Information Technology Act, 2000. Revenge porn and blackmailing cybercrime against women were dealt under various scattered laws.

4.6.3. The Personal Data Protection Bill, 2019

The Personal Data Protection Bill, based on the framework of the European Union Data Privacy Directive (1996), was introduced in the Parliament in 2006 but lapsed subsequently. Prior to the Information Technology Act, 2000, India did not have any legislation addressing the issue of data protection. The Preamble of the Act listed out prevention of cybercrimes and providing adequate data security measures and procedures to protect and facilitate widest possible use of Information Technology worldwide, as one of its main objectives.[154]

However, only after several amendments subsequently did the Information Technology Act, 2000 provide for adequate legal protection for data stored in the electronic medium. It incorporated provisions regarding privacy and data protection by prescribing both civil and criminal liabilities for protecting privacy of individuals.

Further Section 65, in the original the Information Technology Act, 2000, provided for protection of the source code and penalized with imprisonment an fine any tampering with such computer source documents. Section 66 further provided for the definition of hacking and also the punishment for the same. The amendment to Section 66 widened the definition of hacking by including various other means to destroy or alter the data stored in a computer or access the computer in an unauthorized manner without actually mentioning the acts to be hacking. Further, as per section 67C of the amended the Information Technology Act mandates 'intermediaries' to maintain and preserve certain information under their control for durations which are to be specified by law,

[154] Ministry of Communications & Information Technology, Information Technology (Amendment) Act, 2008 comes into force, Press Information Bureau, October 2009, a*vailable at:* http://pib.nic.in/newsite/erelease.aspx?relid=53617 (last visited on 12th Februar , 2020).

failing which they will be subjected to punishment in the form of imprisonment upto three years and fine.

The newly inserted Section 43A makes a start at introducing a mandatory data protection regime in Indian law. The section obliges corporate bodies who 'possess, deal or handle' any 'sensitive personal data' to implement and maintain 'reasonable' security practices, failing which they would be liable to compensate those affected by any negligence attributable to this failure. In addition to the civil remedies spelled out, Section 72A could be used to impose criminal sanctions against any person who discloses information in breach of a contract for services. These amendments have widened the liability for breach of data protection and negligence in handling sensitive personal information.[155]

In February 2011, the Ministry of Information and Technology, published draft rules under Section 43A in order to define "sensitive personal information" and to prescribe "reasonable security practices" that body corporates must observe in relation to the information they hold. These rules have been made in furtherance of India's recognition of a co-regulatory regime for data protection. These rules are evidently an attempt at introducing the Fair Information Practice Principles and the OECD guidelines in the Indian scenario. Additionally, the Government of India, with the help of the Department of Information Technology, is currently working on a holistic law on data protection based on the European Union directive.[156]

The Justice AP Shah Report on Privacy provides for multidimensional and inclusive understanding of the right to privacy to include concerns surrounding data protection on the internet and challenges emerging there from.[157] The privacy approach paper also suggested masquerading a data protection regime through a privacy legislation to address regulations on collection, control, utilization and proper disposal of data,

[155] M. Dasgupta, *Cybercrime in India- A Comparative Study*, 8 (Eastern Law House, New Delhi, 1st ed. 2009).

[156] Data Protection in India, Mazumdar & Co, *available at:* http://www.majmudarindia.com/ pdf / Data%20Protection%20in%20India.pdf. (last visited on 16th Febuary, 2020).

[157] Government of India, "Justice A. P. Shah, Report of the Group of Experts on Privacy" (Planning Commission, October 2012). a*vailable at*: http://planningcommission.nic.in/reports/genrep/ rep_privacy.pdf. (last visited on 16th February, 2020).

which are not covered under the purview of the existing the Information Technology Act. It recommends the applicability of such a regime to public as well private entities and proposes a distinction between personal data and personal sensitive data. [158]

In the present era the digitalization is so common. Thus, every website, mobile apps seek permission to store your information on their server. It is not restricted to any particular area. It took permission from every one sitting in part of the world; therefore, some questions come across such as how critical is this? How can I trust them? Either it is for ads or data analysis? Whatever it is; the Personal Data Protection Bill draft 2019 proposes to store personal data within India only. Hence, without permission it cannot be possess outside the India. This is needed to take approval of Data Protection Agency, as the data cannot be shared to abroad.[159]

The laws were made for the violation of the and heavy penalties were charged i.e. 50 million rupees will be charged for a minor violation and 150 million rupees for serious violation and even the organization executives might be sent to a jail term under the Personal Data Protection Bill, 2019.

4.6.4. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 provides that it is to submit that the defendants were obligated to remove the images and videos from the website or social media platform. Rule 3(2)(b) of the IT Rules, which requires intermediaries, such as, the websites/, internet service providers/ and search engines, within 24 hours of receipt of the complaint made by any individual person in relation to any content, which shows the individual in full or partial nudity or involve in some sexual act or conduct, take all reasonable and practicable

[158] Government of India, "Justice A. P. Shah, Report of the Group of Experts on Privacy" (Planning Commission, October 2012). a*vailable at*: http://planningcommission.nic.in/reports/genrep/ rep_privacy.pdf. (last visited on 16th February, 2020).
[159] *Ibid.*

measures to remove or disable access to such content which is hosted, stored, published or transmitted by it.

4.7. Cybercrime & Cyber security National Policies

(i) National Cyber Security Policy: The government of India introduced the national cyber security policy in the year 2013; that extracts the planned course to defend the country's cyber ecosystem.

(ii) National Critical Information Infrastructure Protection Centre (NCIIPC): The policy was made to protect the India's critical information infrastructure against cyber-crime and terrorism; in 2014.

(iii) National Cyber Security Coordination Centre (NCCC): In 2017, the NCCC was created in order to spread awareness of Cybercrimes in the country.

(iv) Cyber Swachhta Kendra: In the year 2017, this platform was brought into lights for internet users to clean their computers and devices by throwing out viruses and malware.

(v) National Database on Sexual Offenders (NDSO): The Ministry of Home Affairs has launched the National Database on Sexual Offenders (NDSO) on 20th September 2018. This online facility is exclusively for the use of law enforcement agencies having access to Inter-operable Criminal Justice System (ICJS). NDSO is a central database of sexual offenders in the country which is being maintained by the NCRB.[160]

(vi) International Cooperation: Going ahead for the developing a secure cyber ecosystem, India had decided to do a merger with various developed countries like the US, Japan, Singapore etc. Thus, this result in helping India; to face even more critical challenges related with the cyber threats.

(vii) Promoting Research and Development: The government of India took a step to support the cyber security in the country; by offering a fund of 5 crores to the

[160] *Available at*: https://pib.gov.in/PressReleasePage.aspx?PRID=1558130. (last visited on 2nd December 2021).

companies those who are working for the research and revolution of cyber security.

(viii) Sectorial and State CERTs: Computer Emergency Response Team (CERT) is a team of experts who looks after managing the security incidents. The government of India has introduced CERTs on power and finance sectors. They will soon launch the State CERTs are too.

(ix) Security Testing: There are some 10 setups for STQC (Standardisation, Testing and Quality Certification) that helps in testing the IT products across the country.

4.8. Government of India Initiative/ Scheme for Protection of Crime Against Women

(i) National Commission for Women : In January 1992, the Government of India set-up National Commission for Women an statutory body with a specific mandate to study and monitor all matters relating to the constitutional and legal safeguards provided for women, review the existing legislation to suggest amendments wherever necessary, etc.

(ii) Reservation for Women in Local Self -Government: The 73rd Constitutional Amendment Acts passed in 1992 by Parliament ensure one-third of the total seats for women in all elected offices in local bodies whether in rural areas or urban areas.

(iii) The National Plan of Action for the Girl Child (1991-2000): The plan of Action is to ensure survival, protection and development of the girl child with the ultimate objective of building up a better future for the girl child.

(iv) National Policy for the Empowerment of Women, 2001: The Department of Women & Child Development in the Ministry of Human Resource Development has prepared a "National Policy for the Empowerment of Women" in the year 2001. The goal of this policy is to bring about the advancement, development and empowerment of women.[161]

[161] Shahida Murtaza, *Womens Human Rights: A Feminist Discourse* 97 (Anmol Publication, New Delhi, 2015).

Latest Special Schemes[162]

- Beti Bachao Beti Padhao Scheme
- One Stop Centre Scheme
- Women Helpline Scheme
- UJJAWALA : A Comprehensive Scheme for Prevention of trafficking and Rescue, Rehabilitation and Re-integration of Victims of Trafficking and Commercial Sexual Exploitation
- Working Women Hostel
- Ministry approves new projects under Ujjawala Scheme and continues existing projects
- SWADHAR Greh (A Scheme for Women in Difficult Circumstances)
- NARI SHAKTI PURASKAR
- Awardees of Stree Shakti Puruskar, 2014 & Awardees of Nari Shakti Puruskar
- Awardees of Rajya Mahila Samman & Zila Mahila Samman
- Mahila police Volunteers
- Mahila Shakti Kendras (MSK)
- NIRBHAYA
- Uttar Pradesh Budget 2022 proposed setting up cyber help desk at district level.
- Budget for Mission Shakti Programme of Uttar Pradeshn has been proposed for the safety and empowerment of women.

Conclusion

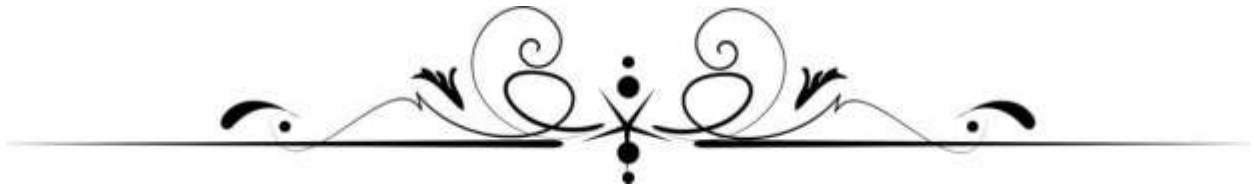
Women have always been the object of crime in India but now the crimes against women are increasing even in the virtual world. Sadly, the legal framework is not adequate yet to protect women from such crimes. Revenge Porn and blackmailing to publish or distribute intimate image is one of such serious cybercrimes against women. Though it is relatively new in India and its rise cannot be denied. It involves sharing of

[162] *Available at*: https://wcd.nic.in/schemes-listing/2405. (last visited on 21st January, 2022).

sexually explicit (read private or nude) pictures of a person without consent. It is done basically by ex-lovers or former partners to gain revenge and cause shame & intimidation to the victim.

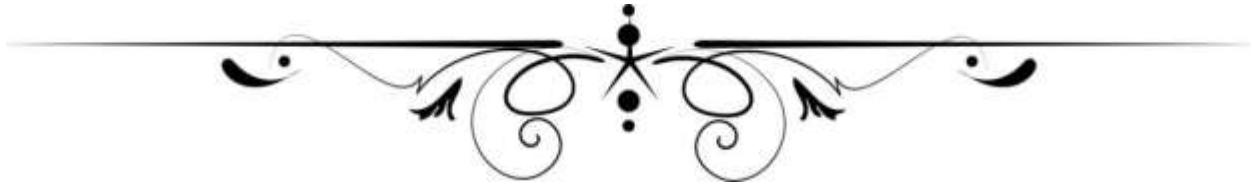
Moreover, we don't have any direct law against revenge porn. So, whenever such crimes take place, they are dealt under the provisions of the Information Technology Act, 2000 (Sections 66E, 67, and 67A) read with the provisions of the Indian Penal Code, 1860 (Sections 354A, 354C, 354D, 509).

Thus, it can be assessed that the only law which solely tackle the problem of cybercrimes is not itself a complete law. Further its provision also unable to deal the problems of women related cybercrimes. More over the traditional laws are also unable to provide the remedies to the problems of cybercrimes in India.



CHAPTER-V

CYBERCRIME AGAINST WOMEN: GLOBAL LEGAL PERSPECTIVE



CHAPTER-V

CYBERCRIME AGAINST WOMEN: GLOBAL LEGAL PERSPECTIVE

5.1. Introduction

Cybercrime against women is increasing with rapid rate globally, which is a serious concern for whole world. With the rapid development of computer technology and internet over the years, the problem of cybercrime against women has assumed gigantic proportions and emerged as a global issue. Cyberspace has created new opportunities for global attacks on the infrastructure of sovereign states, and other serious cybercrime against people especially against women.

Internet operations being of global nature do not recognize any territorial boundaries. This enables the cyber criminals to operate beyond the national geographic limits without being physically present at the scene of crime. The problem of cybercrimes against women therefore, calls for greater international support and cooperation. The global cybercrime against women such as revenge porn and blackmailing constitute a threat to international peace and security, and need a global framework to promote peace, security and justice among the states and its people.

Though much has been done by the United Nations to muster cooperation of member nations to tackle the problem of cyber criminality as a common cause, the response from them has not really been very encouraging excepting that there is general consciousness among the countries that where a cybercrime involving a foreign country or countries is involved, trans-border assistance and cooperation between the concerned countries is the only viable alternative to prevent and control such crimes.

In this background, the researcher has analysed the legal provisions, which have been enacted by the various countries as well as United Nation organisations to protect women from cybercrime particularly revenge porn and blackmailing. An attempt is made to analyse the provisions of various conventions, covenants, treaties etc., which are tackling the problem of revenge porn which is adversely affecting the right to privacy in the present day and age.

5.2. Global Legal Efforts to Prevent and Protect the Cybercrime against Women

5.2.1. The Universal Declaration of Human Rights, 1948

Universal Declaration of Human Rights (UDHR), 1948 was drafted by the United Nation Human Right Commission and it was approved by the General Assembly on 10th December, 1948. The purpose of Universal Declaration of Human Rights was to protect the human right of every individual. Art. 12 of Universal Declaration of Human Rights,[1] explicitly provides the protection of women's honour and reputation. There was no particular provision in this document which deals with the cybercrime against women but the intent of this document will be applicable while any cybercrime committed against women.

5.2.2. The International Covenant on Civil and Political Rights, 1966

International Covenant on Civil and Political Rights (ICCPR) is an international human right treaty, which is adopted by the UN in 1966 and came into force on 23rd September, 1976. It ensures the protection of human rights and recognises the inherent dignity of each individual. Paragraph 2 of Art. 17 of the International Covenant on Civil and Political Rights (ICCPR) outlined that everyone has the right to the protection of the law against unlawful or arbitrary interference with their privacy.

5.2.3. The Convention on Elimination of all form of Discrimination Against Women, 1979

The Convention on Elimination of all forms of Discrimination against Women (CEDAW) is a landmark international agreement which was adopted by UN General Assembly in 1979 to achieve the goal of United Nation provides that equality of rights for women is a basic principle of the United Nations. The Preamble to the Charter of the United Nations sets as one of the Organization's central goals the reaffirmation of "faith in fundamental human rights, in the dignity and worth of the human person, in the equal rights of men and women". The Convention on Elimination of all forms of discrimination

[1] Universal Declaration of Human Rights, 1948, art. 12 state that "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attach on his honour and reputation."

against women is a practical blueprint for every country to achieve progress for women and girls.

Around the world, The Convention on Elimination of all forms of discrimination against women has been used to reduce sex trafficking, domestic violence and female genital mutilation.[2] This convention protect the women against the discrimination and denial of equality treated as offence against human dignity.

The Convention on Elimination of all forms of Discrimination against Women, insists that the state parties have the obligation to ensure the equal rights of men and women to enjoy all economic, social, cultural, civil and political rights.

5.2.4. United Nation Convention on the Rights of the Child, 1989

United Nation adopted its first international legally binding document concerning of child rights. The United Nations Convention on the Rights of the Child, adopted in 1989,[3] and it came into force on the 2nd September, 1990; which contains several provisions aiming to protect children. However, it does not define child pornography, nor does it contain provisions that harmonize the criminalization of the distribution of online child pornography. Articles 34 to 36 of the Convention speak about sexual exploitation of children. Art. 34 directs the State parties to undertake to protect children from all kinds of sexual exploitation and sexual abuse including inducing the child to participate in any sexual practice, exploitative use of children in prostitution and in pornographic materials.[4] Art. 35 directs the State parties to take appropriate action by way of creating domestic laws as well as ratifying bilateral or multilateral treaties to prevent child trafficking. Art. 36, again, directs the State parties to protect the children from any other form of exploitation prejudicial to the welfare of the child. It may be understood here that

[2] Chandrakala and Sunitha (et al.), *Women's Rights and Gender Justice* 62 (Regal Publication, New Delhi, 2015).

[3] UN General Assembly, Convention on the Rights of the child, GA Res 44/25,GAOR, UN Doc A/RES/44/25(December 12, 1989). Available at www.un.org/documents/ga/res/45/a45r121.htm. (last visited on 21st Aug,2021).

[4] The Convention on the Rights of the child, 1989, art. 34 state that "States Parties undertake to protect the child from all forms of sexual exploitation and sexual abuse. For these purposes, States Parties shall in particular take all appropriate national, bilateral and multilateral measures to prevent:
(a) The inducement or coercion of a child to engage in any unlawful sexual activity;
(b) The exploitative use of children in prostitution or other unlawful sexual practices;
(c) The exploitative use of children in pornographic performances and materials".

sexual exploitation may also be a particular form of economic exploitation or a form of child labour. The Convention, therefore, urges the State parties to perceive the matters individually depending upon each form of exploitation, as well as holistically.[5] Only Art. 34 calls upon Member States to prevent the exploitative use of children in pornographic performances. This convention is also relevant for the protection of women from cybercrime.

5.2.5. United Nations Convention Against Transnational Organized Crime, 2000

This treaty, also known as the Palermo Convention, it obligates state parties to enact domestic criminal offenses that target organized criminal groups and to adopt new frameworks for extradition, mutual legal assistance, and law enforcement cooperation. Although the treaty does not explicitly addresses cybercrime, its provisions are relevant to curb the dangers of the cybercrime, which became the organised crime in the world.[6]

5.2.6. Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, 25th May, 2000

This optional protocol was adopted and opened for signature, ratification and accession by General Assembly resolution A/RES/54/263 of 25th May, 2000 and entered into force on 18th January, 2002.[7] The Optional Protocol not only addresses the issue of child pornography in general, but explicitly refers to the role of the Internet in distributing such material.[8] Child pornography is defined as any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes.[9] Art. 3 requires

---

[5] Debarati Halder, *Child Sexual Abuse and Protection Las in India* 23 (Sage Publication, New Delhi, 2018).

[6] United Nations Convention against Transnational Organized Crime and the Protocols Thereto, 2000, *available at:* https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf. (last visited on 4th August, 2021).

[7] Optional Protocol to the Convention on the Rights of the Child on the sale of children, Child prostitution and child pornography, 2000, *available at*: https://treaties.un.org/doc/Treaties/2000/05/20000525%2003-16%20AM/Ch_IV_11_cp.pdf. (last visited on 21st Aug, 2021).

[8] Optional Protocol to the Convention on the Rights of the Child on the sale of children, Child prostitution and child pornography, 2000. The Preface.

[9] Optional Protocol to the Convention on the Rights of the Child on the sale of children, Child prostitution and child pornography, 2000, art.2. states that " For the purposes of the present Protocol:

the parties to criminalize certain conduct which are including acts related to child pornography.[10]

5.2.7. Convention on Cybercrime, 2001 (The Budapest Convention)

The first major legal impetus for seeking inter-governmental cooperation in countering cybercrime came in November, 2001 from the Council of Europe, which is comprised of 47 states and includes Russia but not the United States, China, and other non-European countries. The Convention on Cybercrime, adopted in 2001, is the first international treaty focused on internet related crimes. This is also known as Budapest Convention. This convention emphasizing that an "effective fight against cybercrime requires increased, rapid, and well-functioning international cooperation in criminal matters."[11] Three Articles of the Budapest Convention can be applied to cyber violence against women. Art. 4 on "Data interference in a critical system (which) may cause death or physical or psychological injury", Art. 5 on "System interference in a critical system (which) may cause death or physical or psychological injury" and Art. 9 and sub-provisions which covers child exploitation images on "producing child pornography for electronic distribution and production of child pornography (which) may cause death and necessarily entails physical and/or psychological violence." Other sub-provisions of Art. 9 cover the distribution of child exploitation images and the notion that distribution may itself inflict psychological violence. Articles 2 to 7 and Art. 11 can also, among others, facilitate connection to cyber violence.

---

a. Sale of children means any act or transaction whereby a child is transferred by any person or group of persons to another for remuneration or any other consideration;
b. Child prostitution means the use of a child in sexual activities for remuneration or any other form of consideration;
c. Child pornography means any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes."

[10] Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, 2000, art.3, state that "Each State Party shall ensure that, as a minimum, the following acts and activities are fully covered under its criminal or penal law, whether these offences are committed domestically or transnationally or on an individual or organized basis: Producing, distributing, disseminating, importing, exporting, offering, selling or possessing for the above purposes child pornography as defined in Article 2."

[11] Asoke Mukerji, "The Need for an International Convention on Cyberspace", 16 *Journal of International Relations and Sustainable Development, Pandemics & Geopolitics: The Quickening* 198-209 (SPRING 2020), *available at:* https://www.jstor.org/stable/10.2307/48573761. (last visited on 21st January, 2021).

A country implementing the Budapest Convention should also consider for the implementation of Articles 33, 34 and 40. Istanbul Convention in order to combat psychological violence, stalking and sexual harassment in an online context. Conversely, the Istanbul Convention does not include specific provisions to secure electronic evidence in domestic and international investigations related to online violence against women. Countries implementing the Istanbul Convention should thus consider implementing the procedural powers of Articles 16 to 21 Budapest Convention and becoming Parties to the Budapest Convention to facilitate international cooperation on electronic evidence (Articles 23 to 35 Budapest Convention) in relation to online violence against women".[12]

5.2.8. Additional Protocol to The Budapest Convention, 2003

The Additional Protocol to the Convention on Cybercrime concerns the criminalisation of acts of a racist and xenophobic nature committed through computer systems. It was adopted by the Council of Europe Committee of Ministers in November 2002 and entered into force on 1st March, 2006.

The protocol recognises that computer systems are facilitating forces for communication and freedom of expression but also for the dissemination of racist and xenophobic material and speech and it requires parties to criminalise this dissemination. It focuses on the dissemination of racist and xenophobic material through computer systems, racist and xenophobic-motivated threats and insults and denial, gross minimisation and approval or justification of genocide or crimes against humanity. This protocol entails an extension of the convention's scope, including its substantive, procedural and international co-operation provisions, so as to also cover offences of racist and xenophobic propaganda.[13] Thus, apart from harmonising the substantive law elements of such behaviour, the protocol aims at improving the ability of the parties to

[12] Study for FEMM Committee "Cyber violence and hate speech online against women", *available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU(2018)604979_EN.pdf*. (last visited on 5th Febuary, 2022).

[13] Adriane Van Der Wilk, "Protecting Women and Girls from Violence in the Digital Age" published by Council of Europe, *available at:* https://rm.coe.int/prems-153621-gbr-2574-study-online-a4-bat-web/1680a4cc44. (last visited on 21st December, 2021).

make use of the means and avenues of international co-operation set out in the convention in this area.

5.2.9. The Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse, 2007 (The Lanzarote Convention)

The Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse, 2007 requires criminalisation of all forms of abuse against children. The purpose of this convention are to prevent and combat sexual exploitation and sexual abuse of children, to protect the rights of child victims of sexual exploitation and sexual abuse and promote national and international co-operation against sexual exploitation and sexual abuse of children. To realise the objective of this convention this convention sets up a specific monitoring mechanism to ensure the effective implementation of its provisions by the Parties.

The provisions of the Lanzarote Convention[14] also apply to sexual violence in an online environment. The Lanzarote Committee is currently doing the second round of monitoring and is in the process of examining parties' strategies regarding the "Protection of children against sexual exploitation and sexual abuse facilitated by information and communication technologies (ICTs)". A recent report from the Cyber Crime Committee points at possible synergies between the treaties when it comes to prevention of, protection from and prosecution of cyber violence against women and girls.[15]

5.2.10. Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence, 2011 (The Istanbul Convention)

In 2011, the European Union signed the Istanbul Convention,[16] the first European multi-country treaty on combating violence against women and domestic violence. The

[14] The Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse, *available at:* https://rm.coe.int/1680084822 (last visited on 5th August, 2021).

[15] Directorate General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs Women's Rights & Gender Equality (2016), "The issue of violence against women in the European Union", *available at:* http://www.europarl.europa.eu/RegData/etudes/STUD/2016/556931/IPOL_STU(2016)556931_EN.pdf. (last visited on 3rd March, 2021).

[16] Directorate General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs Women's Rights & Gender Equality (2016), "The issue of violence against women in the European Union", *available at:* http://www.europarl.europa.eu/RegData/etudes/STUD/2016/556931/IPOL_STU(2016)556931_EN.pdf. (last visited on 3rd March, 2021).

Convention sets out minimum standards for signatories regarding prevention, protection, prosecution, violence against women, and domestic violence. Several articles of the Convention can be applied to the specific topic of digital violence: Art. 33 on psychological violence, Art. 34 on stalking, and Art. 40 on sexual harassment. The GREVIO committee is in charge of:

(i) monitoring the implementation of the Convention by its signatories;

(ii) reporting on the state of violence against women and domestic violence; and

(iii) Identifying possibilities of legal harmonisation.

Thus, these conventions apply universally and are not open to arbitrary interpretation. While predating the digital era, their intent and inherent values remain applicable as confirmed by the UN Human Rights Council and the UN General Assembly affirmations that women's rights apply online not just only offline.

5.3. Role of United Nation to Curb The Menace of Cybercrime

The United Nation General Assembly has adopted several resolutions since 2000-2001, and invites Member States, when developing national laws, policy and practice, to combat the criminal misuse of information technologies**.**

5.3.1. Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders.

The Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders which is held in Havana, Cuba, on 27th August to 7th September 1990, the UN General Assembly adopted a resolution dealing with computer crime legislation.[17] Based on its Resolution 45/121 (1990), the UN published a manual in 1994 on the prevention and control of computer-related crime.[18]

[17] UN General Assembly, Eighth United Nation Congress on the prevention of crime and the treatment of offender, GA Res 45/121,GAOR, UN Doc A/RES/45/121 (December 14th , 1990), *available at:* www.un.org/documents/ga/res/45/a45r121.htm.(last visited on 21st Aug,2021).

[18] UN Manual on the Prevention and Control of Computer-Related Crime (United Nations publication, Sales No. E.94.IV.5), *available at:* www.uncjin.org/Documents/EighthCongress.html.(last visited on 21st August,2021).

5.3.2. Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders

During the tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, held in Vienna in 2000, the impact of computer-related crimes was discussed in a specific workshop.[19] The debate focused especially on the categories of crime and transnational investigation, as well as legal response to the phenomenon.[20] The conclusions of the workshop contain major elements of the debate that is still ongoing: criminalization is required; legislation needs to include procedural instruments, international cooperation is crucial and public-private partnership should be strengthened.[21] In addition, the importance of capacity building was highlighted as an issue that was picked up again in subsequent years.[22] The Vienna Declaration called upon the Commission on Crime Prevention and Criminal Justice to undertake work in this regard.

5.3.3. UN General Assembly Resolution on Combating the Criminal Misuse of Information Technologies, 2000

In the year 2000, the UN General Assembly adopted a resolution (Resolution No. 55/63**)** on combating the criminal misuse of information technologies which displays a number of similarities with the G8's Ten-Point Action Plan from 1997.[23] In its resolution, the General Assembly identified a number of measures to prevent the misuse of information technology, including:

---

[19] UN General Assembly, Crimes Related to Computer Networks, UN GAOR, UN Doc. A/CONF.187/10 (February 3, 2000).*available at:* file:///C:/Users/user/Downloads/A_CONF.187_10-EN%20(1).pdf. (last visited on 4th August, 2021).

[20] UN General Assembly, Report of the tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, 2000, UN GAOR, UN Doc. A/CONF.187/15 (July 19, 2000) *available at*: www.uncjin.org/Documents/congr10/15e.pdf. (last visited on 4th August, 2021).

[21] UN General Assembly, Report of the tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, 2000, UN GAOR, UN Doc. A/CONF.185/15 (April 10, 2000). *available at:* www.uncjin.org/Documents/congr10/15e.pdf. (last visited on 4th August, 2021).

[22] "The United Nations should take further action with regard to the provision of technical cooperation and assistance concerning crime related to computer networks".

[23] UN General Assembly, Combating the criminal misuse of information technologies, UN GA Res 55/63, GAOR, UN Doc A/RES/55/63 (January 22, 2001), *available at:* www.unodc.org/pdf/ crime/a_res_55/res5563e.pdf.(last visited on 4th August, 2021).

"States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies; Law enforcement cooperation in the investigation and prosecution of international cases of criminal misuse of information technologies should be coordinated among all concerned States; Law enforcement personnel should be trained and equipped to address the criminal misuse of information technologies;"

Resolution 55/63 invites States to take the necessary steps to combat cybercrime on the regional and international stage. This includes the development of domestic legislation to eliminate safe havens for criminal misuse of technologies, improving law-enforcement capacities to cooperate across borders in the investigation and prosecution of international cases of criminal misuse of information technologies, improving information exchange, enhancing the security of data and computer systems, training law enforcement to deal specifically with the challenges associated with cybercrime, building mutual assistance regimes and raising public awareness of the threat of cybercrime.

5.3.4. UN General Assembly Resolution on Combating The Criminal Misuse of Information Technologies, 2000

In 2001, the UN General Assembly adopted another resolution on combating the criminal misuse of information technology.[24] The resolution refers to the existing international approaches in fighting cybercrime and highlights various solutions.

Resolution 56/121 underlines the need for cooperation among states in combating the criminal misuse of information technologies. It highlights the role that can be played by the United Nations and other international and regional organizations. The resolution further invites states to take into account the direction provided by the Commission on Crime Prevention and Criminal Justice when developing national legislation. However, the resolution defers consideration of the subject, pending work envisioned in the plan of action against technology and computer related crime of the Commission on Crime Prevention and Criminal Justice.

[24] UN General Assembly, Combating the criminal misuse of information technologies, GA Res 56/121, GAOR, UN Doc A/RES/56/121(January 23, 2002), *available at:* http://daccessdds.un.org/doc/UNDOC/GEN/N01/482/04/PDF/N0148204.pdf. (last visited on 4th August, 2021).

5.3.5. United Nation General Assembly Resolution on Creation of a Global Culture of Cyber security (Resolutions 57/239) and Creation of a Global Culture of Cyber security and the Protection of Critical Information Infrastructures (Resolutions 58/199)

Resolutions 57/239 and 58/199 are the two main UN General Assembly resolutions dealing with cyber security. Without going into detail with regard to cybercrime, they recall Resolutions 55/06 and 56/121. Both resolutions furthermore emphasize the need for international cooperation in fighting cybercrime by recognizing that gaps in states' access to and use of information technologies can diminish the effectiveness of international cooperation in combating the criminal misuse of information technology.[25]

5.3.6. Eleventh UN Congress on Crime Prevention and Criminal Justice, 2005

Cybercrime was discussed during the eleventh UN Congress on Crime Prevention and Criminal Justice the ("UN Crime Congress") in Bangkok, Thailand, in 2005. Several challenges associated with the emerging use of computer systems in committing offences and the transnational dimension were addressed both in the background paper[26] and in workshops.[27] Within the framework of the preparatory meetings in advance of the congress, some member countries such as Egypt called for a new UN convention against cybercrime, and the Western Asian regional preparatory meeting called for the negotiation of such convention.[28] The possibility of negotiating a convention was included in the discussion guide for the eleventh UN Crime Congress.[29] However, the

[25] UN General Assembly, On Creation of A Global Culture of Cybersecurity, GA Res 57/239, GAOR, UN Doc A/RES/57/239; UN General Assembly, On Creation of A Global Culture of Cybersecurity and The Protection of Critical Information Infrastructure, GA Res 58/199, GAOR, UN Doc A/RES/58/199.

[26] UN Congress, Report of Eleventh UN Congress on Crime Prevention and Criminal Justice, UN Doc. A/CONF.203/14 (May 17, 2005).

[27] UN Congress, Committee II Report, Eleventh UN Congress on Crime Prevention and Criminal Justice, UN Doc.BKK/CP/19 (May 17, 2005).

[28] UN General Assembly, Report of the Western Asian Regional Preparatory Meeting for the Eleventh United Nations Congress on Crime Prevention and Criminal Justice, UN Doc. A/CONF.2003/RPM.4/1, No. 14(May 4, 2003).

[29] UN Congress, "Considering the feasibility of negotiation of an international instrument on preventing and combating crimes involving information technologies", Discussion guide to the eleventh United Nations Congress on Crime Prevention and Criminal Justice, 2003, UN Doc. A/CONF.203/RM.1 (May

Member States could at this time not decide to initiate a harmonization of legislation. The Bangkok Declaration therefore without mentioning a specific instrument refers to existing approaches.

5.3.7. UN General Assembly Resolution on Follow-up to the Eleventh United Nations Congress on Crime Prevention and Criminal Justice, 2005

After the eleventh UN Congress on Crime Prevention and Criminal Justice in Bangkok, Thailand, in 2005, a declaration was adopted that highlighted the need for harmonization in the fight against cybercrime,[30] addressing, among others, the following issues: UN General Assembly Resolution 60/177 endorsed the 2005 Bangkok Declaration, wherein the international community's efforts to enhance and supplement existing cooperation to prevent computer related crime were encouraged, inviting further exploration of the feasibility of providing assistance to Member States in addressing computer-related crime under the aegis of the United Nations, and in partnership with other similarly focused organizations.

5.3.8. UN General Assembly Resolution on Creation of A Global Culture of Cyber security and Taking Stock of National Efforts to Protect Critical Information Infrastructures, 2010

In March 2010, the UN General Assembly passed a new resolution[31] as part of the "Creation of a global culture of cyber security" initiative. Resolution 64/211 refers to the two major resolutions on cybercrime[32] as well as the two main resolutions on cyber security.[33] The voluntary self-assessment tool for national efforts to protect critical information infrastructures provided as an annex to the resolution calls for countries to

4, 2003), *available at:* https://www.unodc.org/pdf/crime/congress11/BangkokDeclaration.pdf. (last visited on 5th August, 2021).

[30] Bankok Declaration, Declaration Synergies and Responses: Strategic Alliances in Crime Prevention and Criminal Justice, *available at:* www.unodc.org/pdf/crime/congress11/BangkokDeclaration.pdf. (last visited on 4th August, 2021).

[31] UN General Assembly, Creation of a global culture of cyber security and taking stock of national efforts to protect critical information infrastructure, GA Res 64/211, GAOR, UN Doc. A/RES/64/211(March17th, 2010), *available at:* https://undocs.org/pdf?symbol=en/A/RES/64/21.(last visited on 20th August, 2020).

[32] UN General Assembly Resolutions 55/63 and 56/121, *available at:* https://research.un.org/en /docs/ga/resolutions.(last visited on 20th August, 2020).

[33] UN General Assembly Resolutions 57/239 and 58/199, *available at:* https://research.un.org /en/docs/ga/resolutions. (last visited on 20th August 2020).

review and update legal authorities (including those related to cybercrime, privacy, data protection, commercial law, digital signatures and encryption) that may be outdated or obsolete as a result of the rapid uptake of, and dependence upon, new information and communication technologies. The resolution further calls on states to use regional international conventions, arrangements and precedents in these reviews.

The fact that 4 out of 18 subjects of the self-assessment tool related to cybercrime highlights the importance of the ability of law enforcement to combat cybercrime effectively for maintaining cyber security.

5.3.9. Twelfth UN Congress on Crime Prevention and Criminal Justice, 2010

The topic of cybercrime was also discussed at the Twelfth UN Congress on Crime Prevention and Criminal Justice held in Salvador, Brazil in 12-19 April, 2010[34] which aimed at strengthening international cooperation against expanding crime. Within the four regional preparatory meetings for the congress, for Latin America and Caribbean,[35] Western Asia,[36] Asia and the Pacific[37] and Africa,[38] the countries called for the development of an international convention on cybercrime. Similar calls were raised within academia[39]. At the congress itself, Member States took a major step toward more

[34] Twelfth UN Congress on Crime Prevention and Criminal Justice, 2010 this context especially the background paper prepared by the secretariat.

[35] "The Meeting also noted the imperative need to develop an international convention on cybercrime", Report of the Latin American and Caribbean Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in San Jose from 25 to 27 May 2009, UN Doc A/CONF.213/RPM.1/1, Conclusions and Recommendations (May 26,2009).

[36] "The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Western Asian Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Doha from 1 to 3 June 2009, UN Doc A/CONF.213/RPM.2/1, Conclusions and Recommendations No. 47 Recommendations (May 26,2009).

[37] "The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Asian and Pacific Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Bangkok from 1 to 3 July 2009, UN Doc A/CONF.213/RPM.3/1, Conclusions and Recommendations No. 29 Recommendations (May 26,2009).

[38] "The Meeting recommended the development of an international convention on cybercrime, as that would promote the priority of putting into place efficient national legislation, fostering international cooperation and building the skills of law enforcement personnel to address effectively the complex issues of cybercrime investigations, especially those of a cross-border nature", Report of the African Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Nairobi from 8 to 10 September 2009, UN Doc A/CONF.213/RPM.4/1, Conclusions and Recommendations No. 40(May 18,2009).

[39] Vogel, "Towards a Global Convention against Cybercrime, First World Conference of Penal Law" (ReAIDP / e-RIAPL, 2008).

active involvement of the United Nations in the debate on the issue of computer crime and cybercrime.[40] The fact that the delegations discussed the topics for two days and that additional side events were organized highlights the importance of the topic, which was more intensively discussed than during the previous crime congresses.[41]

The deliberations focused on two main issues: how can harmonization of legal standards be achieved, and how can developing countries be supported in fighting cybercrime? The first point is especially relevant if the UN develops comprehensive legal standards or suggests that Member States implement the Council of Europe Convention on Cybercrime. In preparation of the UN Crime Congress, the Council of Europe had expressed concerns regarding a UN approach[42] and had called for support for its Convention on Cybercrime. After an intensive debate, where the limited reach of the Convention on Cybercrime was discussed in particular, the Member States decided not to suggest to ratify the Convention on Cybercrime but to strengthen the UN's role in two important areas, which are reflected in the Salvador Declaration. The Member States thus, recommended a strong mandate for the United Nations Office on Drugs and Crimes (UNODC) to provide global capacity building upon request.

While, taking into account UNODC's experience in capacity building related to criminal legislation and the fact that, unlike the Council of Europe, UNODC provides a global network of regional offices, it is likely that UN through UNODC will play a more important role in this field in the future. The second recommendation highlights that, at the time of the UN Crime Congress, Member States were unable to decide whether to develop a legal text or not. This reflects the controversial discussion during the congress, where those European countries that have already ratified the Convention on Cybercrime, in particular, expressed their support for that instrument while a number of developing countries called for a UN convention.

[40] Schjolberg and Ghernaouti Heli, "A Global Protocol on Cyber security and Cybercrime" (2009).
[41] Regarding the focus of the debate, recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime, Twelfth UN Congress on Crime Prevention and Criminal Justice, A/CONF.213/9.
[42] Contribution of the Secretary General of the Council of Europe to the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, Information Documents SG/Inf (2010) 4, 16.02.2010, page 17.

However, the Member States did respond differently than at the eleventh Crime Congress, where they had referred to existing instruments. This time they did not refer to existing instruments and, even more importantly, they did not decide to recommend the Convention on Cybercrime as a global standard. Instead, the Member States recommended invite to the Commission on Crime Prevention and Criminal Justice to conduct a comprehensive study, which should, inter alia, examine options for strengthening existing and proposing new national and international legal or other responses to cybercrime.

❖ **Intergovernmental Expert Group on Cybercrime**

Following the decision of the Member States to call upon UNODC to set up an intergovernmental working group, the first meeting of the group was held in Vienna in January 2011.[43] The expert group included the representatives of Member States, intergovernmental and international organizations, specialized agencies, private sector and academia.

During the meeting the members of the expert group discussed a draft structure for a comprehensive study analysing the issue of cybercrime, as well as the response.[44] With regard to the legal response, a number of members underline the usefulness of existing international legal instruments, including the United Nations Convention against Transnational Organized Crime (UNTOC) and the Council of Europe Convention on Cybercrime, and the desirability of elaborating a global legal instrument to address specifically the problem of cybercrime. Finally, It was agreed that the decision on whether a global instrument should be developed will be made after the study was conducted.

[43] UNODC, Report on the meeting of the open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime held in Vienna from 17 to 21 January 2011, UN Doc. UNODC/CCPCJ/EG.4/2011/3 (March 31st, 2011), *available at:* www.unodc.org/documents /treaties/organized_crime/EGM_cybercrime_2011/UNODC_CCPCJ_EG4_2011_3/UNODC_CCPCJ_EG4_2011_3_E.pdf. (last visited on 3rd March, 2021).

[44] UNODC, Draft topics for consideration in a comprehensive study on the impact of and response to cybercrime, UN Doc UNODC/CCPCJ/EG.4/2011/2 (March 31st, 2011), *available at:* www.unodc.org/documents/treaties/organized_crime/EGM_cybercrime_2011/UNODC,CCPCJ_EG42011_2/UNODC_ CCPCJ_ EG4_2011_2_E.pdf.(last visited on 3rd March, 2021).

5.2.10. Fourteenth United Nation Congress on Crime Prevention and Criminal Justice, 2021

The Fourteenth Session of United Nation Congress on Crime Prevention and Criminal Justice[45] held in Kyoto, Japan on 7th-12th March, 2021. The theme of 14th Crime Congress, was "*Advancing crime prevention, criminal justice and the rule of law: towards the achievement of the 2030 Agenda*". It brought together more than 5,000 participants from all over the world. A record 152 Member States were represented at the Congress along with 114 non-governmental organizations, 37 intergovernmental organizations, 600 individual experts and several UN entities and institutes. Most of the participants joined online, via a special event platform, while a limited number of participants attended in person in the Kyoto International Conference Centre. In this meeting a paragraph on the nature of crime has become hostage to polarized debates on cybercrime. The paragraph expresses concern about that crime is 'becoming increasingly transnational, organized and complex, thus creating unprecedented challenges….' However, India has proposed adding an extra adjective 'online' and is supported by others in seeking to emphasize cyber elements in this paragraph, which is opposed by Russia and others from their 'like-minded' group on cyber issues, who are seeking to bolster language on new approaches to cyber elsewhere in the document. There is also a bone of contention in how the declaration encourages member states to use technology to fight crime. Western countries have teamed up with Mexico and Honduras to insist that a commitment to use technological tools comes with a commitment to respect for human rights in doing so.

5.4. The United Nations Office for Drugs and Crime (UNODC) And The United Nations Economic and Social Council (ECOSOC) Resolutions for Cybercrime

United Nations through, resolutions and recommendations addresses issues related to cybercrime, the most important being the following: the United Nations Office for Drugs and Crime (UNODC) and the Commission on Crime Prevention and Criminal Justice adopted a resolution on effective crime prevention and criminal justice responses

[45] The Commission on Crime Prevention and Criminal Justice (CCPCJ) was set up in 1991. It is a subsidiary body of the Economic and Social Council.

to combat sexual exploitation of children.[46] In 2004, the United Nations Economic and Social Council[47] adopted a resolution on international cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes.[48] Thereafter, a working group was established in 2005.[49] In which core group of experts on identity-related crime was created to undertake a comprehensive study on the issue. In 2004, The United Nations Economic and Social Council had adopted a resolution on the sale of illicit drugs via the Internet that explicitly took account of a phenomenon related to a computer crime.[50] In 2007, The United Nations Economic and Social Council adopted a resolution on international cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime,[51] neither of these two resolutions explicitly addresses the challenges of Internet-related crimes, but they are applicable to those offences as well.

[46] UN office of Drug and Crime, On Effective crime prevention and criminal justice responses to combat sexual exploitation of children. Regarding the discussion process in the development of the resolution and for an overview of different existing legal instruments, Note by the Secretariat regarding Commission on Crime prevention and criminal justice responses to urban crime, including gang-related activities, and effective crime prevention and criminal justice responses to combat sexual exploitation of children, CCPCJ Resolution 16/2, UN Doc. CN.15/2007/CRP.3(March 13th, 2007), *available at*: www.unodc.org/pdf/crime/session16th/E_CN15 _2007_CRP3_E.pdf. Regarding the initiative relating to the resolution, *available at:* www.america.gov/st/washfile-english/2007/April/20070423135940 ajesrom0.709469.html. (last visited on 3rd March, 2021).

[47] The United Nations Economic and Social Council (ECOSOC) is a principal organ to coordinate economic, social, and related work and serve as a central forum for discussing international economic and social issues. For more information, *available at:* www.un.org/ecosoc/. (last visited on 3rd March, 2021).

[48] UN Economic and social Council, On International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes, ECOSOC Resolution 2004/26, UN Doc E/2004/26 (July 21st, 2004), *available at:* www.un.org/ecosoc/docs/2004/Resolution%202004-26.pdf. (last visited on 3rd March, 2021).

[49] UN Economic and Social Council, Results of the second meeting of the Intergovernmental Expert Group to Prepare a study on Fraud and the Criminal Misuse and Falsification of Identity, Commission on Crime Prevention and Criminal Justice, 16th session, 2007, E/CN.15/2007/8, UN ESCOR, UN Doc E/CN.15/2007/8(April 2nd , 2007*) available at*: https://www.unodc.org/documents/organized-crime/E CN 15_2007_8.pdf.(last visited on 3rd March 2021).

[50] UN Economic and Social Council, On Sale of internationally controlled licit drugs to individuals via the Internet, ECOSOC Resolution 2004/42, UN ESCOR, UN Doc E/CN.7/2004/L.8/Rev.2(March 17th , 2004), *available at:* www.un.org/ecosoc/docs/2004/Resolution%202004-42.pdf. (last visited on 13th April, 2021).

[51] UN Economic and Social Council, on International cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime, ECOSOC Resolution 2007/20, UN ESCOR, UN Doc E/CN.15/2009/2(February 3rd, 2009), *available at:* www.un.org/ecosoc/docs/2007/Resolution%202007-20.pdf. (last visited on 13rd April, 2021).

Based on The United Nations Economic and Social Council Resolution 2004/26[52] and The United Nations Economic and Social Council Resolution 2007/20,[53] the United Nations Office for Drugs and Crime in 2007 established a core group of experts to exchange views on the best course of action.[54] The core group has undertaken several studies that included aspects of Internet-related crimes.[55]

5.5. The United Nations Office for Drugs and Crime/The International Telecommunication Union Memorandum of Understanding (UNODC/ITU MoU)

In 2011, the United Nations Office for Drugs and Crime and the International Telecommunication Union (ITU) signed a memorandum of understanding related to cybercrime.[56] The MoU covers cooperation (especially capacity building and technical assistance for developing countries), training and joint workshops. With regard to the capacity building activities the two organizations can refer to a wide network of field offices in all continents. Further, more the organizations agreed to a joined dissemination of information and knowledge and data analysis. The MoU enables the two bodies to work together on technical assistance to be provided to Member States on cybercrime and cybersecurity.

---

[52] UN Economic and Social Council, on International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes, ECOSOC Resolution 2004/26, UN ESCOR, UN Doc 2004/26, *available at:* https://www.un.org/en/ecosoc/docs/2004/resolution%202004-26.pdf. (last visited on 13rd April, 2021).

[53] UN Economic and Social Council, on International cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime. ECOSOC Resolution 2004/20, UN ESCOR, UN Doc E/CN.15/2009/L.2 (March 26th, 2009), *available at:* https://digitallibrary.un.org/record/657667?ln=en#record-files-collapse-header.(last visited on 3rd October, 2021).

[54] UN Office of Drug and Crime, Reports related to the activities of the working group are published. First meeting of the Core Group of Experts on Identity-Related Crime, Courmayeur Mont Blanc, Italy, 29-30 November 2007, available at: www.unodc.org/documents/organized- crime/Courmayeur_report.pdf. (last visited: October 2021); Second meeting of the Core Group of Experts on Identity-Related Crime, Vienna, Austria, 2-3 June 2008, *available at*: www.unodc.org/documents/organized-crime/Final_ Report_ID_C.pdf. (last visited: October 2021).

[55] UN Economic and Social Council, Legal Approaches to Criminalize Identity Theft, Commission on Crime Prevention and Criminal Justice, ESC 15/2009, UN ESCOR, UN Doc E/CN.15/2009/CRP.13(March 3, 2010) available at: https://www.unodc.org/documents/ commissions/CCPCJ/CCPCJ_Sessions /CCPCJ_19/E-CN15-2010-CRP1_E-CN7-2010-CRP6/E-CN15-2010-CRP1_E-CN7-2010-CRP6.pdf.(last visited on 6th October, 2021).

[56] *Available at:* www.unodc.org/unodc/en/frontpage/2011/May/unodc-and-itu-to-cooperate-moreclosely-to-make-the-internet-safer.html. (last visited on 15rd July, 2021).

5.6. International Telecommunication Union

The International Telecommunication Union,[57] as a specialized agency within the United Nations, plays a leading role in the standardization and development of telecommunications as well as cyber security issues.

The International Telecommunication Union has dealt with security issue since its inception in 1865, from the invention of the telegraph, through the era of radio and television to the deployment of the satellite and internet based technologies.[58]

5.6.1. The International Telecommunication Union Resolutions

The International Telecommunication Union has adopted several cyber security related resolutions that are relevant to cybercrime, while not directly addressing the issue with specific criminal law provisions.

(i) The International Telecommunication Union Plenipotentiary Conference Resolution 130 (Rev. Guadalajara, 2010), on Strengthening the role of The International Telecommunication Union in building confidence and security in the use of information and communication technologies.

(ii) The International Telecommunication Union Plenipotentiary Conference Resolution 149 (Antalya, 2006), on Study of definitions and terminology relating to building confidence and security in the use of information and communication technologies.

(iii) Resolution 45 (Doha, 2006) of the World Telecommunication Development Conference (WTDC), on Mechanisms for enhancing cooperation on cyber security, including combating spam and the report from Meeting on Mechanisms for Cooperation on Cyber security and Combating Spam (31st August to 1st September 2006).

[57] The International Telecommunication Union (ITU) with headquarters in Geneva was founded as the International Telegraph Union in 1865. It is a specialized agency of the United Nations. ITU has 192 Member States and more than 700 Sector Members and Associates. *available at*: www.itu.int. (last visited on 21st April,2021).

[58] Pallvi Sharma, "Role of UN in Tackling Cyber Crime" 8(1), *International Journal of Research in Social Sciences* (2018).

(iv) Resolution 50 (Rev. Johannesburg, 2008) of the World Telecommunication Standardization Assembly (WTSA), on Cyber security.

(v) Resolution 52 (Rev. Johannesburg, 2008) of WTSA, on Countering and combating spam.

(vi) Resolution 58 (Johannesburg, 2008) of WTSA, on Encouraging the creation of national computer incident response teams, particularly for developing countries.

5.6.2. World Summit on the Information Society

Among other activities, The International Telecommunication Union was the lead agency of the World Summit on the Information Society (WSIS) that took place in two phases in Geneva, Switzerland (2003) and in Tunis, Tunisia (2005). Governments, policy-makers and experts from around the world shared ideas and experiences about how best to address the emerging issues associated with of the development of a global information society, including the development of compatible standards and laws. The outputs of the Summit are contained in the Geneva Declaration of Principles, the Geneva Plan of Action; the Tunis Commitment and the Tunis Agenda for the Information Society.

The Geneva Plan of Action highlights the importance of measures in the fight against cybercrime.[59] Cybercrime was also addressed at the second phase of the World Summit on the Information Society in Tunis in 2005. The Tunis Agenda for the Information Society[60] highlights the need for international cooperation in the fight against cybercrime and refers to the existing legislative approaches such as the United Nation General Assembly resolutions and the Council of Europe Convention on Cybercrime.

5.6.3. Global Cyber Security Agenda

The ITU Global Cybersecurity Agenda is a framework for international cooperation aimed that enhancing confidence and security in the information society. As an outcome of the World Summit on the Information Society, The International

[59] WSIS Geneva Plan of Action, 2003, *available at:* www.itu.int/wsis/documents/ doc_multi.asp? lang= en&id=1160|0. (last visited on 3rd July, 2021).

[60] WSIS Tunis Agenda for the Information Society, 2005, *available at:* www.itu.int/wsis /documents/doc_multiasp?lang=en&id=2267|0. (last visited on 3rd July, 2021).

Telecommunication Union was nominated as the sole facilitator for Action Line C5 dedicated to building of confidence and security in the use of information and communication technology.[61] At the second Facilitation Meeting for World Summit on the Information Society Action Line C5 in 2007, the International Telecommunication Union Secretary-General highlighted the importance of international cooperation in the fight against cybercrime and announced the launch of the International Telecommunication Union Global Cyber security Agenda.[62] The Global Cyber security Agenda is made up of seven key goals,[63] and built upon five strategic pillars,[64] including the elaboration of strategies for the development of model cybercrime legislation. The seven goals are the following:

(i) Elaboration of strategies for the development of a model cybercrime legislation that is globally applicable and interoperable with existing national and regional legislative measures.

(ii) Elaboration of strategies for the creation of appropriate national and regional organizational structures and policies on cybercrime.

(iii) Development of a strategy for the establishment of globally accepted minimum security criteria and accreditation schemes for software applications and systems.

(iv) Development of strategies for the creation of a global framework for watch, warning and incident response to ensure cross-border coordination between new and existing initiatives.

(v) Development of strategies for the creation and endorsement of a generic and universal digital identity system and the necessary organizational structures to

[61] For more information on Action Line C5, Available at www.itu.int/wsis/c5/, and also the meeting report of the second Facilitation Meeting for WSIS Action Line C5, 2007, page 1, *available at:* www.itu.int/osg/csd/cybersecurity/pgc/2007/events/docs/meetingreport.pdf. and the meeting report of the third Facilitation Meeting for WSIS Action Line C5, 2008, *available at:* www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/WSIS_Action_Line_C5_Meeting_Report_June_2008.pdf. (last visited on 23rd August, 2021).

[62] *Available at:* www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html.(last visited on 23rd August, 2021).

[63] *Available at:* www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html. (last visited on 23rd August, 2021).

[64] The five pillars are: legal measures, technical and procedural measures, organizational structures, capacity building, international cooperation, *available at*: www.itu.int/osg/csd/cybersecurity/gca /pillars-goals/index.html. (last visited on 25th August, 2021).

ensure the recognition of digital credentials for individuals across geographical boundaries.

(vi) Development of a global strategy to facilitate human and institutional capacity-building to enhance knowledge and know-how across sectors and in all the above-mentioned areas.

(vii) Advice on potential framework for a global multi-stakeholder strategy for international cooperation, dialogue and coordination in all the above-mentioned areas.

In order to analyse and develop measure and strategies with regard to the seven goals of the Global Cyber security Agenda, the International Telecommunication Union Secretary General created a high-level expert group (HLEG) bringing together representatives from Member States, industry as well as the scientific field.[65] In 2008, the expert group concluded negotiations and published the "Global Strategic Report".[66] Most relevant with regard to cybercrime are the legal measures contained in Chapter 1. In addition to an overview of different regional and international approaches in fighting cybercrime,[67] the chapter provides an overview of criminal law provisions,[68] procedural instruments,[69] regulations governing the responsibility of Internet service providers[70] and safeguards to protect fundamental rights of Internet users.[71]

This Agenda focused on elaborating strategies for concrete capacity building mechanism. It objective has to address today challenges related to confidence and security in the use of ICTs.

---

[65] *Available at:* www.itu.int/osg/csd/cybersecurity/gca/hleg/index.html. (Last visited on 3rd March, 2021).

[66] Gercke, "Zeitschriftfuer Urheber- und Medienrecht" 2009, Issue 7, page 533, *available at:* www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html. (last visited on 25th August, 2021).

[67] Gercke, National, "Regional and International Approaches in the Fight against Cybercrime" 1 *Computer Law Review International* 7 (2008).

[68] Global Strategic Report, Chapter 1.6. *available at:* www.itu.int/ITU-D/cyb/events/2009/santo-domingo (last visited on 2nd August, 2021).

[69] Global Strategic Report, Chapter 1.7. *available at:* www.itu.int/ITU-D/cyb/events/2009/santo-domingo (last visited on 2nd August, 2021).

[70] Global Strategic Report, Chapter 1.10. *available at:* www.itu.int/ITU-D/cyb/events/2009/santo-domingo (last visited on 2nd August, 2021).

[71] Global Strategic Report, Chapter 1.11. 1064 23-25 November 2009 (Santo Domingo, Dominican Republic), *available at:* www.itu.int/ITU-D/cyb/events/2009/santo-domingo; 23-25 September 2009 (Hyderabad, India): 2009 ITU Regional Cyber Security Forum for Asia-Pacific; 4-5 June 2009.

5.7. United Nation Resolutions, Strategies and Reports Specifically Dealing with Women Protection on Cyber World

(i) UN Resolution 1325 (2000), adopted by the Security Council on 31st October 2000, which addresses the particular and disproportionate effects of armed conflict on women.[72]

(ii) Resolution 1820 (2008), adopted by the Security Council on 19th June 2008, calling for an end to all acts of sexual violence against women and girls used as a weapon of war, and for the perpetrators to be brought to justice. It emphasizes that rape and other forms of sexual violence may constitute a war crime, a crime against humanity or a constituent act of the crime of genocide. It calls on the United Nations Secretary General to strengthen the policy of zero tolerance against sexual exploitation in United Nations peacekeeping operations and to ensure the protection of women and girls in refugee camps.

(iii) The UN General Assembly unanimously adopted a resolution of 20th November, 2013[73] for the right to privacy in the digital age. The resolution was introduced by Germany and Brazil. The resolution include the statement as follows: "*Affirms that the same right that people have offline must also be protected online, including the right to privacy".*

(iv) The United Nations General Assembly Resolution on the right of privacy in the digital age, passed on 18th December, 2013 and the General Comment of the United Nations Human Rights Committee on the right of privacy, family, home, correspondence, and protection of honour and reputation. *The **UN General Assembly Resolution on Protecting Women Human Rights Defenders (2013)*** recalls that "*information-technology-related violations, abuses, discrimination and violence against women, including women human rights defenders, such as online*

[72] UN Security Council, SC Res 325, SCOR, UN Doc S/Res/325(October 31, 2000), *available at:* https://peacemaker.un.org/sites/peacemaker.un.org/files/SC_ResolutionWomenPeaceSecurity_SRES1325%282000%29%28english_0.pdf. (last visited on 6th June, 2021).

[73] UN General Assembly, Promotion and protection of human rights: human rights questions, including alternative approaches for improving the effective enjoyment of human rights and fundamental freedoms, GA Res 3/18, GAOR, UN Doc A/C.3/68/L.45/Rev.1(November 20, 2013), *available at:* https://documents-dds-ny.un.org/doc/UNDOC/LTD/N13/576/77/PDF/N1357677.pdf?OpenElement. (last visited on 20th December, 2021).

harassment, cyber stalking, violation of privacy, censorship and the hacking of e-mail accounts, mobile phones and other electronic devices, with a view to discrediting them and/or inciting other violations and abuses against them, are a growing concern and can be a manifestation of systemic gender-based discrimination, requiring effective responses compliant with human rights[74]".

(v) Resolution 2331 (2016), adopted by the United Nations Security Council on 20th December 2016, which establishes the following observation: acts of sexual and gender based violence constitute, for some armed groups, a tactic of terrorism. It underlines the "connection between trafficking in persons, sexual violence and terrorism and other transnational organized criminal activities, which can prolong and exacerbate conflict and instability or intensify its impact on civilian populations".

(vi) The ***UN Human Rights Council resolution on the promotion, protection and enjoyment of human rights on the internet (2016),*** affirmed that the rights people have offline must also be protected online.[75]

(vii) The ***UN General Assembly's resolution on the right to privacy in the digital age*** (2016) recalls that violations and abuses of the right to privacy in the digital age may affect all individuals, including with particular effects on women, as well as children and those who are vulnerable or marginalized[76].

(viii) The ***UN Agenda 2030*** for sustainable development has among others the goal to "achieve gender equality and empower all women and men" and includes targets such as "Enhance the use of enabling technology, in particular information and communications technology, to promote the empowerment of women", and

[74] UN General Assembly, Promotion of the Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms: protecting women human rights defenders, GA Res 68/181, GAOR, UN Doc A/RES/68/181 (December 18th, 2013), *available at:* http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/181. (last visited on 3rd March, 2021).

[75] UN Human Rights Council, The promotion, protection and enjoyment of human rights on the Internet, UN Doc A/HRC/RES/32/13 (July1, 2016) *available at:* http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/32/13 (last visited on 3rd March, 2021).

[76] UN General Assembly, "The Right to Privacy in The Digital Age" GA Res 3/71, GAOR, UN Doc A/C.3/71/L.39/Rev.1(November 16th, 2016), *available at*: http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/71/L.39/Rev.1. (last visited on 3rd March, 2021).

"Eliminate all forms of violence against all women and girls in the public and private spheres, including trafficking and sexual and other types of exploitation".

(ix) The Committee on the Elimination of Discrimination against Women (CEDAW Committee) adopted on 2017 the new *General Recommendation35*which reaffirms the UN's commitment to a world free from violence for all women and girls and recognises the new forms of violence against women and girls, redefined "*through technology-mediated environments, such as contemporary forms of violence occurring in the Internet and digital spaces"*.

(x) In 2018, the *Special Rapporteur on Violence against Women* will release a thematic report focusing on online gender-based violence.[77]

(xi) United Nations, Human Rights Council resolution A/HRC/38/L.6, Accelerating efforts to eliminate violence against women and girls: preventing and responding to violence against women and girls in digital contexts.[78]The *UN Human Rights Council on July 4th 2018 voted* resolutions on the "Promotion, protection and enjoyment of human rights on the Internet"[79], several of them concern cyber violence and hate speech online against women and the relations between privacy violations, misuse and theft of data and violence, including against women for their public persona.

Other resolutions aimed at eliminating all forms of violence against women have been adopted by the United Nations General Assembly. Examples include resolutions 61/143 (2006); 63/155 (2008); 64/137 (2009); 65/187 (2010); 67/144 (2012); 69/147 (2014) and 73/148 (2018). International organization such as ITU, Interpol, UNODC, G 8 Group of State, Council of Europe, OECD, Common Wealth and European Union has also taken efforts to ensure the harmonization of legalization in individual Countries.

[77] UN Human Rights Council, Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective, UN GAOR, UN Doc A/HRC/38/47 (June 18,2018), *available at:* https://digitallibrary.un.org/record/ 1641160?ln=en. (last visited on 10th March, 2021).

[78] UN Human Rights Council, Accelerating efforts to eliminate violence against women and girls: preventing and responding to violence against women and girls in digital contexts, GAOR UN Doc. A/HRC/38/L.6. (July 4th, 2018), *available at:* file:///C:/Users/user/Downloads/A_HRC_38_L.33-EN.pdf. (last visited on 2nd March 2021).

[79] UN Human Rights Council, The promotion, protection and enjoyment of human rights on the Internet, UN Doc A/HRC/32/L.20 (June 27th, 2016), *available at:* http://digitallibrary.un.org/record/ 845728. (last visited on 3rd March, 2021).

5.8. Legislation Specifically Targeting Revenge Porn and Blackmailing

For a number of years, there was a relative dearth of legislation particularly focusing the phenomenon of revenge porn. Against this backdrop, across various jurisdictions, prosecutors sought to rely on various species of ad hoc criminal legislation to prosecute perpetrators of the offence, though with limited success, as such legislation were not specifically designed at the outset to target this relatively new phenomenon. Given the now axiomatic uncertainties and challenges surrounding the use of non-specific image-based sexual abuse offences to prosecute the phenomenon, a number of jurisdictions have gone ahead to enact specific legislation aimed at more effectively combating the unauthorized disclosure of intimate images. Several arguments have been advanced in favour of such legislation.[80]

First, legislation in this area would send a strong message that this type of conduct is unacceptable and serve to deter potential perpetrators from offending.

Second, legislation in this area would fill the gap within the existing law in various jurisdictions, and effectively serve a symbolic and educative function for society.

In other words, by providing a tailored image-based sexual abuse offence, this behaviour would be appropriately identified to the public and would clearly highlight and reinforce the 'wrongfulness' of image-based sexual abuse. Indeed, if people become aware that they may be committing an offence by sharing intimate images, they might become a little bit more discretionary about what they share and in what circumstances.[81]

Finally, enacting specific legislation may also appropriately address the fact that there is often an international element in the disclosure of intimate images. States may, in this regard, rely on mutual legal assistance if criminal prosecutions are brought against perpetrators operating across international boundaries.

In attempting to address the revenge porn problem, legal scholars and lawmakers worldwide have grappled to identify the complex legal and moral issues surrounding the production and unauthorized dissemination of intimate photographs and videos.

[80] Phenomenon colloquially referred to as "revenge porn" (Legal and Constitutional Affairs References Committee, February 2016).

[81] D K Citron and M A Frank "Criminalising Revenge Porn" 49 *Wake Forest Law* 345-361 (2014).

The issue has, unsurprisingly, given rise to varying academic opinion as to how it should be addressed. Many academics welcome criminalisation, believing it sends a positive message that the misconduct is harmful and deserving of criminal sanction.

5.8.1. The United Kingdom Legislation on Revenge Porn and Blackmailing

There is some degree of divergence in how the respective legislatures have sought to fashion the criminal offence of image-based sexual abuse across the United Kingdom.[82] Under Section 33 of the England and Wales Criminal Justice and Courts Act, 2015 as well as Section 51 of the Justice Act (Northern Ireland) 2016, an offence is committed when a person (D) discloses to a third party: (a) a private sexual photograph or film (b) without the consent of the person depicted (V), and (c) with the intention of causing V distress. The concept of disclosure is broadly defined so as to cover both electronic distribution as well as physically showing an intimate image or video to a third party. An image or video is 'sexual' if it shows all or part of an individual's exposed genitals or pubic area; or it shows something that a reasonable person would consider to be sexual because of its nature, or its content, taken as a whole, is such that a reasonable person would consider it to be sexual.[83] It would appear, in this connection, that the offence does not cover conduct such as kissing. More generally, it is important to note that the Act specifies that images or videos that were not originally sexual in nature, but which have been edited in some way so that they become sexual, will not be 'sexual' within the Act, [84] thereby excluding persons from liability if the images are 'photoshopped' images, for example; that is, where the person superimposes an image of the victim's head onto an image of a person engaged in a sexual act, as transpired in ***Marina Marshall* v. *Lenisha Augustine***.[85] It would appear, however, that disclosing a private and sexual image or video that has been altered, for example by disguising the subject's face, will still be an offence.

[82] A Gillespie "Trust Me, It's only for me": "Revenge Porn" and the Criminal Law 11*Criminal Law Review* 866 (2015).

[83] The Criminal Justice and Courts Act, 2015, s. 35(3), *available at:* https://www.legislation.gov .uk/ukpga/2015/2/enacted/data.pdf.(last visited on 2nd September, 2021).

[84] The Criminal Justice and Courts Act, 2015, s. 35(5).

[85] *Marina Marshall* v. *Lenisha Augustine* (2001) 0319 DOMHCV. *available at:* https://www.eccourts. org/wp-content/files_mf/1359389407_magicfields_pdf_file_upload_1_1.PDF. (last visited on 4th September, 2021).

The offence requires that the prosecution prove that the defendant specifically intended to cause the victim distress,[86] and contrary to the approach in Victoria, Canada and Scotland, reckless disclosure will not be sufficient. In other words, an intention to cause distress cannot be implied in England and Wales merely because distress was a natural and probable consequence of disclosure.

In contrast to the arguably narrow approach countenanced in England and Wales to the unauthorized disclosure of intimate images, Scotland, through its recently enacted Abusive Behaviour and Sexual Harm (Scotland) Act, 2016 introduced the offence of 'disclosing or threatening to disclose an intimate photograph or film'. A person commits this offence if they disclose or threaten to disclose a photograph or film which shows, or appears to show, another person in an intimate situation and the person intends to cause, or is reckless as to whether the other person will be caused, fear, alarm, or distress.[87] Although this offence is similar to the offence introduced in England and Wales, it has a number of features which make it a more comprehensive response to the harm caused by the non-consensual distribution of intimate images. At the outset, the Scottish offence applies not only to circumstances where the perpetrator intends to cause the victim fear, alarm or distress, but also where the perpetrator is reckless as to this. The mental element also applies to intention to cause or being reckless as to whether the victim will be caused 'fear' and 'alarm' as well as 'distress' and so is wider than the English offence which only applies to intention to cause 'distress'.[88]

In addition, the Scottish offence also applies to threats to disclose intimate photographs and films, which does not apply in England and Wales. Moreover, the definitions of 'intimate situation', 'film' and 'photograph' in the Scottish Act include a wider range of intimate images than the equivalent definitions in the English legislation. For example, the definition of 'intimate situation' applies not only to images where the 'genitals, buttocks or breasts' are exposed, but also where they are 'covered only with underwear'.[89]The Scottish offence is also defined to include images which are altered in

[86] The Criminal Justice and Courts Act, 2015, s. 33(1) (b).
[87] Abusive Behaviour and Sexual Harm (Scotland) Act, 2016, s. 2(1), *available at:* https://www.legislation.gov.uk/asp/2016/22/enacted/data.pdf. (last visited on 6th September, 2021).
[88] Abusive Behaviour and Sexual Harm (Scotland) Act, 2016, s. 1(7).
[89] Abusive Behaviour and Sexual Harm (Scotland) Act, 2016, s. 3(1) (b).

any way[90], such as where a person's face is superimposed on an intimate image, unlike the more limited approach that is countenanced in England and Wales, where Section 35(5)(b) provides that a photograph is not private and sexual if 'it is only private or sexual by virtue of the alteration'.

In view of the above concerns, a number of amendments were proposed[91] to buttress the Criminal Justice and Courts Act (CJCA), which were tagged onto Section 61 of the Police and Crime Bill, including: creating the offence of threatening to disclose private material; expanding the harm caused to the victim to include 'alarm' as well as 'fear' or distress; stipulating that an offence under Section 33 can be committed not only intentionally, but also where the person in so disclosing the intimate image is reckless as to the causing of fear/alarm/distress; expanding the definition of 'sexual' to ensure that the disclosure of pornographic photoshopped images are covered by the law; and adding further offence aimed at criminalizing those who 'knowingly promote, solicit or profit' from the disclosure of private material, where there is a reasonable belief that the disclosure has been done without consent. These revisions to the CJCA, which would have directly mirrored the Scottish model,[92] however, this was rejected on 16th November 2016.[93]

In the interim, notwithstanding the areas of divergences averred to above, a number of cases have been decided upon since the enactment of the offence in 2015 in England and Wales, which provide some interesting perspectives as to the evolving nature of the phenomenon in these jurisdictions.[94] In the case of ***R* v. *Sam Colley***[95], the defendant was sentenced to 12 weeks imprisonment suspended for 18 months after he pleaded guilty to the offence of image-based sexual abuse in circumstances where he sent an intimate picture of a woman to members of her family via Facebook and threatened to

[90] Abusive Behaviour and Sexual Harm (Scotland) Act, 2016, s. 3(2).
[91] D. Reece Greenhalgh "Revenge Porn: Widening the Net?" *Criminal Law and Justice Weekly* (4th July 2016).
[92] D. Reece Greenhalgh "Revenge Porn: Widening the Net?" *Criminal Law and Justice Weekly* (4th July 2016)..
[93] Baroness Williams and Lord Pannick, Speech by Lord Marks Hansard (16th November 2016) Volume 776, *available at:* https://hansard.parliament.uk/lords/2016-11-16/debates/DE488DE7-5743-45D2-9EB1-6C8AEEF6908E/PolicingAndCrimeBill.
[94] List of cases with brief descriptions can be found on the CPS website, *available at:* http://www.cps.gov.uk/news/latest_news/prosecutors_being_advised_to_learn_from_revengeporncases/ (last visited on 8th October, 2002).
[95] (Barkingside Magistrates Court) 7th July, 2015.

post further pictures online. Similarly, in ***R* v. *Simon Humphrey***[96]**,** the defendant was sentenced to 4 months imprisonment suspended for 18 months for setting the victim's image as his 'profile picture' on Facebook intending to humiliate the victim, in circumstances where the victim's child first noticed the picture being used.

In ***R* v. *Alex***,***[97]*** the defendant was sentenced to a 12-month community order, handed a fine and ordered to pay costs in circumstances where he sent the victim a Facebook message from a false account using the private sexual photograph of the victim as his profile picture.

Further, in ***R* v. *William Nelson*,**[98] the defendant was sentenced to 2 months imprisonment suspended for 18 months where he set up a fake Facebook account and posted approximately 30 intimate photographs of the victim, and then sent friend requests to her friends and family from the fake account.

Women have also to date been convicted under the statute. For example, in ***R* v. *Paige Mitchell*,**[99] the defendant was sentenced to 6 weeks imprisonment suspended for 18 months, rehabilitation activity requirement for 50 days and ordered to pay costs where she admitted to posting explicit photos of the victim on to her Facebook profile after an argument. Mitchell went on to caption the pictures with humiliating insults and even referenced the assault. Similarly, in ***R* v. *Kaylea Reid***,[100] the defendant, who had ongoing flirtatious conversations with her employer, was convicted for posting pictures of her naked boss on his wife's business Facebook page.

Interestingly, unlike other offenders, she was spared jail time, and only given a conditional discharge for six months and ordered to pay a victim surcharge fee of £20, because of what the Magistrates described as the victim's 'provocative behaviour'. This case is problematic because it reinforces victim blaming, sets a patently dangerous precedent, and wrongfully conflates consent given in the context of flirtatious conversations with consent to disclose the intimate pictures to the public without authorization.

[96] (St Albans Magistrates' Court) 18th September, 2015.
[97] 2017 SCC 37, [2017] 1 S.C.R. 967 (Kidderminster Magistrates' Court) 13th August, 2015. a*vailable at:* https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/16714/index.do.(last visited on 8th October, 2021).
[98] (Croydon Magistrates' Court) 24th September, 2015.
[99] (Stevenage Magistrates' Court) 1st September, 2015.
[100] (Ipswich Magistrates' Court) 8th November, 2016.

That said, it is nonetheless commendable that the Courts have also penalized those who make use of other platforms to commit image-based sexual abuse, apart from Facebook. For example, in ***R* v. *Jason Asagba***,[101] the defendant was prosecuted after he sent the intimate pictures of the victim to the victim's family via text and hacked into the victim's Facebook account and shared an intimate image on her timeline. Similarly, in ***R* v. *John Duffin*,**[102] the defendant was convicted for saving an intimate picture of a woman and setting it as his 'Whatsapp' profile picture, which allowed all of his contacts to view it. Interestingly, also, distributing images on offline platforms has also been met with the robust disapproval of the courts. For example, in ***R* v. *Luke Brimson***,[103] the defendant was sentenced to 24 weeks in prison suspended for 18 months, given a 2 year Restraining Order and made to pay costs, in circumstances where he distributed intimate pictures of a woman inside and outside of a supermarket. One interesting question which has arisen in recent months which merits special attention relates to whether the sentences imposed by Magistrates in image-based sexual abuse cases can be aptly described as having a deterrent effect or overly excessive.

This issue arose in ***David Derbyshire* v. *R***,[104] where a man who admitted posting the intimate images of his ex-girlfriend on Facebook and Whatsapp successfully appealed against a sentence of 17 weeks imprisonment, notwithstanding the fact that, as the Magistrate had earlier found, the 'offence was so serious because it was a massive breach of trust and there were repeated attempts to keep it on Facebook and Whatsapp'. On appeal, the Crown Court substituted the sentence with an 8-week jail term, suspended for 24 months, with a rehabilitation activity requirement of up to 15 days.[105]

In conclusion, what these cases[106] suggest is that some attempt to curtail the evolving modus operandi of perpetrators of image-based sexual abuse through the

[101] (Reading Magistrates' Court) 16th May, 2015.
[102] (Bristol Magistrates Court) 13th August, 2015.
[103] (Woodspring Magistrates Court) 30th July, 2015.
[104] *David Derbyshire* v. *R* (Bolton Crown Court) 30th May, 2016.
[105] I Proctor 'Man Who Posted Revenge Porn on Facebook and Whatsapp Wins Cut to Sentence' The Bolton News, 6 June 2016, *available at:* http://www.theboltonnews.co.uk/news/bolton/14539021 (last visited on 7th February, 2021).
[106] *R* v. *Clayton Kennedy* (Cardiff Magistrates Court) 6th July, 2015 (the defendant was sentenced to a 12-month Community Order, fined £110 and ordered to pay court costs of £295 and given an indefinite restraining order for posting intimate pictures of a woman onto Facebook, the victim was not aware the photo had even been taken, causing further distress).

imposition of appropriately dissuasive sanctions. That said, it must be borne in mind, as pointed out by *Lord Marks* in the November 2016 debates, out of 1160 reported instances of image-based sexual abuse between April and December 2015, no action was taken in no less than 61% of cases.

In short, it is particularly concerning that many cases were not prosecuted because of insufficient evidence or because the victim did not proceed with the complaint, though this is not an indication that the incidents did not occur.[107]

5.8.2. The United States of America Legislation on Revenge Porn and Blackmailing

At present, the United States does not have in place a federal offence that prohibits image-based sexual abuse. In mid-2016, however, Democratic Congresswoman *Jackie Speier* prepared a 'discussion draft' of the Intimate Privacy Protection Bill 2015, which is now before the House of Representatives. The Bill, if successfully passed, aims to amend chapter 88 of title 18 of the United States Code, by prohibiting, under §1802, the knowing use of electronic communication services or any other facility to:

"*distribute a visual depiction of a person who is identifiable from the image itself or information displayed in connection with the image and who is engaging in sexually explicit conduct, or of the naked genitals or post-pubescent female nipple of the person, with reckless disregard for the person's lack of consent to the distribution"*

The penalty prescribed by the Bill is five years imprisonment, which is consistent with the approach countenanced by the Scottish legislation.

On a state level, an estimated 34 States have thus far prohibited the unauthorized disclosure of intimate images through legislation.[108] In general, the relevant statutes in the respective States, including Oregon[109] and Utah[110], criminalize such disclosure where there is an intention to cause distress. Absent, however, from most states' statutes are

[107] Hansard (16th November 2016) Volume 776, Column 1437. Speech by Lord Marks, *available at* https://hansard.parliament.uk/lords/2016-11-16/debates/DE488DE7-5743-45D2-9EB1 6C8AEEF6908E/PolicingAndCrimeBill. (last visited on 31st October, 2021)

[108] These laws can be viewed at the Cyber Rights Initiative online database, *available at*: https://www.cybercivilrights.org/revenge-porn-laws/. (last Visited on 4th October, 2021).

[109] Oregon Revised Statute, 2021 Edition, *available at*: https://www.oregonlegislature.gov/ bills_laws/pages/ors.aspx. (last visited on 1st January, 2022).

[110] Utah Code, 2021,s. 76-5b-203, *available at*: https://legiscan.com/UT/text/HB0147 /id/2268798/Utah-2021-HB0147-Introduced.pdf. (last Visited on 2nd January, 2022).

references to recklessness in respect of the distress caused, with the exception of the California Penal Code.[111] That said, the penalties prescribed range from between one year and three years, such as the Georgia Code.[112] In some instances, legislation, such as the Texas Penal Code,[113] also prohibits threats to disclose intimate images, with appropriate defences included where the disclosure is for the purposes investigating crime or in the public interest.

Since the enactment of these statutes, a few cases have been decided upon which have sought to interpret and apply the provisions of said statutes, though not without some controversy. In a recent decision ***State* v. *Benjamin Barber***,[114] the Court sentenced the defendant to six months in jail, with five years of probation, in circumstances where he posted sexually explicit videos of himself and his ex-girlfriend to various pornographic websites, contrary to Oregon's anti-image-based sexual abuse statute. Interestingly, the defendant, in his defence, maintained that he was actually the victim in this case since his posting of the videos was as a result of the victim threatening to use said videos against him as blackmail. The Court, however, rejected the defendant's defence as being unsubstantiated.

In a controversial case recently decided upon, ***Antigone Books* v. *Brnovich***,[115] Arizona's image-based sexual abuse law prohibiting the unauthorized disclosure of nude images was struck down as being unconstitutional in light of its overbroad, vague, and overly restrictive impact on freedom of speech.[116] In this case, a group of Arizona booksellers, publishing companies, news articles, librarians, and photographers (including the Voice Media Group, New Times' parent company) sued the state Attorney General's Office, arguing that the law went beyond prohibiting image-based sexual abuse to cover the publication of certain educational materials about breastfeeding, or newsworthy photographs like those taken at the Abu Ghraib prison, among others. In this context, the Court found that the law, in criminalizing the posting of a nude photo with no intent to harm the person depicted, was an unconstitutional infringement of the

[111] The California Penal Code, 1872, s.647 (j) (4).
[112] The Georgia Code, Title 16, ch. 11, Art. 3, Part 1, 16-11-90.
[113] The Texas Penal Code, 1973, s. 21.16.
[114] (Oregon Circuit Court) 1 December 2016.
[115] *Antigone Books* v. *Brnovich*, Case No. 2:14-cv-02100 (Arizona District Court).
[116] M. L. Jones, "*Ctrl + Z: The Right to Be Forgotten*" 71 (New York University Press, 2016).

Claimants' freedom of speech guaranteed under the First Amendment. In response, the Arizona Office of the Attorney General opted not enforce the statute as it felt that this would 'certainly result in further litigation'.[117]

In another case ***State of Vermont* v. *Rebekah Vanburen***[118] similar concerns were expressed regarding the uneasy relationship between recently enacted image-based sexual abuse legislation and the right to freedom of expression. In this case, the female complainant had taken photographs of herself that were nude or partially nude and sent them to the Facebook account of Anthony Coon, with whom she had a prior relationship. At the time she sent them, however, she was not still in a relationship with Mr. Coon, as Mr. Coon had by that time entered into a relationship with the defendant. The defendant managed to access Mr. Coon's Facebook account, and posted the intimate photos of the complainant on a public Facebook page, in the process tagging the complainant in them. A number of people saw the photographs in this manner. The complainant learned of the posting and sought to have it taken down. The defendant admitted that she publicly disclosed the intimate images in order to exact revenge or to get back at the complainant for the prior relationship with Mr. Coon and for sending him these sexual photographs. She told complainant she did it and told her she was seeking to harm her reputation in her work; in fact, the defendant allegedly told officers she wondered if complainant had 'learned her lesson'.

The Vermont Statutes**,** 13 V.S.A. § 2606(b) (l) prohibits '*knowingly disclosing a visual image of an identifiable person who was nude or was engaged in a sexual conduct, without his or her consent, with the intent to harm, harass, intimidate, threaten, or coerce the person depicted, and the disclosure would cause a reasonable person to suffer harm*', the Court granted the defendant's motion to dismiss the claim. The Court, in this connection, found that the statute is unconstitutional under the First Amendment to the United States Constitution in that it is an overbroad restraint on a protected form of speech or expression and not tailored to a compelling or important governmental purpose. While the court accepted that freedom of expression may be limited, the expression

[117] M. Wasser "AZ Revenge Porn Law Not to Be Enforced, Says Federal Judge" Phoenix New Times, 13th July 2015, *available at:* https://www.phoenixnewtimes.com/news/az-revenge-porn-law-not-to-be-enforced-says-federal-judge-7486054.(last visited on 21st April, 2021).

[118] (2018) VT 95, 214 A.3d 791, *available at:* https://harvardlawreview.org/2020/05/state-v-vanburen/. (last visited on 21st April, 2021).

sought to be limited in this case the disclosure of the intimate images had to fall into one of the exceptions, which includes obscenity, defamation, fraud, incitement, or speech integral to criminal conduct. On reviewing the nature of image-based sexual abuse, the Court found that the phenomenon does not fall onto the 'obscenity' category. As such, the statute was subject to strict, rather than rational review, which is a higher threshold to establish its constitutionality.

In arriving at its arguably conservative conclusion, the Court made it clear that, While there is argument that 'revenge pornography' should be considered obscene simply because of the intent it is used, there is no present authoritative law that would allow this court to take such a step in enlarging the area of unprotected speech under the First Amendment.[119]

After subjecting the relevant statute to 'strict scrutiny', the court found that even if it were to assume that the state met its burden of a compelling governmental interest, that is, its citizens privacy rights and perhaps reputational rights, it did not meet its burden of showing there are no less restrictive alternatives, such as civil penalties that would be as effective. The Court, in additionally, quite interestingly, also had concerns over the reality that the facts of this case were not a clear example of the typical image-based sexual abuse case described in many articles and mentioned in support of the statute. In other words, this was not a case of photographs sent or exchanged during a relationship and then used after the relationship ended, usually unpleasantly. Rather, it involved a situation in which the complainant sent the photographs to a person with whom she had a past relationship, but was not presently in a relationship with. On this point, the Court, quite indifferently, concluded that 'the possible over breadth of the statute is of concern'.[120] It is submitted that this flawed and parochial understanding of the term 'image-based sexual abuse' is anachronistic in nature, and symptomatic of the wider problem of improperly construing the scope of the phenomenon.[121]

[119] The Vermont Statute, § 3.
[120] The Vermont Statute, § 5.
[121] Calvert "Revenge Porn and Freedom of Expression: Legislative Pushback to an Online Weapon of Emotional and Reputational Destruction" 24 *Fordham Intellectual Property Media and Entertainment Law Journal* 673 (2013).

5.8.3. Canada Legislation on Revenge Porn and Blackmailing

Canada, like England and Wales, has forged ahead with creating a specific offense that appropriately captures the unauthorized disclosure of intimate images. The Protecting Canadians from Online Crime Act, 2014, which entered into force in March 2015, inserts an offence into Section 162.1 of the Canadian Criminal Code, so that any person who 'knowingly publishes, distributes, transmits, sells, makes available or advertises an intimate image' of another person knowing the person depicted in the image did not consent, or being reckless as to this, is guilty of an offence[122]. Unlike the England and Wales Act, the amended Canadian Criminal Code does not only prohibit intentional disclosure, but also reckless disclosure.

That said, the Act includes a defence, whereby no offence will be committed if the 'conduct that forms the subject-matter of the charge serves the public good and does not extend beyond what serves the public good'.[123]For the purposes of this defence, it is a question of law whether the conduct serves the public good and whether there is evidence of this, but it is a question of fact whether the conduct does or does not extend beyond what serves the public good and the motives of the accused are irrelevant in this assessment. It is important to note that the Canadian offence includes a more substantial maximum penalty of five years imprisonment compared to the maximum two years imprisonment [124] under the Victorian and English offences. The Scottish offence, discussed below in respect of the Abusive Behaviour and Sexual Harm (Scotland) Act, also carries a maximum penalty of five years imprisonment.[125] Moreover, it is also worth noting that the Canadian Act, quite progressively, also makes complementary amendments to authorize the removal of such images from the internet and the recovery of expenses incurred to obtain the removal of such images; the forfeiture of property used in the commission of the offence; a recognizance order to be issued to prevent the distribution of such images; and the restriction of the use of a computer or the internet by a convicted offender.

[122] Protecting Canadians from Online Crime Act, 2014, s. 162.1.
[123] Protecting Canadians from Online Crime Act,2014, s. 162.1(3).
[124] Protecting Canadians from Online Crime Act, 2014, s. 162.1 (1) (a).
[125] Abusive Behaviour and Sexual Harm (Scotland) Act, 2016, s. 2(7) (b).

5.8.4. Australia Legislation on Revenge Porn and Blackmailing

Although legislative activity aimed at combating image-based sexual abuse is at an embryonic stage in Australia, several steps have quite commendably been taken to date towards addressing the phenomenon.[126] At the Commonwealth level, the Criminal Code Amendment (Private Sexual Material) Bill 2015, which targets individuals who share,[127] or threaten to share,[128] private sexual images or film recordings of others without consent and with the intention of, or where there is the risk of, causing that person harm or distress, as well as those who operate image-based sexual abuse websites,[129] has received its second reading, and is likely to become operational in the not too distant future.

It is important to note that, to date, at the state level, only two Australian states have specifically criminalized image-based sexual abuse through legislative enactments. The first is South Australia, which in 2013 enacted Section 26C (1) of the Summary Offences (Filming Offences) Amendment Act, 2013 (SA), thereby making it an offence to distribute 'invasive images' of a person without their consent.[130] The concept of an

[126] D. Plater, "Setting the Boundaries of Acceptable Behaviour"? South Australia's Latest Legislative Response to Revenge Pornography" 2 *Uni SA Student Law Review* 1(2016).

[127] Criminal Code Amendment (Private Sexual Material) Bill 2015, s. 474.24E state that: Using a carriage service for private sexual material:
(1) A person commits an offence if
(a) the person transmits, makes available, publishes, distributes, advertises or promotes material; and
(b) the material is private sexual material; and
(c) the person engages in the conduct mentioned in paragraph (a) without the consent of a subject of the material; and
(d) the person knows of, or is reckless as to, the subject's lack of 6 consent; and
(e) either:
(i) the conduct mentioned in paragraph (a) causes distress or harm to a subject of the material; or
(ii) there is a risk that the conduct mentioned in paragraph (a) will cause distress or harm to a subject of the material; and
(f) the person engages in the conduct mentioned in paragraph (a) 14 using a carriage service.
Penalty: Imprisonment for three years.

[128] Criminal Code Amendment (Private Sexual Material) Bill, 2015 s. 474.24F provide that "Using a carriage service or making a threat about private sexual material".

[129] Criminal Code Amendment (Private Sexual Material) Bill, 2015, s. 474.24G provide that "Possessing, controlling, producing, supplying or obtaining private sexual material for use through a carriage service."

[130] Summary Offences (Filming Offences) Amendment Act, 2013, s. 26C state that "Distribution of invasive image:
(1) A person who distributes an invasive image of another person, knowing or having reason to believe that the other person
(a) does not consent to that particular distribution of the image; or

'invasive image' means 'a moving or still image of a person engaged in a private act; or in a state of undress such that the person's bare genital or anal region is visible, but does not include an image of a person under, or apparently under, the age of 16 years or an image of a person who is in a public place'.[131] The proposed Commonwealth legislation, this Act does not appear to require that an intent to cause distress, which, while making it easier to prosecute the offense, raises questions as to whether such an approach is demonstrably justified, that is, a proportionate approach, having regard to the countervailing right to freedom of expression.[132] The same questions arise in relation to Section 41DA(1) of the Victoria Summary Offences Act, 1966 (Vic), which was amended by the Crimes Amendment (Sexual Offences and Other Matters) Act, 2014 (Vic), and which provides for the imposition of two years imprisonment where:

a. A person (A) intentionally distributes the intimate image of another person
b. to a person other than B; and
c. The distribution of the image is contrary to community standards of acceptable conduct.

It is to be noted that this notion of 'community standards of acceptable conduct' is not defined in the Act. However, it can be argued that, having regard to the English offence which requires that the image or film be private, which is defined as something that is not of a kind ordinarily seen in public, a similar reading of the 'community standards' requirement may be appropriate.[133]

That said, unlike the South Australia Act, the Victoria Act specifically prohibits the making of threats (whether implicitly or explicitly or by conduct) concerning the distribution of intimate images if the distribution of the image would be contrary to community standards of acceptable conduct, and the perpetrator intends that the victim will believe, or believes that the victim will probably believe, that he will carry out the threat, pursuant to Section 41DB (1). Notwithstanding the noble recognition that threats

(b) does not consent to that particular distribution of the image and does not consent to distribution of the image generally, is guilty of an offence.
Maximum penalty: $10,000 or imprisonment for two years."

[131] Summary Offences (Filming Offences) Amendment Act, 2013, s. 26A.
[132] J. Humbach "How to Write a Constitutional "Revenge Porn" Law" 35 *PACE Law Review* 215(2014).
[133] J Quirke (et al.) *Report Harmful Communications and Digital Safety* 99 (Law Reform Commission, 2016).

to distribute intimate images can be used to coerce victims to remain in abusive relationships, it should be noted that an offence against Section 41DB(1) carries a maximum penalty of one year imprisonment, which is a third of the penalty proposed by the Criminal Code Amendment (Private Sexual Material) Bill 2015.

5.8.5. New Zealand Legislation on Revenge Porn and Blackmailing

New Zealand, in keeping with the global legislative trend against image-based sexual abuse, enacted the Harmful Digital Communications Act, 2015 (NZ) (the HDCA Act) in 2015. Section 22 of the Act creates the offence of 'causing harm by posting digital communication'.[134] Interestingly, unlike the statutes previously discussed, the New Zealand Act defines 'harm' as 'serious emotional distress',[135] and defines 'communication' to include the sending or posting of an intimate visual recording (including still pictures) of another individual or an attempt to do so.[136] Online content hosts can be held liable in respect of specific content of a digital communication posted by a person and hosted by the online content host.

Despite the fact that since its enactment Section 22 has been relied upon to charge over 12 persons for image-based sexual abuse, some of whom have been convicted and sentenced to periods of imprisonment,[137] it can be argued that, unlike the Scottish legislation, the New Zealand Act does not appear to treat with instances where a person recklessly posts an intimate image. More generally, the Act has been criticized as for creating an 'overbroad and vague' offence,[138] particularly the definition of harm which

[134] The Harmful Digital Communications Act, 2015, s. 22(2) state that "Where:(a) the person posts a digital communication with the intention that it cause harm to a victim; and (b) posting the communication would cause harm to an ordinary reasonable person in the position of the victim; and (c) posting the communication causes harm to the victim.
In determining whether a post would cause harm, the court may take into account any factors it considers relevant, including: (a) the extremity of the language used; (b) the age and characteristics of the victim; (c) whether the digital communication was anonymous; (d) whether the digital communication was repeated; (e) the extent of circulation of the digital communication; (f) whether the digital communication is true or false; and (g) the context in which the digital communication appeared" (3) state that "A person who commits an offence against this section is liable on conviction to (a) in the case of a natural person, imprisonment for a term not exceeding two years or a fine not exceeding $50,000 and (b) in the case of a body corporate, a fine not exceeding $200,000".

[135] The Harmful Digital Communications Act, 2015, s. 4.

[136] *Ibid.*

[137] N. Henry and A. Powell, "Beyond the "Sext": Technology-Facilitated Sexual Violence and Harassment against Adult Women" 48 *Australian & New Zealand Journal of Criminology* 104(2015).

[138] J Quirke (n 51) page 78.

requires 'serious' and not mere distress, and the discretionary factors which courts can take into account when assessing whether harm is caused. For these and other reasons, the offence has been described as a 'threat to online free speech'.[139]

5.8.6. Other Countries Legislation on Revenge Porn and Blackmailing

Apart from the countries identified to above, a number of other countries from across the globe have taken proactive steps to criminalize image-based sexual abuse. Examples include

(i) *Israel* which passed an amendment to its Prevention of Sexual Harassment Act aimed at criminalizing those who upload intimate photos or videos without the consent of their partners with five years in prison, and victims are eligible for up to 50,000 NIS without proof of damage, and higher compensation if damages are proven.[140]

(ii) *Germany* which amended Section 201a of the Criminal Code to prohibit a person from unlawfully and knowingly making available to third parties an intimate picture that was created with or without the consent of another person located in a dwelling or room especially protected from view and thereby violating that person's intimate privacy.[141]

(iii) *Japan*, pursuant to Art. 3 of the Revenge Porn Prevention Act, criminalizes the provision of a private sexual image of another person without the person's approval via a means of telecommunication to an unspecified number of or to many people, and allows Internet service providers to delete suspected image-based sexual abuse images without the up loader's consent in specified circumstances[142]; and

(iv) Saint Vincent and the Grenadines, pursuant to Section 13(3) of the Cybercrimes Act (2016), also criminalizes a person who, intentionally or recklessly, uses a computer

---

[139] *Ibid* at 80.

[140] J .C. Rodriguez, "Israel Criminalizes "Revenge Porn" in New Bill" *Law360*, 7 January 2015, *available at:* https://www.law360.com/articles/499212/israel-criminalizes-revenge-porn-in-new-bill.(last visited on 2 June 2021).

[141] M. Bohlander, "German Criminal Code (Federal Ministry of Justice, 2010) 98", *available at:* https://ec.europa.eu/antitrafficking/sites/antitrafficking/files/criminal_code_germany_en_1.pdf.(last visited on 2nd June 2021).

[142] S. Matsui "The Criminalization of Revenge Porn in Japan" 24 *Washington International Law Journal* 289(2015).

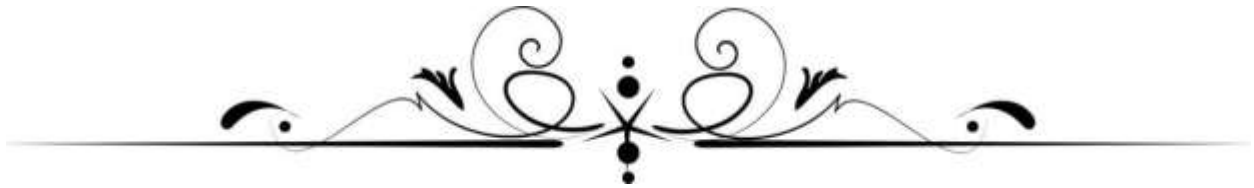
system to disseminate an image that exposes the private affairs of another person, thereby subjecting that other person to public ridicule, contempt, hatred, or embarrassment.[143]

Conclusion

In the present chapter, the researcher study the legal framework at international pertaining to Cyber related crimes in general and women centric provisions related to cybercrimes available at the international level. The researcher further analyses the available legal framework specifically dealing with the problem of Revenge Porn. The researcher also studies some of the judicial approach and fleshes out instances which draw upon over all experience with regards to problem of revenge porn.

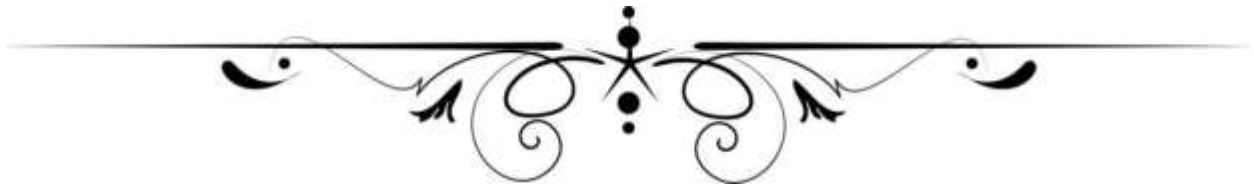
The researcher concluded that, there was no specific and multitude of supranational, international, state and regional laws, conventions, and norms concerned with the protection of privacy around the world indicate that individual privacy is a universally cherished value with significant socio-political implications. Global civilization, having awakened seemingly overnight in an age of transparency, where individual privacy is more a perceived threat to communal well-being than ever, now grapples with an aggressive reconfiguration of hitherto uncompromisable value.

[143] SVG Cybercrimes Act *available at:* http://www.assembly.gov.vc/assembly/images/stories/cybercrime%20bill%202016.pdf. (last visited on 18th November, 2020).



CHAPTER-VI

JUDICIAL ARTICULATION TOWARDS REVENGE PORN AND BLACKMAILING UNDER CYBERCRIME AGAINST WOMEN



CHAPTER-VI

JUDICIAL ARTICULATION TOWARDS REVENGE PORN AND BLACKMAILING UNDER CYBERCRIME AGAINST WOMEN

6.1. Introduction

For understanding the judicial trends towards Cybercrime against women, particularly revenge porn and blackmailing, it is important to consider cases mostly reported by the victims and decided by Supreme Court and various High Courts under cyber laws beneath of Information Technology Act, 2000. The Supreme Court of India and High Courts of various states act as protector of fundamental, constitutional and legal rights of the people/citizens in general and revenge porn and blackmailing in particular under article 32 and 226 respectively. Therefore, it is left to the judiciary as being reasonable and prudent repository of moral standards in society, to administer the laws of the land and also to protect the rights of every citizen/person, in accordance with the law. In this Chapter, the researcher has tried to analyze the decisions of the judiciary in various cases related to privacy, decency, dignity in physical world which also has to be applied to the virtual world equally. The researcher has also analyzed the cases wherein the courts have interpreted the crime of revenge porn and blackmailing through cybercrime to give justice to the victims of such crime.

6.2. Judicial Interpretation of Obscenity and Pornography

The Constitution of India imposes the obligations on the government to secure to all its citizens liberty of thought and expression and guaranteed to all citizens of India freedom of speech and expression under Art. 19(1) (a).[1] Though every citizen of India

[1] The Constitution Of India, art.19(1) state that:
(1) All citizens shall have the right
(a) to freedom of speech and expression;
(b) to assemble peaceably and without arms;
(c) to form associations or unions;
(d) to move freely throughout the territory of India;
(e) to reside and settle in any part of the territory of India; and
(f) *omitted*
(g) to practice any profession, or to carry on any occupation, trade or business

has a fundamental right to freedom of speech and expression, but this fundamental right is subject to certain restrictions mentioned in Art. 19(2)[2] wherein, to maintain the decency and morality are among them, violation of which is not only the violation of the provisions of Art. 19(2) but also a crime provided under sections 292, 293, 294, 499, 502, 509 etc. of the Indian Penal Code involving offences against morality, decency, privacy, law and order. Therefore, obscenity is prohibited. In this regard judicial point of view differs in Pre and Post enactment of The Information Technology Act, 2000.

6.2.1. Obscenity and Pornography Prior to The Information Technology Act, 2000

Prior to the enactment of The Information Technology Act, 2000, the Indian courts followed the landmark decision of United States court of "*Hicklin test*", to decide the cases of obscenity and pornography, which was taken from an 1868 English case, ***Regina* v. *Hicklin***[3]. Under this test, judges considered a work to be obscene if any portion of the material had a tendency "to deprave or corrupt those whose minds are open to such immoral influences, and into whose hands a publication of this sort may fall".

Latter on the issue came before the court again in ***Roth* v. *United State*** [4] case, that 'Is obscenity within the ambit of constitutionally protected freedom of speech or press'. The Supreme Court of the United States observed that *"obscenity was not within the area of constitutionally protected speech or press"*. The court defined the term as defined obscenity as *"material which deals with sex in a manner appealing to prurient interest . . . having a tendency to excite lustful thoughts [or] as [a] shameful and morbid interest in sex".*

In the year 1973, the U.S. Supreme Court evolved a new test for deciding the issue of the obscenity in ***Miller* v. *California,***[5] In this case the court set out the following guidelines for determining whether material is obscene:

---

[2] The Constitution Of India, art.19(2) state that:
"(2) Nothing in sub clause (a) of clause (1) shall affect the operation of any existing law, or prevent the State from making any law, in so far as such law imposes reasonable restrictions on the exercise of the right conferred by the said sub clause in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality or in relation to contempt of court, defamation or incitement to an offence."

[3] (1868)3QB 360.

[4] 354 US 476, 77S. Ct.1304(1957).

[5] 413 U.S.15 (1973).

"(a) Whether 'the average person applying contemporary community standard' would find that the work, taken as a whole, appeals to the prurient interest,

(b) Whether the work depicts or describe, in a patently offensive way, sexual conduct specially defined by the applicable state law, and

(c) whether work, taken as a whole, lacks serious literary, artistic, political, or scientific value".[6]

Indian judiciary whole heartedly followed these principles as well as *Hecklin Test*[7] while dealing the cases related to obscenity. As the whole legal system has been borrowed from England and the Supreme Court of USA, considered as the ideal judicial system, therefore Indian judiciary many times decides the Indian cases in the light of interpretation/ test given by the UK and US judiciary.

Therefore, from earlier times Indian judiciary has interpreted the Indian legal provisions in the light of interpretations given by the British as well US judiciary on such issues.

As stated above that Indian judiciary interpreted the obscenity by using the test laid down by US judiciary in the light of the English judgments. The Indian Judicial court applied the principle laid down in those judgments known as the *"Hickling Test"* and "*Community Standard Test*" and interpreted obscenity in the followings judgments:

Ranjit D. Udeshi* v. *State of Maharashtra[89] The Supreme Court of India in this case adopted a modified version of '*Hicklin Test'* and upheld that there is a difference between 'obscenity' and 'pornography'. The court held that:

---

[6] *Ibid* at 24.

[7] The Hickling Test, the test was given by *Cockburn C.J*. in ***Queen* v. *Hickling*** (1868)3QB 360 and laid down "I think the test of obscenity is this , 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……it is quite certain that it would suggest to the minds of the young of either sex, or even to persons of more advanced years , thoughts of a most impure and libidinous character".

[8] 1965 AIR 881.

[9] This case was related to Ranjit D. Udeshi who was one of the four partners of a firm that owned a book-stall. The partners were prosecuted under section 292 of the Indian Penal Code for selling copies of an allegedly obscene book, Lady Chatterley's Lover, by DH Lawrence. Section 292 punishes any person who sells any obscene book or other material. Udeshi argued that section 292 is violative of the rights to freedom of speech and expression under article 19(1)(a) of the Indian Constitution and that the book is not obscene if considered as a whole.

"There is, of course, some difference between obscenity and pornography in that the latter denotes writings, pictures etc. intended to arouse sexual desire while the former may include writings etc. not intended to do so but which have that tendency. Both, of course, offend against public decency and morals but pornography is obscenity in a more aggravated form."

The Supreme Court further articulated on the test for obscenity, in ***Shri Chandrakant Kalyandas Kakodkar* v. *The State of Maharashtra and Others***[10] and observed that:

"*The concept of obscenity would differ from country to country depending on the standards of morals of contemporary society. What is considered as a piece of literature in France may be obscene in England and what is considered in both countries as not harmful to public order and morals may be obscene in our country? But to insist that the standard should always be for the writer to see that the adolescent ought not to be brought into contact with sex or that if they read any references to sex in what is written whether that is the dominant theme or not they would be affected, would be to require authors to write books only for the adolescent and not for the adults."*

In ***K.A. Abbas* v. *Union of India,***[11] the Chief Justice of Supreme Court of India M. Hidayatullah and other Judges held regarding film censorship that, "our freedom of speech and expression is not absolute, rather limited by reasonable restrictions under Art. 19(2) in the interest of general public to maintain public decency and morality". Therefore, film censorship has full jurisdiction in the field of cinematograph film to prevent and control obscenity and pornography.

In ***Raj Kapoor* v. *State of Maharashtra***,[12] a issue was raised on the controversial film "Satyam, Shivam Sundaram". In this case Justice Krishna Iyer held that "'A' certificate by a high-powered Board of Censors with specialized composition and statutory mandate is not a piece of utter inconsequence. It is relevant material, important in its impact. But we have to examine whether it breaches public morals and decency to invoke the penal provisions However, certificate of the Board has evidentiary value but

[10] (1962 (2) SCC 687).
[11] 1971 AIR 481.
[12] 1980 AIR 258.

does not exclude criminal liability on publication of obscene and pornographic materials".[13]

A controversy regarding a novel named 'Parjapati' was raised in case ***Samaresh Bose* v. *Mr. Amal Mitra*** [14] which was published in 'Sarodiya Desh' for the Bengal written by petitioner.[15] Herein, court held that a Novel written by a well known writer of novels and stories, by which the author intends to expose various evils and ills prevailing in the society with particular emphasis on the obscenity. It has been held that obscenity is not the same as vulgarity. Further, court held 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. The court further stated that characters like Sukhen, Shikha, the father and the brothers of Sukhen, the business executives and others portrayed in the book are not just figments of the author's imagination, Such characters are often to be seen in real life in the society. The author who is a powerful writer has used his skill in focussing the attention of the readers on such characters in society and to describe the situation more eloquently has had used unconventional and slang words so that in the light of the author's understanding, the appropriate emphasis is there on the problems. If we place ourselves in the position of the author and judge the novel from his point of view, we find that the author intends to expose various evils and ills pervading the society and to pose with particular emphasis the problems which ail and afflict the society in various spheres. He has used his own technique, skill and choice of words which may in his opinion, serve properly the purpose of the novel. If we place ourselves in the position of readers, who are likely to read this book, and we must not forget that in this class of readers there will probably be readers of both sexes and of all ages between teenagers and the aged, we*

[13] *Ibid*.
[14] 1986 AIR 967 (MANU/SC/0102/1985).
[15] This case is related with the publication of novel. The issue before court was whether publication is obscene or not. Defendant was a young advocate at that time who complained that the novel contained obscene materials. Print, sale distribution and exhibition of the same which had tendency to corrupt public morals as described sexual feelings after viewing women's private visual body, described close emotional relations with friend's sister.

feel that the readers as a class will read the book with a sense of shock, and disgust and we do not think that any reader on reading this book would become depraved, debased and encouraged to lasciviousness. It is quite possible that they come across such characters and such situations in life and have faced them or may have to face them in life. On a very anxious consideration and after carefully applying our judicial mind in making an objective assessment of the novel we do not think that it can be said with any assurance that the novel is obscene merely because slang and unconventional words have been used in the book in which there have been emphasis on sex and description of female bodies and there are the narrations of feelings, thoughts and actions in vulgar language. Some portions of the book may appear to be vulgar and readers of cultured and refined taste may feel shocked and disgusted. Equally in some portions, the words used and description given may not appear to be in proper taste. In some places there may have been an exhibition of bad taste leaving it to the readers of experience and maturity to draw the necessary inference but certainly not sufficient to bring home to the adolescents any suggestion which is depraving or lascivious. We have to bear in mind that the author has written this novel which came to be published in the Sarodiya Desh for all classes of readers and if cannot be right to insist that the standard should always be for the writer to see that the adolescent may not be brought into contract with sex. If a reference to sex by itself in any novel fit to be read by adolescents, adolescents will not be in a position to read any novel and will have to read books which are purely religious."

Sarodiya Desh is a very popular journal and is read by a large number of Bengalies of both sexes and almost of all ages all over India. Teenagers, young boys, adolescents, grown-up young men, and the elderly read this book. However, the court was not convinced that the book could be called obscene after reading it. Kissing, descriptions of the female characters bodies and figures in the book, and suggestions of sex activities may not have the effect of depraving, debasing, or enticing readers of any age to lasciviousness, and the novel may not be judged obscene on these grounds.[16]

[16] *Ibid* , at Para 35.

Bobby Art International & Ors.* v. *Ompal Singh Hoon[17] case is popularly known as "Bandit Queen" which dealt with the question of obscenity. The court considered that in the context of film called Bandit Queen pointed out that the so called objectionable scenes in the film have to be considered in the context of the message.

Hon'ble Supreme Court concluded regarding objectionable scenes within movie considering within context belonging to entire movie along with context which movie, was going to transfer to community. The court held that "the Tribunal had viewed the film in true perspective and had, in compliance with the requirements of the guidelines, granted to the film an 'A' certificate subject to the conditions it stated. The Court observed that the High Court ought not to have entertained the respondent's writ petition impugning the grant of the certificate based as it was principally upon the slurs allegedly cast by the film on the Gujjar community". Researcher finds that the theme of the film infact, condemns rape, the degradation of women, and violence against women by showing their effect on a village child, transforming her into a cruel dacoit obsessed with wreaking vengeance on a society that has caused her so much psychological and physical harm, are not taken into account in the judgment under appeal, and that scenes of nudity and rape, as well as the use of expletives to the extent permitted by the Tribunal, were designed to generate revulsion towards the criminals and empathy for the victim, but not to arouse prurient or lustful notions.

The issue of obscenity was again raised, when a film directed by Deepa Mehta was 'Fire' in 1998 which depicted lesbianism and focused on the cultural emergency of society. It was argued that it has tendency to destroy very fabric of our pluralistic society. Therefore, the movie was banned for the protection of mother, daughters, wives, sisters and society at large because it corrupts public morality, as the film was full of obscenity and nudity with lesbianism. But later on through the transformative constitutionalism Hon'ble Supreme court decriminalize the same sex relationship in the case of ***Navtej Singh Johar* v. *Union of india***[18] on constitutional morality because every individual rights matters.

[17] 1996 (4) SSC 1.
[18] AIR 2018 SCC 4321.

Therefore, in the name of art, literature and artistic culture no one can create anything which has even tendency to corrupt public morality and decency. Same principle is applicable for the Information Technology related obscene and pornographic materials or cyber pornography.

6.2.2.Obscenity and Pornography after Enactment of The Information and Technology Act, 2000

People are becoming more power-oriented as a result of the advancement of information technology, and they are losing sight of their responsibilities to uphold moral norms and decency in society. With the advancement of the information technology, people change their behavior of expression and used the social media platform to express themselves; which provide a medium for mushrooming the cybercrime against women. There has been a large number of pornographic and obscene materials available in cyberspace. The cyberspace is used by the every age group in the society. The Indian Court interpreted the law and punished the accused according to the tradition law as well as under special law i.e., The Information Technology Act, 2000.

After enactment of the Information Technology Act, 2000 in July 29, 2001, a PIL in ***Jayesh S. Thakkar* v. *State of Maharashtra***[19] was filled before Court wherein the petitioners wrote a suo-moto writ petition for complaining regarding pornographic material available at websites on the internet to the Chief Justice of Bombay High Court. On the basis of this petition, the Division Bench of the Bombay High Court passed an order to appoint a committee for suggesting and recommending preventive measures for protecting from pornographic and obscene material on the internet. The committee its reports on 30th January, 2002, wherein several recommendations have been given by Bombay High Court's Special Committee through the public opinions on internet relating to Protecting Minors from Unsuitable Internet Material. Reference can be taken from ***T. T. Antony* v. *State of Kerala***[20] case, in which it was held by the court that "*an object need not be visible to the naked one to be an obscene object".*

[19] *Available at*: http://www.cyberlaw.org/cybercrimes. (last visited on 3rd December, 2021).
[20] (2001) 6 SCC181.

The question was again answered by the Hon'ble Court in ***Ajay Goswami* v. *Union of India*** [21] case wherein the petitioner submitted that the grievance of freedom of speech and expression enjoyed by the newspaper industry is not keeping balance with the protection of children from harmful and disturbing material. In this case further, prayer made to command the authorities to strike a reasonable balance between the fundamental right of freedom of speech and expression enjoyed by the press and the duties of the Government, being signatory of the United Nations Convention on the Rights of Child, 1989 and Universal Declaration of Human Rights, 1948 to protect the vulnerable minor from abuse, exploitation and harmful effects of such expression.

The further prayer was that the authorities concerned should provide for classification or introduction of a regulatory system for facilitating climate of reciprocal tolerance which should include an acceptance of other people's rights to express and receive certain ideas and actions; and accepting that other people have the right not to be exposed against their will to one's expression of ideas and actions. The first question that the court posed "Is the material in newspaper really harmful for the minors". In that context, the court observed that:

"*The moral value should not be allowed to be sacrificed in the guise of social change or cultural assimilation. The court then posed whether the minors have got any independent right enforceable under Article 32 of the Constitution*."

During discussion, the court referred to earlier authorities pronounced by Supreme Court, referred to Section 13 (2) of the Press Council Act 1978, Section 292 of the Indian Penal Code and Section 4 and 6 of the Indecent Representation of Women (Prohibition) Act, 1986 and thereafter proceeded to deal with test of obscenity and in that context observed as follows:

"In judging as to whether a particular work is obscene, regard must be had to contemporary mores and national standards. While the Supreme Court in India held Lady Chatterley's Lover to be obscene, in England the jury acquitted the publishers finding that the publication did not fall foul of the obscenity test. This was heralded as a turning point in the fight for literary freedom in UK. Perhaps "community mores and standards" played a part in the Indian Supreme Court taking a different view from the

[21] AIR 2007 SC 493.

English jury. The test has become somewhat outdated in the context of the internet age which has broken down traditional barriers and made publications from across the globe available with the click of a mouse."

Further, Court observed that:

"*The term obscenity is most often used in a legal context to describe expressions (words, images, actions) that offend the prevalent sexual morality. On the other hand, the Constitution of India guarantees the right to freedom of speech and expression to every citizen. This right will encompass an individual's take on any issue. However, this right is not absolute, if such speech and expression is immensely gross and will badly violate the standards of morality of a society. Therefore, any expression is subject to reasonable restriction. Freedom of expression has contributed much to the development and well-being of our free society*."

In ***Sharat Babu Bigumati* v. *Government (NCT of Delhi),***[22][23] Supreme Court held that,

"*If legislative intendment is discernible that a latter enactment shall prevail, the same is to be interpreted in according with the said intention. We have already referred to the scheme of the Information Technology Act, 2000 and how obscenity pertaining to electronic record falls under the scheme of the Act. We have also referred to Sections 79 and 81 of the Information Technology Act, 2000 Act. Once the special provisions having the overriding effect do cover a criminal act and the offender, he gets out of the net of the Indian Penal Code,1860 and in this case, Section 292. It is apt to note here that electronic forms of transmission is covered by the IT Act, which is a special law. It is settled position in law that a special law shall prevail over the general and prior laws. When the Act in various provisions deals with obscenity in electronic form, it covers the offence under Section 292 Indian Penal Code*."

In the significant case of ***The State of Tamil Nadu* v. *Dr. L. Prakash***[24] the judiciary convicted the accused under Section 67 of Information Technology Act, 2000.

[22] (2017) 2 SCC18.

[23] The core issue that has emerged in this case was whether the Company could have been made liable for prosecution without being impleaded as an accused and whether the Directors could have been prosecuted for offences punishable under the aforesaid provisions without the Company is being arrayed as an accused.

[24] Writ Petition No. 7313 of 2002 decided on 15th March, 2002

The Fast Track Court sentenced him with life imprisonment and other 3 accused with 7 years rigorous imprisonment. Court also imposed fine of 1.27 lakh for posting prurient matter in electronic form under information Technology Act, conspiracy and intimidation under Indian Penal Code.[25]

6.3. Freedom of Speech and Expression in The Era of Technology

The right to freedom of speech and expression is not unqualified and subjected to certain restriction. Art. 19 of the Constitution of India, has guarantees the freedom of speech and expression, also provides reasonable restrictions on various grounds, including the grounds of decency and morality. This means that free speech has to be balanced against the contemporary community standards of morality and decency when it comes to penalising obscene acts or content.

Various judgments of Supreme Court have referred to the importance of freedom of speech and expression both from the point of view of the liberty of the individual and from the point of view of our democratic form of government.

In the early case, the Court stated that freedom of speech lay at the foundation of all democratic organizations.[26] A Constitution Bench said that freedom of speech and expression of opinion is of paramount importance under a democratic constitution which envisages changes in the composition of legislatures and governments and must be preserved.[27] In a separate concurring judgment Beg, J. observed, that the freedom of speech and of the press is the Ark of the Covenant of Democracy because public criticism is essential to the working of its institutions.[28] In ***S. Khushboo* v. *Kanniamal & Anr***.,[29] case Court stated, in paragraph 45 that the importance of freedom of speech and expression though not absolute was necessary as we need to tolerate unpopular views. This right requires the free flow of opinions and ideas essential to sustain the collective

[25] In this case, on December 2001, Chennai Police arrested the accused an orthopedic surgeon along with his 3 staffs. The co-accused Ganesh, assisted for making pornographic images of his clients forcefully and putting up those images of women patients on internet. Further, he is also circulated in abroad in CD's.
[26] *Romesh Thappar* v. *State of Madras*, (1950) S.C.R. 594.
[27] *Sakal Papers (P) Ltd. & Ors.* v. *Union of India*, (1962) 3 S.C.R. 842.
[28] *Bennett Coleman & Co. & Ors.* v. *Union of India & Ors.*, (1973) 2 S.C.R. 757.
[29] (2010) 5 SCC 600.

life of the citizenry. While an informed citizenry is a pre-condition for meaningful governance, the culture of open dialogue is generally of great societal importance.

In ***Shreya Singhal* v. *Union of India*** [30] a writ petitions was filed under Art. 32 of the Constitution of India raised very important and far-reaching questions relatable primarily to the fundamental right of free speech and expression guaranteed by Art. 19(1) (a) of the Constitution of India. The issue before court was the constitutionality of Section 66 of the Information Technology Act of 2000. Originally, this section was not in the Act as enacted, but it was come into force by virtue of an Amendment Act of 2009 with effect from 27th October, 2009. The arguments were raised by several counsels for the petitioners deal with the unconstitutionality of this section.

The Additional Solicitor General of India arguing for applying a 'relax standard of reasonableness of restriction', pointed out the following distinctive characteristics of internet:

(i) Internet is without boundaries and has a global reach; it has a greater audience and the harassment, abuse etc. can be viewed by people sitting in different geographical locations.

(ii) Literate as well as illiterate people can access internet and the information spread through it since only one click is sufficient to download an objectionable content including text or audio-visual content; similarly, perpetrators need not spend huge amount of money to upload or post any abusive, inflammatory, damaging content. A simple portable smart device like a mobile phone or a laptop or a tablet can be used for this by the perpetrator sitting in any location using any anonymous identity. As such, internet is the better medium when compared to print or television medium to spread rumours and affecting trillions of people within shortest period without any check.

(iii) Pre-censorship is not possible for internet since each individual uploading or posting a content may become publisher, producer, printer, director and broadcaster.

(iv) Internet has the potentiality to morph images, change voices etc. by way of advanced technology which may create serious social disorder;

[30] *Shreya Singhal* v. *Union of India,* AIR 2015 SC 1523.

(v) Internet provides wider opportunity to invade privacy of individuals and violate basic right to life, liberty and dignity as has been guaranteed under Art. 21.

(vi) On the internet unlike other mediums like newspaper, television etc., it is possible to remain anonymous and sexually harass, outrage the modesty of others or using filthy language especially to create social disorder;

(vii) Internet helps the perpetrator to carry on his/her attacks anonymously. Anonymous nature of the perpetrator can be revealed only after thorough investigation, which must be carried out by the criminal justice machinery with the cooperation of the websites concerned in many cases.

(viii) Using free speech and expression on the internet or the pattern of using the internet itself depends upon individualistic approach. There is a huge lacuna regarding check and balance and ethical norms in this regard.[31]

These observations are crucial when discussing the reasons as why should be considered about crimes against women and girls on the internet. The courts in their various recent judgment have held that right to speech and expression is a crucial right to every citizen irrespective of gender & sex.

But the Hon'ble Supreme Court had struck down Section 66-A of the Information Technology Act, 2000, on the ground that same is being violative of Art. 19 (1)(A) of the Constitution of India.

6.4. Judicial Approach Towards Protection of Right to Privacy in Cyber Space

As its constitutional obligations to protect the rights of the citizens and people judiciary has played a very significant role in India. The Supreme Court of India is protector of the fundamental right therefore, the right to privacy protected in physical world should also be protected in cyber space.

Right to privacy was no expressly enshrined in any Article in the Constitution of India. This right, come into arena of Constitution through liberal judicial interpretation. Journey start from the judgment of Supreme Court in ***M.P. Sharma* v. *Satish Chandra*** [32]

[31] *ibid* at 29-31.
[32] AIR1954 SC 300.

and ***Kharak Singh* v. *State of U.P***[33] in which legal position regarding the existence of the fundamental right to privacy is doubtful. But, this doubt is finally settled by the judiciary in the case of ***K.S. Puttaswamy (Retired) and Another* v. *Union of India and other*** [34] declared that right to privacy as "fundamental right".

Apex Court in the case ***M.P Singh* v. *Satish Chandra***,[35] Stated that,

"*A power of search and seizure is in any system of jurisprudence an overriding power of the State for the protection of social security and that power is necessarily regulated by law. When the Constitution makers have thought fit not to subject such regulation to constitutional limitations by recognition of a fundamental right to privacy, analogous to the American Fourth Amendment, we have no justification to import it, into a totally different fundamental right, by some process of strained construction.*"[36]

The Court further observed, in ***Kharak Singh* v. *State of Uttar Pradesh***[37]

"*…...Nor do we consider that Art. 21 has any relevance in the context as was sought to be suggested by learned counsel for the petitioner. As already pointed out, the right of privacy is not a guaranteed right under our Constitution and therefore the attempt to ascertain the movement of an individual which is merely a manner in which privacy is invaded is not an infringement of a fundamental right guaranteed by Part III.*"[38]

Further, it was submitted that such impermissible difference of opinion commenced with the judgment of Supreme Court in ***Gobind* v. *State of Madhya Pradesh***,[39] which formed the basis for the subsequent decision of this Court wherein the "right to privacy" has asserted or at least referred to. The most important of such cases are ***R. Rajagopal* v. *State of Tamil Nadu***,[40] and ***People's Union for Civil Liberties (PUCL)* v. *Union of India***[41] the above judgments referred to were rendered by smaller Benches of two or three Judges.

[33] AIR 1963 SC 1295.
[34] AIR 2016 SC 4161.
[35] *M.P Singh* v. *Satish Chandra*, AIR1954 SC 300.
[36] *Ibid.*
[37] *Kharak Singh* v. *State of Uttar Pradesh*, AIR 1963 SC 1295.
[38] *Ibid.*
[39] AIR 1975 SC 1378.
[40] AIR 1995 SC 264.
[41] (1997) 1 SCC 301.

Therefore, learned Attorney General and *Shri Venugopal* has submitted that for settle the legal position, the matters is required to be heard by a larger Bench Of this Apex Court as these matters throw up for debate important questions:

(i) Whether there is any "right to privacy" guaranteed under our Constitution.

(ii) If such a right exists, what is the source and what are the contours of such a right as there is no express provision in the Constitution adumbrating the right to privacy.

In light of the mandate provided in Art. 145(3) of the Constitution of India, it was suggested to the Hon'able Supreme Court that these matters should be considered and determined by larger bench of at least five judges. On behalf of the petitioners Shri Gopal Subramanium and Shri Shyam Divan, learned senior counsel very vehemently opposed the suggestion that the batch of matters is required to be heard by a larger bench. First argument was that, the conclusions recorded by this Court in ***R. Rajagopal*** and ***PUCL*** are legally tenable for the reason that the observations made in ***M.P. Sharma*** regarding the absence of right to privacy under our Constitution are not part of ratio decidendi of that case and, therefore, do not bind the subsequent smaller Benches. Secondly, Coming to the case of ***Kharak Singh***, in which majority did hold that the right of a person not to be disturbed at his residence by the State and its officers is recognised that it is to be a part of a fundamental right guaranteed under Art. 21 which is nothing but an aspect of privacy. The observation in para 20 of the majority judgment at best can be construed only to mean that there is no fundamental of privacy against the State's authority to keep surveillance. Even such a conclusion cannot be good law any more in view of the express declaration made by a seven-Judge bench decision of this Court in ***Maneka Gandhi* v. *Union of India***[42], thirdly, they further argued that both ***M. P. Sharma*** and ***Kharak Singh*** came to be decided on an interpretation of the Constitution based on the principles expounded in ***A.K. Gopalan* v. *State of Madras.***[43] Such principles propounded by ***A.K. Gopalan*** themselves came to be declared wrong by a larger Bench of this Court in ***Rustom Cavasjee Cooper* v. *Union of India.***[44] Therefore, there is no need for the instant batch of matters to be heard by a larger Bench.

[42] (1978) I SCC 2483.
[43] AIR 1950 SC 27.
[44] (1970) SCC 248.

The Court observed that, It is true that ***Gobind*** did not make a clear declaration that there is a right to privacy flowing from any of the fundamental rights guaranteed under Part III of the Constitution of India, but observed that "Therefore, even assuming that the right to personal liberty, the right to move freely throughout the territory of India and the freedom of speech create an independent right of privacy as an emanation from them which one can characterise as a fundamental right, we do not think that the right is absolute". Therefore, the Court proceeded to decide the case on such basis.

Elaborate submissions are made at the bar by the learned counsel for the petitioners to demonstrate that world over in all the countries where Anglo-Saxon jurisprudence is followed, 'privacy' is recognised as an important aspect of the liberty of human beings. It is further submitted that it is too late in the day for the Union of India to argue that the Constitution of India does not recognise privacy as an aspect of the liberty under Art. 21 of the Constitution of India. At least to the extent that the right of a person to be secure in his house and not to be disturbed unreasonably by the State or its officers is expressly recognised and protected in ***Kharak Singh*** case though the majority did not describe that aspect of the liberty as a right of privacy, it is nothing but the right of privacy.

The Court opined that the cases on hand raise far reaching questions of importance involving interpretation of the Constitution. What is at stake is the amplitude of the fundamental rights including that precious and inalienable right under Art. 21. If the observations made, in ***M.P Sharma*** and ***Kharak Singh*** are to be read literally and accepted as the law of this country, the fundamental rights guaranteed under the Constitution of India and more particularly right to liberty under Art. 21 would be denuded of vigour and vitality. At the same time, the opinion that the institutional integrity and judicial discipline require that pronouncement made by larger Benches of this Court cannot be ignored by the smaller Benches without appropriately explaining the reasons for not following the pronouncements made by such larger Benches. With due respect to all the learned Judges who rendered the subsequent judgments, where right to privacy is asserted or referred to their Lordships concern for the liberty of human beings, the humble opinion of the judges of the Court that there appears to be certain amount of apparent unresolved contradiction in the law declared by Court.

Therefore, the Court opinion is that to give a quietus to the kind of controversy raised in this batch of cases once for all, it is better that the ratio decidendi of ***M. P. Sharma*** and ***Kharak Singh*** is scrutinised and the jurisprudential correctness of the subsequent decisions of this Court where the right to privacy is either asserted or referred be examined and authoritatively decided by a Bench of appropriate strength.

Thereafter, on 24th August 2017, a Constitutional Bench of nine judges of the Supreme Court of India in ***K S Puttaswami (Retd.)*** upheld that Privacy is a Fundamental Right, which is entrenched in Article 21 of the constitution to protect the Right to Life & Liberty.

In this case the Court also discussed about the informational privacy under para 170 as produce as follows:

"*We are in an information age. With the growth and development of technology, more information is now easily available. The information explosion has manifold advantages but also some disadvantages. The access to information, which an individual may not want to give, needs the protection of privacy. The right to privacy is claimed qua the State and non-State actors. Recognition and enforcement of claims qua non-state actors may require legislative intervention by the State*."

From this case the researcher analyses that as right to privacy declared as protected fundamental right. The violation of this right should be criminalised and legislature should enact proper legislation on it. There is opinion given by the judges in this case which is as follows:

Justice *S. A. Bobde* view on dignity and privacy and he opinioned that "It is difficult to see how dignity whose constitutional significance is acknowledged both by the Preamble and by this Court in its exposition of Art. 21, among other rights can be assured to the individual without privacy. Both dignity and privacy are intimately intertwined and are natural conditions for the birth and death of individuals, and for many significant events in life between these events. Necessarily, then, the right of privacy is an integral part of both 'life' and 'personal liberty' Under Art. 21, and is intended to enable the rights bearer to develop her potential to the fullest extent made possible only in consonance with the constitutional values expressed in the Preamble as well as across Part III."

Hon'ble Supreme Court of India declared privacy a fundamental right Justice *Kaul,* in his separate but concurring judgment on the nine-judge Bench observed that:

"*…The impact of the digital age results in information on the internet being permanent. Humans forget, but the Internet does not forget and does not let humans forget. Any endeavour to remove information from the internet does not result in its absolute obliteration. The footprints remain. It is thus, said that in the digital world preservation is the norm and forgetting a struggle and the right of an individual to exercise control over his personal data and to be able to control his/her own life would also encompass his right to control his existence on the internet. Such a right would not be an absolute right. The existence of such a right does not imply that a criminal can obliterate his past, but that there are variant degrees of mistakes, small and big, and it cannot be said that a person should be profiled to the nth extent for all and sundry to know…."*

Allahabad High Court in Re, Banners placed on Road Side[45] in the City of Lucknow applied the proportionality principle as laid down in ***Puttaswamy*** judgment and observed that:

"…learned Advocate General failed to satisfy us as to why the personal data of few persons have been placed on banners though in the State of Uttar Pradesh there are lakhs of accused persons who are facing serious allegations pertaining to commission of crimes whose personal details have not been subjected to publicity. As a matter of fact, the placement of personal data of selected persons reflects colorable exercise of powers by the Executive."

In entirety, having no doubt that the action of the State which is subject matter of the public interest litigation is nothing but an unwarranted interference in privacy of people. The same hence, is in violation of Art. 21 of the Constitution of India.

6.5. "Right to be Forgotten" in Cyberspace

Technology has also brought into focus the fact that digital life is permanent, i.e., nothing ever is erased. This has brought forward the concern of individuals, who would like to forget some events of their past, but the search engines are not letting them forget their past as they are linked omnipresent, which the robotic spiders index find as soon as

[45] *In-Re Banners Placed on Road Side* v.*State of U.P*, on 9th March , 2020

key word search is being made. This has led to the question that how far such indexing and its publication on search engine is permissible? Is it violative of personnel freedom and privacy? That the concept of the right to be forgotten has recently elicited a strong response from numerous jurisdictions around the world. Many common law countries such as the United States, the United Kingdom, Canada, Australia, and India have substantially embraced and made the "Right to be Forgotten" available to its citizens.

Google Spain SL, Google Inc.* v. *Agencia Espanola de Proteccio'n de Datos, Mario Costeja Gonzalez Case[46]In this case, one Mario Costeja González disputed that the Google search results for his name continued to show results leading to an auction notice of his reposed home. González said that the fact that Google continued to show these in its search results related to him was a breach of his privacy, given that the matter was resolved, the center notes. In the European Union, the right to be forgotten empowers individuals to ask organisations to delete their personal data. It is provided by the European Union's General Data Protection Regulation (GDPR), a law passed by the 28-member bloc in 2018.

According to the EU GDPR's website, the right to be forgotten appears in Recitals 65 and 66 and in Art. 17 of the regulation, which states, "The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay".

In 2019, the European Union's highest court ruled that the 'right to be forgotten' under European law would not apply beyond the borders of European Union member states. This means this ruling is not applicable against the non-European member. The European Court of Justice (ECJ) ruled in favour of the search engine giant Google, which was contesting a French regulatory authority's order to have web addresses removed from its global database.

[46] Google Spain SL, and Google Inc. v. Agencia Espanola de Proteccio'n de Datos(AEPD), Mario Costeja Gonzalez (C-131/12,Grand Chamber, decided on 13 May, 2014), *available at:* https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0131&from=EN; Explained: The 'Right to be Forgotten' in India, and Ashutosh Kaushik's case in Delhi HC Indian Express, 30 July 202.

This ruling was considered an important victory for Google, and laid down that the online privacy law cannot be used to regulate the internet in countries such as India, which are outside the European Union.

Indian case on this issue was the ***Ashutosh Kaushik* v. *Union of India & Ors*** [47] before Delhi HC, in which Ashutosh Kaushik who won reality shows Bigg Boss in 2008 and MTV Roadies 5.0 has approached the Delhi High Court with a plea saying that his videos, photographs and articles etc. are published at various platforms to be removed from the internet citing his "Right to be Forgotten". In the plea, Kaushik also argued that the "Right to be Forgotten" goes in sync with the "Right to Privacy", which is an integral part of Art. 21 of the Constitution, which concerns the right to life.[48] The case is still pending in the court of law.

Another case was the ***Subhranshu Rout @ Gugul* v. *State of Odisha*** [49] in which the Odisha High Court headed by Justice *S. K. Panigrahi* held that:

"*The information in the public domain is like toothpaste, once it is out of the tube one can't get it back in and once the information is in the public domain it will never go away.,"* thereby confirming the verdicts of several other High Courts by holding that an individual has a right to expect intermediaries (such as Facebook, Twitter) to remove sensitive information relating to them online.[50] This comes three years after the landmark

---

[47] *Available at:* https://www.livelaw.in/news-updates/roadies-bigg-boss-winner-ashutosh-kaushik-moves-delhi-high-court-for-right-to-be-forgotten-177933. (last visited on 21st January, 2022).

[48] Explained: The 'Right to be Forgotten' in India, and Ashutosh Kaushik's case in Delhi HC Indian Express, 30th July, 2021.

[49] *Available at*: https://indiankanoon.org/doc/6266786/. (last visited on 21st January, 2022).

[50] The case is related to the posting of intimate images on social media and complainant need for a right to be forgotten. In this case, the accused (petitioner) had created a fake Facebook ID in the name of the prosecutrix and uploaded objectionable photos using the fake ID. The police had failed to take any step on the complaint of the prosecutrix. The pictures were captured with the consent of the victim when they were in a relationship. The present case deals with intimate pictures of a woman being published online. The victim claimed she had been in love with the accused for around a year before the incident occurred. Both parties were from the same village and had also been classmates. Having learned one day that the victim was alone at home, the accused visited and raped her. While doing so, he also captured pictures and a video of the incident without her consent.
After the act, he threatened to kill her and then upload her pictures onto the internet if she told anyone. The woman informed her parents of the incident and in response, the accused created a fake Facebook profile in her name and uploaded their intimate pictures. The police were apathetic to the victim's plight, and it was only after some time that they convinced the accused to delete the fake profile and its content.

judgment of ***K. S. Puttuswamy***, which upheld that the Right to Privacy is a fundamental right under Art. 21 of the Indian Constitution."

If the right to be forgotten is not recognized in matters like the present one, any accused will surreptitiously outrage the modesty of the woman and misuse the same in the cyber space unhindered. Undoubtedly, such an act will be contrary to the larger interest of the protection of the woman against exploitation and blackmailing, as has happened in the present case. The sloganeering of betibachao and women safety concerns will be trampled.

The argument before the court was that there was no crime as the accused and the victim were rational adults in a consensual relationship. It is also claimed that he was going to marry her unconditionally. In addition, the counsel also argued that as he was a Diploma holder seeking employment, the detention was going to hinder his prospects.

The counsel for the State contended that in addition to the intercourse being non-consensual, the accused also photographed the incident and threatened the woman with it. It was clear from her statement under Section 161 Cr.P.C that she had been subjected to blackmail and threats after the rape.

While there is a serious penal deterrent for such heinous crimes, there exist no mechanisms to ensure that the victim's right to be forgotten is fulfilled. In the present case, it was only after the police visited the accused did he take down the content. There was no mechanism whereby the victim could directly approach the intermediary (Facebook) and ask them to take it down.

It's also argued that though the statute prescribes penal action for the accused for such crimes, the rights of the victim, especially, her right to privacy which is intricately linked to her right to get deleted in so far as those objectionable photos have been left unresolved. There is a widespread and seemingly consensual convergence towards an adoption and enshrinement of the right to get deleted or forgotten but hardly any effort has been undertaken in India till recently, towards adoption of such a right, despite such an issue has inexorably posed in the technology dominated world. Presently, there is no statute in India which provides for the right to be forgotten/getting the photos erased from the server of the social media platforms permanently.

The Court of law recognized the intrinsic significance of one's right to be forgotten in the larger context of our fundamental Right to Privacy which enshrined in Art. 21 through judicial interpretation. It is their right to enforce the right to be forgotten as a right in rem. Capturing the images and videos with consent of the woman cannot justify the misuse of such content once the relation between the victim and accused gets strained as it happened in the present case.

Reasoning on these lines, the Odisha HC dismissed the bail application. The Right to Privacy is finally being given due consideration in our country, but the lack of an actual legislative framework to implement it still poses a major hurdle. It is hoped that the proposed draft Personal Data Protection Bill, 2018 shall provide much needed clarity and security when it comes to our right to be forgotten.

6.6. Cases Related to Pornography

Considering case ***Ambikesh Mahapatra & another* v. *State of West Bengal & others***,[51] in which Mahapatra stood-up to oppose random arrest order, to develop and publish cartoon focusing Chief Minister Mamata Banerjee through summon petitions. Upon contrary, taken case belonging Shaheen Dhada, that was being handcuffed in order to Facebook post upon Mumbai strike upon juncture death belonging to Shiv Sena supremo Bal Saheb Thackeray. She had for withdrawing her own post, was handcuffed along with harassed online also offline. She cannot fight against insulting at primary. She does not personally file summons petition, although she receive large support extracting public following leading TV channels, newspapers initiated promoting clippings displaying her after being arrested. Her face being hidden through her dupatta.

This kind was single quick reaction through her for saving her own self extracting being focused through possible sexual perpetrators, trolls that might deliberately destroying her character upon net, also for saving herself extracted basic media attention. Her action for trying for hiding her face was neither exception. Millions belonging another Indian women fear exact by time they got for seeing criminal posts either hear regarding their own suffering. Her arrest was censured as single severe abuse belonging law through none another as comparing Justice Markendeya Katju, who has been single

[51] *Ambikesh Mahapatra & Ors.* v. *State of West Bengal & Ors*, WP No. 33241(w) of 2013.

judge into Supreme Court untimely. She was lucky enough for making quickly getting single limelight in order to unlawful done towards her through criminal justice machinery.

However, not various women were as lucky as her into receiving help extracting their families also public on big. It is since of these reasons which Cybercrimes targeting women comprising criminal expression, speech become research worthy[52].

In ***Rishi Narula* v. *The State Nct of Delhi and Others***, [53] Supreme Court of India seen which standards of modern society into India were rapidly altering. The adolescents, adults facilitating to them numerous pieces of literature, stories, novels, classics comprising romance, love, sex content. Within cinema and art field also teens displayed conditions that at least century area ago will considering disparaging towards public morality, however persisting regard towards modified situations, were much accepted considering allowed into any how moulding for debasing either debauching mind.

In ***Aveek Sarkar* v. *State of West Bengal***[54] case Court referred to English, U.S. and Canadian judgments and moved away from the *Hicklin test* and applied the contemporary community standards test. In this case a German magazine by name "STERN" having worldwide circulation published an article with a picture of Boris Becker, a world renowned Tennis player, posing nude with his dark-skinned fiancée by name Barbara Feltus, a film actress, which was photographed by none other than her

[52] Debarati Halder and K. Jaishankar, *Cybercrime against Women in India* 133 (Sage Publication, New Delhi, 2017).

[53] 2016 Indlaw DEL 234.

[54] *Aveek Sarkar* v. *State of West Bengal*, (2014) 4 SCC 257. The case is related to "Sports World", a widely circulated magazine published in India reproduced the article and the photograph as cover story in its Issue 15 dated 5th May, 1993 with the caption "Posing nude dropping out of tournaments, battling Racism in Germany. Boris Becker explains his recent approach to life" Boris Becker Unmasked. Anandabazar Patrika, a newspaper having wide circulation in Kolkata, also published in the second page of the newspaper the above-mentioned photograph as well as the article on 6th May,1993, as appeared in the Sports World.

A practicing lawyer at Alipore Judge's Court, Kolkata, claimed to be a regular reader of Sports World as well as Anandabazar Patrika filed a complaint under Section 292 of the Indian Penal Code against the Appellants herein, the Editor and the Publisher and Printer of the newspaper as well as against the Editor of the Sports World, former Captain of Indian Cricket Team, late Mansoor Ali Khan of Pataudi, before the Sub-Divisional Magistrate at Alipore. Complaint stated that as an experienced Advocate and an elderly person, he could vouchsafe that the nude photograph appeared in the Anandabazar Patrika, as well as in the Sports World, would corrupt young minds, both children and youth of this country, and is against the cultural and moral values of our society. The complainant stated that unless such types of obscene photographs are censured and banned and accused persons are punished, the dignity and honour of our womanhood would be in jeopardy

father. The article states that, in an interview, both Boris Becker and Barbaba Feltus spoke freely about their engagement, their lives and future plans and the message they wanted to convey to the people at large, for posing to such a photograph. Article picture Boris Becker as a strident protester of the pernicious practice of "Apartheid". Further, it was stated that the purpose of the photograph was also to signify that love champions over hatred.

Supreme court examined whether the photograph of Boris Becker with his fiancée Barbara Fultus, a dark-skinned lady standing close to each other bare bodied but covering the breast of his fiancée with his hands can be stated to be objectionable in the sense it violates Section 292 Indian Penal Code.

Hon'ble Apex Court applied the community Standard test, and held that they were not prepared to say such a photograph was suggestive of deprave minds and designed to excite sexual passion in persons who was likely to look at them and see them, which would depend upon the particular posture and background in which the woman was depicted or shown. Breast of Barbara Fultus has been fully covered with the arm of Boris Becker, a photograph, of course, semi-nude, but taken by none other than the father of Barbara. Further, the photograph, in our view, had no tendency to deprave or corrupt the minds of people in whose hands the magazine Sports World or Anandabazar Patrika would fall.

When viewed in that angle, we are not prepared to say that the picture or the article which was reproduced by Sports World and the Anandabazar Patrika be said to be objectionable so as to initiate proceedings under Section 292 Indian Penal Code or under Section 4 of the Indecent Representation of Women (Prohibition) Act, 1986.We have found that no offence has been committed under Section 292 Indian Penal Code and then the question whether it falls in the first part of Section 79 Indian Penal Code has become academic. We are sorry to note that the learned Magistrate, without proper application of mind or appreciation of background in which the photograph has been shown, proposed to initiate prosecution proceedings against the Appellants. Learned Magistrate should have exercised his wisdom on the basis of judicial precedents in the event of which he would not have ordered the Appellants to face the trial. The High Court, in our view, should have exercised powers under Section 482 Cr.P.C. to secure the ends of justice.

Another case in 2004, which is considered to be the first case of conviction under section 67 of Information Technology Act, 2000 which made this section historical important is ***State of Tamil Nadu* v. *Suhas Katti***.[55] In this case, some defamatory, obscene and annoying messages were posted about the victim on a yahoo messaging group which resulted in annoying phone calls to her. She filed the FIR and the accused was found guilty under the investigation and was convicted under section 469, 509 of Indian Penal Code and section 67 of Information Technology Act. This case was another significant step of the Indian law enforcement agencies where within 7 months of filing FIR the conviction was achieved successfully. This was the first case of the Cybercrime Cell Chennai. For the speedy disposal of this case great assistance had been given by Naavi.com and the Cyber Evidence Archival Center. In this case Indian police had shown their ability as investigator by producing satisfactory evidence against the accused. The defendant was charged for annoying, obscene and defamatory message in the yahoo message group relating to a divorcee woman. The accused at first opened a false account in the name of the victim and then sent her information through electronic-mails. It annoyed the victim because she had to face harrowing calls.

In February 2004 the victim filed the complaint about the fact before police. The Chennai police traced the accused at Mumbai and arrested him immediate after few days. It was found out by the police that the accused was victim's family friend, known to her and wanted to marry her. But she did not marry the accused. However, she married another one who ended it in divorce later on. After her divorce the accused again became very crazy about her and started contacting her but she refused for the same. Then the accused started harassing her through internet. The charge sheet was filed against the accused under Sections 469, 509 of the Indian Penal Code, 1860 and Section 67 of the Information Technology Act, 2000 on 24th March, 2004 before the Hon'ble Additional CJM, Egmore. There were 34 documents and other material objects and 18 witnesses were produced before the court by Chennai police with great help the Cyber Evidence Archival Center of which 12 witnesses were examined on the side of prosecution. On the basis of the expert witness the court held that the crime is conclusively proved. On 5th November 2004 the court delivered the judgment that the accused was found guilty of

[55] *State of Tamil Nadu* v. *Suhas katti*, Case No. 4680 of 2004.

offences under Sections. 469, 509 of the Indian Penal Code and Section 67 of the Information Technology Act. Therefore, the accused was convicted and was sentenced for the offence to undergo rigorous imprisonment for two years under s. 469 of the Indian Penal Code i.e., forgery for the purpose of harming reputation and to pay Rs. 500 fine; for the offence under s. 509 of the Indian Penal Code i.e., word, gesture or act intended to insult the modesty of a woman with one year simple imprisonment and Rs. 500 fine; and for the offence under s. 67 of the Information Technology Act 2000 with two years rigorous imprisonment and Rs. 4,000 fine. The court held that all those sentences must run concurrently. The accused was lodged at Central Prison at Chennai and he paid the above mentioned fine.

In 2005, in India the first case which was registered under section 65 of the Information Technology Act is ***Syed Asifuddin* v. *State of Andhra Pradesh and Anr.***[56] In this case the court held that the cell phones fulfilled the definition of 'computer' under the Information Technology Act and the unique Electronic Serial Numbers which are programmed into each handset like ESN, SID (System Identification Code), MIN (Mobile Identification Number) are the 'Computer Source Code' within the definition under the Information Technology Act which is required to be kept and maintained by the law.

In ***Avinash Bajaj* v. *State (NCT) of Delhi*** [57] case obscene material was put up for sale by one person on the website baazee.com and sold/transmission of these clip to several people resided in different parts of country which took place in a very short time period. The issue was raised whether it was a publication under section 67 before the amendment or website had indirectly published the material. The court held that the ultimate transmission of the obscene material wouldn't have been possible without the initial facilitation by the website and therefore, the website had liable under the section.

6.7. Judicial Approach Towards Teen Revenge Porn In India

In India, the very first reported case of teen revenge in the cyber space came out in 2001. When a 16 year Delhi school boy created a porn website and posted porn images

[56] (2005) Cri.LJ 4314.
[57] (2008) 150 DLT 769: (2008) 105 DRJ 721.

of girls of his own class and of the teachers with lewd remarks, publishing in detail about their sexual preferences. The reports suggest that he did this as revenge to these girls who used to taunt him. The boy was arrested under Section 67 of the erstwhile Information Technology Act, 2000 for charges of obscenity in the cyber space and later on juvenile court released him on bail. The extreme punishment came when he was rusticated from the school. This case drew huge attention of the media, the public the law researchers and also the police as this was the first ever case of teen revenge through cyberspace in India.[58]

Airforce Bal Bharti School Case 2001 was filed before the Juvenile Court, Delhi on the charge of cyber pornography in 2001. Some jurists say this is the first Indian cyber pornographic case which was charge sheeted in the juvenile court. The brief facts in issue were that a student of the Airforce Bal Bharti School, Lodhi Road, New Delhi was arrested by the Delhi Police in the year 2001 April. The alleged accused was then a class XII student who created a pornographic website as revenge of being teased by classmates and teachers. He listed in that website the names of his 12 school mates' girls and teachers in sexually explicit manner. He was then suspended by the School Authorities though the juvenile court allowed his bail prayer. However, he was charged under Section 67 of the Information Technology Act, 2000, and Sections 292, 293, 294 of the Indian Penal Code and the Indecent Representation of Women Act. The most significant steps were taken by the law enforcement agencies in India in this case.

Delhi MMS Case, 2004 in this case the teachers and parents of Delhi Public School at R.K. Puram's were worried about the reputation and moral application of the mobile phone pornographic activities in society by a student aged about 17 years. The school boy was a member of Delhi Under-17 cricket team. He played against Himachal Pradesh at Una and also against Haryana (Gurgaon). He had withdrawn himself before the match against Jammu and Kashmir in December 12-14 after the incident of MMS-video oral sex clip incident and he then went to Nepal for certain period in December 2004. Most of the recipients of that MMS clip were of the age of 18 or below. A Delhi Public School boy allegedly filmed his girlfriend in an act of oral sex with him on his cell phone camera which is to be called as MMS clip or Multimedia Messaging Service clip.

[58] Debarati Halder, *Cybercrime against Women in India* 133 (Sage Publication, New Delhi, 2017).

This video clip was then forwarded by him to his friends, and then his friends sent it to others. Gradually, within a minute it was available to almost all users and even it was available for small price to the roadside vendors.

The clip was copied to VCD (Video Compact Disk) for sale and distribution. One Indian Institute of Technology (IIT), Kharagpur student named Ravi Raj of 23 years age put that MMS clip of 2.37 minutes for auction on the Baazee.com which was India's top auction website and owned by e-Bay. The clip contained title "DPS Girl Having Fun" for sale on 24th November 2004. On 9th December 2004 at night the case was registered. On 11th December 2004, the Delhi Police Crime Branch reached Mumbai and found out that Alice Electronics of Kharagpur through Mr. Ravi Raj, IIT placed the video clip on Mumbai based auction website Bazzee.com. That student of IIT Kharagpur also sold the CD to 8 persons by that time. When notified the clip, Bazzee.com removed the same because they had their own guidelines against pornographic material. It was found out that the Alice Electronics was a fake company. VCD was posted on webpage for regular interaction of sellers and buyers and was removed after few days. However selling of such VCD in public is offence under Indian Penal Code and the Information Technology Act 2000.

The Delhi police arrested Delhi Public School student from the Indira Gandhi International Airport when he returned from Nepal on 19th December, Mr. Ravi Ray Singh 23, year's old student of the Indian Institute of Technology, Kharagpur in West Bengal and the portal's CEO, Mr. Avnish Bajaj in December 2004. Principal Magistrate Santosh Snehi Mann of the Juvenile court ordered not to disclose name of the school boy and the school on the basis of request from Mr. Puneet Mittla, Learned counsel for the school. He said that those school students are psychologically affected by media before annual examinations of school. The court informed the same fact to the Press Council of India. The Court held that the media is not 'sensitive', rather they are attempting to 'sensationalise' the matter and this is not the proper way to create awareness by media. Throughout the hearing the judge only could see the face of that boy. And directed that 17 years old boy must be placed under the custody of the Juvenile Welfare Officer for one day. However his father can accompany him while police may ask question to the boy in presence of Juvenile Welfare Officer.

However, the counsel for the boy contended that the charge against his client is totally false and it is very difficult to prove who was that particular person because there was no visual of his face in the clip and he prayed for bail under Section 12 of the Juvenile Justice Act, 2000 though he was arrested under Sections 293, 294, 201 of the Indian Penal Code 1860 and Section 67 of the Information Technology Act, 2000. Section 201 of Indian Penal Code was invoked here because it was alleged that he destroyed mobile phone to destroy the evidence of MMS clip circulated by him. Court held that there was no likelihood of his being exposed to moral, physical or psychological danger if released.

In 2012, BBC journalist Gethin Chamberlin published a sensational news report about the circulation of videos of Andaman Jarawa women who were caught dancing at the instruction of the tourists, tour operators and the police. The videos became viral through social media, especially YouTube. Till today a search in the search engines with key words such as Andaman Jarawa dance, tribal dance, vulgar dance of Andaman and so on may pull up videos of Andaman Jarawa women, who were caught shaking their bodies (women captured in the video were in their tribal attire and were half naked) on their own tribal songs. The clippings are not longer than five to eight minutes. But the clippings are still floating on the internet with sexist taglines and many posters have their posts in these videos, which have obscene, offensive and vulgar words to degrade the morals of these women.

6.8. First Conviction on Revenge Porn Case in India

In a landmark case ***West Bengal* v. *Boxi*** (Decided by Judicial Magistrate, Tamluk) [59] on revenge pornography decided in March 2018, a 23-year old man from

[59] The fact of the case was that, accused, Animesh Boxi (alias Animesh Bokshi alias Animesh Bakshi) was in a relationship with the victim (her name was not disclosed to protect her identity under section 228 Indian Penal Code) for three years prior to the incident that occurred in July 2017. Over the course of the relationship, Boxi demanded intimate photos from the victim and allegedly "hacked into her phone" to get his hands on them. He then started blackmailing her, saying that he would upload the photos and videos online if she refused to spend time with or "go for outings with" him. A few days later, the victim's brother discovered the nude pictures and videos on a porn site (PornHub) with the video which gave the victim's name and also identified her father.
Boxi was charged under sections 354A (Sexual Harassment), 354C (Voyeurism), 354D (Stalking) and 509 (Criminal Intimidation) of the Indian Penal Code, 1860 and sections 66C (Identity theft), 66E

West Bengal was sentenced to serve five years of jail time as well as pay a fine of Rs 9,000 when a court in the East Midnapore district ruled in favour of his 20-year old girlfriend. The man was deemed to have shared a sexually explicit video of his then-girlfriend after the termination of their relationship, in an attempt to blackmail her into getting back with him. In this case, the accused was convicted under Sections 354A, 354C, 354 and 509 of the Indian Penal Code, as well as Sections 66E, 66C, 67 and 67A of the Information Technology Act. In other cases, victims have also invoked Section 499 of the Indian Penal Code that deals with criminal defamation.[60]

This case is of historic significance as it is the first conviction in a 'revenge porn' case in India and the harsh punishment sends out a strong message to perpetrators of revenge pornography.

The trial was conducted by the judge Gautam Nag and held that the accused person guilty of the charges. The main issue before the Court was whether the prosecution was able to prove beyond reasonable doubt that Boxi was guilty of non-consensually uploading intimate images and videos of the victim online. The prosecution relied upon electronic evidence and witness testimonies. The electronic evidence included, inter alia, Boxi's mobile number which was listed as the registration number of the PornHub account through which the video was uploaded; the IP address indicating that the SIM card through which the video was uploaded was registered in Boxi's name; and the email and porn website's user accounts in Boxi's name through which the video was uploaded. The defense took various points on the prosecution's procedural shortcomings such as delays in filing the list of articles and documents seized, charges being framed under incorrect provisions and the defective examination of witnesses, among others.

With regard to the charges of sexual harassment, voyeurism, stalking and criminal intimidation under Sections 354 and 509 of the Indian Penal Code , the Court said that Boxi had demanded sexual favours from the victim, captured images of her in

(Violation of privacy) and 67/67A (Transmitting obscene material online) of the Information Technology Act 2000.

[60] *Available at:* https://www.criminaldefenselawyer.com/resources/revenge-porn-laws-penalties.htm.(last visited on 15th September, 2021).

circumstances where she would not have expected to have been observed and stalked her thoroughly online. The Court rejected Boxi's defense that sexual harassment, voyeurism and stalking had not caused the victim any physical injury. It said that injury to the victim's reputation was sufficient because it fell within the ambit of 'injury' as laid down in Section 44 of the Indian Penal Code. The Court also found Boxi guilty of transmitting private images online contrary to Section 66E, Section 67 and 67A of the Information Technology Act as well as identity theft under Section 66C as he had hacked into the victim's phone and taken the pictures secretly. Accordingly, the Court found Boxi guilty of all the offences as charged and sentenced him to five years imprisonment along with a fine of Rs. 9,000. It also ordered that the victim be paid compensation under the state's Victim Compensation Scheme.[61]

In 2018, a Suo Motu writ petition was taken up by the Supreme Court based on a letter by *NGO Prajwala* which had enclosed two clippings of rape being circulated on the internet, the Supreme Court of India ordered the Government to frame guidelines for taking action for removal of child pornography, rape and gang rape videos from the internet.[62] In the absence of sufficient and specific legal framework, the scope of having guidelines on regulating revenge porn still subsists. Perhaps a fresh petition for the same can be filed which may clear the confusion created by multiplicity of laws applicable on the subject.

The recent case before the court ***Shivaprasad Sajjan*** **v. R/At No. 560/B on 17 February, 2022**.[63] In this case the accused and complainant were classmates in BMS college of Engineering. They had close friendship with each other and taking undue advantage of same, accused made a proposal of marriage to the complainant. When she refused to the proposal made by the accused, being agitated and annoyed the accused went to Sri. Venkateshwara Net Zone, Cyber Cafe, situated at No.417, near bus stop, 6th block, Rajajinagar and created different E-mail ID's namely Sharkyvicious@hotmail.com, Sharkysid@hotmail.com, Sapienthr@hotmail.com,

[61] *Available at:* https://globalfreedomofexpression.columbia.edu/cases/state-of-west-bengal-v-boxi/ (last visited on 2nd August, 2021).
[62] In Re: Prajwala Letter Dated 18.2.2015 Videos of Sexual Violence and Recommendations, Suo Moto Writ Petition (Crl) No (S). 3/2015, order dated 11.12.2018
[63] *Available at:* https://indiankanoon.org/doc/156468380/ (last visited on 18th Febuary, 2022).

Shivensajjan@hotmail.com, Shivbono@hotmail.com, aliceinachain@hotmail.com and sapientundone@hotmail.com, and transmitted several lascivious, obscene, pictures and messages to the email IDs of the complainant namely averma@sapient.com and also to her company's colleagues email IDs nchoudhury@sapient.com, sdhavan@sapient.com, between May 2008 to August 2008. After perusal of those obscene, lascivious and pornographic pictures and messages, the complainant has filed a complaint against the accused before the jurisdictional police. Consequently the cybercrime police have registered a case against accused pursuant to the said complaint in Crime No. 31/2008 for the offence punishable under Section 67 of Information Technology Act 2000. The Investigating officer, after having conducted the detail investigation, has filed chargesheet against the accused for the aforesaid offence.

Conclusion

The cases of revenge porn and blackmailing cases are mushrooming in India. But due to lack of awareness the case proximity, the victim did not report such cybercrime. Therefore, the cases were not reached to the courts. The concept of 'revenge porn' has been prevailing since 2010. On 06th February, 2020 at an IAMAI event, Shri Ravishankar Prasad, Hon'ble Minister of Law in Justice; Communications; and Electronics and Information Technology, Government of India expressed his concern over this issue by saying "Revenge porn is creeping in India...girlfriend and boyfriend split up... then what happens, platform is being abused..." Several Nation States have expressly criminalised revenge porn in their territories, however in India there exists no such legislation. Prosecutors and Judicial Officer are not able to present case in court in proper manner in a large number of cybercrime cases due to their lack of understanding.

CHAPTER-VII

ANALYSIS OF DATA COLLECTED FROM LUCKNOW CITY RELATED SOCIAL AWARENESS AND IMPACT OF CYBERCRIME AGAINST WOMEN

CHAPTER-VII

ANALYSIS OF DATA COLLECTED FROM LUCKNOW CITY RELATED SOCIAL AWARENESS AND IMPACT OF CYBERCRIME AGAINST WOMEN

This chapter presents and analyses the primary data collected from the 542 participants of various colleges and universities with different academic back ground and it also includes the analysis of the data collected from 22 Police stations in the city of Lucknow, Uttar Pradesh.

In this chapter the researcher attempts to provide an idea about the state of awareness about cybercrimes especially targeting women, considering the technological requirement and rapid development in this field. The Researcher also tried to bring out the similarity of status and perceptions between the general crime against women and cybercrimes, through data analysis and in the form of chart and tabular representation.

Nearly two-thirds of the smart phone users store personal and intimate information on their mobile device including intimate images of themselves. University/ College/ School going teens are more vulnerable to fall prey to become the victim of revenge porn and blackmailing. Individuals aged 18-24 are slightly more at risk than teenagers for online digital abuse.

The researcher has tried to evaluate and examine the level of awareness among the users of technology about the definition of cybercrime in general and revenge porn and blackmailing in particular. The Researcher has also tried to evaluate the awareness, approach and understanding of the police administration about the definition of cybercrimes and the procedural part for the administration of justice in the cases of cybercrime. The researcher also has objectives to analyse the initiatives or status of technological, infrastructural development and training and capacity building of the growing administrative system to be well equipped for the vastly growing incidents of cybercrimes against women.

To draw the inference, researcher has collected the data through questionnaires method, whereas the original plan of personal interviews with administrative agencies

was hampered by the COVID-19 situation due to the imposition of lockdown and minimal movement in the last 2 years. Due to the COVID-19 situation and closure of the educational institutions' researcher has to reframe the questionnaire in google forms format and send it to the students by email & WhatsApp groups of several institutions.

The finding shows the development under cybercrimes and the inception phase of the administrative measures taken by the police or other stakeholders. Similarly, the perception of the technology users for blaming and shaming of the victim and holding the victim responsible for the consent of creation of such content or using internet and social media is also being evaluated in this chapter. The basis of analysis, results and inferences was drawn. The survey was conducted by means of a structured questionnaire circulated among more than 600 students of different universities and colleges and 28 police stations of Lucknow. About 542 students of different academic background and of various profiles, filled the questionnaire whereas 22 Station House Officers (SHOs) of various police stations gave their inputs about the questions in the questionnaire. Through textual discussion, tabular and graphic representation the data obtained is critically analyzed and reported.

The responses of 542 students and 22 police stations have been considered for the study with the rate of 87.00 percent. Such a response ratio has been regarded as encouraging the earlier research and studies on the sector and the aspects of the topic assumed for research activity.

A random sample method was used for the selection of respondents and interaction with those who are available in the police stations during the survey. A detailed questionnaire survey was conducted during the research period across the selected area. The question was designed with the intention to know the awareness in the technology users in society, especially youngsters, students and educated class, about the definition of cybercrime in general and revenge porn and blackmailing in particular. It was quite difficult for the researcher to convince the respondents to give their honest inputs in the questionnaire as several respondents chose not to answer the questionnaire because of the fact that the questionnaire included some personal questions about the respondent as well as their near and dear ones. The questionnaire contained queries about the incidences of crime if any happened with the respondents or his/her near and dear

one's. Respondents were hesitant to answer such questions specially the question that about the identity of the offender and whether the offender was a member of the family, boyfriend/ partner or near relative. Respondents did not want to talk to about these questions and what action was taken against them. The question of perceptions that whether the women using internet and social media and uploading their information was also a tough one as most of them are considering themselves as the culprit by using the channel and having a perception of blaming and shaming the women sharing information on internet and social networking sites.

The interview and filling the questionnaire with the police department personnels was also challenging as due to the COVID-19 situation and in general also the hesitation and poor entertaining quality was quite apparent. Police department was quite hesitant to inform the researcher about the capacity, usage of technology and investigative methods and number of cases in which final report and charge sheet has been filed or not. Due to this there were some discrepancies found in the data where the police department refrained from giving thoughtful answers about the number of cases registered and the charge sheet submitted in the registered cases. In most of the interviews the files and records were not referred while answering the questions accurately. General tendency to escape the responsibility of giving answers and laying it off on others was also seen on most of the interviews where several persons in a single police station have been asked for the answers or time.

After collection of data the responses received from the responded are presented in the form of table, pie chart, figure analyses and interpreted by using descriptive method of analysis. This chapter provides a brief discussion of often results. Based on the finding of the present research the conclusions and suggestions were drawn, which are summarized in the next chapter. For proper evaluation of data questionnaire has been divided into three parts i.e., Part A, Part B and Part C. Part A tells about the demographic profile of the respondent. Part B consists of 23 questions with space for the suggestions from the respondents. Part C consists of 12 questions with space for suggestions from the administrative agencies.

Section A:

Demographic Description of the Respondents:

It is very important to reveal the sampling profile of the respondent under this study; hence this section briefly describes the demographic profile of the respondents. The sample size of 542 respondents especially studying in various Universities/Colleges/ Schools as observed for demographic information. In the demographic profile gender, age, marital status has been considered. Furthermore, frequency distribution is calculated for all the cases and summarized. These frequency distributions contained data about the mentioned demographic information.

1. Gender Profile of the Respondents

Gender status, generally, cover two categories viz. male and female. After generating the profile of the respondents on gender basis, contrary to expectation it has been observed that female respondents are dominant as out of 542 respondents, there are 176 (32.5%) male and 366 (67.5%) female (Table7.1)

Table No. 7.1 Gender Profile of the Respondents

Gender Profile of the Respondents					
S. No.	**Gender**	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	**Female**	366	67.5	67.5	67.5
2	**Male**	176	32.5	32.5	100.0
	Total	542	100.0	100.0	

Source: Primary Data

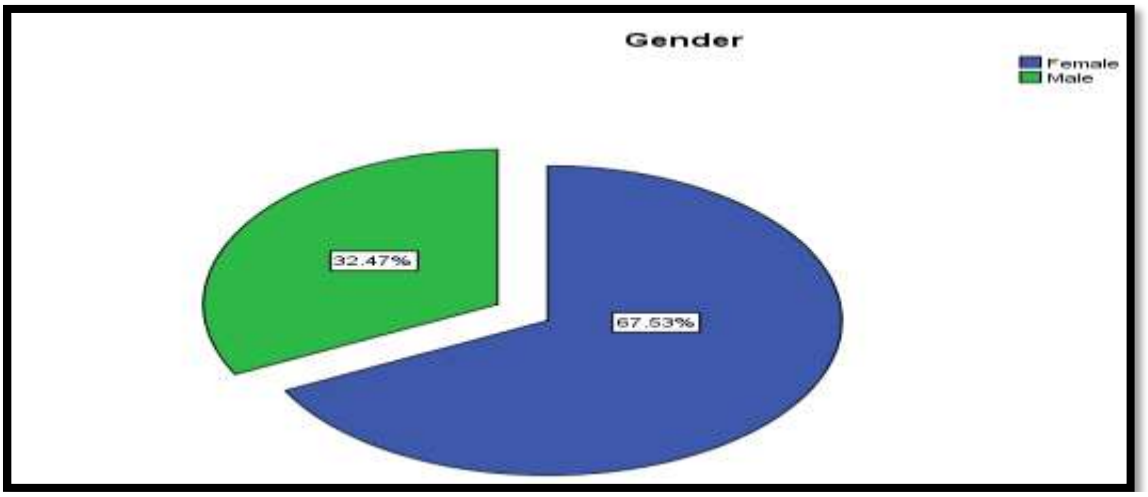


Figure No.7.1

The pie chart Figure No. 7.1 vividly shows the percentage of gender group of respondents participated in the survey. It also expresses the correctional bias of the researcher for the valid number of participants on different ground after re-verification of the responses and where there they understand the questions well enough while answering the same. As the respondents under this study are randomly selected and the classification is not structured however the researcher focus on fulfilling the gender gap so that most of the respondents can be female. This is one of the reasons that the number of respondents are female.

2. Age Profile of the Respondent

Table No. 7.2 Age of Respondent

Age of Respondent					
S. No.	**Age (in years)**	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	**17 and under**	48	8.9	8.9	8.9
2	**18-24**	400	73.8	73.8	82.7
3	**25-34**	80	14.8	14.8	97.4
4	**35 and above**	14	2.6	2.6	100.0
	Total	542	100.0	100.0	

Source: Primary Data

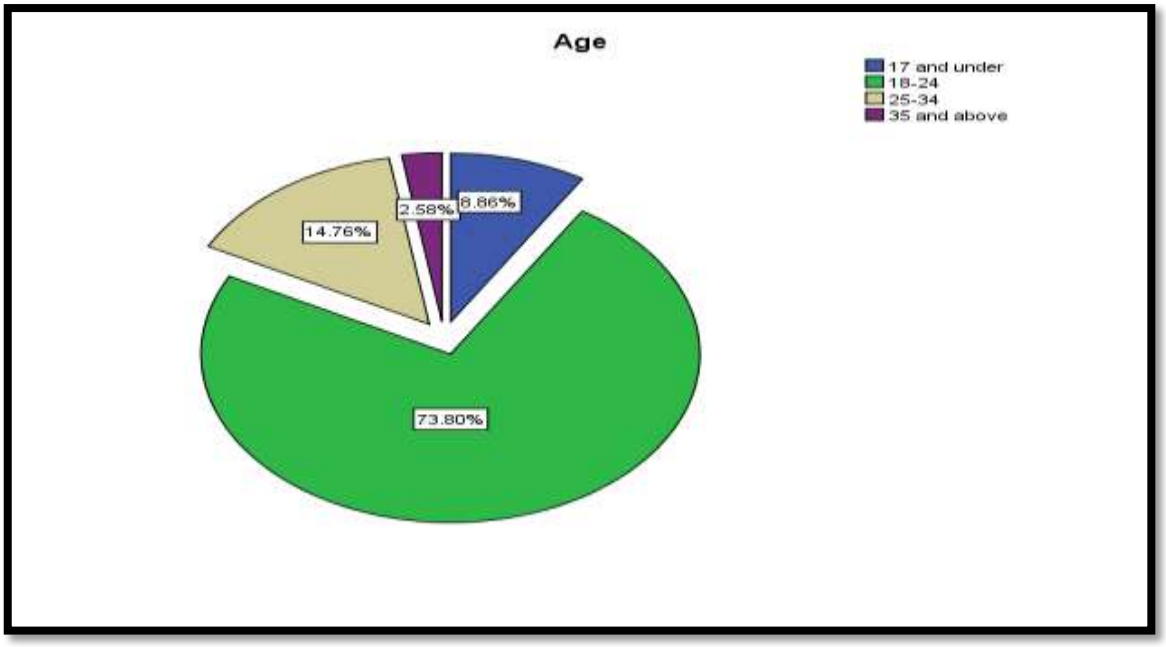


Figure No. 7.2

The pie chart in figure 7.2 vividly shows the percentage of age group of respondents in my study.

Respondents have been divided into four groups on the basis of their age viz. 17 and under, 18-24 years, 25-34 years, and 35 years & above. In the present study, out of total 542 respondents, 48 (8.9%) respondents are in the age group of 17 and under, whereas age group between 18-24 years covers the maximum respondent i.e., 400 (82.7 %) respondents. The age group between 25-34 years cover 80 (14.8%) respondent and rest of the respondent fall into the age bracket of 35 and above covering minimum respondents i.e., 14 (2.6%) (Table 7.2). Most of the respondents under this study are considered as young as they are more techno savvy against their older counterparts especially in terms of use of mobile smart phone as a medium to disseminate the information.

3. Marital Status of the Respondent

Table No. 7.3 Marital Status

Marital Status				
Marital Status:	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
Married	37	6.8	6.8	6.8
Unmarried	505	93.2	93.2	100.0
Total	542	100.0	100.0	

Source: Primary Data

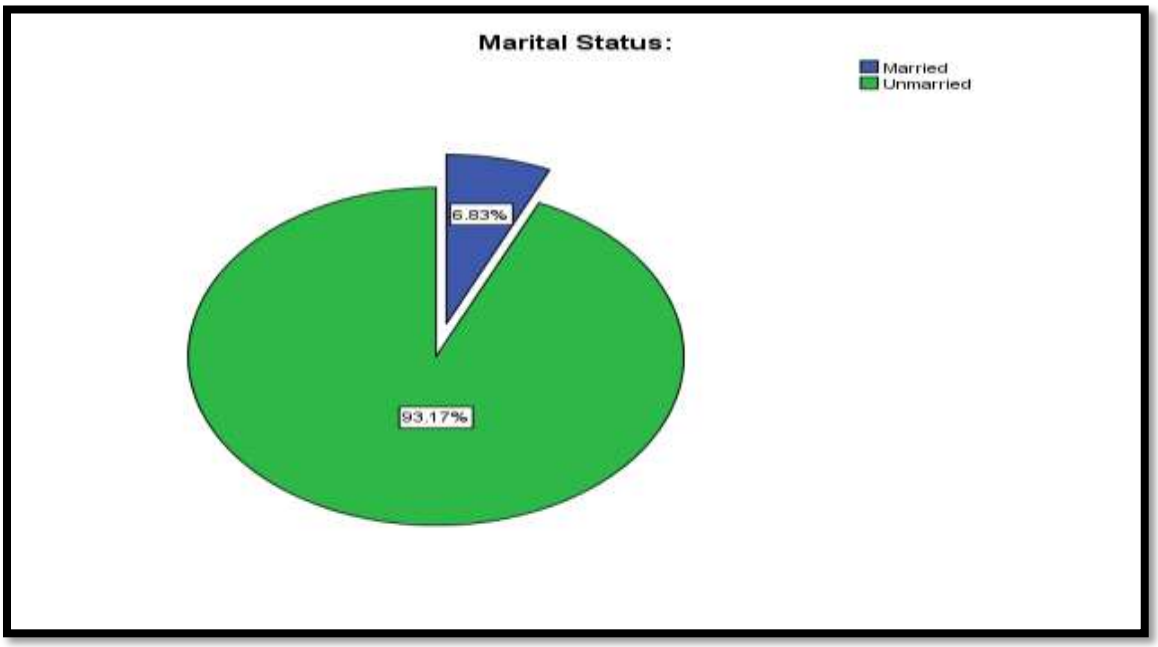


Figure No. 7.3

The Table No.7.3 and Figure No.7.3 shows the marital status of the respondents. In present study, out of 542 respondent, 505 (93.2%) are unmarried which shows the most of the respondent are unmarried and 37 (6.8%) are married respondent which form the minimum number of respondents. One of the reasons for the low percentage of the married respondents is that the study is focused around the universities where the available category is scarce.

4. Academic Profile of the Respondent

Table No. 7.4

Academic qualification of the Respondent Education					
S. No.	**Education**	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	**Doctorate**	33	6.1	6.1	6.1
2	**Intermediate**	58	10.7	10.7	16.8
3	**other**	2	.4	.4	17.2
4	**Post Graduate**	95	17.5	17.5	34.7
5	**Under Graduate**	354	65.3	65.3	100.0
	Total	542	100.0	100.0	

Source: Primary Data

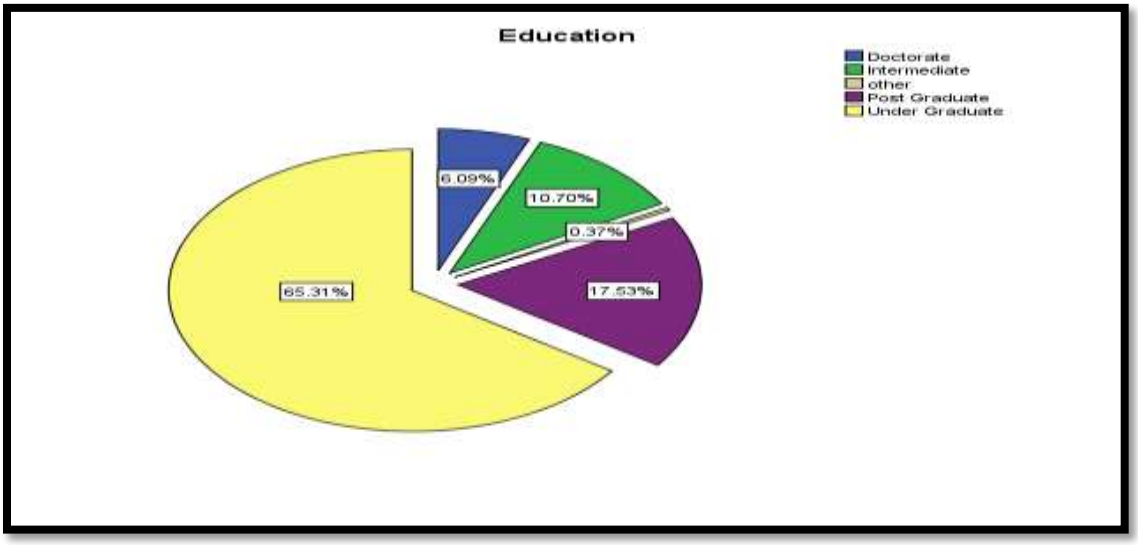


Figure No. 7.4

The academic qualification has been sub divided in to five groups these are "Intermediate", "Under Graduate", "Post Graduate", "Doctorate" and "Others". In the present study out of 542 respondents, 58 (10.7%) respondents are in "Intermediate".

The respondent who falls "Under Graduate" group are 354 (65.3%), "Post Graduate" group are 95 (17.5%), "Doctorate" group are 33 (6.1%) and respondents under

"Others" group are 2 (0.4%). The other are the students doing different courses other than the degree courses like Diploma and other technical courses. It has been observed that maximum number of respondents i.e., 65.3% belongs to the group "Under Graduate" whereas minimum number of respondents i.e., 0.4% belong to the group "Others" (Table No.7.4).

Section B:

Question 1: Are you aware about "Cybercrime"?

Table No. 7. 5

Are you aware about "Cybercrime"?					
S. No.	**Respondent Response**	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	**No**	6	1.1	1.1	1.1
2	**Not Sure**	14	2.6	2.6	3.7
3	**Yes**	522	96.3	96.3	100.0
	Total	542	100.0	100.0	

Source: Primary Data

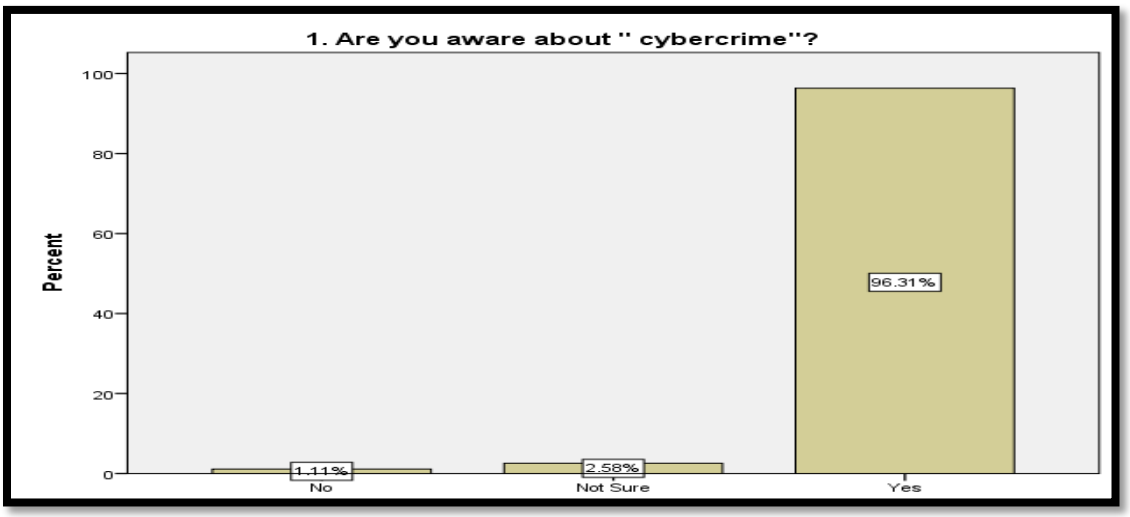


Figure No.7. 5

The above, Table No.7.5 and Figure No. 7.5, reveals the information about the awareness as to cybercrime and the acquaintance about the subject matter. The Table shows that out of 542 respondent, 522 (96.3%) respondents gave a positive response, 6 (01.1%) respondents answered in the negative, which forms a minimal number of respondents and 14 (2.58%) answered as not sure. As the majority of the respondents are of young age and students most of them are at least aware about the cybercrime and what constitutes the cybercrime.

Question 2: Do you know Right to privacy has been enshrined under Article 21 of the Constitution of India as Fundamental Right?

Table No. 7. 6

Do you know Right to privacy has been enshrined under Article 21 of the Constitution of India as Fundamental Right.					
S. No.	**Respondent Response**	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	**Yes**	442	81.5	81.5	81.5
2	**Not Sure**	40	7.4	7.4	88.9
3	**No**	60	11.1	11.1	100.0
	Total	542	100.0	100.0	

Source: Primary Data

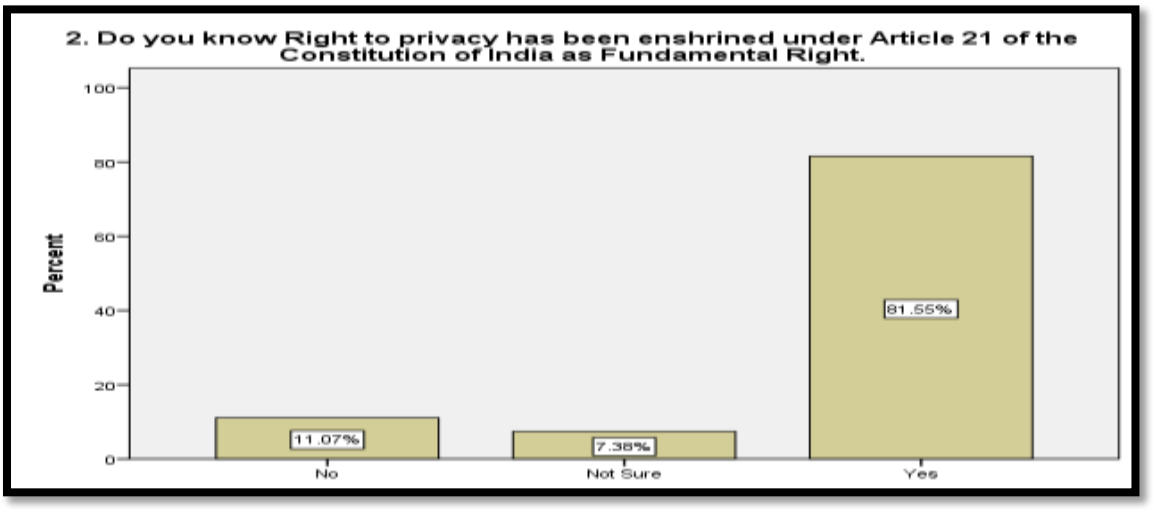


Figure No. 7. 6

The above Table No.7.6 and Figure No. 7.6, shows the information about the right to privacy. The above Table shows that out of 542 respondent, 442 (81.55%) respondents give responses in yes, 60 (11.1%)Respondents said no and only minimal number of respondents 40 (7.4%) said not sure. The study shows that most of the respondents are the well aware about the right to privacy, which is enshrined in our constitution. The total 542 respondents were given response to this question, out of which 522 respondents that they know the right to privacy has been enshrined under Art. 21 of the Constitution of India and 6 respondents were given the response in negative that they have not even known what is right to privacy. 14 respondents replied that they were not sure. The finding shows that there are satisfactory numbers of people know the right to privacy as a fundamental right. Which also determines the popularity of the subject and recent debates over the privacy in general public platforms.

Question 3:

The privacy in virtual world as well as in real life literally shrinking

Table No. 7.7

S. No	Respondent Response	Frequency	Percent	Valid Percent	Cumulative Percent
1	**Strongly Agree**	232	42.8	42.8	42.8
2	**Neutral**	46	8.5	8.5	51.3
3	**Disagree**	8	1.5	1.5	52.8
4	**Agree**	256	47.2	47.2	100.0
	Total	542	100.0	100.0	

Source: Primary Data

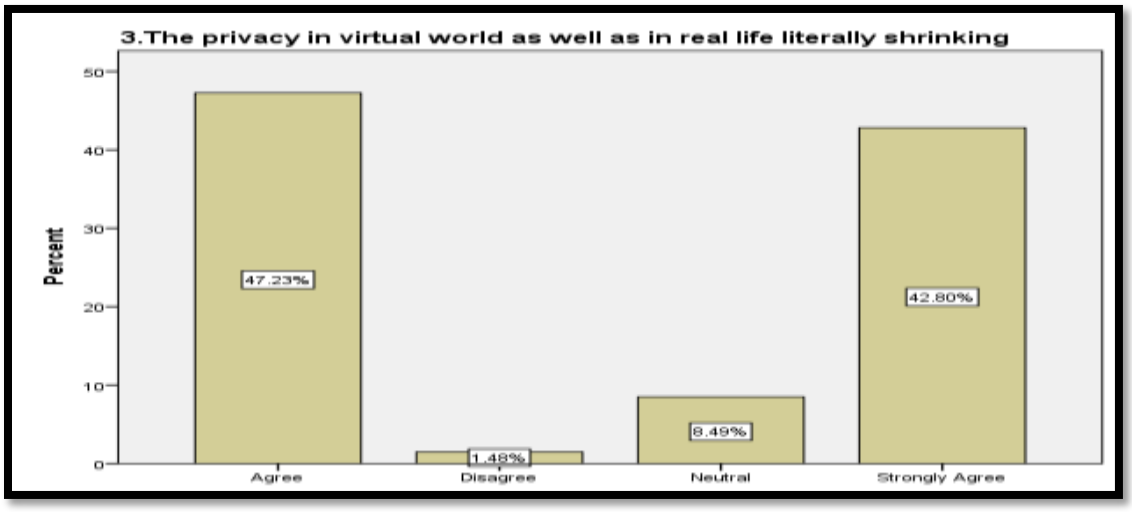


Figure No. 7.7

The above Table No. 7.7 and Figure 7.7 reveals the understanding about the right to privacy. The Table 7.7 shows that out of 542 respondent 232 (42.8%) respondents strongly agree to the statement, 256 (47.2%) agree, 8 (1.5%) respondents disagree and 46 (8.5%) respondents remained neutral and no respondent strongly disagrees. The result shows that most of the respondents understand the right to privacy; they agree that technology has affected our privacy therefore the privacy in physical as well as in virtual world is shrinking as above 90% respondents either agree or strongly agree with the premise.

Question 4: Women and children were more prone to obscene cybercrime

Table No. 7.8

Women and children were more prone to obscene cybercrime					
S. No.	**Respondent Response**	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	**Strongly Agree**	216	39.9	39.9	39.9
2	**Neutral**	46	8.5	8.5	48.3
3	**Disagree**	2	.4	.4	48.7
4	**Agree**	278	51.3	51.3	100.0
	Total	542	100.0	100.0	

Source: Primary Data

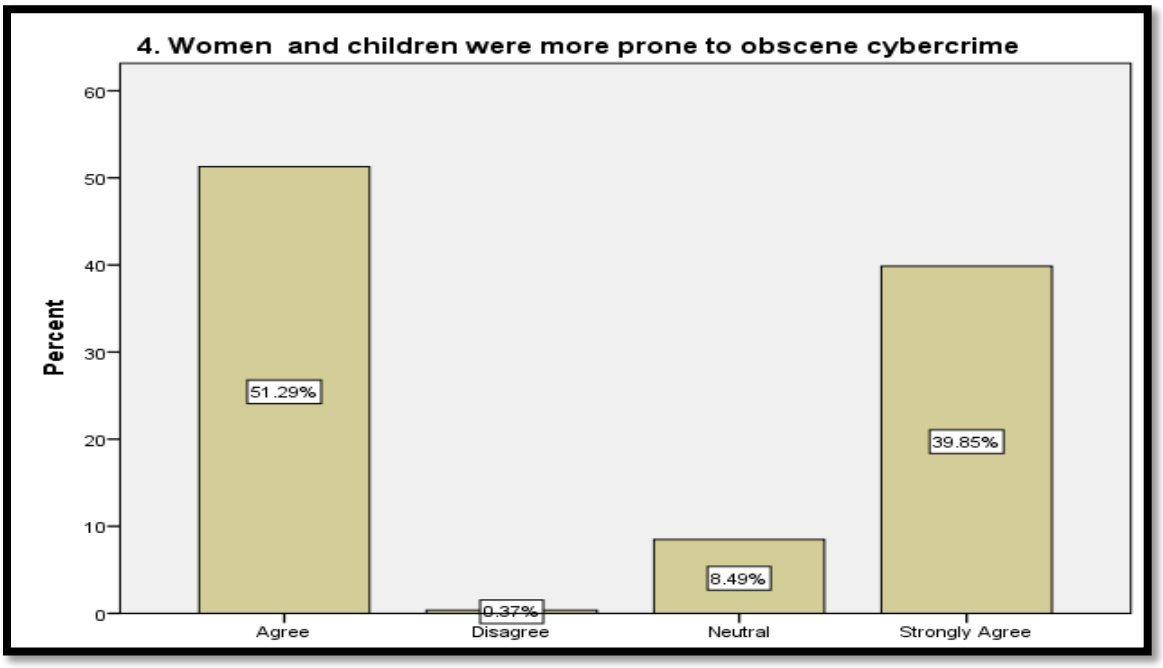


Figure No. 7.8

The above Table No. 7.8 and Figure No. 7.8 shows that out of 542 respondents 216 (39.9%) respondents strongly agree to the statement, 278 (51.29%) respondents agree, 2 (0.4%) respondents disagree and 46 (8.5%) respondents prefer to remain neutral, no respondent strongly disagrees. The percentage of response in favor of agree and strongly agree shows us that the general perception about the potential of the cyber space to victimize the children and women is more against the male and its adult counterpart. It also shows that the majority have a perception that the women and children are the subject matter of the cybercrime due to a preferable targeted audience in general scenes because the cyber space is providing a lot of content for their consumptions.

Question 5:

Women in India make most vulnerable target on the internet due to their gender and the consumability of image of Indian women as porno- materials.

Table No. 7.9

Women in India make most vulnerable target on the internet due to their gender and the consumability of image of Indian women as porno- materials.					
S. No.	**Respondent Response**	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	**Agree**	264	48.7	48.7	48.7
2	**Disagree**	22	4.1	4.1	52.8
3	**Neutral**	36	6.6	6.6	59.4
4	**Strongly Agree**	218	40.2	40.2	99.6
5	**Strongly Disagree**	2	.4	.4	100.0
	Total	542	100.0	100.0	

Source: Primary Data

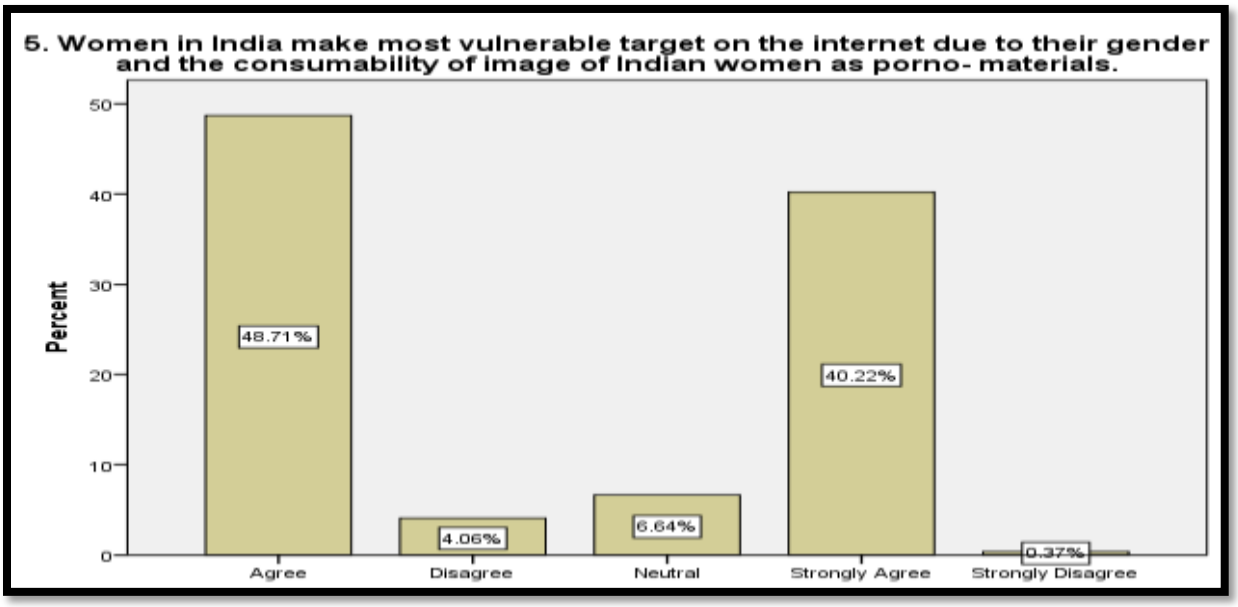


Figure No. 7. 9

The above Table No. 7.9 and Figure No. 7.9 shows that out of 542 respondents 216 (40.22%) respondents strongly agree to the statement, 278 (48.71%) respondents agree, 22 (4.06%) respondents disagree and 46 (6.64%) respondents remained neutral, no respondent strongly disagreed. The researcher draws result from the responses from more than 88% of respondents that the vulnerability factor comes the perception where the women are considered to be commoditized in the cyber space's and personal data or information like images can be used against their consent for the entertainment or for other sensual purposes. The usage of the women as the content for the cyber space is quite agreed upon and the commoditization of women in general is popular in the general space of internet users.

Question No. 6.

Social norms and orthodox values prevent the victim and their family member to report the cybercrime against women?

Table No. 7.10

Social norms and orthodox values prevent the victim and their family member to report the cybercrime against women.					
S. No	**Respondent Response**	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	**Agree**	202	37.3	37.3	37.3
2	**Disagree**	30	5.5	5.5	42.8
3	**Neutral**	38	7.0	7.0	49.8
4	**Strongly Agree**	268	49.4	49.4	99.3
5	**Strongly Disagree**	4	.7	.7	
	Total	542	100.0	100.0	100.0

Source: Primary Data

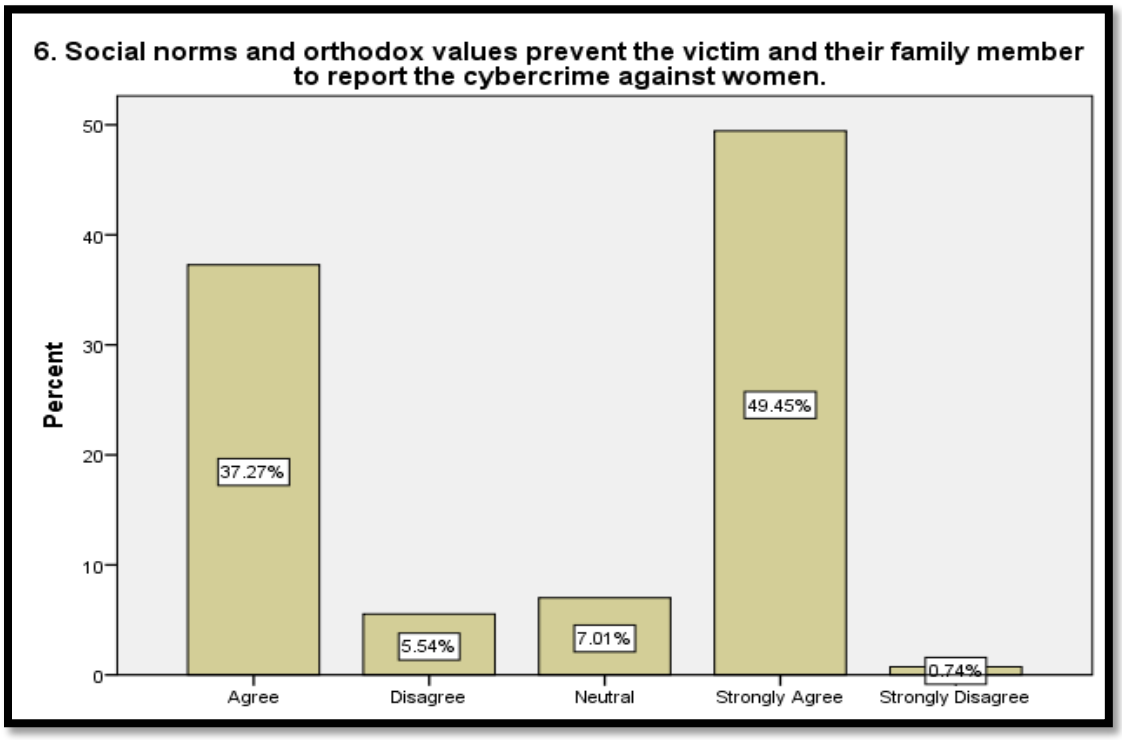


Figure No.7.10

The above Table No. 7.10 and Figure No. 7.10 shows that out of 542 respondent 268 (49.45%) respondents strongly agree to the statement, 202 (37.27%) respondents agree, 30 (5.54%) respondents disagree and 38 (7.0%) respondents prefer to be neutral, 4 (0.75%) respondents strongly disagree. This data validates the less or meager number of reporting of cybercrime and the reason for the same is the orthodox values like risk of blaming and shaming of the victim by the society, loss of sexual integrity and the Virtues of life there after the reporting of the case which will bring indignity to the family and relatives of the victim. Majority of the respondents agreed with the notion of social response against the reporting of the case.

Question No. 7: Whether you are familiar with term Revenge Porn and Blackmailing?

Table No. 7.11

Whether you are familiar with term Revenge Porn and Blackmailing					
S. No	**Respondent Response**	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	**No**	88	16.2	16.2	16.2
2	**Not Sure**	48	8.9	8.9	25.1
3	**Yes**	406	74.9	74.9	100.0
	Total	542	100.0	100.0	

Source: Primary Data

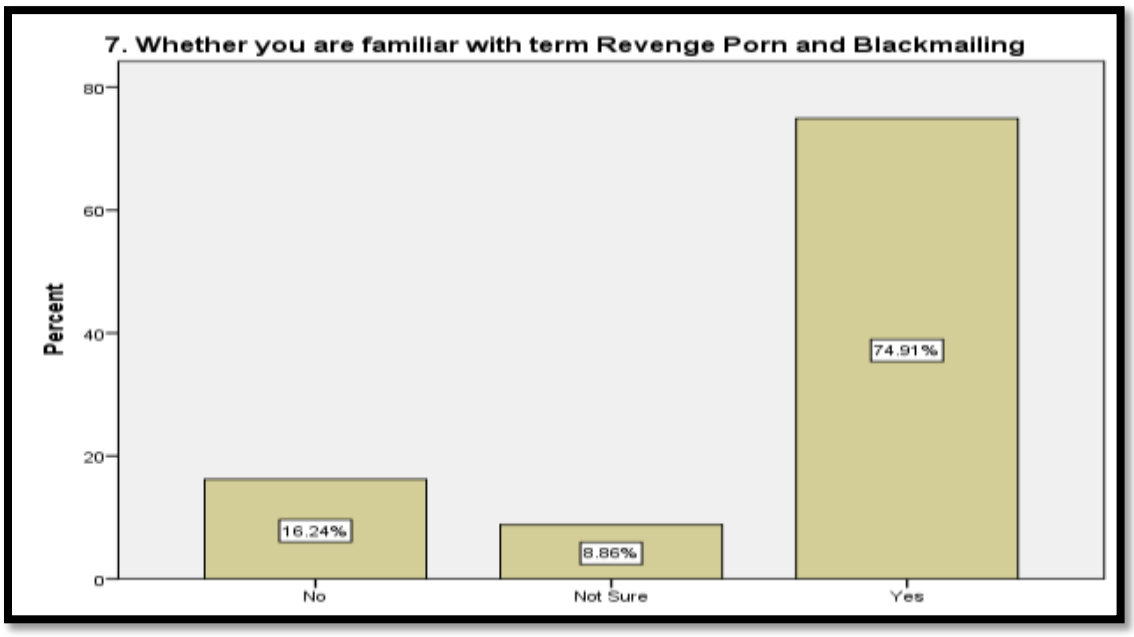


Figure No. 7.11

The above Table No. 7.11 and Figure No. 7.11, reveal that the respondent familiarity with the term revenge porn and blackmailing. The Table shows that out of 542 respondents, 406 (74.9%) respondents gave positive response that respondent in yes, 88 (16.2%) respondents said no, which form the minimal number of respondent and 48 (8.9%) are answered not sure. This question examines the familiarity of the

respondents towards revenge porn. This is further gauged by examining knowledge level and exposure to information about revenge porn. Nearly 75% respondent is familiar with the subject matter which is huge in terms of the newness of the subject.

Question No.8: If yes, I have learned about it from

Table No. 7.12

If yes, I have learnt about it from					
S. No.	**Respondent Response**	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	**Friends**	58	10.7	10.7	10.7
2	**Internet source**	232	42.8	42.8	53.5
3	**News channel/ Print media**	166	30.6	30.6	84.1
4	**Other channel(i.e., Conference/Seminar/ Special events)**	30	5.5	5.5	89.7
5	**University**	56	10.3	10.3	100.0
	Total	542	100.0	100.0	

Source: Primary Data

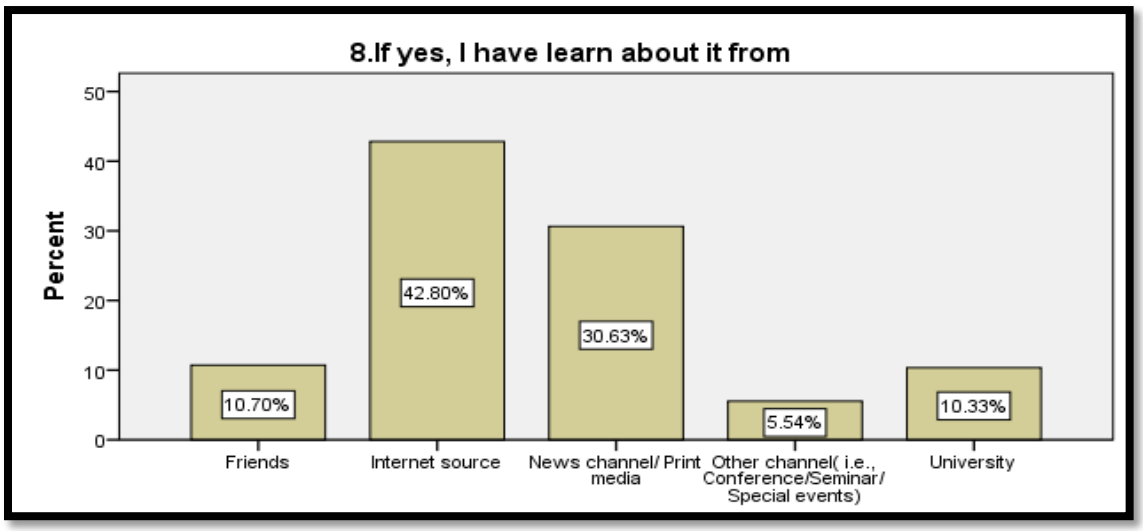


Figure No.7. 12

The above Table No. 7.12 and Figure No. 7.12 further explain the source of information of the respondent about the previous question of awareness about the subject of Revenge porn. 58 (10.7%) of respondents learned the subject matter from their friends. 232 (42.8%) respondents learnt the subject matter from the internet sources itself. 166 (30.63%) respondents learnt this subject from electronic and print media. 56 (10.33%) respondents learnt the subject matter in university and 30 (5.54%) respondents learnt the subject through special event, seminars or conferences. The researcher can draw form the mixed response that different platforms have the idea and conversation about the revenge porn whereas the internet is the most popular source among them all as 42% respondent got to know about the subject through internet sources however electronic and print media is the second at large source. Whereas the other platforms have some discussion too in university and in conferences. The popularity of the subject on different platforms can be drowning from the data.

Question No.9: Do you able to describe what revenge porn and blackmailing is to someone else?

Table No. 7.13

Do you be able to describe what revenge porn and blackmailing is to someone else					
S. No.	**Respondent Response**	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	**No**	108	19.9	19.9	19.9
2	**Not Sure**	88	16.2	16.2	36.2
3	**Yes**	346	63.8	63.8	100.0
	Total	542	100.0	100.0	

Source: Primary Data

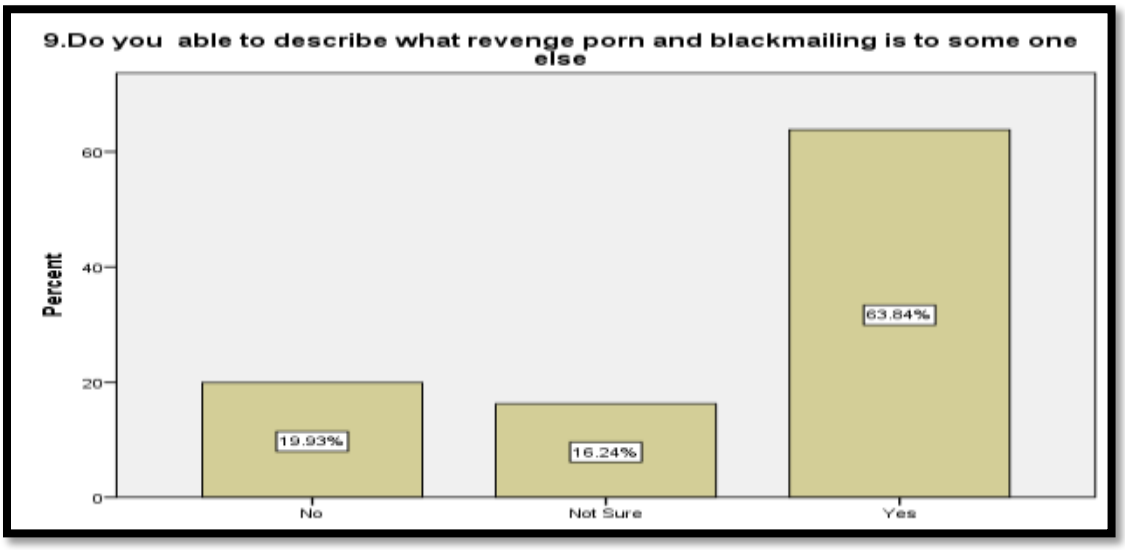


Figure No.7. 13

The above Table No. 7.13 and Figure No. 7.13 show the understanding of revenge porn and blackmailing of the respondent. The Table shows that out of 542 respondents, 346 (63.8%) respondents gave positive response, 108 (19.9%) respondents said no, and 88 (16.2%) said that they were not sure. Researcher also draws for these dynamics of responses that term itself suggests the definition. 64% respondents are able to explain, means they know the essential to constitute such crime or violation and it is quite possible that the respondents themselves faced such situation or learnt these from the near one's experiences.

Question No. 10: Social media play a vital role for increasing the cybercrime against women

Table No. 7.14

Social media play a vital role for increasing the cybercrime against women					
S. No.	**Respondent Response**	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	**Agree**	244	45.0	45.0	45.0
2	**Disagree**	12	2.2	2.2	47.2
3	**Neutral**	68	12.5	12.5	59.8
4	**Strongly Agree**	214	39.5	39.5	99.3
5	**Strongly Disagree**	4	.7	.7	100.0
	Total	542	100.0	100.0	

Source: Primary Data

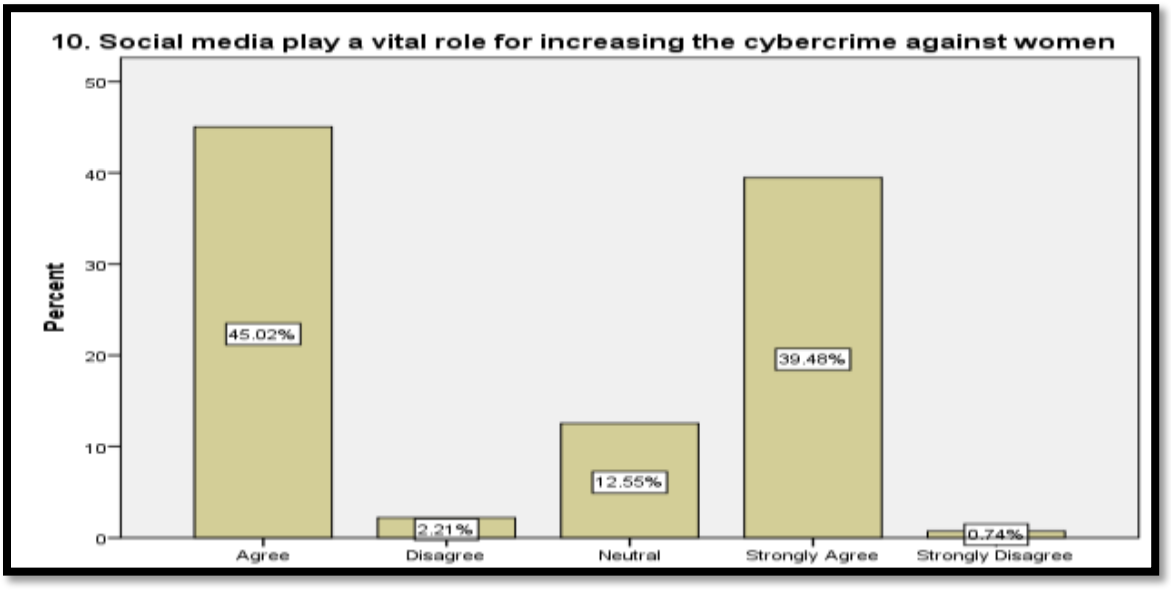


Figure No.7.14

The above Table No. 7.14 and Figure No. 7.14 shows that out of 542 respondents 214 (39.5%) respondents strongly agree to the statement, 244 (45%) respondents agree,

12 (2.2%) respondents disagree and 68 (12.5%) respondents are neutral, 4 (0.7%) respondents strongly disagree. This table further explains the data sharing and personal information like images of women which further increases the vulnerability factor of the women where the private movements of the family and virtual promotion in self to look good and act like the trends increasing such risk for the sensual information. Some of the features and ability to be popular by the trending images are also one of the factors for sharing such images on social media. Whereas breach of the privacy policy by social media platforms in terms of sharing the private information and images uploaded on the site is also quite common on which respondents have a belief on. 13% neutral respondents are also telling the same story that social media platforms have the potential for such breach of privacy policy but where they are doing it, it is a matter of inexperience to the respondents.

Question No.11: The women experience revenge porn cybercrime from known people such as acquaintances, friends and/or family member

Table No. 7.15

The women experience revenge porn cybercrime from known people such as acquaintances, friends and/or family member					
S. No.	**Respondent Response**	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	**Agree**	256	47.2	47.2	47.2
2	**Disagree**	42	7.7	7.7	55.0
3	**Neutral**	116	21.4	21.4	76.4
4	**Strongly Agree**	126	23.2	23.2	99.6
5	**Strongly Disagree**	2	.4	.4	100.0
	Total	542	100.0	100.0	

Source: Primary Data

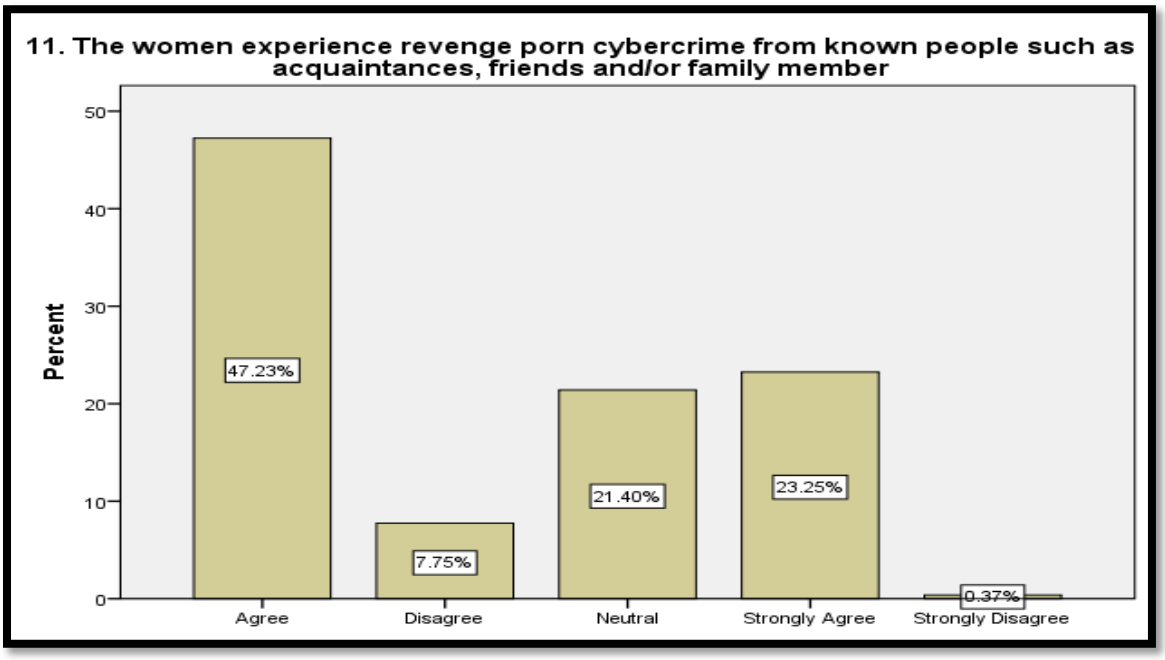


Figure No. 7.15

The above Table No. 7.15 and Figure No. 7.15 shows that out of 542 respondents 126 (23.2%) respondents strongly agree to the statement, 256 (47.2%) respondents agree, 42 (7.7%) respondent disagree and 116 (21.4%) respondents are neutral, 2 (0.4%) respondents strongly disagree. The researcher analyses that 48% respondent agree and 23% respondent strongly agreeing. That shows the research porn cybercrime are mostly committed by the known people such as friends, family member due to their interpersonal communication, which motivated for committing such cybercrime against women. Researcher also draws the similarity of the data with the physical sexual exploitation of women is also mostly by the acquaintance and close family members as they have the access for the information about the time table of the victim to be alone and confidence of the other for accessing the space where the victim would be comfortable.

Question No. 12: Whether you or person known to you threatened / blackmailed that your intimate picture/ video would be distribute or shared publicly?

Table No. 7.16

Whether you or person known to you threatened / blackmailed that your intimate picture/ video would be distribute or shared publicly?					
S. No.	**Respondent Response**	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	**No**	372	68.6	68.6	68.6
2	**Not Sure**	44	8.1	8.1	76.8
3	**Yes**	126	23.2	23.2	100.0
	Total	542	100.0	100.0	

Source: Primary data

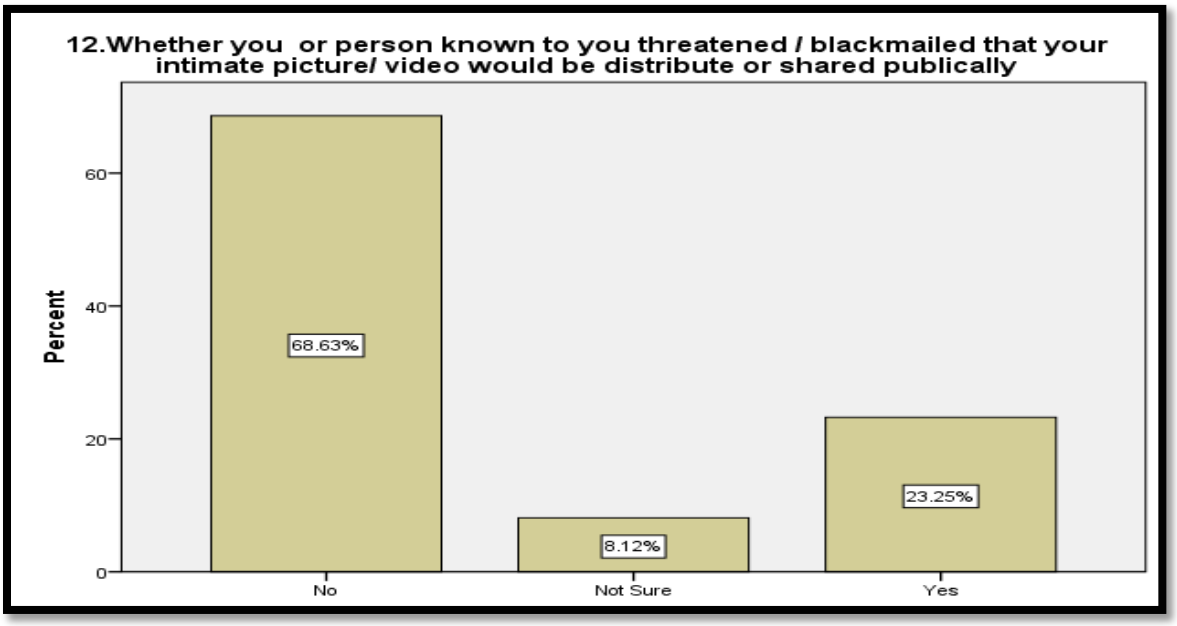


Figure No. 7.16

The above Table No. 7.16 and Figure No. 7.16, shows that out of 542 respondents, 126 (23.2%) respondents give positive response, 372 (68.6 %) respondents said no, and 44 (8.1%) are not sure. The present study shows that most of the respondent answer in negative i.e., 68% and they are not threatened or blackmailed for sharing the

intimate image publicly. This question intended to bring out the pre requisite of the crime where attempt or blackmailing related incidences happened or not with the respondents.

Question No.13: Whether revenge porn and blackmailing offence committed against you/ person known to you?

Table No. 7.17

Whether revenge porn and blackmailing offence committed against you/ person known to you.					
S. No.	**Respondent Response**	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	**No Response**	2	.4	.4	.4
2	**No**	362	66.8	66.8	67.2
3	**Not Sure**	52	9.6	9.6	76.8
4	**Yes**	126	23.2	23.2	100.0
	Total	542	100.0	100.0	

Source: Primary Data

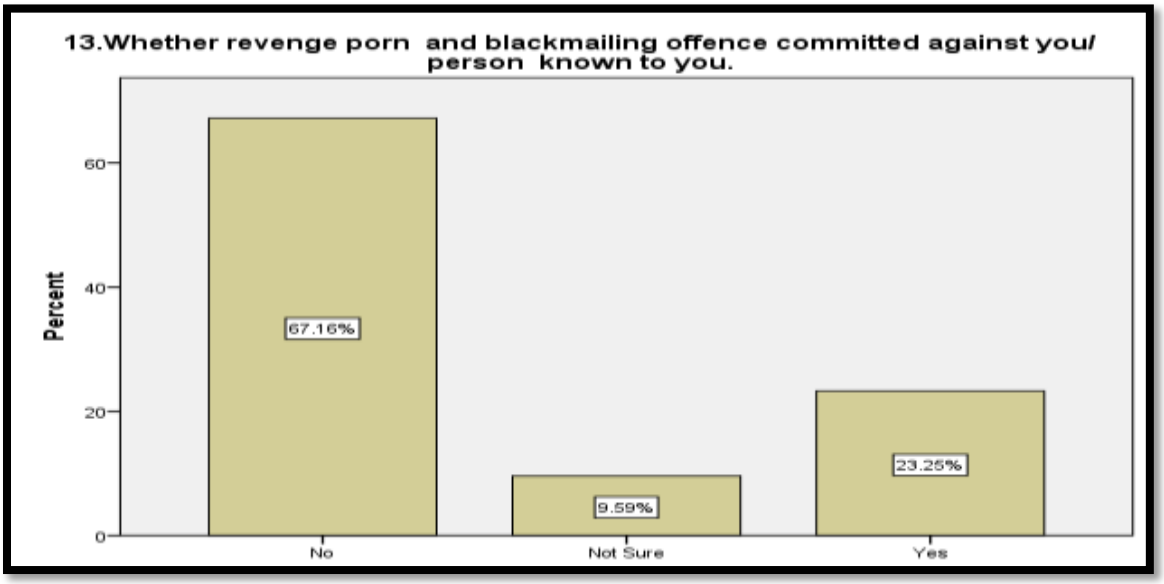


Figure No. 7.17

The above Table No. 7.17 and Figure No. 7.17, reveals the information about the victimization of the respondent. The Table shows that out of 542 respondents, 126 (23.2%) respondents gave positive response, 362 (66.6%) respondents answered in negative and 52 (9.6%) respondents preferred to be answer the question as not sure, which form the minimal number of respondents 2 (0.4%) did not prefer to respond. This question intended to bring forth the incidences of crime committed with or related person of respondents. It also instigates the acknowledgement of such crime with any other related person for which the respondents have familiarity of the culprit.

Researcher also draws from the dynamics that 23% of the respondents either facing the violation or familiar with the exploitation in one way or another whereas 9 % respondents are not sure which also indicating the chances for the same.

Question No. 14: Do you know who 'leaked' your picture/ video?

Table No. 7.18

Do you know who 'leaked' your picture/ video?					
S. No.	**Respondent Response**	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	**No**	324	59.8	59.8	59.8
2	**Not Sure**	36	6.6	6.6	66.4
3	**Yes**	182	33.6	33.6	100.0
	Total	542	100.0	100.0	

Source: Primary Data

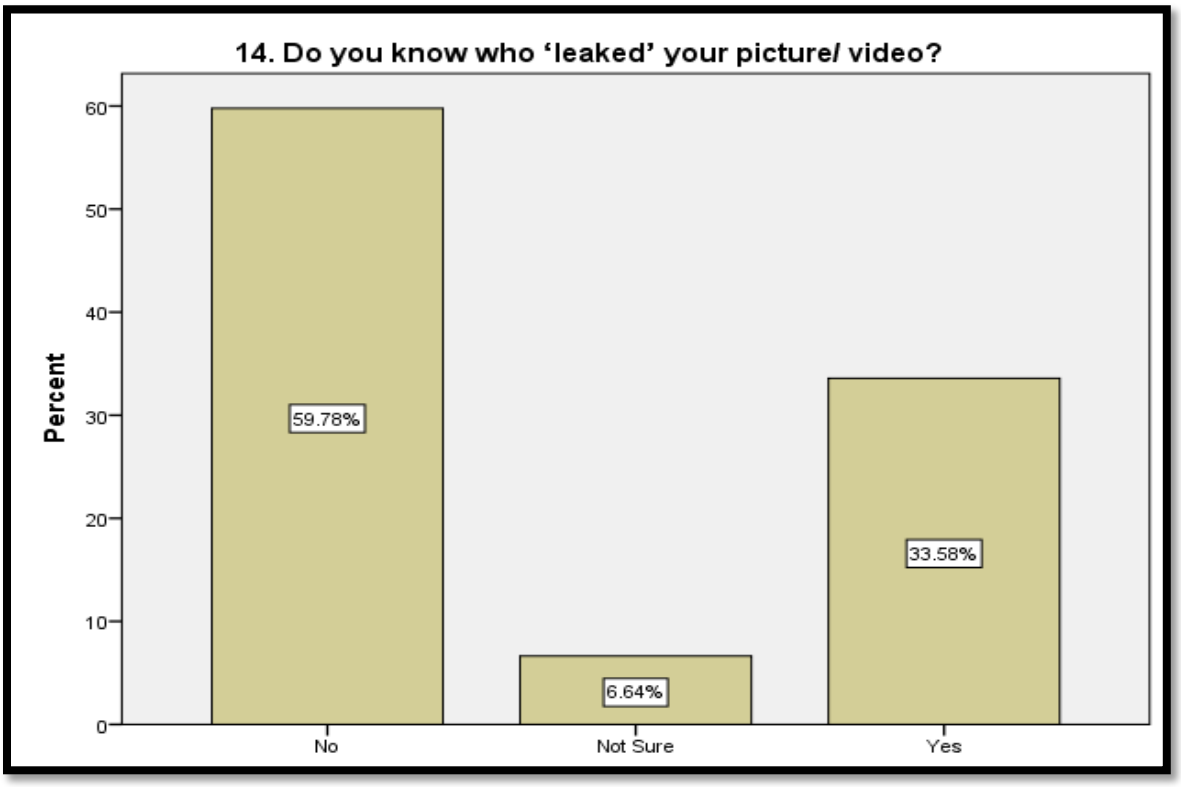


Figure No.7.18

The above Table No. 7.18 and Figure No. 7.18 reveal that out of 542 respondents, 182 (33.6%) respondents gave positive response, 324 (59.8%) respondents said no, which form the minimal number of respondent and 36 (6.6%) are not sure. The researcher draws from this data that one third of the respondents are familiar with the crime as well as the culprit.

Question No. 15: If yes, then tell us who

Table No. 7.19

if yes, then tell us who					
S. No.	**Respondent Response**	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	**No response**	314	57.9	57.9	57.9
2	**A boyfriend/ partner**	32	5.9	5.9	63.8
3	**A friend**	52	9.6	9.6	73.4
4	**A social media follower**	16	3.0	3.0	76.4
5	**A stranger**	10	1.8	1.8	78.2
6	**An ex boyfriend/ partner**	36	6.6	6.6	84.9
7	**Other**	82	15.1	15.1	100.0
	Total	542	100.0	100.0	

Source: Primary Data

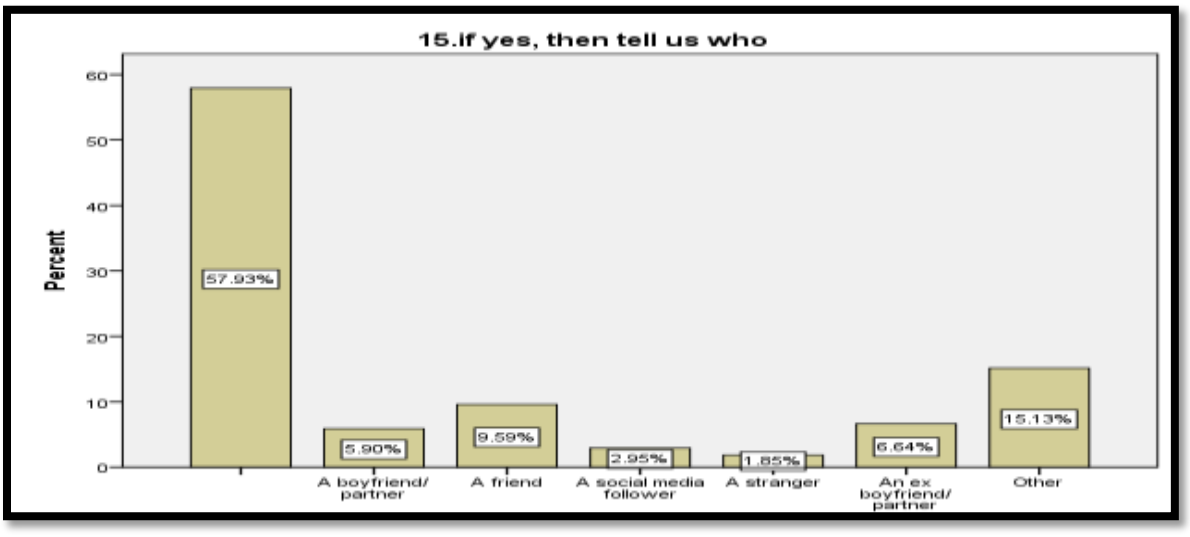


Figure No.7.19

The above Table No. 7.19 and Figure No. 7.19 shows that out of 542 respondent 314 (57.9%) did not responded to this question that is who leaked your intimate image; if yes tell us who? Only 228 (43.1%) respondents gave the answer, which shows that 32 (5.9%) respondents said that it's leaked by their boyfriend/ partner, 52 (9.6%) said it's by a friend, 16 (3%) said by social media followers, 10 (1.8%) by stranger, 36 (6.6%) an ex-boyfriend/ partner, and 82 (15.1%) said its leaked by others. The researcher draws from the varied responses that several categories of known persons are involved in the crime where the distant strangers and unknown followers are also a part of it. The slightest of mistake with the selection of friend and person with whom we are sharing the consent to speak is violating the right of privacy for further communication and using the images or any other content by the culprit.

Question No 16: How did you find out about it?

Table No. 7.20

How did you find out about it					
S. No	**Respondent Response**	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	**No response**	354	65.3	65.3	65.3
2	**A colleague told me**	8	1.5	1.5	66.8
3	**A friend told me**	32	5.9	5.9	72.7
4	**A social media follower told me**	8	1.5	1.5	74.2
5	**I discovered it**	14	2.6	2.6	76.8
6	**My boyfriend /partner told me**	8	1.5	1.5	78.2
	Other	118	21.8	21.8	100.0
	Total	542	100.0	100.0	

Source: Primary Data

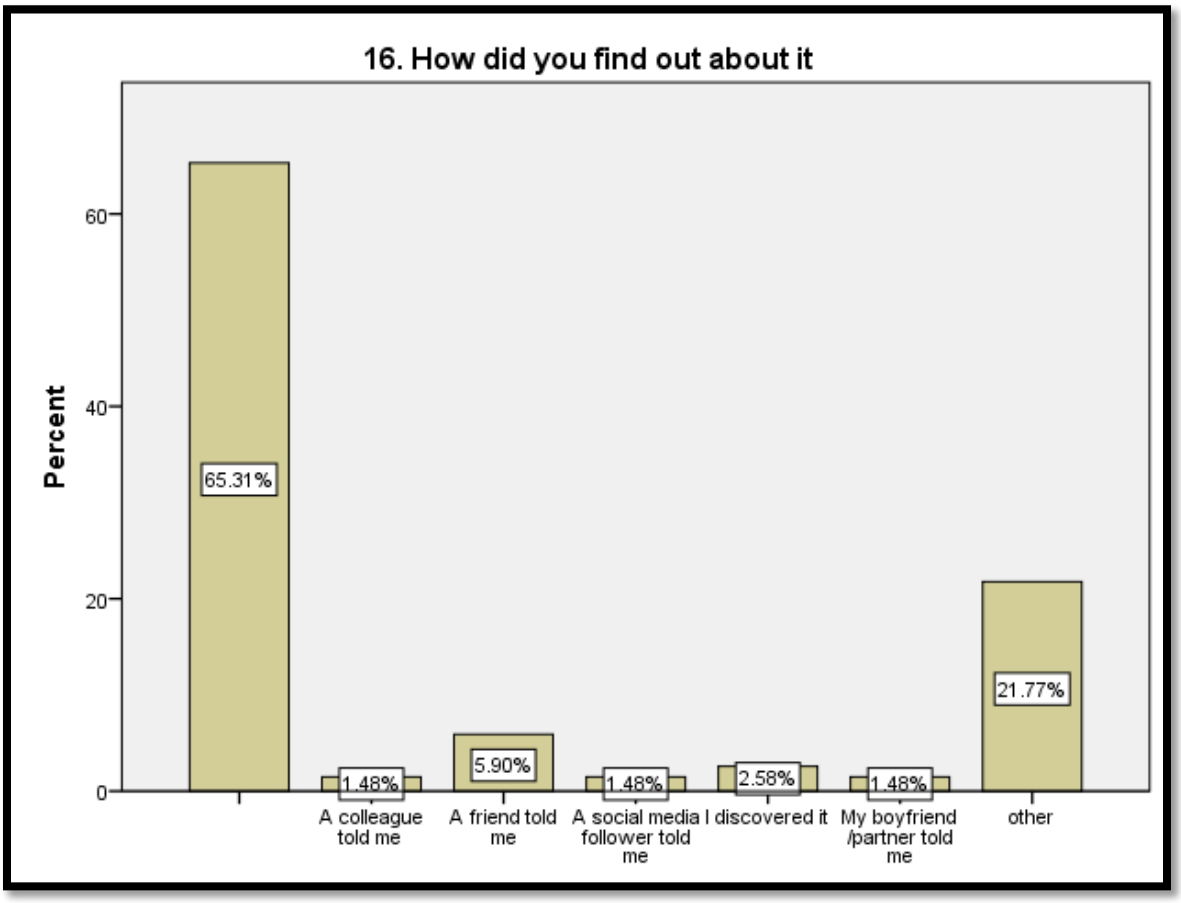


Figure No.7.20

The above Table No. 7.20 and Figure No. 7.20 shows that 354 (65%) respondents either prefer not to respond and thus incidences have not happened to them. The persons who responded yes in the previous question, among them, 8 (1.5%) respondents got to know about the crime by their colleagues, about 32 (6%) person got to know about the content by friends, about 8 (1.5%) person got to know from social media followers, 14 (2.6%) respondents discovered the content themselves, 8 (1.5%) respondent got to know through the boyfriends and 118 (21.8%) respondents came to know from other persons.

Question No. 17: Where was your picture / video shared?

Table No.7.21

Where was your picture / video shared?					
S. No.	**Respondent Response**	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	**No response**	364	67.2	67.2	67.2
2	**By email**	4	.7	.7	67.9
3	**It was shared to someone in person**	8	1.5	1.5	69.4
4	**On a blog/ website**	4	.7	.7	70.1
5	**On social media**	38	7.0	7.0	77.1
6	**On whatsapp group or by message**	22	4.1	4.1	81.2
7	**Uploaded to a porn site**	4	.7	.7	100.0
8	**Others**	98	18.1	18.1	99.3
	Total	542	100.0	100.0	

Source: Primary Data

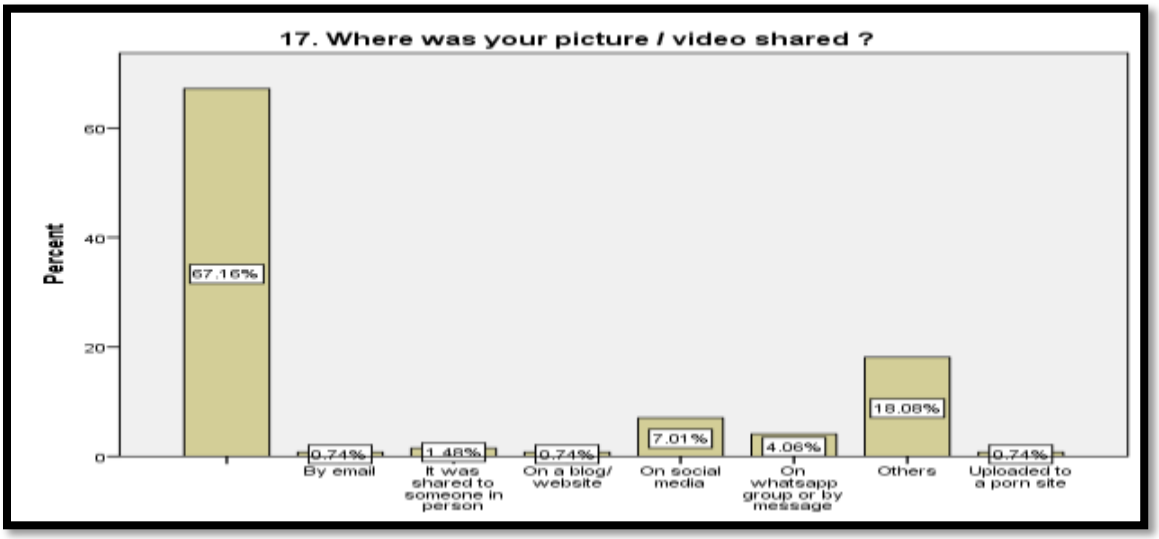


Figure No.7.21

The above Table No. 7.21 and Figure No. 7.21 intend to draw the variety of platforms where the content is shared. 4 (0.7%) respondents found the content on social media and 98 (18.08%) respondents found their content on other internet platforms. Around 4 (1%) respondents either found the content on email, blog or uploaded on the porn site. However, the 22 (4%) respondents mention the Whatsapp as a platform for such sharing. 8 (1.5%) respondents mention that the sharing was in the form of hard copy or in person where the soft copy is shown to the victim.

Question No. 18: A victim of revenge porn and blackmailing is to blame for the sharing of her image or videos

Table No. 7.22

A victim of revenge porn and blackmailing is to blame for the sharing of her image or videos					
S. No.	**Respondent Response**	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	**Agree**	102	18.8	18.8	18.8
2	**Disagree**	138	25.5	25.5	44.3
3	**Neutral**	156	28.8	28.8	73.1
4	**Strongly Agree**	80	14.8	14.8	87.8
5	**Strongly Disagree**	66	12.2	12.2	100.0
	Total	542	100.0	100.0	

Source: Primary Data

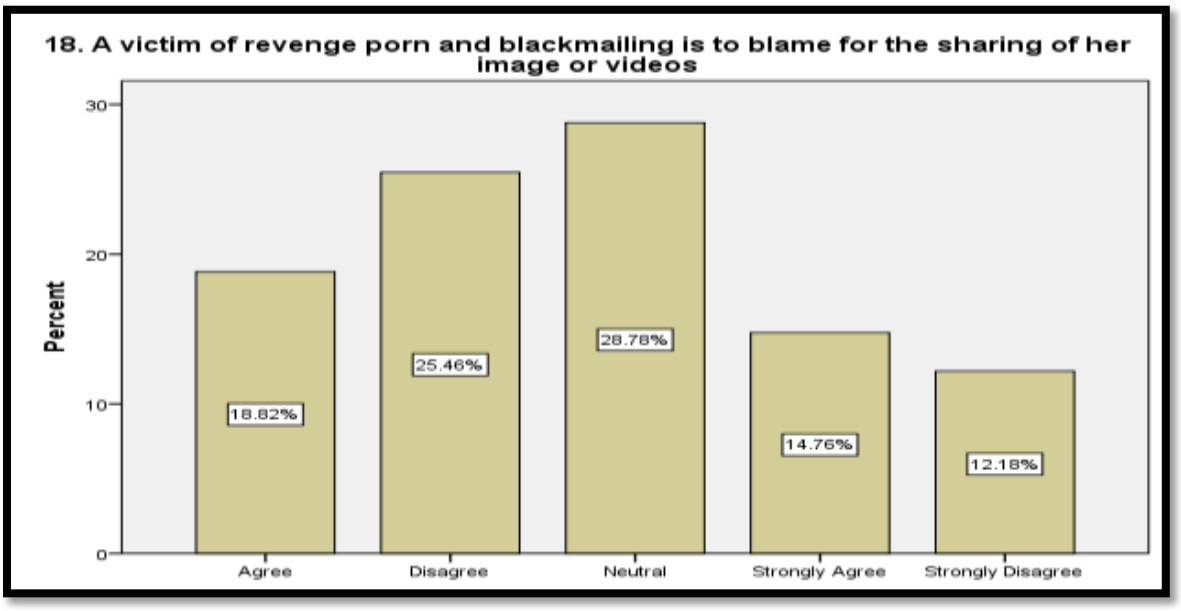


Figure No. 7.22

The above Table No. 7.22 and Figure No. 7.22 shows that out of 542 respondent 66 (12.2%) respondents strongly disagree to the statement, 102 (18.8 %) respondent agree, 138 (25.5%) respondents disagree and 156 (28.8%) respondents preferred to be neutral, 80 (14.8%) respondent strongly agree. This question is intended to bring out the feeling of the respondents that who should be blamed for the crime or incidence. Researcher also draws from these responses that the 19% respondents agree that the blame should be on the victim which shows the general perception about the crime while using internet or such technological platforms which itself supposed to be problematic especially with the adolescence who are the prime respondents in this case as the study is conducted in education institutions.

Question No: 19: Consent to have filmed sexual activity is consent to publish it online

Table No.7.23

Consent to have filmed sexual activity is consent to publish it online					
S. No.	**Respondent Response**	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	**Agree**	62	11.4	11.4	11.4
2	**Disagree**	110	20.3	20.3	31.7
3	**Neutral**	118	21.8	21.8	53.5
4	**Strongly Agree**	26	4.8	4.8	58.3
5	**Strongly Disagree**	226	41.7	41.7	100.0
	Total	542	100.0	100.0	

Source: Primary Data

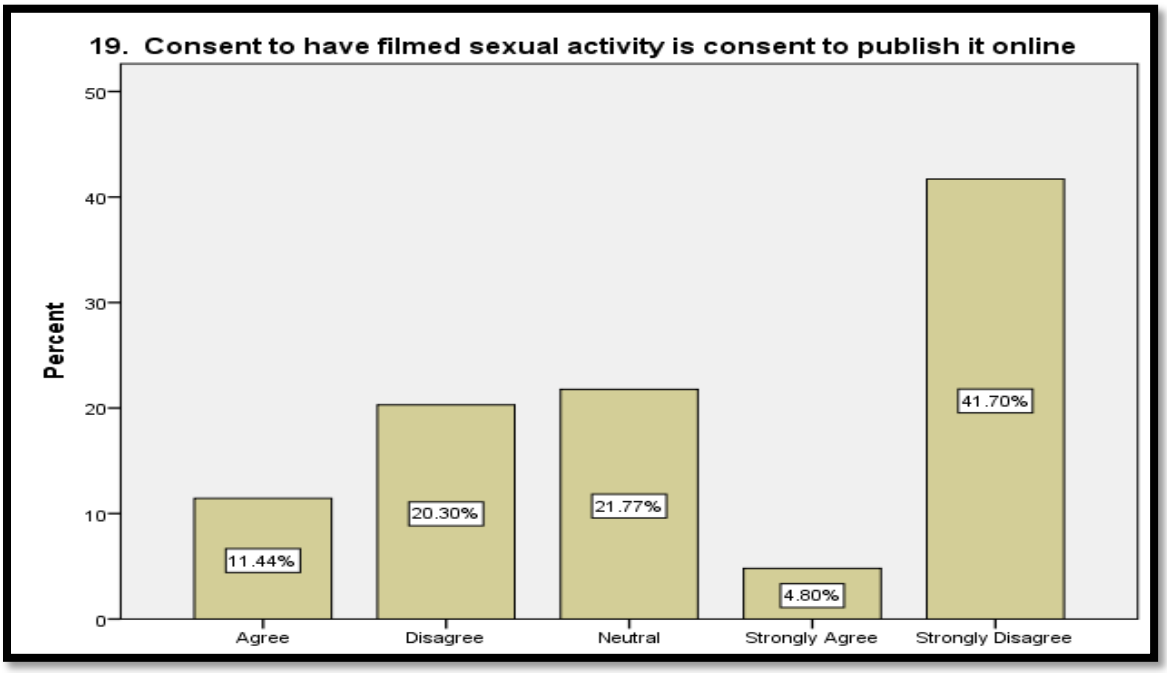


Figure No.7.23

The above Table No. 7.23 and Figure No.7.23 shows that out of 542 respondents 226 (41.7%) respondents strongly disagree to the statement, 62 (11.4%) respondents agree, 110 (20.3%) respondents disagree and 118 (21.8%) respondents prefer to be neutral, 26 (4.8%) respondent strongly agree. The question intends to bring the responses on the perception that where someone who is filming the sexual activity is also allowing his partner to share the same on any other platform or with other persons. The researcher draws from the statistics that 11% respondent belief it in positive that the consent of filming is also a consent of dissemination of such content where 4.8% respondents strongly agree with the notion which means they have a strong sense for blaming the victim for the same. Whereas 21% respondents are neutral in their responded which means they are not sure whom to blame but they are also presumptive at least half of the changes that the blame should be on the persons too who are giving the consent at the time of filming the content.

Question No.20: Are you aware of "the Information Technology Act, 2000?"

Table No. 7.24

Are you aware of "the Information Technology Act, 2000"					
S. No.	**Respondent Response**	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	**No**	108	19.9	19.9	19.9
2	**Not Sure**	40	7.4	7.4	27.3
3	**Yes**	394	72.7	72.7	100.0
	Total	542	100.0	100.0	

Source: Primary Data

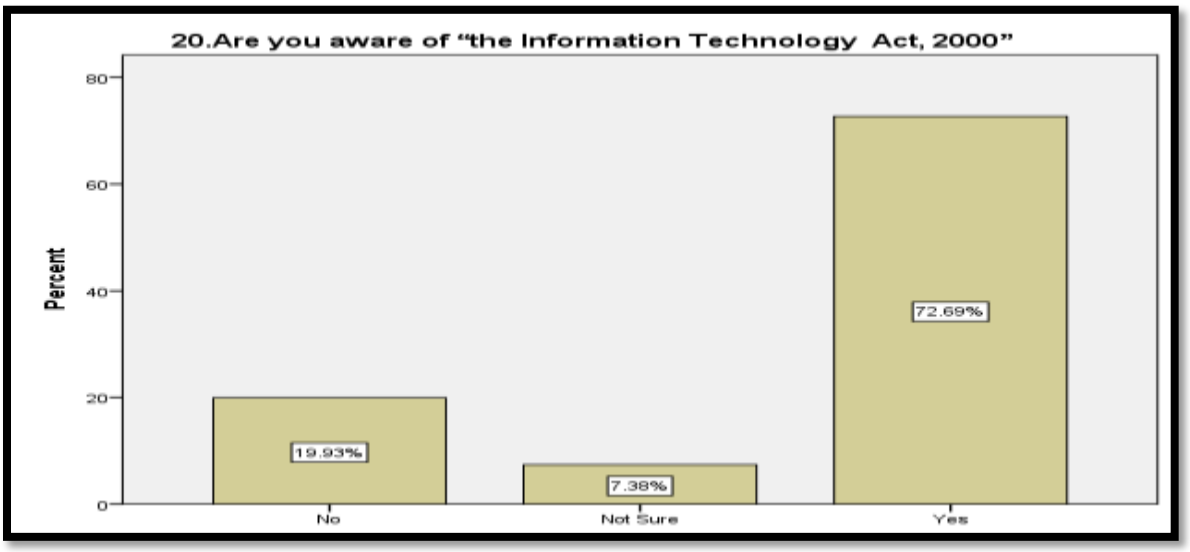


Figure No. 7.24

The above Table No. 7.24 and Figure No. 7.24, shows that out of 542 respondent, 394 (72.7%) respondents gave positive response, 108 (19.9%) respondent said no, and 40 (7.4%) said not sure, which form the minimal number of respondents. This question tries to show the awareness of the legislation. It also brings out the subject that to address the issue of understanding that such crime can be addressed by such legislation.

Question No.21: Do you know the "National Cyber Crime Report" portal where cybercrime against women can be reported online

Table No. 7.25

Do you know the "National Cyber Crime Report" portal where cybercrime against women can be reported online					
S. No.	**Respondent Response**	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	**No**	94	17.3	17.3	17.3
2	**Not Sure**	40	7.4	7.4	24.7
3	**Yes**	408	75.3	75.3	100.0
	Total	542	100.0	100.0	

Source: Primary Data

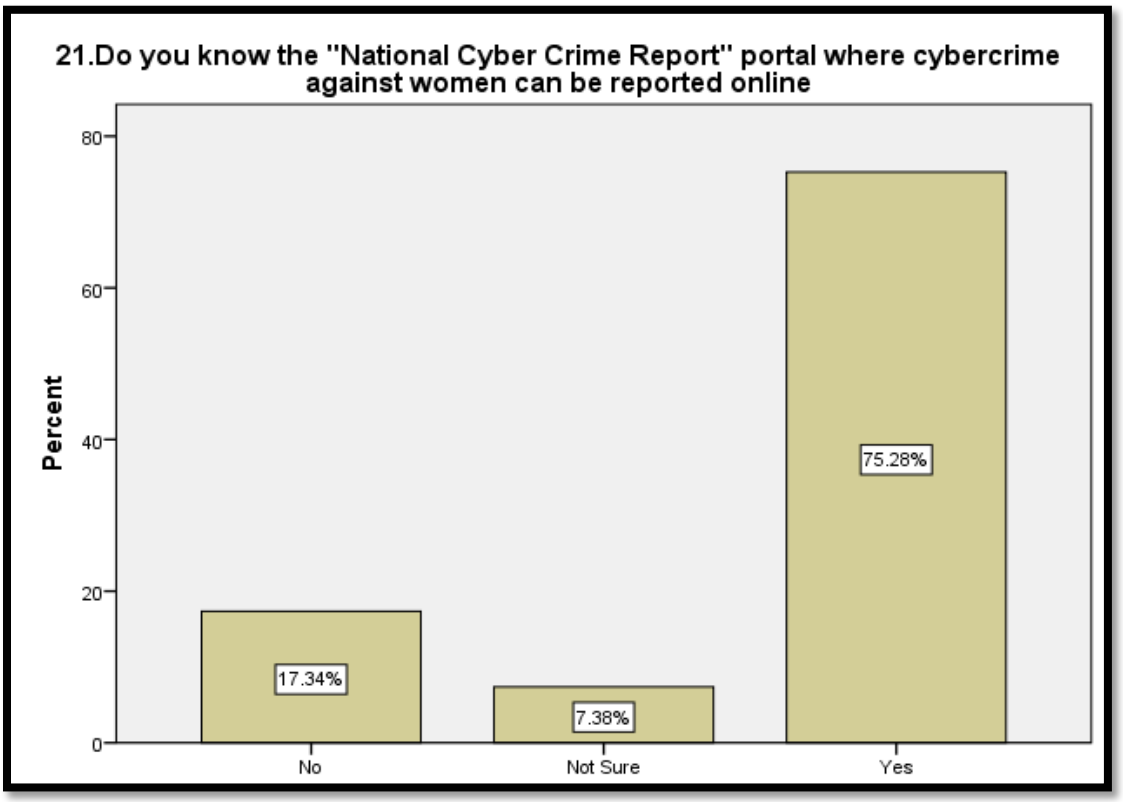


Figure No. 7. 25

The above Table No. 7.25 and Figure No. 7.25 shows that out of 542 respondents, 408 (75.3%) respondents said yes, 94 (17.34 %) respondents said no, and 40 (7.4 %) said not sure, which form the minimal number of respondents. This question tries to show the awareness of the administrative support structure for such crime or is there any platform for which can be approached for access to justice? It also brings out the subject that to address the issue of understanding that such crime can we addressed by such administrative agencies.

Question No.22: If you come across a cybercrime, how would you report to it?

Table No. 7.26

If you come across a cybercrime, how would you report to it?					
S. No.	**Respondent Response**	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	**No Response**	70	12.9	12.9	12.9
2	**Inform the cyber cell 152260**	64	11.8	11.8	24.7
3	**Inform the cyber cell 155260**	132	24.4	24.4	49.1
4	**Inform the police**	88	16.2	16.2	65.3
5	**Keep silence**	2	.4	.4	65.7
6	**Report online**	146	26.9	26.9	92.6
7	**Talk to family or friends**	40	7.4	7.4	100.0
	Total	542	100.0	100.0	

Source: Primary Data

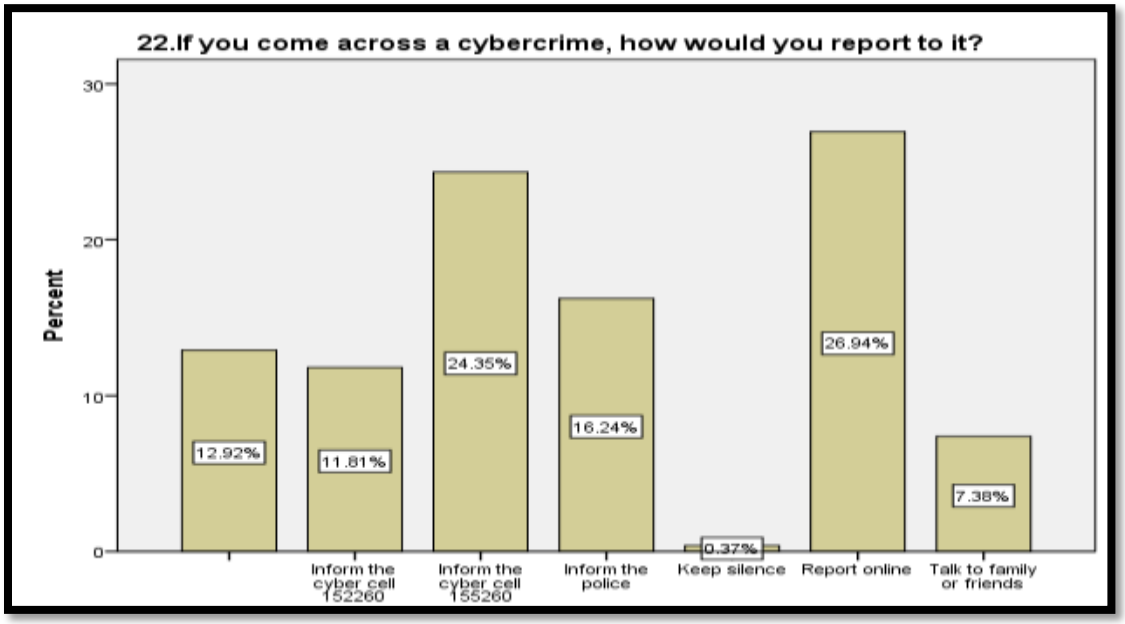


Figure No.7. 26

The above Table No. 7.26 and Figure No.7.26 shows that victims reporting behavior, which depict that out of 542 respondents, 146 (26.9%) said that; they report online if any cybercrime committed against them while 132 (24.4%) respondents inform the cyber cell no. 155260, and 40 (7.4%) respondents talk to their family, 88 (16.2%) respondents inform the local police only 2 (0.4%) said that the keep silence against the crime which form the minimal number. Its observe that only minimal respondent keep silence and respondent are well aware the cybercrime reporting but the reporting regard to sexual offence are very low. This question also brings out the awareness of the platforms for the access to justice in cases on such incidents of crime.

Question 23: Have you ever experience any of these crime commissions

Table No. 7.27

Have you ever experience any of these crime commissions					
S. No.	**Respondent Response**	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	**No Response**	232	42.8	42.8	42.8
2	**Any other**	82	15.1	15.1	57.9
3	**Cyber Bullying**	2	.4	.4	58.3
4	**Cyber Fraud**	36	6.6	6.6	64.9
5	**Email harassment**	4	.7	.7	65.7
6	**Fake avatar (Fake Profile)**	106	19.6	19.6	85.2
7	**Online stalking**	44	8.1	8.1	93.4
8	**Revenge porn**	14	2.6	2.6	95.9
9	**Sextortion**	6	1.1	1.1	97.0
10	**Trolling**	16	3.0	3.0	100.0
	Total	542	100.0	100.0	

Source: Primary Data

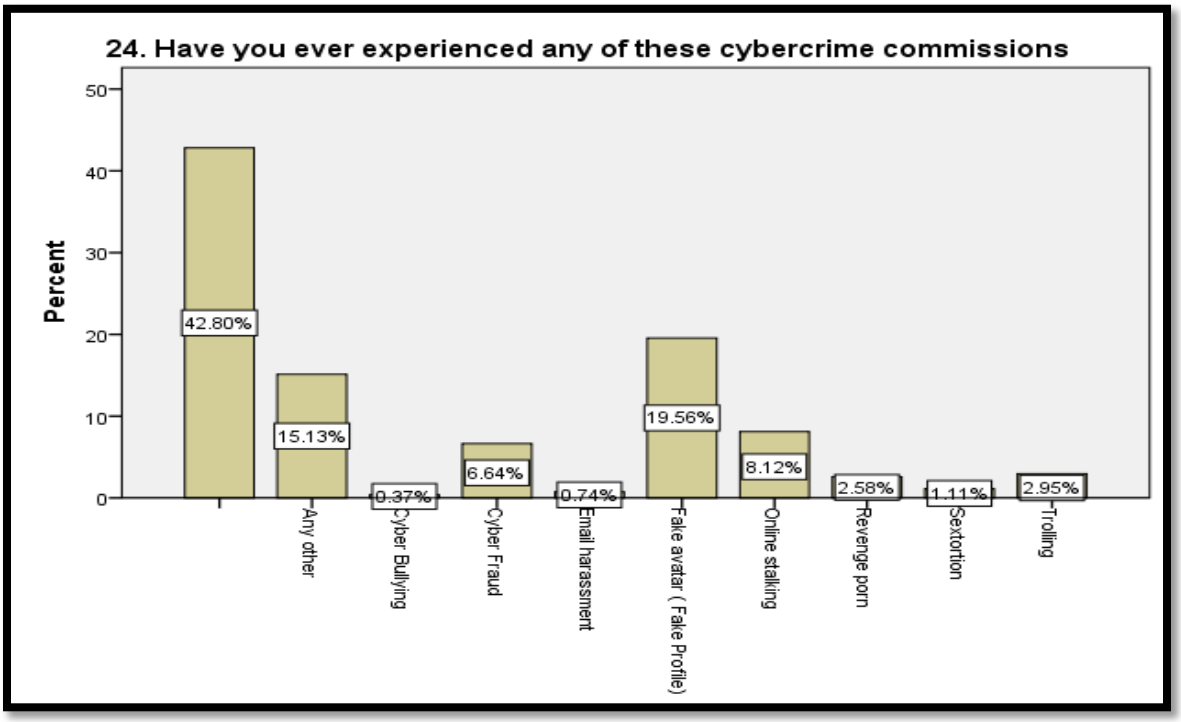


Figure No. 7.27

The above Table No. and Figure No. 7.27 show that out of 542 respondents said that 14 (2.6%) respondent said that revenge porn cybercrime against them committed, 6 (1.1%) said that Sextortion offence committed against them, 16 (3%) the victim of trolling, 44 (8.1%) respondents Online Stalked, 106 (19.6%) said that cybercrime committed through Fake Profile, 2 (0.4%) respondents the victim of Cyber Bullying, 4 (0.7%) respondents said that the Email harassment cybercrime committed against them, 36 (6.6%) respondents said that Cyber Fraud committed, 82 (15.1%) respondent said "any other" cybercrime against committed against them but they do not mentioned the name of the crime and 232 (42.8%) respondents prefer not to respond. The researcher draw result that it observed from the table and figure that fake profile or fake avatar are high crime rate committed against the respondents while.

Question No. 24: If reported, whether police have taken action against accused

Table No. 7.28

If reported, whether police have taken action against accused					
S. No.	**Respondent Response**	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	**No**	61	11.3	11.3	11.3
2	**Not Sure**	266	49.1	49.1	60.3
3	**Yes**	215	39.7	39.7	100.0
	Total	542	100.0	100.0	

Source: Primary Data

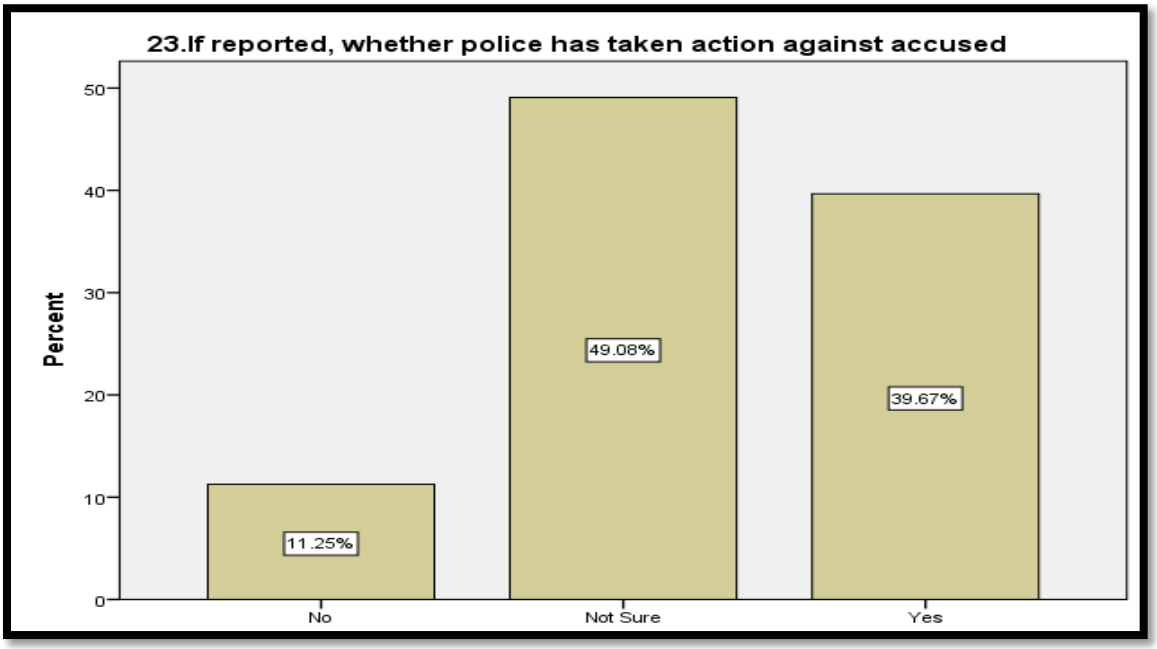


Figure No. 7.28

The above Table No. 7.28 and Figure No. 7.28 shows that out of 542 respondent, 215 (39.67%) respondents said yes, 61 (11.25%) respondents said no, which form the minimal number of respondent and 266 (49.08%) said not sure. It has observed by the researcher that the victim of cybercrime having knowledge of the about the proceedings of the case. The researcher draws from the responses that the in 40% cases of reporting

the police take affirmative action for the crime, whereas in 50% cases reported the respondents not sure that the affirmative or required action has been taken or not.

Section C:

Question No.1. **Do you know the term Revenge Porn and Blackmailing**.

Table No. 7.29

Do you know the term Revenge Porn and Blackmailing					
S. No	**Respondents Response**	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	**Yes**	12	54.5	54.5	54.5
2	**No**	10	45.5	45.5	100.0
	Total	22	100.0	100.0	

Source: Primary Data

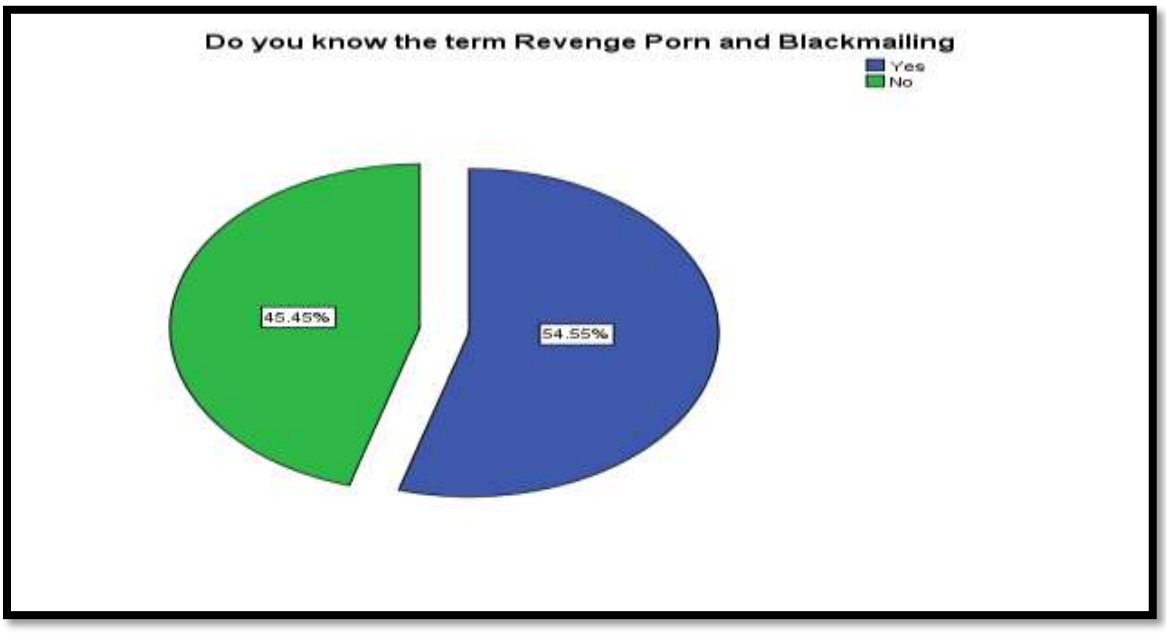


Figure No. 7.29

Above Table No. 7.29 and Figure No. 7.29 shows that 12 (54.55%) respondents said yes and 10 (45.5%) said No. The researcher infers from the data that 54% respondents from the police administration were aware about this type of crime in cyber space where as 45% respondents unaware about the same. One of the important aspects is almost half of the respondents unaware about the crime so we can infer that these police stations has not registered any case yet under these crimes.

Question No.2. Do you know that under which section the offence of Revenge Porn and Blackmailing lies.

Table No. 7.30

Do you know the under which section the offence of Revenge Porn and Blackmailing lies.					
S. No.	**Respondents Response**	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	**Yes**	11	50.0	50.0	50.0
2	**No**	11	50.0	50.0	100.0
	Total	22	100.0	100.0	

Source: Primary Data

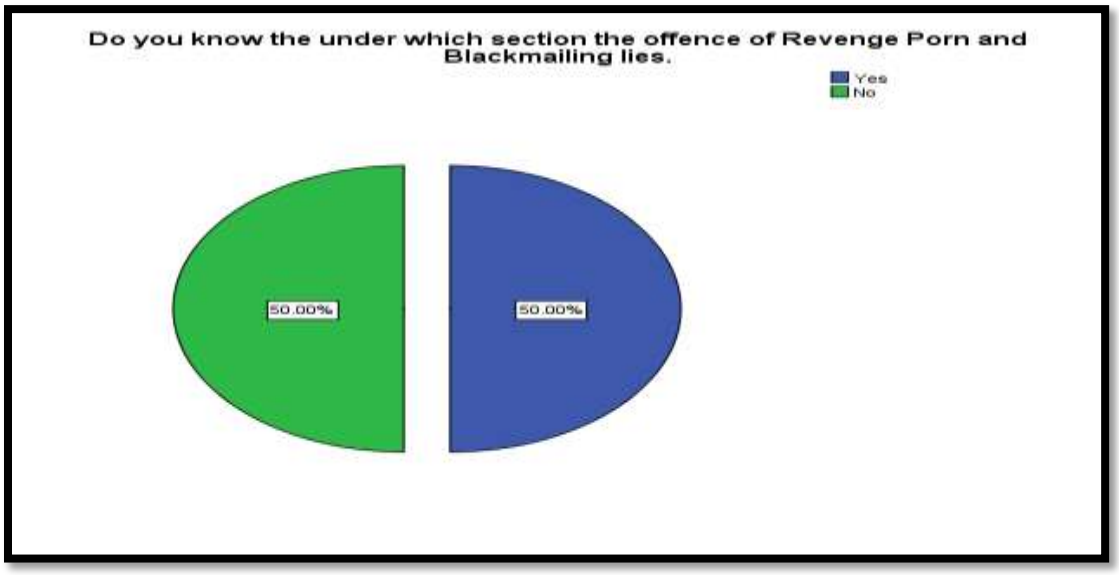


Figure 7.30

Above Table No. 7.30 and Figure No. 7.30 shows that 11 (50%) respondents said yes and 11 (50%) said no. It is to draw from this statistics that equal number of people are aware and unaware about the crime that under which section this crime should be booked. One of the important aspects of this figure is some of the people who are aware about the crime is also not familiar with the section under which it should be registered as 54% respondents aware about the crime but only 50% of the respondents aware about the proper section of the filing.

Question No.3: Do you know the investigation procedure for cyber offence committed against women?

Table No. 7.31

Do you know the investigation procedure for cyber offence committed against women					
S. No.	**Respondents Response**	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	**Yes**	20	90.9	90.9	90.9
2	**No**	2	9.1	9.1	100.0
	Total	22	100.0	100.0	

Source: Primary Data

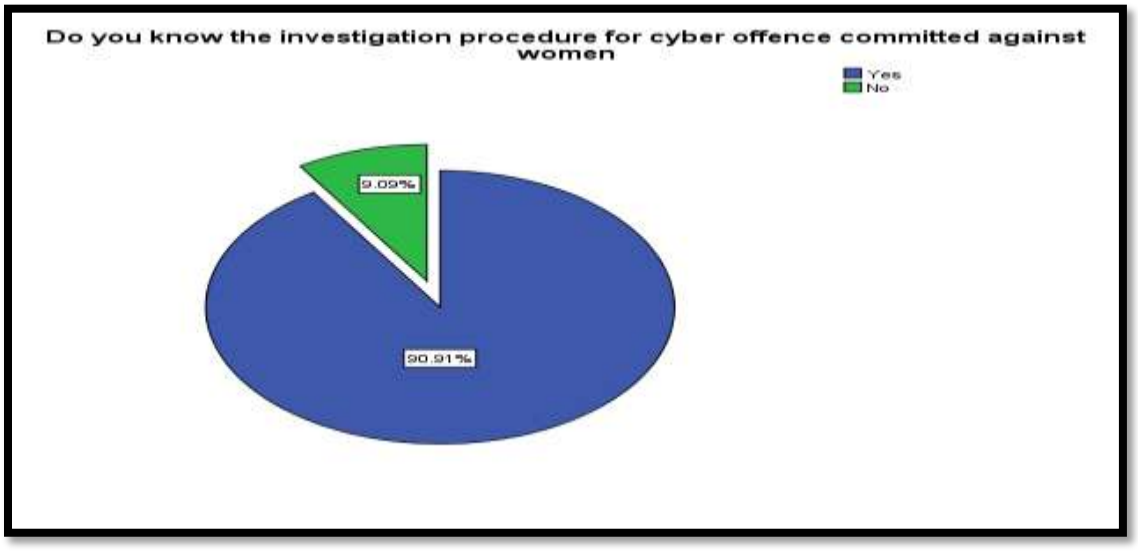


Figure No. 7.31

Above Table No. 7.31 and Figure No. 7.31 shows that 20 (90.91%) respondents said yes and 10 (9.09%) said no. Researcher draws from this statistic that most of the respondents aware about the procedure of investigation for this crime. It is also inferred from this data that majority of the respondents under impression that the general procedure of investigation under any other crime will apply here too and equally work for this section.

Question No.4: Does the cybercrime against women complaint record and investigated by women police officer in police station

Table No. 7.32

Does the cybercrime against women complaint record and investigated by women police officer in police station					
S. No.	**Respondents Response**	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	**Yes**	16	72.7	72.7	72.7
2	**No**	6	27.3	27.3	100.0
	Total	22	100.0	100.0	

Source: Primary data

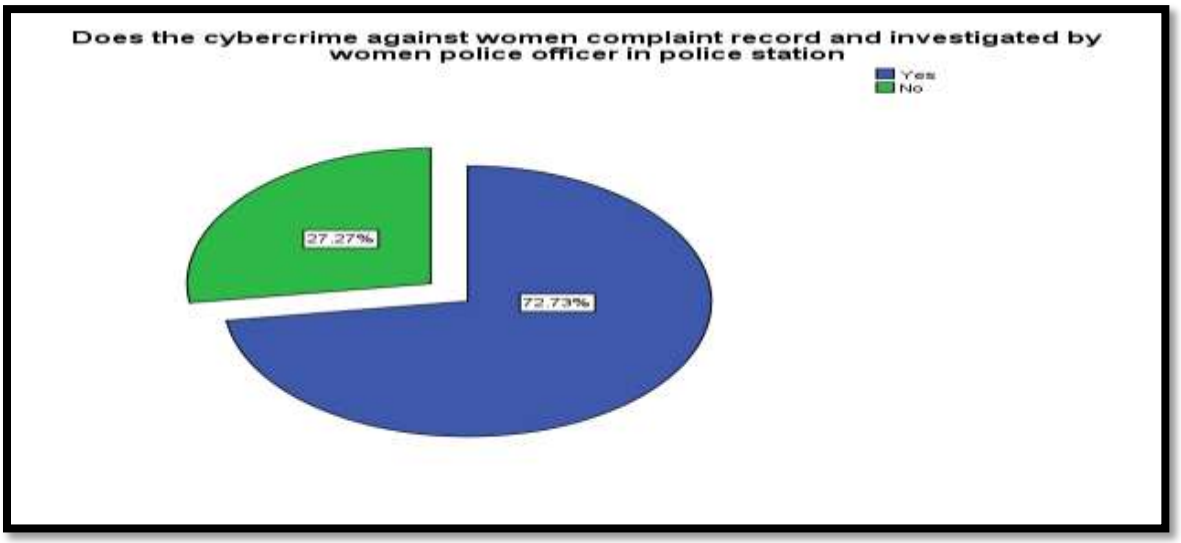


Figure No. 7.32

Above Table No. 7.32 and Figure No. 7.32 shows that 16 (72.7%) respondents said yes and 6 (27.27%) said no. The researcher draws from this data that 75% police stations have female officers to investigate the crime. However, it would be interesting to know that how many police stations has female Sub Inspector (SI) or Investigating officer (IO) are there on an average at each police station but such data is not available due to which we can't compare it with nation or state averages.

Question No. 5: Whether you are well equipped with the technologies to fight the cybercrime against women

Table No. 7.33

Whether you are well equipped with the technologies to fight the cybercrime against women					
S. No.	**Respondent Response**	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	**Yes**	8	36.4	36.4	36.4
2	**No**	14	63.6	63.6	100.0
	Total	22	100.0	100.0	

Source: Primary Data

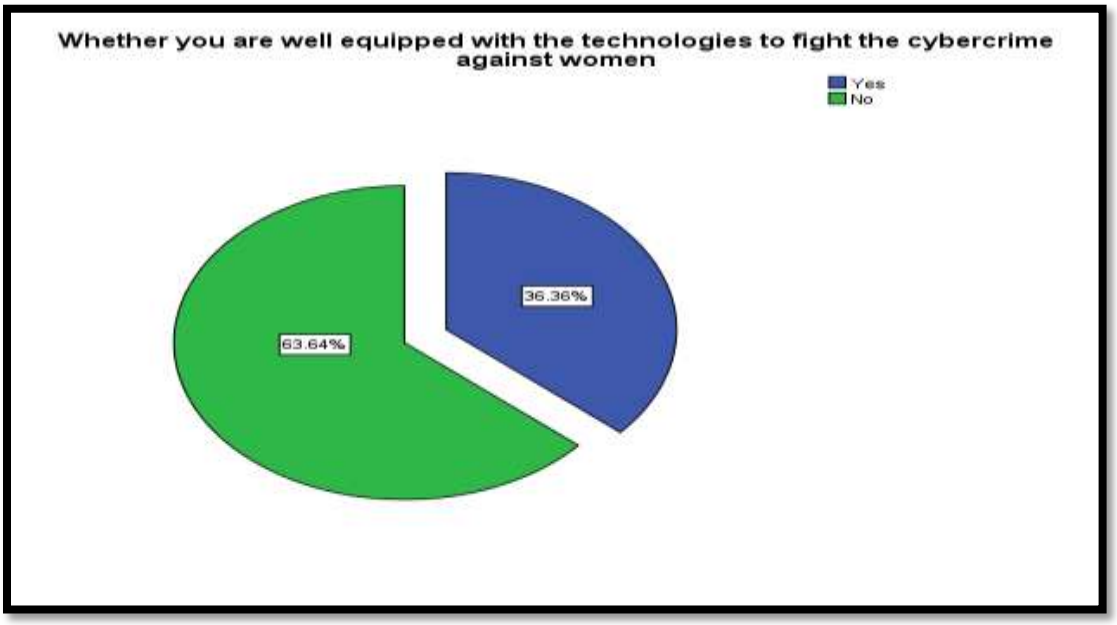


Figure No. 7.33

Above Table No. 7.33 and Figure No. 7.33 reveals that 8 (36.36%) respondents said yes and 14 (63.64%) said no. Researcher draws from this data that 64% police stations think that they are not well equipped with the technology or the technical skills for the response against these crimes. Whereas 36% respondents are stating that they are well equipped with the modern technology and expertise to deal with such cyber-crimes. Researcher also draws from this data that the need for such equipment is also felt by the police officers dealing with these crimes.

Question No. 6: Are you satisfied with the tools and techniques provided by the government to deal with cybercrime specifically?

Table No. 7.34

Are you satisfied with the tools and techniques provided by the government to deal with cybercrime specifically					
S. No.	**Respondent Response**	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	**Yes**	7	31.8	31.8	31.8
2	**No**	15	68.2	68.2	100.0
	Total	22	100.0	100.0	

Source: Primary Data

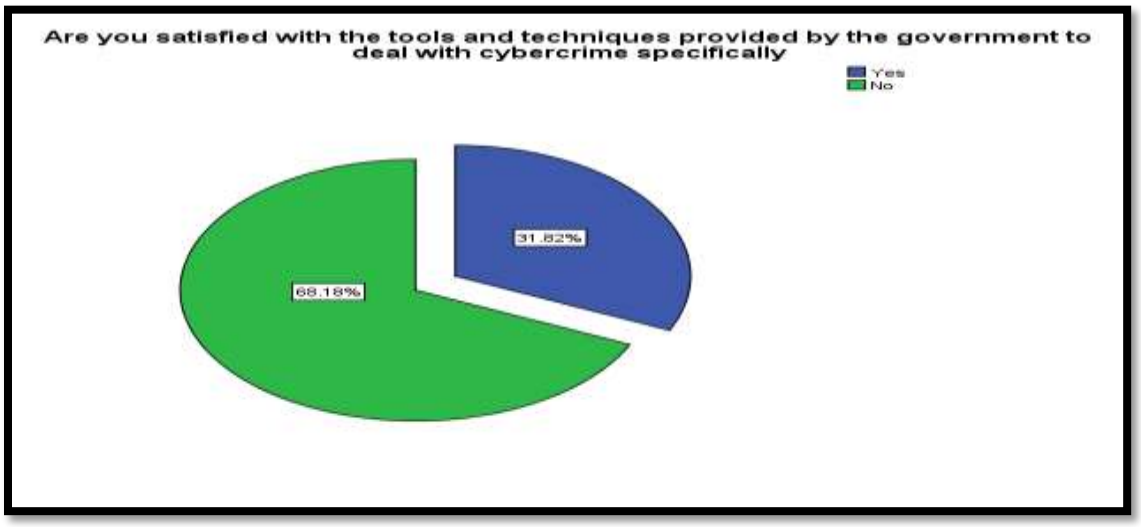


Figure No. 7.34

Above Table No. 7.34 and Figure No. 7.34 shows that 7 (31.8%) respondents said yes and 15 (68.2%) answered no, Researcher draws from this data that 68% police stations think that they are not well equipped with the technology or the technical skills provided by the government for the response against these crimes. Whereas 32% respondents stating that they are well equipped with the modern technology and have expertise to deal with such cybercrimes provided by the government. Researcher also draws from this data that the need for such equipment is also felt by the police officers dealing with these crimes.

Question No.7: How many cases reported in your police station during year 2020 to 2021 as regard to cybercrime against women?

Table No. 7.35

How many cases reported in your police station during year 2020 to 2021 as regard to cybercrime against women					
S. No.	**Cases**	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	**0-10**	4	18.2	18.2	18.2
2	**10-50**	6	27.3	27.3	45.5
3	**50-100**	6	27.3	27.3	72.7
4	**More than 100**	6	27.3	27.3	100.0
	Total	22	100.0	100.0	

Source: Primary Data

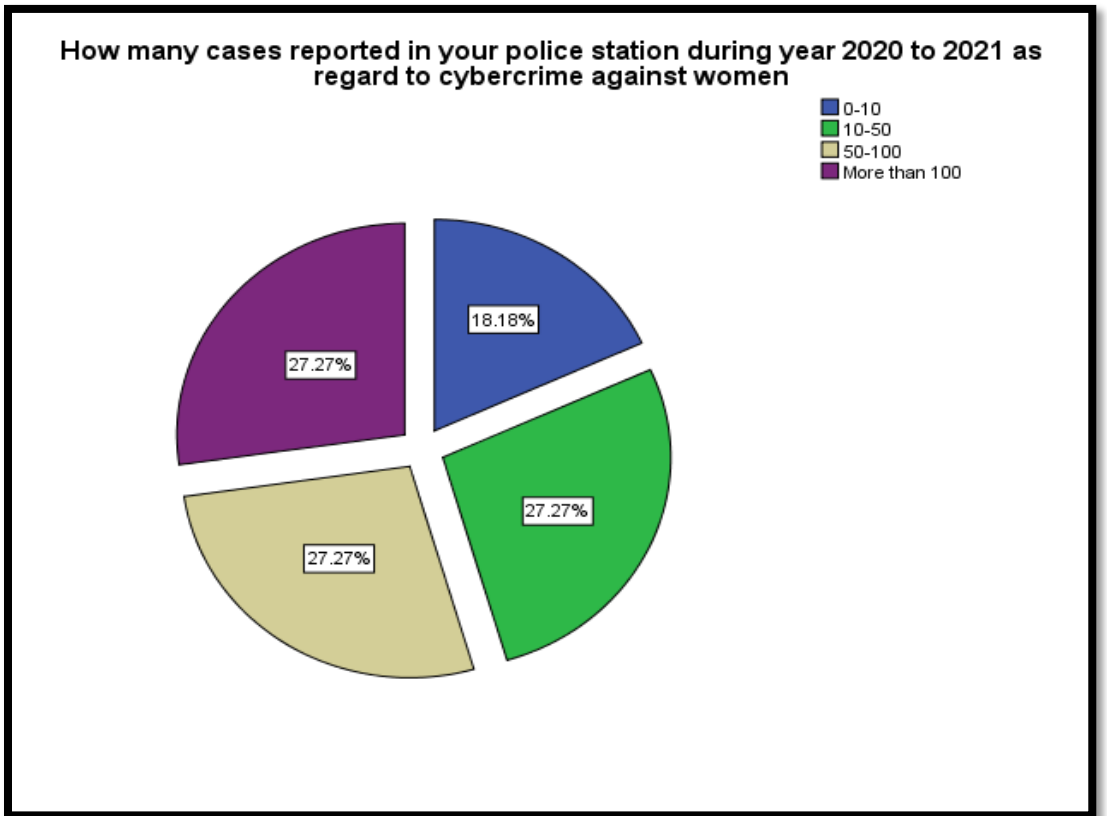


Figure No. 7.35

Above Table No. 7.35 and Figure No. 7.35 shows that 4 (18.2.%) has 0 to 10 cases, 6 (27.3%) has 10 to 50 registered cases, 6 (27.3%) police stations have 50 to 100 registered cases, 6 (27.3%) police stations have more than 100 registered cases. The researcher draws form this is average number of reported cases that only 18% police stations have less than or equal to 10 cases this year otherwise 27% police stations have 10 to 50 cases registered whereas 27% police station and 50 to 100 or more than 100 cases registered under these crimes in their police stations.

Question No.8: How many cybercrimes against women are recorded at online portal in your jurisdiction?

Table No. 7. 36

How many cybercrimes against women are recorded at online portal in your jurisdiction?					
S.No.	**Cases**	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	**0-10**	6	27.3	27.3	27.3
2	**10-50**	10	45.5	45.5	72.7
3	**50-100**	4	18.2	18.2	90.9
4	**More than 100**	2	9.1	9.1	100.0
	Total	22	100.0	100.0	

Source: Primary Data

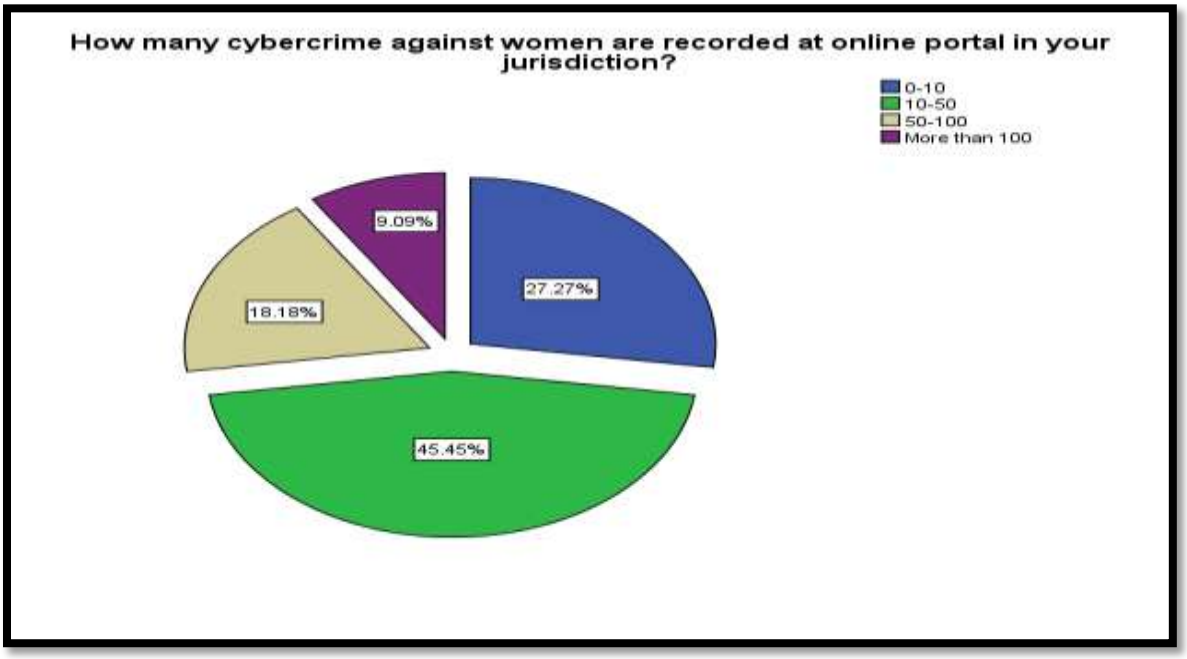


Figure No. 7.36

The above Table No. 7.36 and Figure No. 7.36 states that 27.27% police station reported cases between 0-10 through online platform, 45.45% respondents have 10-50 registered through online platform, 18.8% respondents registered 50-100 cases through online platform and only 9.09% police stations mentioned that more than 100 cases were registered through online platform. Researcher is also drawing from this data and comparing the previous question responses that although 27% police stations have reported more than 100 cases in this year but he percentage of online filing of such complaint is low to 9% only where further means there is a lack of awareness about the online platform or lack or required technical skills to file such complaints through online platform.

Question No.9: How many cyber cases were investigated by your police station?

Table No. 7.37

How many cyber cases were investigated by your police station					
S. No	**Cases**	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	**0-10**	0	0	0	0
2	**10-50**	10	45.5	45.5	45.5
3	**50-100**	4	18.2	18.2	63.6
4	**More than 100**	8	36.4	36.4	100.0
	Total	22	100.0	100.0	

Source: Primary Data

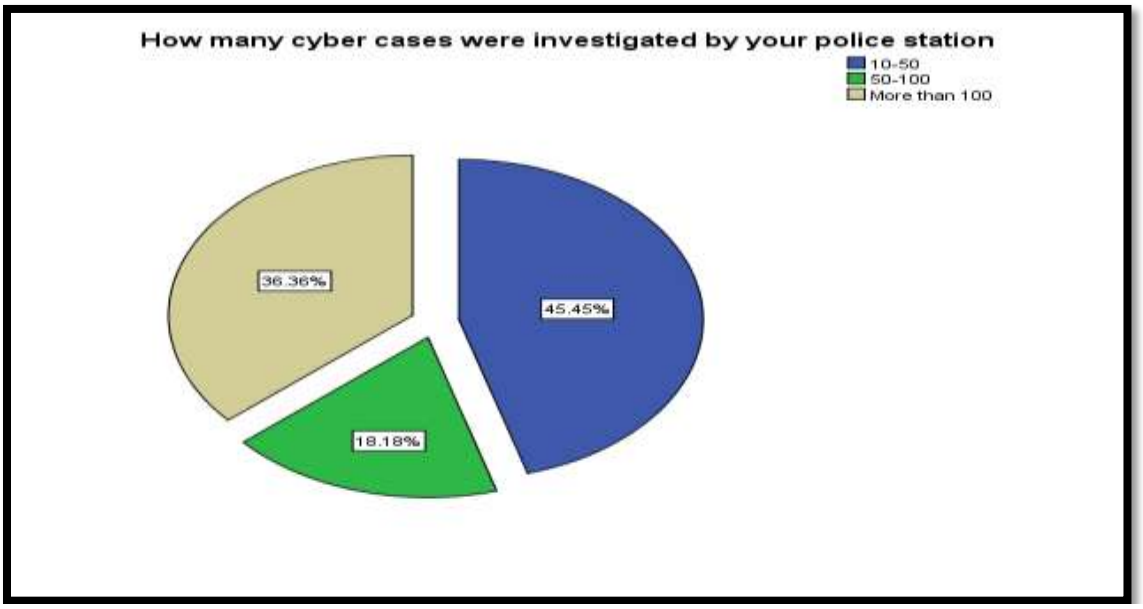


Figure No. 7.37

The Table No. 7.37 and Figure No. 7.37 states that 45.45% respondents investigated 10-50 cases in this year, 18.18% respondents investigated 50-100 cases in this year and 36.36% respondents investigated more than 100 cases this year. Researcher draws from this data that the police station having more cases has conducted more investigation.

Question No.10: In how many case the investigating officer file final report due to lack of evidences?

Table No. 7.38

In how many case the investigating officer file final report due to lack of evidences.					
S. No.	**Cases**	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	**0-10**	4	18.2	18.2	18.2
2	**10-50**	8	36.4	36.4	54.5
3	**50-100**	2	9.1	9.1	63.6
4	**More than 100**	8	36.4	36.4	100.0
	Total	22	100.0	100.0	

Source: Primary Data

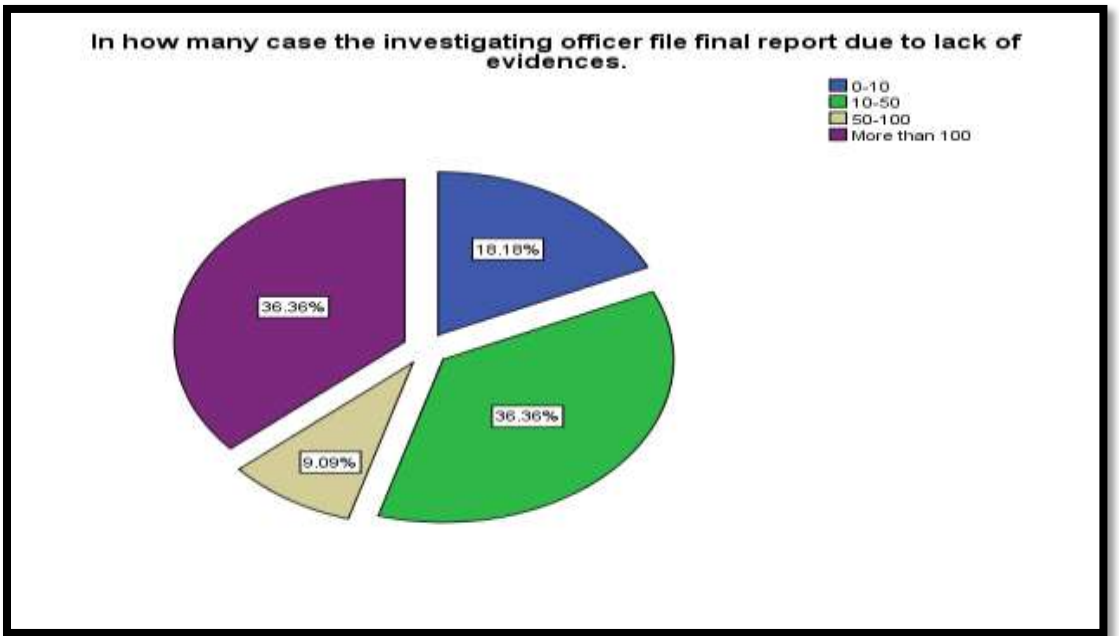


Figure No. 7.38

The Table No. 7.38 and Figure No.7.38 is stating the operational action taken by the police department for the investigation in the cyber-crimes where 4 (18.18%) respondents filed final report in 0-10 cases, 8 (36.36%) filed final report in 10-50 cases, 2 (9.09%) respondents file final report in 50-100 cases whereas 8 (36.36%) respondents file final report in more than 100 cases.

Question No. 11: In how many cases the investigation officer files charge sheet.

Table No. 7.39

In how many cases the investigation officer files charge sheet.					
S. No.	**Cases**	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	**0-10**	14	63.6	63.6	63.6
2	**10-50**	8	36.4	36.4	100.0
3	**50-100**	0	0	0	0
4	**More than 100**	0	0	0	0
	Total	22	100.0	100.0	

Source: Primary Data

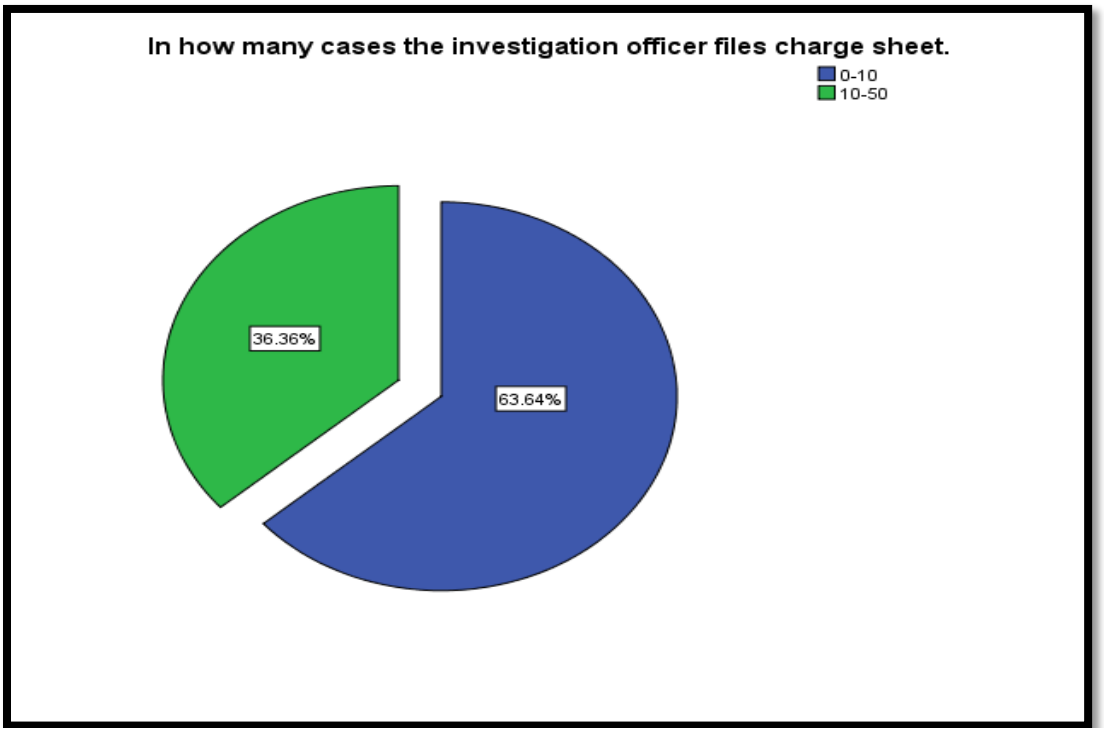


Figure No. 7.39

In Table No. 7.39 and Figure No. 7.39 the question stated about the operational action of filing a charge sheet in cases where 14 (63.62%) respondents mentioned that they filed the charge sheet in 0-10 cases where 8 (36.36%) stating that they filed charge sheet in 10-50 cases. Researcher draws from this data that majority of the cases where investigation started has filed the charge sheet, however this data also suggests that the average of the filing of charge sheet in number of cases is not uniform therefore not process dependent due to lack of skills and infrastructure as mentioned in earlier questions.

Question No.12: Whether cyber training programme were provided to police officer in Police Station

Table No. 7.40

Whether cyber training programme were provided to police officer in police Station					
S. No.	**Cases**	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
1	**Yes**	10	45.5	45.5	45.5
2	**No**	12	54.5	54.5	100.0
	Total	22	100.0	100.0	

Source: Primary Data

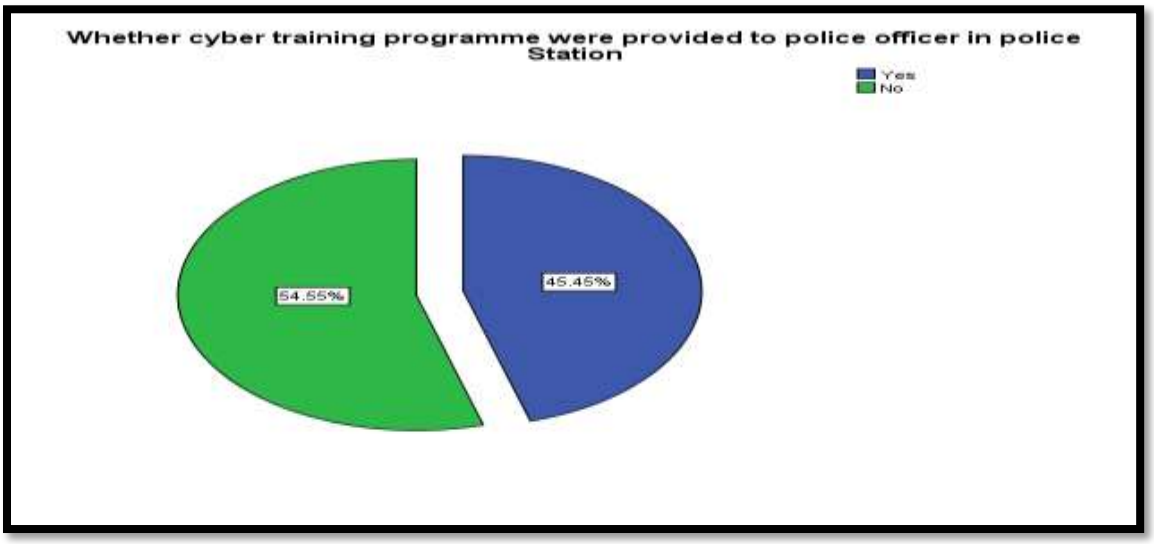
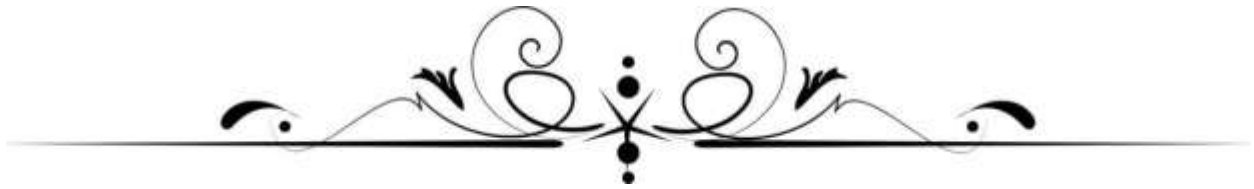


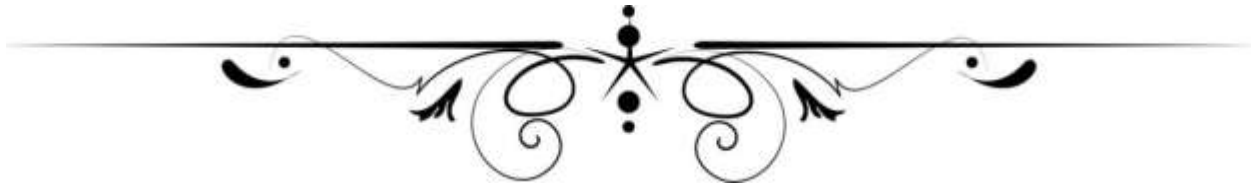
Figure No. 7.40

Above Table No. 7.40 and Figure No. 7.40 shows that 10 (45.5%) respondents said yes and 12 (54.5%) said no. Researcher also draws from the data that 45% police station does aware off the basic training programs and technical skills they required for handing such cases where as 55% respondents are not aware of the training programs conducted at police stations, they do not have any other technical assistance of specialist for the same.



CHAPTER-VIII

CONCLUSION AND SUGGESTIONS



CHAPTER- VIII

CONCLUSION & SUGGESTIONS

The invention of the computer and internet have brought enormous changes in our behavior and life and at the same time brings the dark side of internet such as cybercrime which makes the life of women miserable especially.

Crime against women is not a new phenomenon but due to the development of technology and the changing nature of crime, it deviated into cybercrime against women. The cybercrime against women rapidly increasing day by day and its form changes with the changing of the technology. The growth in internet access has accelerated due to the boom in access *via* mobile phone, and who make massive use of cyberspace are particularly vulnerable to cybercrime. On one side, the internet is serving as a boon, but on the other side, due to rising cybercrime in the virtual world, it has made the life of women insecure. The Internet and social media, changing and deviating the nature of such crime further where, internet is used as extraordinary vehicles for communication, information and citizen mobilization, but they can also give discrimination, hatred and violence to a voice. Women of all ages and milieu are in jeopardy with the coming up of internet. The revenge porn and blackmailing is one of the cybercrime against women which needs conceptual understanding and interpretation which seeks attention of the legislator to frame laws at national as well as at international level to curb this menace.

Cybercrime against women is increasing at a rapid rate globally, which is a serious concern for the whole world. With the rapid development of computer technology and internet over the years, the problem of cybercrime against women has assumed gigantic proportions and emerged as a global issue. In the information age, cybercrimes are growing impetuously and the digital strokes are changing the legal landscape globally. Legal means to control cybercrime was missing from all the legal system of the world until sporadic and then regional and collective legal response started coming up.

A rapid increase in the use of computer and internet has given rise to new forms of crimes like publishing sexually explicit materials in electronic form, video voyeurism and breach of confidentiality and leakage of data by intermediary, e-commerce frauds like personation commonly known as Phishing, identity theft and offensive messages

through communication services. So, penal provisions are required to be included in the Information Technology Act, 2000 the Indian Penal code, the Indian Evidence Act and the Code of Criminal Procedure, 1973 to prevent such crimes.

Women have always been the object of crime in India but now the crimes against women are increasing even in the virtual world. Sadly, the legal framework is not adequate yet to protect women from such crimes. Revenge porn and blackmailing to publish or distribute intimate image is one of such serious cybercrimes against women. Though, it is relatively new in India and its rise cannot be denied. It involves sharing of sexually explicit (private or nude) pictures of a person without consent. It is done basically by jilted ex-lovers or former partners to gain revenge and cause shame & intimidation to the victim. The revenge porn and blackmailing and related offences violate the rights of the women that are in general and right to privacy in particular.

The concept of privacy has been recognized throughout the world. It is an essential requisite of human personality embracing within it a high sense of morality, dignity, decency and value orientation. For preservation of the society, the moral and social value cannot be ignored. The importance of the concept of the right to privacy though not specifically not explicitly written in the constitution of India or in the statute, it is carved out through process of judicial interpretation can be appreciated. Thus, decisions discussed in chapter VI enable the researcher to conclude that courts have taken the cherished concept of right to privacy to a new and unprecedented height with zeal to translate the philosophy of right to life and personal liberty into reality.

The privacy right in India is still in a state of infancy and evolution. The development of new technologies posed a serious threat to the citizen's right to privacy.

In India, there is no specific law for regulating the cybercrime of revenge porn and blackmailing. Revenge porn and blackmailing is regulated by the way of various provisions of scattered laws, but it is not fully helpful for regulating the cybercrime of revenge porn and blackmailing. However, India does not have any direct law against revenge porn cybercrime. So, whenever such crimes take place, they are dealt with under the various provisions of the Information Technology Act, 2000 (Sections 66E, 67, and 67A) read with the provisions of the Indian Penal Code, 1860 (Sections 354A, 354C, 354D, 509). Cybersecurity expert *Dr. Pavan Duggal* stated that:

"While the lawmakers have to be complemented for their admirable work removing various deficiencies in the Indian cyber law and making it technologically neutral, yet it appears that there has been a major mismatch between the expectation of the nation and the resultant effect of the amended legislation. The most bizarre and startling aspect of the new amendments is that these amendments seek to make the Indian cyber-law a cybercrime friendly legislation; a legislation that goes extremely soft on cyber criminals, with a soft heart; a legislation that chooses to encourage cyber criminals by lessening the quantum of punishment accorded to them under the existing law; ..... a legislation which makes a majority of cybercrimes stipulated under the IT Act as bailable offences; a legislation that is likely to pave way for India to become the potential cybercrime capital of the world……"

After analyzing the above mentioned view of Pawan Duggal, a well known cybercrime expert in India, it can be assessed that there is no comprehensive law in India to tackle the cybercrime particularly cybercrime of revenge porn and blackmailing against women. Moreover, the traditional laws are also unable to provide the remedies to the victims of cybercrimes in India.

There is lack in legal system in meaningful response to demand for representation of cybercrime against women due to the unavailability of sufficient skilled lawyers working on issues of revenge porn and blackmailing cybercrime against women. On reflection of the legal provisions, it observed that there is lack of will power in the lobby of legislators to define revenge porn and blackmailing as existing in current techno-based world order as well as loopholes in legal discourse on the issue existing under Information Technology Act, 2000. Legislation should guarantee that the fundamental rights enumerated under the Indian Constitution, must be implemented as per the current and changing society. The patriarchal society is silences on the victims of this newly emerged crime. The fact that recognition and criminalization of revenge porn and blackmailing will help the society and authorities to understand that such behavior is unacceptable in democratic setup. When victims are confident in the legal system then, they will take a stand, instead of suffering in silence.

Hence, the course of action should be legal recognition of 'revenge porn' as a crime and formulation of an express provision which deals with it explicitly. This could be in similar vein as is the pattern followed by the British legal system, where an express criminal provision has been framed to deal with disclosure of private sexual photographs and films without the consent of the individual depicted and with the intent to cause distress, however tailoring it in accordance to India's socio-legal fabric. Further in, the researcher's, opinion since the crime of 'revenge porn' created a lawless situation and failed a multitude of victims in the dispensation of justice, the law made, should have retrospective application.

Internet operations being of global nature do not recognize any territorial boundaries. This enables the cyber criminals to operate beyond the national geographic limits without being physically present at the scene of crime. The problem of cyber crimes against women therefore, calls for greater international support and cooperation.

Though much has been done by the United Nations to muster cooperation of member nations to tackle the problem of cyber criminality as a common cause, the response from them has not really been very encouraging except that there is a general consciousness among the countries that where a cybercrime involving a foreign country or countries is involved, trans-border assistance and cooperation between the concerned countries is the only viable alternative to prevent and control such crimes.

The researcher concluded that, there was no specific multitude of supranational, international, state and regional laws, conventions, and norms concerned with the protection of privacy around the world. Which indicate that individual privacy is a universally cherished value with significant socio-political implications. Global civilization, having awakened seemingly overnight in an age of transparency, where individual privacy is more a perceived threat to communal well being than ever, now grapples with an aggressive reconfiguration of hitherto uncompromisable value.

Revenge porn and blackmailing cases are mushrooming in India. The concept of 'revenge porn' has been prevailing globally since 2010. On 06 Feb 2020 at an IAMAI event, *Shri Ravishankar Prasad*, Former Hon'ble Minister of Law and Justice; Communications; and Electronics and Information Technology, Government of India expressed his concern over this issue by saying "*Revenge porn is creeping in*

India...girlfriend and boyfriend split up... then what happens, platform is being abused..." Several Nation States have expressly criminalised revenge porn in their territories; however in India there exists no such legislation.

The research find out that victims of abuse of intimate image are normally female and that the impacts of this abuse of intimate images are highly gendered. It also finds that generally there are two types of perpetrators of intimate image abuse exist. Type one perpetrators share images anonymously on large pornography sites, with motivations largely unknown, and type two perpetrators use threats to share images as part of a broader pattern of coercive and controlling behaviour. Both types of perpetrator are predominately male. These patterns of victimization and perpetration support the need for the current intimate image abuse law to be adjusted.

As it is a well known fact that the crime of revenge porn and blackmailing are committed generally against women who are the soft target of the cybercrime, but it is a bitter truth that women victim of these cybercrime never came forward to register the case.

It is fact that, Honor related social norms prevent the victims of cybercrime to file the case against perpetrators. The researcher came to the conclusion after analysis of the collected data in chapter VII, that most of the respondent accepted the fact that the aggrieved women always faced most of time the family and society blaming the women victim for such crime as society considered that women by her presence of beauty, dressing, etc, provoked the criminals to commit the crime against women. The women are the co-partners (accomplice) of the crime and victim both here. The women are blamed for sexting, sharing of intimate images and other activities at social media, therefore, the reporting of such crime is very less but victimization is more.

Revenge Porn and related offences violate the right to privacy of the victims. Right to privacy is one of the precious fundamental rights conferred under Art. 19(1) (a) and Art. 21 of the Constitution of India, through the liberal interpretation of freedom of speech and expression and right to life by the Indian judiciary. The researcher, came into conclusion that revenge porn violates the right to privacy. Privacy is considered to be the extension of liberty of human beings. The protection of privacy requires the attention of

state and non-state actors, where the 'informational confidentiality' is linked with the private matters like sexual integrity, autonomy on the person's body.

There is plethora of laws for the protection of women against cybercrime, but there is Inadequacy of law specific to cybercrime affecting individuals especially targeting the women. Researcher in chapter IV and chapter V discussed the plethora of laws in India and internationally but their effectiveness to address the issue is lacking due to several reasons. The law addressing the cybercrime against generally and revenge porn and blackmailing specifically are inadequate. The researcher analysed under chapter IV traditional laws dealing specifically for crime against women i.e., Constitution of India, 1950; Indian Penal Code, 1860; Immoral Trafficking (Prevention) Act, 1956; The Dowry Prohibition Act, 1961, Domestic Violence Act, 2005; The Protection of Children From Sexual Offences Act, 2012 and Sexual Harassment of Women At Workplace, 2013 and critically analysed the Information Technology Act, 2000 *vide* amended in 2008 for protective laws for protection of women against cybercrime. International conventions, treaty, MoU of organizations and UN General Assembly resolution for protection of women from cybercrime specifically revenge porn and blackmailing. Researcher came to conclusion, that the laws are not defining cybercrime adequately due to which the rate of conviction is very low. The reason behind is the fast development of technology and the privacy policies of the internet platforms where the protection of the victim is not considered in terms of dignity and human rights but to facilitate the business model of the platforms.

There are no comprehensive laws in India which could deal with the cybercrime against women in general and revenge porn and blackmailing in particular. However, there are several laws but they are not considering the technicality involved while defining the crimes which provides the loophole for the escape of the accused as the procedural aspect of the legislations is not compatible in respect of technological infrastructure and skills required for the same. Under these edges laws are not addressing the subject matter of modern development like revenge porn and blackmailing under cybercrime against women.

The administration of criminal justice system is not acquainted and equipped with digital technology to provide justice to women victims of revenge porn and blackmailing

and to prevent them in future. The cybercrime and its severity is increasing day by day to combat this crime. A technically and legally sound criminal justice administration system is direly required. During the research, the researcher came into contact with the police administration system which is basically the investigating authority of the crime and the decision of the judiciary is based on the inquiry report & presentation of the case before court by the police authorities. The researcher during the research work contacted various authorities of the police stations to know the process of investigation of the cases of cybercrime particularly in the matter of cybercrime against women. The information was gathered from the police officials through questionnaire. After discussing with the police officers in the Lucknow, researcher did the analysis of the questionnaire filled by them in chapter VII filled by them. Where the primary data with police administration is collected is strongly suggesting that the technical skill, infrastructure and expert human resource for the same is lacking in the administrative agencies. The conclusion drawn by the researcher that the police lack the relevant training and understanding of technology behind revenge pornography to respond effectively against the crime.

SUGGESTIONS

1. There essential amendment should be made in The Information Technology Act, 2000 and The Protection of Children from Sexual Offences, 2012 to create revenge porn and blackmailing a new criminal offence under this Act.
2. Deterrent punishment for the proposed new offence of revenge porn and blackmailing should be inserted through amendment in The Information Technology Act, 2000 and The Protection of Children from Sexual Offences, 2012 to punish the accused of such offences. This may prevent the committing the offence in future and made an example for whole society.
3. With the changing nature of the technology, there is need to modernise the investigating agencies under Code of Criminal Procedure, 1973 empower them and facilitate cybercrime investigation activity without any fallibility.
4. "Cyber Police Cadre" should be created in every state which should be federally managed.

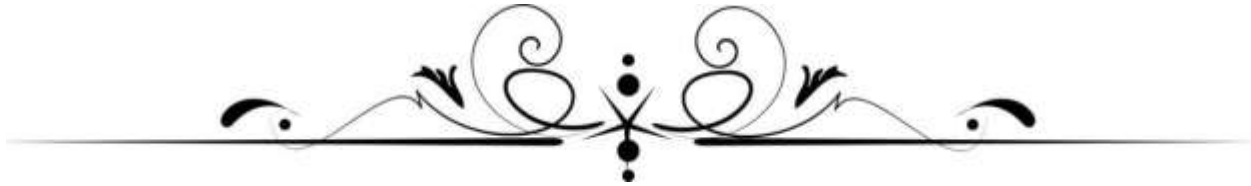
5. There is need of the hour to establish "cybercrime courts" in each and every district for the speedy disposal of the cases, which develop faith over judicial system.
6. Training on cyber crime against women with gender sensitization should be introduced so that the police can effectively respond to such cybercrime.
7. Free legal aid service should be provided to the women victim who fall prey to cybercrime.
8. There is a need for awareness-raising campaigns educating women and girls about cyber crime against women, their legal rights and the available support services.
9. The police administrative system should be made more well-equipped and trained in technology.
10. The "video hashing" technology is should be deployed to prevent re-uploading of content/ image/ videos.
11. Social media should deploy the Artificial Intelligence (AI) and machine learning tools to address the issues publication of intimate images.
12. Government should encourage women victims to report cybercrime when any revenge porn and blackmailing offence is committed against them.

The revenge porn and blackmailing case cannot be completely removed from the society. Complete alleviation of revenge porn and blackmailing under cybercrime against women is almost an impossible thing. But it could be mitigated by guarding themselves especially teen girls and women while using cyberspace. Some of the preventive and counter measures that can be adopt by women.

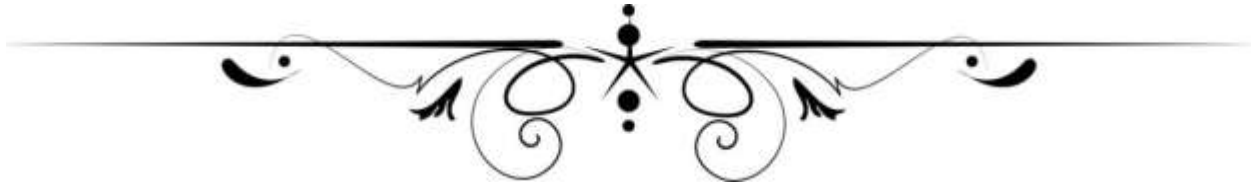
- ❖ They do not share intimate images & videos with anyone not even with their partners/ boyfriend.
- ❖ They can avoid taking explicit photos / pictures / shooting videos because these days no electronic devices are safe and it can be easily hacked.
- ❖ If any such cybercrime is committed against any women, first they should talk to their family and share the problem without any hesitation.
- ❖ If such cybercrime is committed against them, they must report the crime to the cyber police station or should file a complaint immediately at their nearest police station, give detailed information about all the crimes against them i.e., blackmail, coercion, harassment etc.

- If the image / picture or video appears on social media, immediately report it on that website and its organization. Revenge porn photo removal options are provided in most social media sites including Whatsapp, Facebook, Instagram, Twitter, Reddit, Snapchat etc. victim women can also check Cyber Civil Rights Initiative Comprehensive and learn to remove these posts online.
- Victim of revenge porn and blackmailing may ask search engines to remove the intimate image from different sites. For example, follow the instructions on the remove unwanted & explicit personal images from Google page.
- If any website has posted a picture without women victim consent and refuse to remove it, then victim can file a complaint to Federal Trade Commission (FTC) against the website and its parent organization.
- The first and foremost action should be to file a complaint with the Cybercrime cell as it will prevent the obscene material immediately from going viral. Also, it would help to find out the perpetrator in case of absence of knowledge.
- If women victim have any difficulties while filing a complaint at the police station, then she can call the National Commission for Women's helpline and explain the facts in details. The National Commission for Women will also assist with further legal matters.

Revenge Porn and blackmailing collectively are under-reported. Many were unaware of the fact that they were victimized. A culture of silence caused by victim shaming in the criminal justice system and society at large, forbid women from taking a stand. Having a defined law for these offenses would, in turn, bring recognition to these offenses. This would contribute to reducing victimization. Furthermore, there need to be provisions in the procedure in which these crimes are handled. A safe reporting system can be introduced by having trained qualified female counselors, to help the victims deal with the trauma along with, offering legal aid and counseling.



BIBLIOGRAPHY



BIBLIOGRAPHY

Primary Source

Legislations/ Statutes

- Abusive Behaviour and Sexual Harm (Scotland) Act, 2016
- Criminal Code Amendment (Private Sexual Material) Bill ,2015
- Protecting Canadians from Online Crime Act, 2014
- Summary Offences (Filming Offences) Amendment Act, 2013
- The California Penal Code, 1872
- The Constitution of India, 1950
- the Criminal Code Amendment (Private Sexual Material) Bill , 2015
- The Criminal Justice and Courts Act, 2015
- The Criminal Procedure Code, 1973
- The Dowry Prohibition Act, 1961
- the England and Wales Criminal Justice and Courts Act , 2015
- The Georgia Code
- The Harmful Digital Communications Act, 2015
- The Immoral Trafficking (Prevention) Act, 1956
- The Indecent Representation of Women (Prohibition) Act,1986
- The Indian Evidence Act,1872
- The Indian Penal Code, 1860
- The Information and Technology Act, 2000
- The Information and Technology(Amendment) Act, 2008
- the Justice Act (Northern Ireland), 2016
- The Protection of Children from Sexual Offence Act, 2012
- The Protection of Women from Domestic Violence Act, 2005
- The Sexual Harassment at Workplace (Prevention, Prohibition and Redressal) Act, 2013
- The Texas Penal Code, 1973
- The Vermont Statute

Draft, Convention and Policy

- Additional Protocol to The Budapest Convention, 2003
- Convention on Cyber Crime, 2001 (The Budapest Convention)
- Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence, 2011 (The Istanbul Convention)
- National Cyber Security Policy, 2013
- Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, 2000
- The Convention on Elimination of all form of Discrimination Against Women, 1979
- The Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse, 2007 (The Lanzarote Convention)
- The International Covenant on Civil and Political Rights, 1966
- The Universal Declaration of Human Rights, 1948
- United Nation Convention on the Rights of the Child, 1989
- United Nations Convention Against Transnational Organized Crime , 2000

Reports

- NCRB Report, 2016, 2020
- Global Strategic Report, 2016
- J. S. Verma Committee Report, 2013
- The Justice A. P. Shah Report, 2012
- The Wolfenden Committee Report, 1958

Secondary Sources

Books

- Agarwal, H.O., *International Organisations*, Central Law Publications, Allahabad, 2011.
- Allen, *Legal Duties Winfield, Province of Law of Tort,* Tagore Law Lectures, 1930.
- Augastine, Paul. T., *Computer Crime*, Crescent Publishing Corporation, 2007.
- Augastine, Paul. T., *Cyber Crime & Legal Issue*, Crescent Publishing Corporation, 2007.

- Bailey, J., Flynn, A. and Henry, N. (ed.), *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*, Emerald Publishing Limited, Bingley, 2021.
- Bajpai, G.S., *On Cyber Crime &Cyber Law*, Serials Publications, New Delhi, 2011.
- Barkha and Mohan, U. Rama, *Cyber Law & Crime: IT Act 2000 & Computer Crime Analysis* , Asia Law House, Hyderabad, 2006.
- Barua, Yogesh, *Cyber Surveillance and Security*, Dominant Publishers & Distributers Pvt. Ltd., New Delhi, 2012.
- Bist, Shruti, *Cybercrime against Women-Investigative & Legislative Challenges*, Blue Rose Publication, New Delhi, 2020.
- Chandrakala, N. B., and Priyadarsini, G. Indira (ed.), *Women Rights and Gender Justice,* Regal Publication, New Delhi, 2015.
- Chaubey, Manish Kumar, *Cyber Crimes & Legal Measures,* Regal Publication, New Delhi, 2013.
- Chaugh, Babita, Women and Crime, Rajat Publication, New Delhi, 2015.
- Chawla, Monica, *Gender Justice: Women and Law in India*, Deep & Deep Publication, New Delhi, 1st ed., 2006, Reprint 2013.
- Clough, Jonathan, *Principles of cybercrime*, Cambridge University Press, 2nd edn., 2015).
- Coora, Deepti and Merrill, Keith, *Cyber Cops, Cyber Criminals and the Internet*, IK Books, New Delhi, 2002.
- Dasgupta, M., *Cybercrime in India- A Comparative Study*, Eastern Law House, New Delhi, 1st ed. 2009.
- Dudeja, V. D., *Information Technology and Cyber Laws (A Mission with Vision),* Commonwealth Publication, New Delhi, 2001.
- Duggal, Pavan, *Cyber Law-An Exhaustive Section Wise Commentary on The Information Technology Act*, Universal Law Publishing, New Delhi, 2nd edn., 2017.
- Godbole, Nina and Belapure, Sunit, *Cyber Security: Understanding Cybercrimes, Computer Forensics and Legal Perspectives*, Wiley Publication, New Delhi, 2017.
- Goldsmith, Jack and Wu, Tim, *Who Controls the Internet*, Oxford University Press, New Delhi, 2006.
- Halder, Debarati and Jaishanker, K., *Cyber Crimes against Women in India*, New Delhi: Sage Publication, 2017.

- Halder, Debrati, *Child Sexual Abuse and Protection Laws in India*, Sage Publication, New Delhi, 2018.
- Hooper, Anthony, "General Principles of Criminal Responsibility" in Harris, *Criminal* Law, Sweet & Maxwell, London, 1968.
- Jain, Atul, *Cybercrime: Issues threats and Management*, Isha Books Publications, New Delhi, 2005.
- Jaswal, V. S and Jaswal, S. T., *Cyber Crime and Information Technology Act, 2000*, Regal Publication, New Delhi, 2014.
- Jyoti Ratan, *Cyber Laws & Information Technology*, (Bharat Law House, Delhi, 3rd ed., 2017.
- Kamath, Nandan, *Law Related to Computers Internet & E-Commerce*, Universal Law Publication, New Delhi, 4th ed., 2009.
- Klare, Hugh J., *Changing Concept of Crime and its Treatment*, Pergamon Press Oxford, 1st edn., 1960, reprint 1969.
- Lal Batuk, *Commentary on the INDIAN PENAL CODE, 1860*, Thomas Reuters, 3rdedn. 2016.
- Mali, Prashant, *Cyber Law & Cyber Crimes, Information Technology Act, 2000 With IT Rules, 2011*, Snow White Publication Pvt. Ltd., 2nd edn., 2015.
- Matthan, Rahul, *The Law relating to Computers and the Internet*, Butterworths India Publication, New Delhi, 2000.
- Merkow, Mark S. and Brietharyst, James, *The E-Privacy Imperative*, American Management Association, New York, 2002.
- Mishra, R.C., *Cyber-crime: Impacts in the New Millennium*, Author Press, New Delhi, 2002.
- Murtaza, Shahida, *Womens Human Rights: A Feminist Discourse*, Anmol Publication, New Delhi, 2015.
- Narwal, Nitu and Sharma, R.K., *Domestic Violence against Women: Legal Protection, Legislative and Judicial Aspect*, (Regal Publication, New Delhi, 2013.
- Newman, Robert. C., *Computer Security, Protecting Digital Resources*, Jhones and Bartlett Publishers, 2010.

- Nigam, R.C., *Law of Crimes in India, Principles of Criminal Law,* Asia Publishing House, Vol.1, 1956.
- Orji, Uchenna Jerome, *Cyber Security: Law and Regulation*, Wolf Legal Publisher, 2012.
- Ormerod, David C. and Lair, Karl, *Smith and Hogan's Criminal Law*, Oxford University Press, London, 2015.
- Paranjape, N. V., *Criminology and Penology*, Central Law Publication, Allahabad,14th edn., 2009.
- Polak, Sara and Trottier, Daniel (ed.), *Violence and Trolling on Social Media*, Amsterdam University Press, Netherland, 2020.
- Pradhan, R. K., *Cyber Crime and Cyber Terrorism*, Manglam Publication, Delhi, 2010.
- Rastogi Anirudh, *Cyber Law-Law of Information Technology and Internet*, 2nd ed. 2014.
- Rowbottom, Jacob, *Obscenity Laws and the Internet: Targeting the Supply and Deman,* Criminal Law Review, Sweet & Maxwell, London, 2006.
- Samuels, Darren and Rohsenow, Thomas, C*yber Security*, Arcler Press, 2015.
- Sathyanarayana, Matt. Bishop and Venkatramanayya, S., *Introduction To Computer Security,* Pearson Education,2009.
- Sharma, S.C., *Study of Techno- Legal Aspects of Cybercrime and Cyber Law Legislations*, 2nd ed., 2008).
- Sharma, Sunita, *Women and Crime*, Crescent Publishing Corporation, New Delhi, 2017.
- Sharma, Vakul, *Information Technology-Law & Practice*, Universal LexisNexis, 5th ed. 2016.
- Singer, P.W. and Friedman, Allan, *Cyber Security and Cyber War: What Everyone Need To Know*, Oxford University Press, 2014.
- Singh, A., *Constitution and Women's Rights*, Axis Book, New Delhi, 2013.
- Sinha Chanchal and Tyagi Prateeksha, "Women's Indecent Portrayal in Media" in *Vidya Jain and Rashmi Jain, Women Media and Violence*, Rawat Publication, New Delhi, 2016.
- Smith, J. C. and Hogan, Brian, *The Element of a Crime in Criminal Law,* Butterworth & co., 1988.
- Soni, Suman, *Women in 21st Centuary*, DND Publications, Jaipur, 2012.
- Spinello, Richard. A, *Cyber Ethics Morality and Law in Cyberspace*, Jones & Bartlett Learning, Burlignton, 6th edn. 2016.

- Srivastava, O. P., *Principles of Criminal Law*, Eastern Book Company, Lucknow,4th edn., 2005.
- Stephenson, Peter, *Investigating Computer- Related Crime*, CRC Press, Washington DC, 2000.
- Stewart, S. W, *A Modern View of the Criminal Law*, Pergamon Press, 1969.
- Talat Fatima, *Cyber Crimes,* Eastern Book Company, Lucknow, 2016.
- Tayal, Vimlendu, *Cyber Law Cybercrime Internet and E-commerce*, Bharat Law Publication, Jaipur, 2011.
- Tiwari, R. K. and Shastri, P. K., *Computer Crime and Computer Forensics*, BioGreen Books, New Delhi, 2002.
- Trivedi Tanuja, *Women Rights and Duties*, Jnanada Prakashan, Arunachal Pradesh, 2017.
- Tunner, J.W. C., *Kenny's Outline of criminal Law*, Cambrige University Press, London, 19th edn., 1966.
- Verma Amita, C*yber Crimes and Law*, Central Law Publication,1st ed.,2009.
- Verma, S.K. and Mittal Raman (eds.), *Legal Dimensions Of Cyber Space*, Indian Law Institute, New Delhi, 2004.
- Viswanathan, T., *The Indian Cyber Laws: with Cyber Glossary*, New Delhi, 2001.
- Williams, D., *Race, Ethnicity, and Crime: Alternate Perspective*, Algora Publication, United States, 2012.

Articles

- A Gillespie "Trust Me, It's only for me": "Revenge Porn" and the Criminal Law 11*Criminal Law Review* 866(2015).
- A Gillespie "Trust Me, It's only for me": "Revenge Porn" and the Criminal Law 11*Criminal Law Review* 866(2015).
- A. Levendowski, "Using Copyright to combat Revenge porn" 3*NYU Journal of Intellectual Property and Law* 422-446 (2014).
- Abbate, Janet. "Government, Business, and the Making of the Internet" 75 *The Business History Review* 147–176(2001).
- Afroditi Pina, "The Malevolent Side of Revenge Porn Proclivity: Dark Personality Traits and Sexist Ideology" 8(1) *International Journal of Technoethics* 31(2017).

- Al Habsi, and A. Butler, "Blackmailon Social media: what do we know and what remain unknown?" 34(3) *Security Journal* 525-540(2021).
- Allen,and L. Anita, "Gender and Privacy in Cyberspace" *Faculty Scholarship at Penn Law* 789(2000).
- Asoke Mukerji, "The Need for an International Convention on Cyberspace", 16 *Journal of International Relations and Sustainable Development, Pandemics & Geopolitics: The Quickening* 198-209 (SPRING, 2020).
- Barry M. Leiner and Vinton G. Cerf, *et al.*, "Brief history of internet" 39 *ACMSIG COMM Computer Review* 22-31(2009).
- Calvert "Revenge Porn and Freedom of Expression: Legislative Pushback to an Online Weapon of Emotional and Reputational Destruction" 24 *Fordham Intellectual Property Media and Entertainment Law Journal* 673(2013).
- D K Citron and M A Frank "Criminalising Revenge Porn" 49 *Wake Forest Law* 345-361(2014).
- D. Halder, "Examining the Scope of Indecent Representation of Women (Prevention) Act, 1986, In the Light of Cyber Victimization of Women in India," 11 *National Law Journal* 88-208(2013).
- D. Plater, "Setting the Boundaries of Acceptable Behaviour"? South Australia's Latest Legislative Response to Revenge Pornography" 2 *Uni SA Student Law Review* 1(2016).
- D. Reece Greenhalgh "Revenge Porn: Widening the Net?" *Criminal Law and Justice Weekly* (2016).
- Danielle K. Citron, "Cyber Mobs, Disinformation, and Death Videos: The Internet As It Is (And As It Should Be)" 118 *Michigan Law Review* 1073 (2020).
- Danielle Keats Citron and Mary Anne Franks, "Criminalizing Revenge Porn," 49 *Wake Forest Law Review* 346 (2014).
- E Poole "Fighting Back against Non-Consensual Pornography" 49 *USF Law Review* 181-184(2015).
- Eric Barendt, "Problems with the "Reasonable Expectation of Privacy" Test' 8(2*) Journal of Media Law* 129–37 (2016).

- Harpreet Singh Dalla and Geeta, "Cyber Crime-A Threat to Persons, Property, Government and Societies" 3 *International Journal of Advanced Research in Computer Science and Software Engineering* 235 (2013).
- Hate-Speech Protocol to Cybercrime Convention" 96(4), *The American Journal of International Law*, 973-975 (2002).
- Holly Hancock, " The Impact of The Image on Personal Life: Is Current Law out of Focus?" 13(1) *Journal of Media Law*, 54-80(2021).
- Ian Watson, *The Universal Machine: From the Dawn of Computing to Digital Consciousness* 89 (Springer, 2012).
- J. Humbach "How to Write a Constitutional "Revenge Porn" Law" 35 *PACE Law Review* 215(2014).
- Justine Mitchell "Censorship in Cyberspace: Closing the Net on Revenge Porn" 25(8) *Entertainment Law Review* 283- 283 (2014).
- Katherine A. Mitchell, "The Privacy Hierarchy: A Comparative Analysis of the Intimate Privacy Protection Act *vs.* the Geolocational Privacy and Surveillance Act", 73 *University Miami Law Review* 569 (2019).
- M. A. Franks, Criminalizing Revenge Porn: Frequently Asked Questions (*University of Miami School of Law, Working Article* (2013).
- M. Kamal, and W.J. Newman, "Revenge Pornography: Mental Health Implications and Related Legislation, 44 *Journal of the American Academy of Psychiatry and the Law* 359-367(2016).
- Mary Anne Franks, "Criminalising Revenge Porn: A Quick Guide" *Social Science Research Network* (2013).
- Mayura U. Pawar and Archana Sakure, "Cyberspace and Women" 8 *A Research, International Journal of Engineering and Advanced Technology* 1670 (2019).
- Michael Salter, "Responding to revenge porn: Challenging to online legal impunity" in L. Comella and S. Tarrant (eds.), *New Views on Pornography: Sexuality, Politics and The Law* (Westport, 2015).
- N. Henry and A. Powell, "Beyond the "Sext": Technology-Facilitated Sexual Violence and Harassment against Adult Women" 48 *Australian & New Zealand Journal of Criminology* 104(2015).

- Nicola Henry and Anastasia Powell, "Technology-Facilitated Sexual Violence, Trauma, Violence & Abuse" 19 *A Literature Review of Empirical Research* 195-208(2018)
- P. Baranetd., "On distributed communications, MIS. I-XI" *RAND Corporation Research Documents*, Aug. 1964.
- Pallvi Sharma, "Role of UN in Tackling Cyber Crime" 8(1), *International Journal of Research in Social Sciences*(2018).
- Paul Bernal, Data gathering, Surveillance and human Rights: Recasting the Debate, 1 *International Journal of Cyber Policy* 249(2016).
- Randy K. Lippert and Kevin Walby, "Governing through Privacy: Authoritarian Liberalism, Law and Privacy knowledge" 12 *Law Culture & Human* 329-333(2013).
- Ravi Kumar S. Patel and Dhaval Kathiriya, "Evolution of Cybercrimes in India" 2(4) *International Journal of Emerging Trends & Technology in Computer Science* 241 (2013).
- Rebecca Campbell, The Psychological Impact Of Rape Victims Experiences with Legal, Medical and Mental Health Systems" 63 *Americal Psychological Journal* 702(2008).
- Roni Rosenberg And Hadar Dancig Rosenberg, Reconceptualizing Revenge Porn, 63(199) *Arizona Law Review* 199-228(2021).
- Ruth Gavison, "Privacy and Limits of Law" 89 *Yale law Journal* 421-435(1980).
- S Bloom 'No Vengeance for 'Revenge Porn' Victims: Unravelling Why This Latest Female-Centric, Intimate-Partner Offense Is Still Legal, and Why We Should Criminalize It' 42 *Fordham Urban Law Journal* 234-237(2016).
- S W Brenner, "Cybercrime metrics: Old wine, new Bottles?" 9 *Virginia Journal Of Law and Technology* (2004).
- S. Warren and L. Brandeis, "The Right to Privacy" 4 *Harvard Law Review* 193(1890).
- Saloni Agrawal, "Online Sextortion" 6(1) *Indian Journal of Health, Sexuality & Culture Volume* 18(2020).
- Samantha Brunick, "Revenge Porn: Can Victims Get Images off the Internet" *United States Attorneys' Bulletin* (2016).
- Sangeeta Goel, "Third generation sexism in workplaces: Evidence from India" 24(3) *Asian Journal of Women's Studies*, 368-387(2018).

- Sanjay Jain and Saranya Mishra, "Scandalizing the judiciary: An analysis of the uneven response of the Supreme Court of India to sexual harassment allegations against judges", 18(2) *International Journal of Constitutional Law* 563-590 (2020).
- Shobhna Jeet, "Cyber-crimes against women in India: Information Technology Act, 2000", 47 *Elixir Criminal Law* 8891-8895(2012).
- Sidney M. Jourard, "Some Psychological aspect of Privacy" 31 *Law and Contemporary Problems* 307 (1966).
- Sophie Maddocks, From Non-consensual Pornography to Image-based Sexual Abuse: Charting the Course of a Problem with Many Names, 33(97) *Australian Feminist Studies* 345-361(2018).
- Thomas P Crocker, "From Privacy to Liberty: the Fourth Amendment after Lawrence" 57 *UCLA Law Review1,* 23(2009).
- U. Mayura and Archana Sakure, "Cyberspace and women", 8 *International Journal of Engineering and Advance Technology"* 1671 (2019).
- V. G. Cerf and R. E. Kahn, "A Protocol for Packet Network Interconnection" 5 *IEEE Trans. Comm. Tech.* 627-641(1974).
- Watney and Murdoch "The Evolution of Internet Legal Regulation in Addressing Crime and Terrorism," 2 *Journal of Digital Forensics, Security and Law* (2007).
- Watney, Murdoch, "The Evolution of Internet Legal Regulation in Addressing Crime and Terrorism" 2 *Journal of Digital Forensics, Security and Law* 3(2007).
- Zak Franklin, "Justice for Revenge Porn Victims: Legal Theories to Overcome Claims of Civil Immunity by Operators of Revenge Porn Websites" 102 *California Law Review* 1303-1307(2014).

Websites

- https://medium.com/@subhashpathirana/history-of-computer-7504d590f989.
- https://www.researchgate.net/publication/336700280_History_of_computer_and_its_generations. https://www.livescience.com/20718-computer-history.html.
- https://medium.com/@subhashpathirana/history-of-computer-7504d590f989
- https://www.internetsociety.org/wp-content/uploads/2017/09/ISOC-History-of-the-Internet_1997.pdf.

- www.jstor.org/stable/3116559
- https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html
- https://trai.gov.in/sites/default/files/PR_No.04of2020.pdf
- http://rchiips.org/nfhs/NFHS5 _FCTS/Final%20Compendium%20of%20fact%20sheets_India%20and%2014%20States _UTs%20(Phase-II).pdf .
- https://commons.erau.edu/jdfsl/vol2/iss2/3
- https://www.merriam-webster.com/dictionary/crime
- https://Www.Icsi.Edu/Media/Webmodules/Publications/Cyber_Crime_Law_And_Practice.Pdf
- https://www.researchgate.net/publication/265032559_Cybercrime_Metrics_Old_Wine_New_Bottles/link/5743026108ae298602ee6bd5/download.
- http://tnsja.tn.gov.in/article/Cyber%20Crime%20by%20KNBJ.pdf
- https://www.unodc.org/documents/congress//Previous_Congresses/10th_Congress_2000/017_ACONF.187.10_Crimes_Related_to_Computer_Networks.pdf
- https://www.bl.uk/collection-items/wolfenden-report-conclusion.
- https://www.jstor.org/stable/10.2307/26638194
- https://www.hidden-pockets.com/debarati-halder-legal-reourse-revenge-pornography-cyber-stalking/.
- http://www.asianlaws.org/cyberlaw/library/cc/what_cc.htm.
- https://ncrb.gov.in
- https://www.un.org/womenwatch/daw/vaw/voverview.htm#:~:text=The%20Declaration%20defines%20violence%20against,public%20or%20in%20private%20life'.
- https://www.un.org/sexualviolenceinconflict/wpcontent/uploads/2020/01/report/reporting-on-violence-against-women-and-girls-a-handbook-for-journalists/371524eng.pdf
- https://www.getinclusive.com/blog/crimewomen-brief-history-laws-us.
- https://www.devex.com/news/how-the-legal-system-is-failing-to-protect-women-and-girls-from-sexualviolence-89573
- https://www.nytimes.com/2001/11/25/magazine/virtual-rape.html.
- https://www.jstor.org/stable/24395601

- http://www.rollingstone.com/culture/news/the-most-hated-man-on-the-internet-20121113#ixzz3v3DNTckW
- https://nymag.com/news/features/sex/revenge-porn-2013-7/.
- *https://www.bustle.com/articles/91760-google-tackles-revenge-porn-by-pledging-to-remove-it-from-search-results-hooray.*
- https://www.thecut.com/2016/06/hillary-asked-how-shell-help-stop-revenge-porn.html#_ga=2.56867882.1811959676.1645281638-1339713292.1645281637.
- https://articles.ssrn.com/sol3/articles.cfm?abstract_id=2337998.
- https://www.monash.edu/__data/assets/pdf_file/0006/1981455/04_Evans.pdf
- https://www.monash.edu/__data/assets/pdf_file/0006/1981455/04_Evans.pdf.
- https://www.cybercivilrights.org/wpcontent/uploads/2016/09/Guide-for-Legislators-().’16.pdf
- https://www.researchgate.net/publication/324360144_Revenge_pornography_A_conceptual_analysis_Undressing_a_crime_of_disclosure.
- https://iisb.org/pdf/june2020/June_2020_Final.pdf
- http://saharareporters.com/2022/02/13/offence-sexual-blackmail-sextortion-and-revenge-porn-rights-and-remedies-victims-stanley
- http://links.jstor.org/sici?sici=0017-811X%2818901215%294%3A5%3C193%3ATRTP%3E2.0.CO%3B2-C
- https://lcp.law.duke.edu/.
- https://www.jstor.org/stable/pdf/795891.pdf?refreqid=excelsior%3Aa69621708b426c3274a05ea64b89984d&ab_segments=&origin
- https://doi.org/10.1080/17577632.2021.1933704
- https://doi.org/10.1080/ 17577632.2021.1933704
- http://links.jstor.org/sici?sici=0017-811X%2818901215%294%3A5%3C193%3ATRTP%3E2.0.CO%3B2-C
- https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20
- https://scholarship.law.upenn.edu/faculty_scholarship/789
- https://madrascourier.com/opinion/the-dangerous-rise-of-revenge-porn-in-india/
- https://www.igiglobal.com/gateway/article/178531#pnlRecommendationForm

- https://law.yale.edu/sites/default/files/area/center/isp/documents/danielle_citron_-_criminalizing_revenge_porn_-_fesc.pdf..
- www.Indianexpress.com/article/india/india-others/hisar-blackmail-rape-arrest-of-3-law-students-has-campus-in-turmoil/
- https://thewire.in/women/sulli-deals-github-delhi-police-fir
- http://www.legalserviceindia.com/artic les/etea.htm.
- https://www.uncitral.org/pdf/engl ish/texts/electcom/05 -89450_Ebook.pdf.
- http://www.majmudarindia.com/ pdf / Data%20Protection%20in%20India.pdf
- http://planningcommission.nic.in/reports/genrep/ rep_privacy.pdf
- https://pib.gov.in/PressReleasePage.aspx?PRID=1558130.
- https://wcd.nic.in/schemes-listing/2405.
- www.un.org/documents/ga/res/45/a45r121.htm.
- https://treaties.un.org/doc/Treaties/2000/ 05/20000525%2003-16%20AM/Ch_IV_11_cp.pdf.
- https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf.
- https://www.jstor.org/stable/10.2307/48573761
- https://rm.coe.int/prems-153621-gbr-2574-study-online-a4-bat-web/1680a4cc44.
- https://rm.coe.int/1680084822
- http://www.europarl.europa.eu/RegData/etudes/STUD/2016/556931 /IPOL_STU(2016)556931_EN.pdf
- www.un.org/documents/ga/res/45/a45r121.htm.
- www.uncjin.org/Documents/EighthCongress.html
- www.uncjin.org/Documents/congr10/15e.pdf
- www.unodc.org/pdf/ crime/a_res_55/res5563e.pdf
- http://daccessdds.un.org/doc/UNDOC/GEN/N01/482/04/PDF/N0148204.pdf
- https://www.unodc.org/pdf/crime/congress11/BangkokDeclaration.pdf.
- https://undocs.org/pdf?symbol=en/A/RES/64/21
- https://research.un.org/en /docs/ga/resolutions

- www.unodc.org/documents /treaties/organized_crime/EGM_cybercrime_2011/UNODC_CCPCJ_EG4_2011_3/UNODC_CCPCJ_EG4_2011_3_E.pdf.
- www.america.gov/st/washfile-english/2007/April/20070423135940 ajesrom0.709469.html.
- https://www.unodc.org/documents/organized-crime/E CN 15_2007_8.pdf.
- www.un.org/ecosoc/docs/2004/Resolution%202004-26.pdf.
- www.un.org/ecosoc/docs/2004/Resolution%202004-42.pdf.
- https://digitallibrary.un.org/record/657667?ln=en#record-files-collapse-header
- https://www.unodc.org/documents/ commissions/CCPCJ/CCPCJ_Sessions /CCPCJ_19/E-CN15-2010-CRP1_E-CN7-2010-CRP6/E-CN15-2010-CRP1_E-CN7-2010-CRP6.pdf
- www.unodc.org/unodc/en/frontpage/2011/May/unodc-and-itu-to-cooperate-moreclosely-to-make-the-internet-safer.html.
- www.itu.int
- www.itu.int/wsis/documents/ doc_multi.asp?lang=en&id=1160|0
- www.itu.int/wsis /documents/doc_multiasp?lang=en&id=2267|0
- www.itu.int/osg/csd/cybersecurity/pgc/2007/events/docs/meetingreport.pdf
- www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/WSIS_Action_Line_C5_Meeting_Report_June_2008.pdf
- www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html
- www.itu.int/osg/csd/cybersecurity/gca/hleg/index.html.
- www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.
- www.itu.int/ITU-D/cyb/events/2009/santo-domingo
- https://peacemaker.un.org/sites/peacemaker.un.org/files/SC_ResolutionWomenPeaceSecurity_SRES1325%282000%29%28english_0.pdf.
- https://documents-dds-ny.un.org/doc/UNDOC/LTD/N13/576/77/PDF/N1357677.pdf?OpenElement.
- http://ap.ohchr.org/documents/ dpage_e.aspx?si=A/HRC/RES/32/13
- https://digitallibrary.un.org/record/ 1641160?ln=en
- file:///C:/Users/user/Downloads/A_HRC_38_L.33-EN.pdf.

- http://digitallibrary.un.org/record/ 845728.
- https://www.legislation.gov .uk/ukpga/2015/2/enacted/data.pdf
- https://www.eccourts. org/wp content/files_mf/1359389407_magicfields_pdf_file_upload_1_1.PDF.
- http://www.assembly.gov.vc/assembly/images/stories/ cybercrime%20bill%202016.pdf.
- https://ec.europa.eu/antitrafficking/sites/antitrafficking/files/criminal_code_germany_en_1.pdf
- https://www.law360.com/articles/499212/israel-criminalizes-revenge-porn-in-new-bill
- https://harvardlawreview.org/2020/05/state-v-vanburen/
- https://www.phoenixnewtimes.com/news/az-revenge-porn-law-not-to-be-enforced-says-federal-judge-7486054
- http://www.theboltonnews.co.uk/news/bolton/14539021
- https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/16714/index.do
- http://www.cps.gov.uk/news/latest_news/prosecutors_being_advised_to_learn_from_revenge_porn_cases/.
- https://hansard.parliament.uk/lords/2016-11-16/debates/DE488DE7-5743-45D2-9EB1-6C8AEEF6908E/PolicingAndCrimeBill.
- http://www.cyberlaw.org/cybercrimes.
- https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0131&from=EN
- https://www.livelaw.in/news-updates/roadies-bigg-boss-winner-ashutosh-kaushik-moves-delhi-high-court-for-right-to-be-forgotten-177933
- https://indiankanoon.org/doc/6266786/.
- https://www.criminaldefenselawyer.com/resources/revenge-porn-laws-penalties.htm.
- https://globalfreedomofexpression.columbia.edu/cases/state-of-west-bengal-v-boxi/

Journals

- European Criminal Law Journal
- Indian Bar Journal
- Journal of Minorities Rights
- Seminar Journal
- International Journal of Scientific & Engineering

- Allahabad Law Journal
- Andhra Law Times
- Journal of Indian Law Institute
- Criminal Law Journal

News Papers

- The Hindu
- The Times of India
- The Indian Express
- The Tribune
- Amar Ujala (Hindi)
- Hindustan Times
- Nav Bharat (Hindi)

ANNEXURES

ANNEXURE-I

Consent form

"Revenge Porn and Blackmailing under Cybercrime against Women in India: A Socio-Legal Study in Lucknow City"

Hello, my name is 'Irshad Ahmad'; I am research scholar in the Department of Law, School of Legal Studies, Babasaheb Bhimrao Ambedkar (A Central) University, Lucknow. I am working on thesis titled **"Revenge Porn and Blackmailing under Cybercrime against Women in India: A Socio-Legal Study in Lucknow City"** under the supervision of **Prof. Sudarshan Verma**, Department of Law, SLS, BBA University, Lucknow.

The purpose of the questionnaire is to collect information for academic purpose.

I assure you that all the information provided by you, will kept confidential and will be used for academic purpose only.

I therefore, humbly request you to kindly spare your valuable time and share your views by filing up the following questionnaire.

Regards

Irshad Ahmad
Research scholar
Department of Law, BBAU
Contact No.09335282933
Email add.: adv.irshadahmad@gmail.com

Do you agree to participate in this study?

Yes [ ]

No [ ]

Respondent Profile

Name:……

Age:

17 and under [ ]

18-24 [ ]

25-34 [ ]

35 and over [ ]

Gender:

Male [ ]

Female [ ]

Transgender [ ]

Marital Status:

Married [ ]

Unmarried [ ]

Education:

High School [ ]

Intermediate [ ]

Graduate [ ]

Post Graduate [ ]

Doctorate [ ]

other ……....

Occupation:

City:

Email Id:

Mobile No. (Optional):

Kindly read the questions carefully and select one of the responses given against each of them by tick marking (√)

1. Are you aware about "cybercrime"?

Yes **[ ]**

No **[ ]**

Not sure **[ ]**

2. Do you know Right to privacy has been enshrined under Article 21 of the Constitution of India as Fundamental right?

Yes **[ ]**

No **[ ]**

Not sure **[ ]**

3. The privacy in virtual world as well as in real life literally shrinking

Strongly Agree **[ ]**

Agree **[ ]**

Neutral **[ ]**

Disagree **[ ]**

Strongly Disagree **[ ]**

4. Women and children were more prone to obscene cybercrime.

Strongly Agree **[ ]**

Agree **[ ]**

Neutral **[ ]**

Disagree **[ ]**

Strongly Disagree **[ ]**

5. Women in India make most vulnerable target on the internet due to their gender and the consumability of image of Indian women as porno- materials.

Strongly Agree [ ]
Agree [ ]
Neutral [ ]
Disagree [ ]
Strongly Disagree [ ]

6. Social norms and orthodox values prevent the victim and their family member to report the cybercrime against women.

Strongly Agree [ ]
Agree [ ]
Neutral [ ]
Disagree [ ]
Strongly Disagree [ ]

7. Whether you are familiar with term Revenge Porn and Blackmailing

Yes [ ]
No [ ]
Not sure [ ]

8. if yes, I have learn about it from

University [ ]
Friends [ ]
Internet source [ ]
News channel/ print media [ ]
Other Channel (i.e., Conference/seminar/special events) [ ]

9. Do you able to describe what revenge porn and blackmailing is to someone else.

Yes [ ]
No [ ]
Not sure [ ]

10. Social media play a vital role for increasing the cybercrime against women

Strongly Agree **[ ]**

Agree **[ ]**

Neutral **[ ]**

Disagree **[ ]**

Strongly Disagree **[ ]**

11. The women experience revenge porn cybercrime from known people such as acquaintances, friends and/or family member

Strongly Agree **[ ]**

Agree **[ ]**

Neutral **[ ]**

Disagree **[ ]**

Strongly Disagree **[ ]**

12. Whether you or person known to you are threatened / blackmailed that your intimate picture/ video would be distribute and shared publically.

Yes **[ ]**

No **[ ]**

Not Sure **[ ]**

13. Whether revenge porn and blackmailing offence committed against you/ person known to you.

Yes **[ ]**

No **[ ]**

Not Sure **[ ]**

14. Do you know who 'leaked' your picture/ video?

Yes **[ ]**

No **[ ]**

Not Sure **[ ]**

15. if yes, tell us who

A boyfriend/ partner **[ ]**

An ex boyfriend/ partner **[ ]**

A friend **[ ]**

A social media follower **[ ]**

A stranger **[ ]**

Other please specify:…….

16. How did you find out about it

I discovered it **[ ]**

A friend told me **[ ]**

My boyfriend /partner told me **[ ]**

A colleague told me **[ ]**

A social media follower told me **[ ]**

Someone on an app told me **[ ]**

Other (please specify):……..

17. Where was your picture / video shared ?

On social media **[ ]**

On whatsapp group or by message **[ ]**

By email **[ ]**

Uploaded to a porn site **[ ]**

On a blog/ website **[ ]**

It was shared to someone in person **[ ]**

Others(please specify):……..

18. A victim of revenge porn and blackmailing is to blame for the sharing of her image or videos.

Strongly Agree **[ ]**

Agree **[ ]**

Neutral **[ ]**

Disagree **[ ]**

Strongly Disagree **[ ]**

19. Whether consent to have filmed sexual activity is consent to publish it online.

Strongly Agree **[ ]**

Agree **[ ]**

Neutral **[ ]**

Disagree **[ ]**

Strongly Disagree **[ ]**

20. Are you aware of "the Information Technology Act, 2000"

Yes **[ ]**
No **[ ]**
Not sure **[ ]**

21. Do you know the National Cyber Crime Report portal where cybercrime against women can be reported online

Yes **[ ]**
No **[ ]**
Not sure **[ ]**

22. If you come across a cybercrime, how would you report to it?

Report online **[ ]**
Inform the police **[ ]**
Inform the cyber cell 152260 **[ ]**
Talk to family or friends **[ ]**
Keep silence **[ ]**

23. If reported, whether police has taken action against accused

Yes **[ ]**
No **[ ]**
Not Sure **[ ]**

24. Have you ever experience any of these cybercrime commission

Revenge porn **[ ]**

Sextortion **[ ]**

Email harassment **[ ]**

Trolling **[ ]**

Fake avatar **[ ]**

Online stalking **[ ]**

Any other……

25. In your own words, tell us what happened:

……

……

……

……

……

Any Suggestion:……

……

……

……

.....

ANNEXURE-II

Questionnaire for Police Station Lucknow City

Hello, my name is 'Irshad Ahmad'; I am research scholar in the Department of Law, School of Legal Studies, Babasaheb Bhimrao Ambedkar (A Central) University, Lucknow. I am working on thesis titled **"Revenge Porn and Blackmailing under Cybercrime against Women in India: A Socio-Legal Study in Lucknow City"** under the supervision of **Prof. Sudarshan Verma**, Department of Law, SLS, BBA University, Lucknow.

The purpose of the questionnaire is to collect information for academic purpose.

I assure you that all the information provided by you, will kept confidential and will be used for academic purpose only.

Regards

Irshad Ahmad
Research Scholar
Department of Law, BBAU
Contact No.09335282933
Email add.: adv.irshadahmad@gmail.com

Details of Police Station.

Name of Police Station:

Name of SHO

Area:

Jurisdiction**:**

Kindly read the questions carefully and give response accordingly.

1. Do you know the term Revenge Porn and Blackmailing.

   Yes **[ ]**

   No **[ ]**

2. Do you know the under which section the offence of Revenge Porn and Blackmailing lies.

   Yes **[ ]**

   No **[ ]**

3. Do you know the investigation procedure for cyber offence committed against women?

   Yes **[ ]**

   No **[ ]**

4. Does the cybercrime against women complaint record and investigated by women police officer in police station

   Yes **[ ]**

   No **[ ]**

5. Whether you are well equipped with the technologies to fight the cybercrime against women

   Yes **[ ]**

   No **[ ]**

6. Are you satisfied with the tools and techniques provided by the government to deal with cybercrime specifically?

   Yes **[ ]**

   No **[ ]**

7. How many cases reported in your police station during year 2020 to 2021 as regard to cybercrime against women?

   0-10 [ ]

   10-50 [ ]

   50-100 [ ]

   More than 100 [ ]

8. How many cybercrime against women are recorded at online portal in your jurisdiction?

   0-10 [ ]

   10-50 [ ]

   50-100 [ ]

   More than 100 [ ]

9. How many cyber cases were investigated by your police station

   0-10 [ ]

   10-50 [ ]

   50-100 [ ]

   More than 100 [ ]

10. In how many case the investigating officer file final report due to lack of evidences.

    0-10 [ ]

    10-50 [ ]

    50-100 [ ]

    More than 100 [ ]

11. In how many cases the investigation officer files charge sheet.

    0-10 [ ]

    10-50 [ ]

    50-100 [ ]

    More than 100 [ ]

12. Whether cyber training programme were provided to police officer in police Station

    Yes **[ ]**

    No **[ ]**

    Not Sure **[ ]**

13. When offence revenge porn committed and reported in your police station what is your first step.

    ……

    ……

    ……

14. What is done by you to stop the circulation of exotic/ explicit material in cyberspace

    ……

    ……

    ……

    ……

15. Any Suggestion;

    ……

    ……

    ……

    ……

    ……

Curiginal

Document Information

Analyzed document	irshad final thesis.docx (D138440328)
Submitted	2022-05-30T07:52:00.0000000
Submitted by	O. P. Saini
Submitter email	gbl.bbau@gmail.com
Similarity	7%
Analysis address	gbl.bbau.bbau@analysis.urkund.com

Sources included in the report

W	URL: https://www.researchgate.net/publication/344153821_CYBER_CRIME_AGAINST_WOMEN_RIGHT_TO_PRIVACY_AND_OTHER_ISSUES Fetched: 2020-12-22T23:14:36.9400000	14
W	URL: https://internetlegalstudies.com/category/cyber-crimes-against-women-2/page/2/ Fetched: 2022-01-19T17:12:12.2030000	13
W	URL: https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2486125_code2288059.pdf?abstractid=2486125 Fetched: 2022-05-03T09:52:57.9130000	3
W	URL: https://sflc.in/sites/default/files/wp-content/uploads/2012/07/eBook-IT-Rules.pdf Fetched: 2019-09-26T09:24:34.9070000	19
W	URL: https://www.ijlmh.com/wp-content/uploads/2019/03/Cyber-Crimes-against-Women-A-Gloomy-Outlook-of-Technological-Advancement.pdf Fetched: 2020-01-31T07:09:40.5600000	6
W	URL: https://www.sciencedirect.com/topics/computer-science/cybercrime Fetched: 2019-11-30T04:24:48.7870000	3
W	URL: https://www.ie-ei.eu/IE-EI/Ressources/file/biblio/CriticalLookattheRegulationofCybercrime.doc Fetched: 2019-10-31T15:55:56.7530000	1
W	URL: https://ijirt.org/master/publishedpaper/IJIRT154098_PAPER.pdf Fetched: 2022-05-19T13:48:45.5030000	9
W	URL: https://www.ijlmh.com/wp-content/uploads/Infobahn-Related-to-Matron.pdf Fetched: 2021-09-27T04:45:53.8170000	67
W	URL: https://www.coe.int/en/web/cyberviolence/cyberviolence-against-women Fetched: 2021-07-21T19:16:23.9900000	3
W	URL: https://www.linkedin.com/pulse/revenge-porn-legal-remedies-cyber-crime-driven-vengeance-rajesh Fetched: 2022-05-30T07:52:30.5670000	1
W	URL: https://feminisminindia.com/2016/12/07/image-based-sexual-abuse-or-revenge-porn/ Fetched: 2021-05-16T14:37:07.8070000	1

W	URL: https://js.ugd.edu.mk/index.php/BSSR/article/download/3578/3239/ Fetched: 2021-11-03T16:04:05.8730000	4
W	URL: https://www.maravipost.com/the-offence-of-sexual-blackmail-sextortion-and-revenge-porn-the-rights-and-remedies-of-victims-by-stanley-alieke/ Fetched: 2022-05-30T07:52:36.2000000	5
W	URL: http://www.sethassociates.com/wp-content/uploads/2008/08/Women-and-Cyber-Crime.pdf Fetched: 2021-08-25T06:25:52.4870000	17
W	URL: https://www.ijlmh.com/wp-content/uploads/Privacy-in-Digital-Era-Blackmailing-Revenge-Porn-and-its-Relevant-Laws-in-India.pdf Fetched: 2022-04-15T01:16:23.0030000	1
W	URL: https://blog.ipleaders.in/everything-about-cybercrimes-against-women/ Fetched: 2021-12-26T10:45:13.3800000	1
W	URL: https://infosecawareness.in/concept/women/cyber-laws-in-india Fetched: 2021-10-03T03:35:29.9530000	3
W	URL: http://lawjusticepublishing.com/book.asp?pid=43 Fetched: 2022-05-30T07:52:33.0600000	1
W	URL: https://rm.coe.int/gender-mainstreaming-toolkit-15-gender-equality-and-cybercrime-cybervi/168092e9b4 Fetched: 2020-04-13T10:22:48.9230000	2
W	URL: https://www.mediadefence.org/ereader/wp-content/uploads/sites/2/2020/12/Module-7-Cybercrimes.pdf Fetched: 2021-04-30T20:01:59.1670000	1
W	URL: https://eige.europa.eu/sites/default/files/documents/cyber_violence_against_women_and_girls.pdf Fetched: 2020-01-31T07:10:08.3900000	5
W	URL: https://www.cigionline.org/documents/1961/SaferInternet_Paper_no_2_SuBHPxy.pdf Fetched: 2021-09-18T14:25:27.9100000	5
W	URL: https://www.schindlers.co.za/2020/south-africa-cracks-down-on-revenge-porn/ Fetched: 2022-05-30T07:52:32.9300000	1
W	URL: https://en.wikipedia.org/wiki/Revenge_porn Fetched: 2019-12-20T16:42:09.0130000	7
W	URL: http://www.mjilonline.org/no-more-revenge-criminalizing-non-consensual-pornography-through-the-convention-on-cybercrime/ Fetched: 2020-11-25T19:26:24.9500000	1
W	URL: https://blog.ipleaders.in/victim-revenge-porn/ Fetched: 2021-08-31T07:48:57.5670000	1

URL: https://indiankanoon.org/search/?

W	formInput=section%2066a%20information%20technology%20act+doctypes:judgments Fetched: 2020-01-05T09:32:10.2370000	1
W	URL: https://lawpanch.com/revenge-porn-is-one-type-of-cyber-crime/ Fetched: 2021-11-21T11:06:52.0400000	1
W	URL: http://cybercrimejournal.com/Starr&Lewisvol12issue2IJCC2018.pdf Fetched: 2022-03-24T13:52:55.8200000	2
W	URL: https://www.nujssacj.com/post/the-menace-of-revenge-porn-not-just-an-act-of-harassment-but-also-of-violation-of-right-to-privacy Fetched: 2021-08-31T08:10:19.9730000	3