Asian Journal of Social Science and Management Technology
ISSN: 2313-7410
Volume 4, Issue 3, May-June, 2022
Available at www.ajssmt.com

An Analytical Study Relating to the Legal Dimensions against Cyberviolence in India

(Special Reference in retaliation to porn and blackmailing on the Internet)

Ms. Deepali Rani Sahoo[1], Dr. Pooja Kapoor[2]

Assistant Professor, Symbiosis Law School, Noida, Symbiosis International (Deemed University).

Abstract: Cybercrimes can involve criminal activities that are traditional in nature, such as Hacking, fraud, Phishing, Cyberstalking, Identity stealing,Cyber Extortion, Pornography, Blackmailing, Software piracy, defamation and mischief, all of which are subject to the Indian Penal Code. The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the Information Technology Act, 2000.Our research paper gives a bird eye view relating to the legal dimensions towards cybercrime in India. It also gives special reference to the cybercrime relating to pornography and blackmailing through internet. The study of area has been taken in to consideration of certain cases from Delhi NCR region for the proper study.

Keywords: Doxing, Sexualised extortion, creepshots, up skirting, digital voyeurism, UNCITRAL Model Law, Cyberbullying

1. Introduction

It is believed that the first recorded cybercrime took place in the year 1820. This can be true with the fact that, computer did exist since 3500 BC in India, China and Japan.The modern computer began with the analytical engine of Charles Babbage.Cybercrime is a crime involving computers or digital devices, in which a computer can be eithera target of the crime, a tool of the crime or contain evidence of the crime. Since most informationprocessing these days depends on the use of information technology, the control, prevention andinvestigation of cyber activities is paramount to the success of the Organizations, Government'sagencies and individuals. The procurement and retention of highly skill cybercrime expert byGovernment and Business Enterprises cannot be overemphasized.This will ensure compliancewith international acceptable standard of usage of computer and other technological devices inthework places.Although prevention as they say is better than cure, irrespective of the deterrent measures toprevent and or control cybercrime, there may still be breaches, where this occur. Forensics experts will be called in to conduct thorough digital forensic investigations, analysis, documentation, and reconstruction of the crime scene, as well as present the evidence of the findings to the appropriate authorities or jury which could result in the culprit's arrest, prosecution, and conviction.The Internet is basically the network of networks used across for communication and sharing of data. Cybercrime also known as the computer crime is the use of an instrument for illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identitiesor violating privacy. In the last decade, victimisation of women has taken a different dimensiondue to misuse of digital communication technology which has nowbecome a new way for perpetrators to harasswomen. Cyber victimisation ofwomen can be categorised into two main groups: textual victimisation andgraphical victimisation. Graphical victimisation may include producing, creatingor publishing obscene, derogatory, and

pornographic, including revengepornographic materials on the web to shame the victim. Assuming that theimpact of cyber graphical victimisation can be devastating on women andgirls, many policies making bodies, including the European Union, had framedpolicies and guidelines to create laws to penalise creation, productionand publication of child pornographic materials.

2. Objective of the Research

- The main objective of the research is to find out the way or reason of doing any crime related to cyber.
- To illustrate the various terminologies related to the Cyberviolence.
- To identify the laws relating to cybercrime related to releasing of porn videos and blackmailing on the websites.
- To appraise the legal framework both internationally and nationally.
- To discover the protection to a person by the court of law if the porn video is released on any porn sites.

3. Scope of the Research

To complete the study on the cyberviolence related to retaliation of porn and taking revenge by blackmailing on internet. The article begins with a conceptual exploration of the causes and impacts of cyberviolence and move on to presenting the views of individuals who have been involved in the surrounding debate in some capacity or other.The case studies and samples will be collected from Noida to places coming under the jurisdiction and limitations of Delhi NCR. Data collected will be systematically and logically analysis, where possible we may come up with hypothesis for further testing, proof or disproof existing hypothesis and conclude with ourobservations and recommendations related to cyberviolence.

4. Literature Review

- Catherine D. Marcum and George E. Higgins Cybercrime in, Krohn, M. D., Hendrix, N., Penly Hall, G., & Lizotte, A. J. (Eds.). (2019). *Handbook on Crime and Deviance. Handbooks of Sociology and Social Research.* Cybercrime is the “destruction, theft, or unauthorized or illegal use, modification or copy of information, programs, services, equipment or communication network”.
- According to Council of Europe “any criminal offence committed against or with the help of a computer network is identified as cybercrime”. Computer or computation related device is an essential for cybercrime perpetration and victimization. No country is immune as cybercrime is a worldwide problem.
- ‘Computer crime or cybercrime is a form of crime where the Internet or computers are used as a medium to commit crime’. Shabnam, N., Faruk, M. O. and Kamruzzaman, M. (2016). Underlying Causes of Cyber-Criminality and Victimization: An Empirical Study on Students. Social Sciences. Vol. 5, No. 1, pp. 1-6.
- Cybercrime takes place in a different context than traditional crimes, ‘which may lead to different risk factors for both offending and victimization’. While traditional offending and victimization require physical interaction between victims and offenders, on the other hand, in cybercrime ‘there is no physical convergence in space and time of offenders and victims’. Kranenbarg, M. W., Holt, T. J. & van Gelder J.L. (2019). Offending and Victimization in the Digital Age: Comparing Correlates of Cybercrime and TraditionalOffending-Only, Victimization-Only and the Victimization-Offending Overlap, Deviant Behavior,40:1, 40-55.
- 'Online sexuality' like 'pornography, sex shops, sex work, sex education, sex contacts, and sexual subcultures' which engaged large volume of Western people irrespective of age, gender and sex. Doring N.M. (2009). 'The Internet’s impact on sexuality: A critical review of 15 years of research'. *Computers in Human Behavior*. Vol. 25, Issue 5, pp.1089-1101.

5. Material and Methodology

Tools of data collection: - Google Form was used to record responses. In a data set, we collected 189 responses based on that we conclude the data. The Survey process was the means for information gathering, which was used by the scholars for the determination of assembling information from the respondents.

Data collection and procedure: -The research is constructed on primary information gathering from Google form and the data for the study was acquired from the respondents. The information was composed by a simple random sampling process. Belief and understandings of the respondents were composed through the Survey method. The scholar after building an understanding with the respondents defined the determination, importance, and meaning of the study.

Result and discussion: -In Figure 1 we show the age collection of respondents. The age of the respondents, 62.3% of the respondents belong to the age group of 15-21years, 22.5% of the respondents belong to the age group of 22-28 years, only 15.2% of the respondents belong to the age group of 29-35 years.

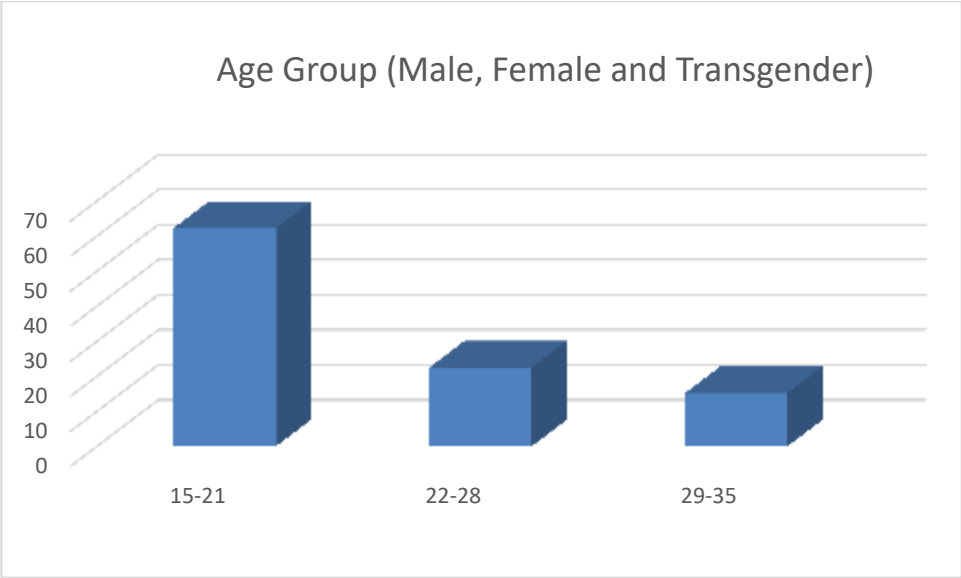


Figure 1

Response based on gender: -In Figure 2 respondents were categorized according to gender. Respondents based on gender, 51% of the respondents were male and 43% of the respondents were female and 6% were transgender.

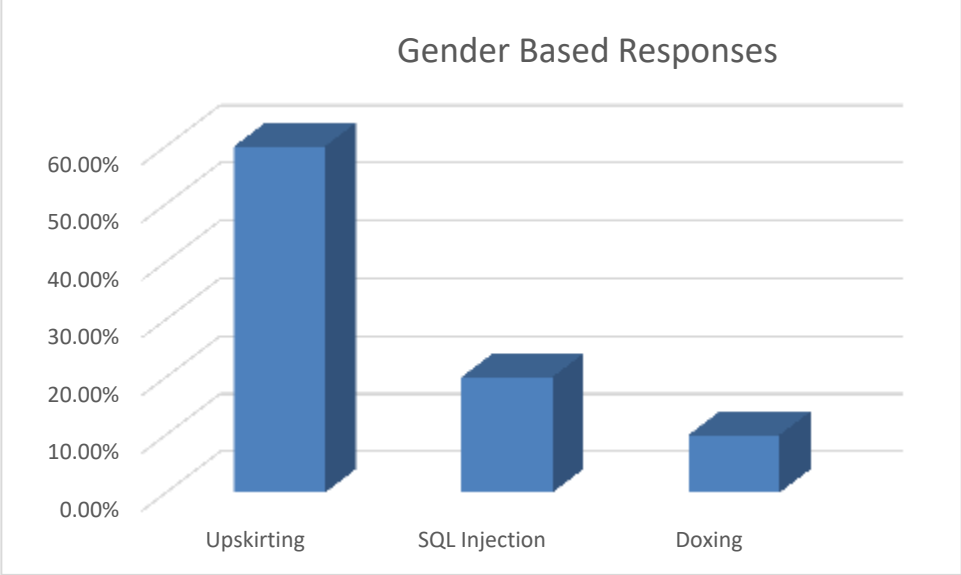


Figure 2

Awareness of different cyberviolence

In the Figure 3 respondents were asked about they know about cyber-violence in multiple-choice question form in which 66% of the respondents know about Phishing, 60% of the respondents know about Upskirting, 20% of the respondents know about SQL Injection, 10.00% of the respondents know about Doxing, 52% of the respondents know about Cyberstalking, 76.0% of the respondents know about Identity Stealing, 41% of the respondents know about Cyber Extortion, 10% of the respondents know about Digital Voyeurism, 91% of the respondents know about Pornography, 4% of the respondents know about Salami Slicing Attack, 4% of the respondents know about Salami Slicing Attack, 83% of the respondents knows about cyberbullying.

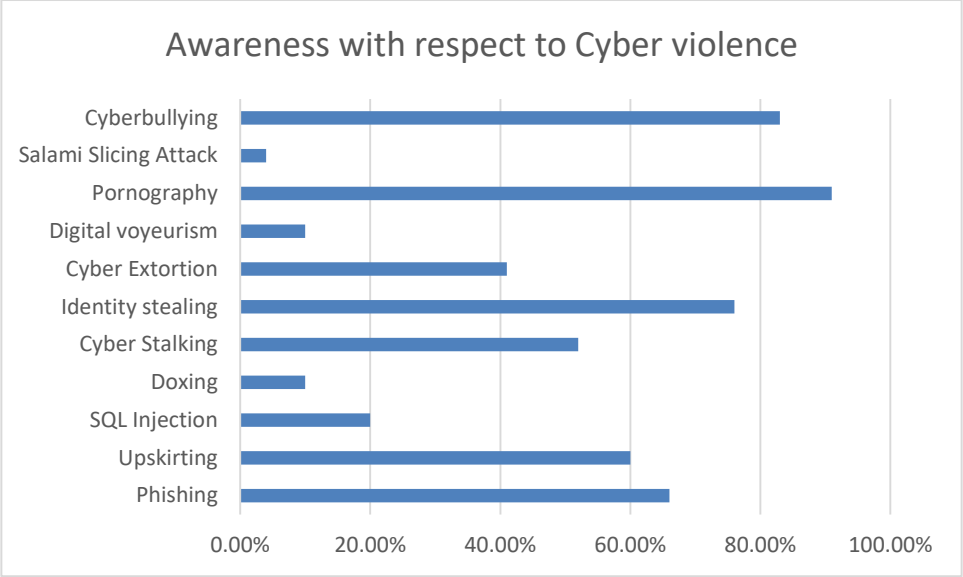
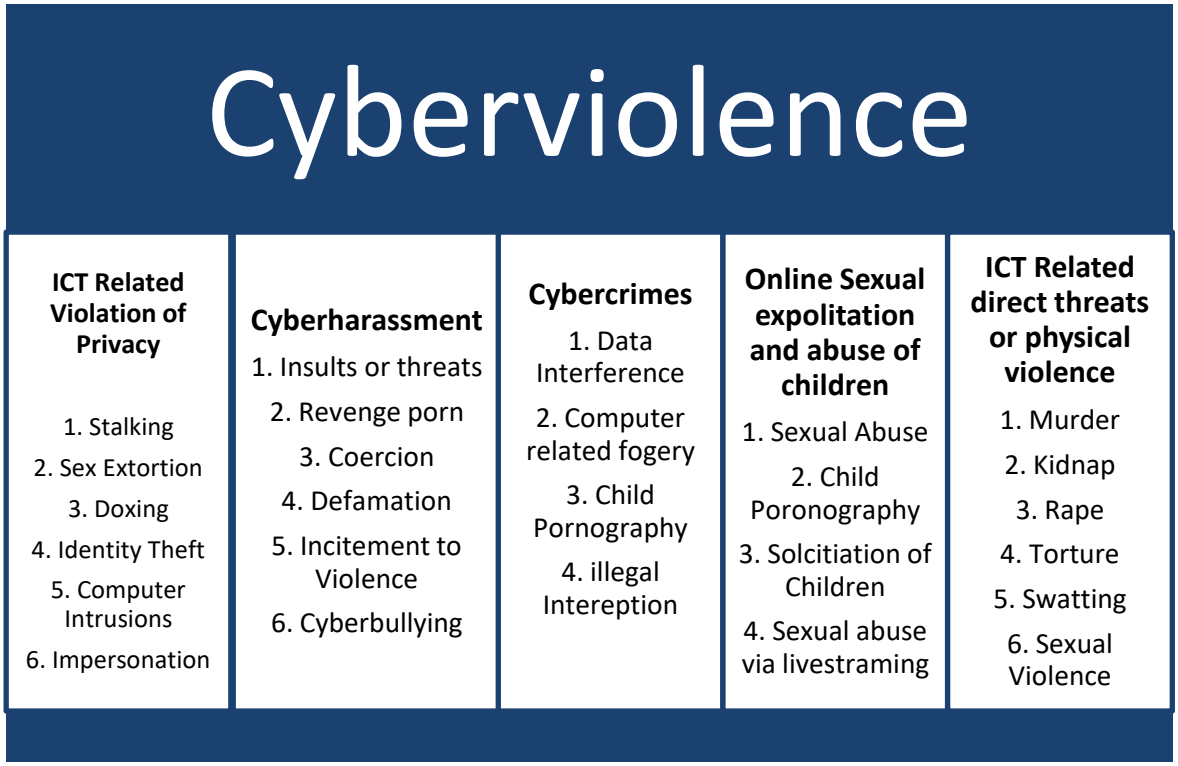


Figure 3

Outcome of the Research: - It will have its special significance in solving various informationsecurity related problems of Government Agencies, the business community and individualsalike. When all these are achieved, we will end up making our cyber space a safer place forbusinesstransaction, therebyindirectlyaffectingtheeconomy. Theinternetwill beabetter andsafer place for transactions and users will be better informed of security tips for the safety oftheirtransactions.All the cybercrimes are not intimated to the cyber police in India, not properly investigating by cyber police or cyber cases brought before the court are not properly handled by the court. Even cyber criminals are not prosecuted by court because of technical problem.



Meaning and Definition of Cyberviolence:

It is a fast-growing area of crime is broadly defined as a crime conducted using electronic medium to perpetrate it. According to Interpol, law enforcement generally makes a distinction between the two main types of Internet-related crimes (Interpol, 2016)

- Advanced cybercrime - these are sophisticated attacks against computer hardware and software.
- Cyber-enabled crime – they are 'traditional' crimes that have evolved with the advent of the Internet, such as financial crimes, terrorism, and pornography.
- According to **Professor Augustine Odinma"**cybercrime is any illegal act perpetrated in, on or through the Internet with the intent to cheat, defraud or cause the malfunction of a network device that may include a computer, phone, etc."
- According to **Roger Revelle** "Ever since men began to modify their lives by using technology they have found themselves in a series of technological traps".

Types of the Cyberviolence: - A conceptual Framework

Hacking

Hacking is basically gaining unauthorized access to your system profit, protest, information gathering, or to evaluate system weaknesses. The provisions for hacking are given in IT Act, 2000 under section 43-A and 66 and section 379 & 406 of Indian Penal Code. The punishment for hacking is 3 years or shall be imposed with fine up to 5 lakhs.

Credit Card Fraud

Card fraud begins either with the theft of the physical card or with the comprise of data associated with the account. Provisions of such fraud are given under Section 66 C and 66 D of IT ACT, 2000 and section 468 & 471 of Indian Penal Code, 1860.

Phishing: A malicious individual or group who scam users. They do so by sending e-mails or creating web pages that are designed to collect an individual's online bank credit card, or other login information. The provisions to prosecute any person for phishing are given under section 66 C, 66 D and 74 of the IT Act with imprisonment up to 3 years or with fine up to 1 lakh rupees.

Doxing is a harmful act carried out by hackers against someone with whom they disagree or detest. It is the act of disclosing personally identifiable information about another person online, such as their true name, home

address, workplace, phone number, financial information, and other details. This information is subsequently disseminated to the general public without the victim's consent.

Cyber Stalking: It can be defined as the use of electronic communications to harass or frighten someone, for example by sending threatening emails. The provisions are given under IT Act, 2008 under section 72 and section 354 C (voyeurism) of the Indian Penal Code. Also, section 67 provides imprisonment up to 3 years with fine. The cases of Cyber Stalking is found in India too. For example: - YogeshPrabhu Vs. state of Maharashtra, 2006(3) MhLj 691 and JibinBabu Vs. State of Kerala, decided by the Kerala High Court on August 26, 2020.

Identity stealing: An attempt to get access to a computer in order to obtain personal information about a user, which they subsequently use to steal that person's identity or acquire access to their valuable accounts, such as banking and credit cards. Cybercriminals buy and sell identity information on darknet marketplaces, including financial accounts and other types of accounts like video streaming services, webmail, video and audio streaming, online auctions, and more. Personal health information is sometimes targeted by identity thieves.

Cyber Extortion: An attack or threat of an attack followed by a demand for payment to stop the attack. Cyberextortion in the form of ransomware is one example. After gaining access to a company's networks, the attacker encrypts all of the company's papers and data — everything of value — rendering the material unavailable until a ransom is paid. Typically, this takes the form of a cryptocurrency like bitcoin. Ransomware is frequently delivered into an organization via phishing emails, but it can also be introduced using exploits, USB drives, and other malware-infected media. It operates quickly. It spreads from machine to machine over the corporate network, infecting endpoint devices (PCs, laptops), servers, and network storage media.

Upskirting: Taking a picture under a person's clothing without their knowledge with the goal of viewing their genitals or buttocks for sexual enjoyment or to distress the victim is known as upskirting. It frequently takes place in a crowded public setting, making it difficult for the victim to notice that a photograph is being taken. Victims are frequently distressed and humiliated.

Voguers on the internet: - A voyeur is a person who gets sexual enjoyment from secretly watching others undress or engage in sexual activity.

Pornography: Basically, pornography is nothing but marketing of man or woman sex, shown as object for those who get involved into sexual acts. Pornographers use the internet to sell their material to sex addicts and to the interested parties. Watching and keeping of these kinds of materials is illegal in India. Nowadays pornography has become a kind of a business to the society as people indulge themselves to gain the economic benefits from them.

Blackmailing: Blackmailing amounts to Criminal intimidation, which is well defined in the Indian Penal Code section 503 as :- Whoever threatens another with any injury to his person, reputation or property, or to the person or reputation of any one in whom that person is interested, with intent to cause alarm to that person, or to cause that person to do any act which he is not legally bound to do, or to omit to do any act which that person is legally entitled to do, as the means of avoiding the execution of such threat, commits criminal intimidation. The offence of Criminal intimidation can be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both. This section penalizes the capturing or publishing the image of a private area of any person without consent.Imprisonment which may extend to 3 years.Blackmailing is an act done by cowards; one must not fear from threats in the first place. The society should not criticize the nudes leak. Instead, it should support the victim in his/her battle to punish the wrongdoer. It’s obvious for the victim to panic, but you must take all the right actions without delay, because delay may lead to unpredictable results.

Software Piracy is a type of cyber-attack that involves the illegal copying, distribution, and use of software applications for commercial or personal gain. This sort of cybercrime is frequently related with trademark infringements, copyright infringements, and patent infringements.

Salami Slicing Attack: Money laundering is the most common application of the salami-slicing technique, but it is not restricted to that. The salami method can also be used to collect small amounts of data over time in order to build a full picture of a company. This act of information dissemination could be used against a person or a company. Websites, advertisements, discard bin documents, and other sources can all be used to compile a database of factual intelligence on the target.

Cyberbullying: It is a form of "bullying," which is defined as physical or mental violence perpetrated by a person or group of people against another person or group of people with the intent of making the victim feel persecuted. Some of the most prevalent venues for cyberbullying are social networking sites. Cyberbullying has a lot of negative repercussions, according to research. Cyberbullying victims had reduced self-esteem, more suicidal ideation, and a range of emotional reactions, including fear, rage, and melancholy.

The internet is unforgiving and never forgets. If you share something once, it will live on the internet in some form or another for the rest of your life.The following table shows the number of cybercrimes reported in India from 2018-2020.

Cyber Crimes (State/UT-wise) - 2018-2020						
SL	**State/UT**	**2018**	**2019**	**2020**	**Mid-Year Projected Population (in Lakhs)**	**Rate of Total Cyber Crimes (2020)**
[1]	**[2]**	**[3]**	**[4]**	**[5]**	**[6]**	**[7]**
STATES:						
1	Andhra Pradesh	1207	1886	1899	526.0	3.6
2	Arunachal Pradesh	7	8	30	15.2	2.0
3	Assam	2022	2231	3530	347.9	10.1
4	Bihar	374	1050	1512	1219.0	1.2
5	Chhattisgarh	139	175	297	292.4	1.0
6	Goa	29	15	40	15.5	2.6
7	Gujarat	702	784	1283	691.7	1.9
8	Haryana	418	564	656	292.1	2.2
9	Himachal Pradesh	69	76	98	73.6	1.3
10	Jharkhand	930	1095	1204	381.2	3.2
11	Karnataka	5839	12020	10741	665.0	16.2
12	Kerala	340	307	426	353.7	1.2
13	Madhya Pradesh	740	602	699	837.6	0.8
14	Maharashtra	3511	4967	5496	1236.8	4.4
15	Manipur	29	4	79	31.4	2.5
16	Meghalaya	74	89	142	32.6	4.4
17	Mizoram	6	8	13	12.1	1.1
18	Nagaland	2	2	8	21.8	0.4
19	Odisha	843	1485	1931	454.7	4.2
20	Punjab	239	243	378	301.8	1.3
21	Rajasthan	1104	1762	1354	786.1	1.7
22	Sikkim	1	2	0	6.7	0.0
23	Tamil Nadu	295	385	782	761.7	1.0
24	Telangana	1205	2691	5024	375.4	13.4
25	Tripura	20	20	34	40.4	0.8
26	Uttar Pradesh	6280	11416	11097	2289.3	4.8
27	Uttarakhand	171	100	243	113.1	2.1
28	West Bengal	335	524	712	977.2	0.7
	TOTAL STATE(S)	**26931**	**44511**	**49708**	**13151.8**	**3.8**
UNION TERRITORIES :						
29	A&N Islands	7	2	5	4.0	1.3
30	Chandigarh	30	23	17	12.0	1.4

31	D&N Haveli and Daman & Diu[@]	0[+]	3[+]	3	10.4	0.3
32	Delhi	189	115	168	203.2	0.8
33	Jammu & Kashmir[@]	73[*]	73[*]	120	133.4	0.9
34	Ladakh [@]	-	-	1	3.0	0.3
35	Lakshadweep	4	4	3	0.7	4.4
36	Puducherry	14	4	10	15.5	0.6
	TOTAL UT(S)	**317**	**224**	**327**	**382.1**	**0.9**
	TOTAL ALL INDIA	**27248**	**44735**	**50035**	**13533.9**	**3.7**
● Crime Rate is calculated as Crime Incidence per one lakh of population						
● Population Source: Report of Technical group on Population Projections(July, 2020) National Commission on Population, MoHFW						
● As per data provided by States/UTs ● States/UTs may not be compared purely on the basis of crime figures						
'+' Combined data of erstwhile D&N Haveli UT and Daman & Diu UT						
'*' Data of erstwhile Jammu & Kashmir State including Ladakh						
'@' Data of newly created Union Territory						

Source: - National Crimes Record Bureau

International Framework

Traditional criminal law and the criminal justice system in general face various issues as a result of cybercrime. As a result of the virtual aspect of many cybercrimes, inconsistencies among criminal justice systems may impede the phenomenon's repression. The European Convention on Cybercrime, held in Budapest on November 23, 2001, took the most major approach to cybercrime and international cyber law. It is one of the most important international conventions addressing cybercrime and electronic evidence. The Council of Europe, Canada, Japan, South Africa, and the United States of America collaborated on the document. This Convention is divided into four chapters with a total of 48 articles. This Convention is a global treaty on criminal justice that provides States with:

1. The criminalization of certain actions by means of computers and internet;
2. Procedural law to examine cybercrime and admission of electronic evidence in relation to any crime; and
3. International police and judicial collaboration on cybercrime and electronic evidence.

The UN General Assembly adopted the Guidelines Concerning Computerized Personal Data Files in 1990, with the goal of taking necessary precautions to secure the files from both natural and man-made threats. The United Nations General Assembly has passed several resolutions aimed at raising global cyber security awareness, combating illegal misuse of information networks, and preventing cybercrime. The United Nations Commission on International Trade Law (UNCITRAL) adopted the UNCITRAL Model Law on Electronic Commerce to assist countries in drafting legislation to allow and facilitate e-commerce and e-government. The Model Law is intended to help countries improve their laws governing commercial transactions including the use of computerised or other modern communication technologies.Establishes rules for validating contracts made by electronic methods, as well as procedures for creating and governing e-contracts.

1. Defines what constitutes genuine electronic writing and what constitutes an original document.
2. Ensures that electronic signatures are legal for both legal and commercial uses.
3. Allows computer and electronic evidence to be included into judicial proceedings.

Law and Cybercrime in
India today: -

Cyberlaw is significant because it encompasses nearly all elements of transactions and activities on and with the Internet, the World Wide Web, and Cyberspace. At first glance, Cyberlaws may appear to be a highly technical field with little relevance to ordinary Cyberspace operations. The truth, on the other hand, is that nothing could be further from the truth. Every action and reaction in Cyberspace has certain legal and Cyber legal implications, whether we recognize it or not.The Information Technology Act (IT Act) and the Indian Penal Code both encompass cybercrime. The Information Technology Act of 2000, which went into effect on October 17, 2000, regulates cybercrime and electronic commerce. In the year 2008, the IT Act was revised. The Act establishes the definition of cybercrime as well as the penalties associated with it. Under this IT Act, amendments to the Indian Penal Code, 1860, and the Reserve Bank of India Act were made. This Act's goal is to protect e-government, e-banking, and e-commerce transactions.

Some important sections of the IT Act under which cybercrimes may be registered are as follows:

Section 65

- Tampering with Computer Source Documents.
- Imprisonment up to 3 years and/or up-to Rs Two lakh fine.

Section 66

- Hacking with computer systems or unauthorized usage of computer system and network.
- Punishment if found guilty can be imprisonment up to three years and/or a fine of up to Rs 5 lakh.

Section 67

- Punishment for publishing or transmitting obscene content in electronic form
- Imprisonment for 3years or fine of 5,00,000.
- For subsequent conviction imprisonment for 5years and with 10,00,000 rupees fine.

Section 379

Punishment for theft for up to three years and/or fine.

Since many cybercrimes are committed using stolen mobile/computers or stolen data this IPC Section comes into the picture.

Section 420

- Cheating and dishonestly inducing delivery of property.
- Cybercrimes like creating Bogus websites, cyber frauds are punishable under this section of IPC with a seven-year jail term and/or fine.
- This section of the IPC deals with crimes related to password thefts for committing frauds or creating fraudulent websites.

Section 463

- Making false documents or false electronic records.
- Crimes such as Email spoofing are punishable under this section with imprisonment of up to seven years and/or fine.

Section 468

- Committing forgery for the intention of cheating attracts imprisonment of up to seven years and/or a fine.
- Email spoofing is one such crime punishable under this section.
- Apart from the above laws, there are many more sections under IT Act and IPC, which have provisions for cybercrimes.

Section 293 of Indian Penal Code (IPC) 1860

- Sale, etc., of obscene objects to young person
- Imprisonment for 3years or Fine of 2,000 rupees
- For subsequent conviction imprisonment for 7years and also with 5,000.

Cyber Crimes under IPC:

- Sec 503 IPC: Sending threating messages by email.
- Sec 499 IPC: Sending defamatory messages by email

- Sec. 463 IPC: Forgery of electronics records
- Sec 420 IPC: Bogus Websites, Cyber Frauds
- Sec. 463: Email Spoofing
- Sec. 383 IPC: Web Jacking
- Sec. 500 IPC: E mail abuse

Cyber Crimes under the Special Acts:

- Online sale of drugs under narcotic drugs and psychotropic substances act
- Online sales of Arms Act
- S.354D of the IPC suffers from another major drawback in its sentencing policy. This provision has made cyber stalking essentially a criminal act and, as such, has prescribed criminal recourse for the same. The provision has made the offence of stalking (including cyber stalking) a cognizable, but bailable offence. As per this provision, it is punishable with imprisonment for a maximum period of three years with fine in the case of first conviction. However, for the second conviction, the offence has been made cognizable, non-bailable and punishable with imprisonment for a period of maximum five years with fine. In both cases, the provision has empowered “any magistrate” to try the offence. However, this provision as such, does not prescribe any civil remedy like the US or UK laws by ways of restraining orders, including no contact orders which may prevent the stalker from contacting the victim. It is broadly understood that once the accused is arrested and imprisoned, his devices would be ceased by the police and he would not be allowed to use any means to communicate with the victim.

Case Analysis

If you pick up a newspaper in Noida on any given day and turn to the city pages, you are certain to come across at least one, if not more, reports of technology-related crimes. Cybercrime appears to be all too frequent in Noida, ranging from credit card fraud to social media account hacking. According to the Delhi Police, there was a huge increase in cybercrime in Delhi during the Covid-19-induced lockdown, with as many as 135 such offences reported every day on average in May, based on an analysis of roughly 33,000 cases filed until November 2020. People who had increased their usage of digital platforms for purchasing were targeted by a slew of fake sites with dubious reputations.The public would not have used those sites for shopping under normal circumstances. The cybercrime unit analysed the crimes and found that 62 percent were online financial frauds, 24 percent were social media harassment, such as morphing photos of people and sexual harassment, and the remaining 14 percent were other crimes such as hacking, identity theft, and data theft. Fake call centres were operating in north and northwest Delhi, as well as NCR areas such as Noida and Gurugram, defrauding individuals by promising tech support in the name of reputable software companies.

Nasscom vs. Ajay Sood & Others:-In a landmark judgment in the case of National Association of Software and Service Companies vs. Ajay Sood & Others, the Delhi High Court declared 'phishing' on the internet to be an illegal act, entailing an injunction and recovery of damages. The court also stated, by way of an example, that typical phishing scams involve persons who pretend to represent online banks and siphon cash from e-banking accounts after conning consumers into handing over confidential banking details. The Delhi HC stated that, even though there is no specific legislation in India to penalize phishing, it held phishing to be an illegal act, by defining it under Indian law as "a misrepresentation made in the course of trade, leading to confusion, as to the source and origin of the email causing immense harm, not only to the consumer, but even to the person whose name, identity or password is misused." The court held the act of phishing as passing off and tarnishing the plaintiff's image.

This case achieves clear milestones: It brings the act of "phishing" into the ambit of Indian laws, even in the absence of specific legislation; it clears the misconception that there is no "damages culture" in India for violation of IP rights. this case reaffirms IP owners' faith in the Indian judicial system's ability and willingness to protect intangible property rights and send a strong message to IP owners that they can do business in India without sacrificing their IP rights.

SMC Pneumatics (India) Pvt. Ltd. vs. JogeshKwatra:-In India's first case of cyber defamation, the High Court of Delhi assumed jurisdiction over a matter where a corporation's reputation was being defamed through emails and passed an important ex-parte injunctionobserving that a prima facie case had been made out by the plaintiff. Consequently, in this cyber fraud case in India, the Delhi High Court restrained the defendant from sending derogatory, defamatory, obscene, vulgar, humiliating and abusive emails, either to the plaintiff or to its sister subsidiaries all over the world, including their Managing Directors and their Sales and Marketing departments. Further, Hon'ble Judge also restrained the defendant from publishing, transmitting or causing to be published any information in the actual world, as also in cyberspace, which is derogatory or defamatory or abusive.

Bazee.com case:-In December 2004, the CEO of Baazee.com was arrested after a CD containing inappropriate information was sold on the website. The CD was also available in Delhi's marketplaces. Later, the CEO was released on bail bond. This raised the question of how we should distinguish between Internet Service Providers and Content Providers. The accused bears the burden of proving that he was the Service Provider rather than the Content Provider. It also creates a lot of questions about how police should handle cyber-crime cases, and it necessitates a lot of education.

Ravish Kumar is one of the most respected Hindi news anchors in India, who in August 2015, made a public exit from social media platforms including Facebook and Twitter. In an interview with Scroll.in, an online news website, he famously said, "I have stopped tweeting because social media space is no longer a citizen's space. It has been usurped by political parties to peddle their ideology and propaganda. It's an online lynch mob where anyone with organizational support of 500 can send out 10 lakh tweets and declare me a thief."

Considering the case of United States vs. Cassidy, 814 F. Supp 2D 574 (D. md. 2011) where the defendant was allegedly conducting cyber stalking through negative socialising; i.e. creating a fake Twitter account through which he had directed numerous Tweets to the victim and her religious centre. See more in Young , 2013: 61. The court emphasised on the victim's choices to 'ignore' the blog posts or Tweets when they are not directed to a 'captive audience' and made in the public forums. Interpretation of harassing conduct in the back drop of cyber stalking has also been done in the same line by the courts in the UK; consider the cases of Majrowski vs. Guys & St. Thomas NHS trust [2006] UKHL 34; [2006] ICR 1199 HLand Conn vs. Sunder land City Council([2007] EWCA Civ 1492, [2007] 2 All ER (D) 99), where the court held that simple conduct which would not amount to criminal conduct, would not attract the PHA (Salter, Bryden, 2009). However, it depends upon the courts to build up the difference between conducts which may be categorised as 'civil conduct' which may escape the heavy liability as that of criminal conducts which may attract heavy punishment in PHA.

6. Conclusion and Suggestions

Indian Laws are well drafted and can handle all kinds of challenges as posed by cyber criminals. However, the enforcement agencies are required to be well versed with the changing technologies and laws.Crimes are not to be measured by the issue of events, but by the intensions of men. The greatest crimes do not arise from a want of feelings for others but from an over sensibility for us and an over indulgence in our own desire.In our opinion retaliation of porn upon and revenge on blackmailing is athreat towards a person's loss of life and property. There should be stringent laws and special steps and punishment with fine should be enforced by the law, court of laws and guide by Government ofIndia to stop such kind of heinous crime related to cyber.There is a whole other world that exists in cyberspace, make sure your information travels safely.As we can see that there where so many cybercrimes happening in India before the amendment of Information Technology Act, the rate of crime has not stopped, nor it have come down but it is reaching its high.When it came to taking perpetrators of internet abuse accountable, law enforcement agencies were grossly underprepared.

Wehave tried to find out various reason that despite of such a tight act and high penalties and punishments. What are the loopholes in the act which is blocking the proper implementations of such a force full act.Cybercrime cell should provide some preventive measure for online transaction.Online banking system should provide secure mechanism for secure transaction.Cybercrime should solve as soon as possible pending

cases.In rural area there are not awareness about cybercrime so aware them by some advertisement.Students are most victim of cybercrime, so make them aware about cybercrime.

Though advancements in technology have made it easier and more user-friendly for consumers to carry out their everyday tasks, it has also resulted in a harsh world of security threats from organisations such as hackers and crackers. Various information technology solutions have been established to curtail such detrimental behaviours in order to meet the technology's core objectives of providing users with a sense of security. The following are some of the most common measures used to combat cybercrime:

A) Encryption: This is a crucial technique for securing data while it is in transit. This approach converts plain text (readable) to cypher text (coded language), which the recipient of the data can decode by transforming it back to plain text using the private key. No one can access the sensitive information except the recipient, who is in possession of the secret key to decrypt the data.

B) Synchronized Passwords: These are password schemes that are used to alter the password for both the user and the host token. The password on a synced card is changed every 30-60 seconds, making it only usable for a single log-on session. To impute passwords and pass phrases, other relevant methods introduced include signature, voice, fingerprint identification, retinal and biometric recognition, and so on.

C) Firewalls: These keep classified materials from being leaked or accessed by erecting a barrier between the system and potential intruders. Only data that is recognised and confirmed by one's system would be allowed to enter into the computer. It only allows those who have already registered with the computer access to the system.

D) Digital Signatures: These are formed by applying algorithms to cryptography. This is widely used in the banking industry, where customers' signatures are verified using this method before banks engage in large transactions.

Recent Steps taken by Government

- **Cyber Surakshit Bharat Initiative** was launched in 2018 with an aim to spread consciousness about cybercrime and building capacity for safety measures for Chief Information Security Officers (CISOs) and frontline IT staff across all government departments.
- **National Cyber security Coordination Centre (NCCC)**was developed in 2017, its mandate is to scan internet traffic and communication metadata (which are little snippets of information hidden inside each communication) coming into the country to detect real-time cyber threats.
- **Cyber Swachhta Kendra**a platform was introduced in 2017 for internet users to clean their computers and devices by wiping out viruses and malware.
- Training of 1.14 Lakh persons through 52 institutions under the **Information Security Education and Awareness Project (ISEA)** – a project to raise awareness and to provide research, education and training in the field of Information Security.
- **International cooperation:** Looking forward to becoming a secure cyber ecosystem, India has joined hands with several developed countries like the United States, Singapore, Japan, etc. These agreements will help India to challenge even more sophisticated cyber threats.

Cyber Violence is essentially an emotional crime and, hence, it needs to be dealt with by way of restorative process along with therapeutic jurisprudential approach. the police, the lawyers, the judges and the counsellors must be trained properly to understand the cyberviolence in the light of cyber victimisation. Restorative process may provide respite to women who fear breach of privacy during legal procedures. This is because restorative process allows the victim to choose a place for mediation and also the persons to be present for the restorative process from the options as may be suggested by the legal actors. This may not only ensure the fulfilment of goals set up by therapeutic jurisprudence, but may also encourage more women victims to report the crimes and seek for proper redress.

Limitation of the Study

Cyber stalking is essentially an emotional crime and, hence, it needs to be dealt with by way of restorative process along with therapeutic jurisprudential approach. If restorative process is included in the laws dealing

with cyber stalking, the victims may be prevented from committing further harm in the course of saving themselves from their stalkers. Additionally, the restorative process may also find out ways to heal the damage suffered by the victim by including not only the offender himself, but also the web service providers. The laws criminalising cyber stalking may make the offender feel repent by making him understand about the illegalities of his behaviour in the course of cyber stalking.

7. References

1. Barkha, Rama Mohan, U. (2011) Cyber Law and Crimes, IT Act 2000 & Computer Crime analysis. (3rd ed.), ISBN: 978-93-81113-23-3.
2. Cybercrime classification, [Online], Available: http:// shodhganga. inflibnet.ac.in/ bitstream /10603/7829/12/12_ chapter % 203.pdf [29 September 2013].
3. Cybercrime system requirements in India: Most necessary thing inIndia, [Online], Available: http://www.cyberlawsindia.net/ requires. html [13 May 2012].
4. Cybercrime, [Online], Available: http://www.britannica.com [5 March 2012].
5. Godbole, N., Belapure, S. (2011) Cyber Security, 'Understanding Cybercrimes', Computer Forensics and Legal Perspectives, Wiley India Pvt. Ltd., (1st ed.), ISBN: 978- 81-265-2179-1.
6. IT Infrastructure in India, [Online], Available: http://business.mapsofindia.com/ indiabudget/infrastructure/it.html [16 June 2013].
7. Muthu Kumaran, B. (2008) 'Cybercrime scenario in India', criminal investigation department review, Chief Consultant, Gemini Communication Ltd., p. 17.
8. Pillai, (2008). 'Govt. framing norms for social infrastructure in SEZs', Economic Times, [Online], Available: http://articles.economictimes.indiatimes.com/2008-06- 20/news/28488069.
9. Srivastava, B., Abhichandani, T., Biswas, A., akare, M. (2011). Report on Internet in India (I-Cube), Internet & Mobile Association of India (IAMAI), p. 3.
10. Hinduja, S.,Patchin, J. W. (2009). Bullying beyond the schoolyard: Preventing and responding to cyberbullying. Thousand Oaks, CA: Corwin Press.
11. Halder, D., Jaishankar, K. (2011) Cyber Gender Harassment and Secondary Victimization: A Comparative Analysis of US, UK and India. Victims and Offenders, 4, pp. 386- 398.
12. Verma, A. (2009) Cyber Crimes and Law. India: Central Law Publishers.
13. Baer, M. (2010) Cyberstalking and the Internet Landscape We Have Constructed. Virginia Journal of Law & Technology, 15, pp. 154-172.

INFO

Corresponding Author: ***Ms. Deepali Rani Sahoo,*** ***Assistant Professor, Symbiosis Law School, Noida, Symbiosis International (Deemed University.***

How to cite this article: ***Ms. Deepali Rani Sahoo, Dr. Pooja Kapoor,*** ***An Analytical Study Relating to the Legal Dimensions against Cyberviolence in India, Asian. Jour. Social. Scie. Mgmt. Tech.2022; 4(3): 01-13.***