Page 161 - 171

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 3 | Issue 2

2020

Violence Online: Women and Wild Web

P. SUJEE[1] AND A.B. ABIRAMI[2]

ABSTRACT

Most of the offenses against the body involve physical violence. But one of the most prevailing and growing offenses with the same gravity is cybercrime. In the digital era, information and communication technology is helping billions to build the gap between people. But we do not realize that the gap is becoming so thin that every person is becoming capable of stepping into another's shoe, infringing their privacy and even lowering the dignity of another. In such a case, women are most affected. Though they fall prey with various other offenses, "Violence online" affects them traumatically. This paper provides the study on cybercrime against women and laws governing them in the US, INDIA, and UK. The advancements in technology are intended to provide better living, but the same technology is being misused in various walks of life without any physical bounds. When this became a burning issue in India, various provisions were established in Penal provisions, Information Technology Act, 2000 and Privacy laws seeking protection to the victims. But these laws fail to meet the growing cybercrime rate. In a country like India, where the society looks down upon women, the laws prevailing does not sufficiently recognize these online crimes. This paper provides a descriptive case study in India to introspect the gaps between cybercrime against women and laws relating to the same. This paper aims to bring out the various types of cybercrimes and the reasons for the commissioning of these crimes are researched. Various cases are analysed to conclude. Suggestions as to the reforms required in the legal system to curb the rising criminals and changes in the attitude of the society towards the victim are discussed in the conclusion.

I. INTRODUCTION

The headway of innovation has made man subject to the Internet for his needs. The web has given man simple access to everything while sitting at one spot. Long-range informal communication, internet shopping, putting away information, gaming, web-based contemplating, online employments, each conceivable thing that man can consider should be possible through the mechanism of the web. The web is utilized in pretty much every circle.

[1] Student at SASTRA Deemed to be University, India
[2] Student at SASTRA Deemed to be University, India

 [ISSN 2581-5369]

With the advancement of the internet and its related advantages, the idea of digital violations has also been born. Digital crimes are committed in various forms. A couple of years back, there was an absence of mindfulness about the wrongdoings that could be submitted through the web. In the issues of digital wrongdoings, India is likewise not a long way behind different nations where the pace of frequency of digital violations is additionally expanding step by step. This paper will bring out the various forms of cybercrimes and laws relating to it in the UK, US, and India.

II. CYBERCRIME AND ITS DIFFERENT FORMS

Cybercrime in general means the usage of computer technology as a tool to commit criminal activities. It will undermine society's ability to maintain internal and external order.

Cybercrimes are unlawful activities where the computer is either the tool used or the target or both. Cybercrime is an umbrella term covering phishing, credit card frauds, bank robbery, illegal downloading, industrial espionage, child pornography, kidnapping children via chat rooms, scams, cyber terrorism, creation and/or distribution of viruses, spam, etc., it also covers the traditional crimes in which computers or networks are used to enable the criminal activity.

There are various forms of cybercrimes as mentioned above. The explanation of those are given below:

1. HACKING

Hacking is recognized as one of the most common kinds of law-breaking. Hacking normally refers to unlawful access to an ADP system. Some samples of hacking embody breaking the password-protected websites and circumventing password protection on a laptop system, it additionally includes the use of faulty hardware or computer code implementation to illicitly acquire a password to enter into an ADP system. Three main factors that have supported the increasing range of hijacking attacks are: (a) inadequate and incomplete protection of laptop systems, (b) development of computer code tools that automatize the attacks and (c)the growing role of personal computers as a target of hacking attacks.

2. PORNOGRAPHY

Pornography means demonstrating sexual acts to cause sexual urges. The meaning of pornography includes obscene sites, explicit magazines created utilizing Personal Computer and the web sex entertainment conveyed over cell phones. The Internet is by and large profoundly utilized as a medium to explicitly manhandle youngster’s PC's and the web has turned into a need for each family unit, the youngsters have simple access to the web. There

 [ISSN 2581-5369]

is simple access to the obscene substance on the web. Paedophiles draw the kids by conveying explicit material and after that, they attempt to meet them for sex or to take their bare photos incorporating their commitment to sexual positions. Now and then Paedophiles contact kids in the visit rooms acting like youngsters or an offspring of comparable age and later they begin to get friendlier with them and win their certainty. At that point gradually paedophile's begin sexual talk to enable youngsters to shed their hindrances about sex and afterward get them out for an individual collaboration. At that point begins genuine misuse of the kids by offering them some cash or encouraging them great open doors throughout everyday life. The paedophiles at that point explicitly misuse the youngsters either by utilizing them as sexual items or by taking their obscene pictures to sell those over the web.

3. CYBER STALKING

Stalking can be named as the repeated demonstrations of provocation focusing on the injured individual, for example, following the person, making hassling telephone calls, slaughtering the victim's pet, vandalizing their property, leaving composed messages or items. Stalking might be trailed by genuine brutal acts, for example, physical damage to the person. Digital Stalking means repeated demonstrations of provocation or undermining conduct of the cybercriminal towards the victim by utilizing internet providers. Both sort of Stalkers i.e., Online and Offline, want to control the person's life.

4. SOFTWARE PIRACY

Programming robbery alludes to the illicit duplicating of real projects or the forging and circulation of items instead of the original. These sorts of wrongdoings additionally incorporate copyright encroachment, trademarks infringement, robbery of PC source code, patent infringement and so on. Domain names are likewise trademarks protected under trademark laws. Digital squatters register domain name indistinguishable from prevalent provider's name to pull in their clients and get advantage from them.

5. PHISHING

Phishing is the demonstration of sending an email to a client erroneously professing to be a real endeavor trying to trick the client into giving up private data that will be utilized for fraud. The email guides the client to visit a site where they are approached to refresh individual data, for example, passwords and MasterCard details, the government managed savings and ledger numbers that the real association as of now has. The webpage is a counterfeit and set up just to take the client's data. By spamming enormous gatherings of individuals, the phisher relied on the email being perused by a level of individuals who

 [ISSN 2581-5369]

had recorded credit card numbers legitimately.

6. EMAIL SPOOFING

Email spoofing refers to mails which tend to appear from one source but, it comes from another source. It leads to monetary damages.

7. CYBER TERRORISM

Use of technology to attack the military forces, power plants, air traffic controls, telecommunication networks, etc.

III. CYBER LAWS IN UK

The 2016 statistics revealed that out of all the crimes recorded by the Police in England and Wales the total number of crimes labelled as cybercrime or online crime was 0.8 percent. By 2019 it has increased to 2 percent which shows a sharp increase in online crimes in the UK. The CROWN PROSECUTION SERVICE has said that cybercrime is an umbrella term which includes two types of cyber activity, (i) cyber dependent crimes where the target and the tools used are cyber devices, for example, malware attacks, (ii) cyber-enabled crimes, where the traditional crimes are furthered by cyber devices. Broadly cybercrimes can be classified into offenses against the confidentiality, integrity, and availability of computer data

and systems; (ii) computer-related offenses; and (iii) content-related offenses. Out of the 31,148 online offenses recorded in 2016, 15,137 were harassment and stalking. This number has risen to 50,680 by 2018 which is trice the figure in 2016. The National Cyber Security Centre which is a part of the Government Communications Headquarters acts as a bridge between industry and government, providing a unified source of advice, guidance, and support on cybersecurity.

One of the significant Acts in this area brought in the UK is The Computer Misuse Act, 1990. This Act protects cybercrimes which include: (i) Unauthorised access to computer material. (ii) Unauthorized access with intent to commit or facilitate the commission of further offenses, (iii) Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of the computer, etc.(iv) unauthorized acts causing danger and obtaining, supplying of articles in furtherance of such acts. The Act also provides for imprisonment or fine for the commission of such offenses. This Act was amended by the Police and Justice Act, 2006 and now it includes unauthorized acts with intent to impair the operation of the computer, which effectively adds Denial-of-Service attacks

 [ISSN 2581-5369]

as an offense.

The amendment makes explicit that the offense does not have to be against a specific computer, program or data. Additionally, it states that an offense is caused even if Denial-of- Service is only temporary.

IV. CYBER LAWS IN US

Cybercrime is the fastest-growing type of criminal activity in the United States; it's affecting more and more people each year. The USA is one of the countries which evaluated the dark and ugly sides of the internet (i.e.) cybercrime. Cybercrime is estimated to be fast-growing in the State of Florida. The USA has witnessed a hub of cases in cybercrime against women and has and still mitigates such crime to prevent future victimization. Hacking, denial-of-service attacks, infecting software with the virus, the use of software to commit cybercrimes, identity theft or identity fraud, and electronic fraud all constitute cybercrime in the US. The various laws in the US regarding cybercrime are:

1. **COMPUTER FRAUD AND ABUSE ACT,1984 (CFAA)**

This Act criminalizes unauthorized access to computers, knowingly causes transmission of the program with the intent to cause damage without authorization, defrauding traffics with intent to affect the interstate or foreign commerce, extortion with the threat to leak confidential information or cause damage to the personal computer. The Act also provides for punishment which may extend up to 20 years of imprisonment, restitution, criminal forfeiture and/or fine.

2. **TITLE 18 OF UNITED STATES CODE**

- Section 1028 and 1028A - deal with identity theft
- Section 1029 - prosecute phishing and identity theft.
- Section 2701 (Stored Communication Act) – deals with unauthorized access to a stored communication, includes electronic theft.
- Sections 1462 and 1465 – deals with importation, transportation, and sale of obscene matters.
- Sections 2510-2522 – Interception of wire, oral, or electronic communication
- Sections 2701-2712 – Preservation and disclosure of stored wire and electronic communication sections 3121-3127 – Pen registers and trap and trace devices.

 [ISSN 2581-5369]

Other than the above-mentioned laws there are other statutes which criminalize acts that adversely affects or threatens the security, confidentiality, integrity or availability of IT systems, infrastructure, communication works, device or data such as the WIRETAP ACT, CAN-SPAM ACT, etc.

V. CYBER LAWS IN INDIA

India is undergoing technological growth by leaps and bounds which in itself is good, but it is important to notice that the vulnerabilities associated with cyberspace are being witnessed at a faster phase in recent times. The Cyber Crime Statics by the National Crime Record Bureau published in 2017 reveals that the cybercrime rate has increased by 6.3 percentage in the year 2016 (in comparison with 2015 cybercrime rate), from the statistics it can be said that the cybercrime incidents in India inevitably poses both internal and external threats. Bengaluru is India's cybercrime capital.

To overcome these issues and to prevent such happenings The Information Technology Act, 2000 was enacted. The Act criminalizes certain activities as cybercrime. Apart from the Information Technology Act, 2000; The Indian Penal Code, 1860 has also been amended to punish cybercrimes.

1. CYBERCRIMES UNDER THE INFORMATION TECHNOLOGY ACT, 2000:

- Section 65 – Tampering with Computer source documents.
- Section 66 – deals with Hacking Computer systems, Data alteration.
- Section 67 - Publishing obscene information.
- Section 70 - Un-authorised access to the protected system.
- Section 72 - Breach of Confidentiality and Privacy.
- Section 73 - Publishing false digital signature certificates.

2. CYBER CRIMES UNDER THE INDIAN PENAL CODE, 1860:

- Section 503 - Sending threatening messages by email.
- Section 500 - E-Mail Abuse.
- Section 499 - Sending defamatory messages by email.
- Section 463 - Forgery of electronic records.
- Section 420 - Bogus websites, cyber frauds.
- Section 463 - Email spoofing.
- Section 383 - Web-Jacking.

 [ISSN 2581-5369]

3. CYBER CRIMES UNDER THE SPECIAL ACTS:

- Online sale of Drugs under the Narcotic Drugs and Psychotropic Substances Act.
- Online sale of Arms Act.

VI. REASONS FOR THE EXPANSION OF CYBER CRIME AGAINST WOMEN IN INDIA

LEGAL REASONS:

The object of the IT Act is crystal clear from its preamble that, it was created for enhancing e-commerce. Therefore, it covers a business or monetary crime i.e. hacking, fraud, and breach of confidentiality, etc. However, the drafters were unaware of the security of internet users. Most cybercrimes are being prosecuted under Section 66 (Hacking), 67(publishing or transmittal obscene material in electronic form), 72(breach of confidentiality). The foremost of the cybercrimes apart from e-commerce connected crime are being handled in these three sections. Cyber defamation, cyber defamation, email spoofing, cyber-sex, hacking and invasive into one's privacy is domain is incredibly common currently days however IT Act isn't expressly mentioning them underneath specific Sections or provisions. Whereas IPC, Criminal Procedure Code, and the Indian Constitution provide special protection to women and kids. For example, the modesty of women is protected underneath Section 506 and rape, forceful wedding, snatch and abortion against the need of the women are offenses and prosecuted underneath IPC. Indian constitution guarantees equal right to measure, education, health, food and work to women. However, an equivalent, modesty of women appears to not be protected generally apart from Section 67 that covers cyber-sex in Toto. Because it has been mentioned earlier that the transcendental nature of net is one in every of the most reasons for the expansion of cybercrime. Thus, Section 75 of the IT Act deals with the offenses or dispute committed outside India however it's not talking regarding the jurisdiction of the crimes committed within the computer network especially the question of place for reportage the case arises. Once the crime is committed in one place affected at another place and so reported at another place. Though within most of the cases, for the matter of territorial jurisdiction Criminal Procedure Code is being followed.

SOCIOLOGICAL REASONS:

Most of the cybercrimes stay unreported because of the hesitation and timidness of the victim and her concern of defamation of the family's name. Persistently she believes that she is chargeable for the crime done to her. The women are a lot of liable to the danger of cybercrime because the perpetrator’s identity remains anonymous and he might perpetually threaten and blackmail the victim with totally different names and identities. Although the women internet

 [ISSN 2581-5369]

surfers are terribly less in range, however the opposite teams targeting them on top of India, women still don't attend the police to complain against molestation, whether or not it's within the universe or the virtual world they like to shun off the matter as they feel that it should disturb their family life.

VII. CASE STUDY

1. BENGALURU AS THE CAPITAL CITY OF CYBERCRIME:

Bengaluru was registered with the greatest number of cybercrime cases in the year 2018. There were 5035 FIR's registered at the cybercrime police station in the city. According to the annual report released by the National Crime Records Bureau (NCRB) in 2016, with 762 cases, Bengaluru had the second-highest number of cybercrime cases among the metropolitan cities behind Mumbai with 980 cases. Other metros in the list were Hyderabad recording 291 cases, Kolkata 168, Delhi 90 and Chennai 36. From 762 to 5,035, the number of cybercrime cases has seen a drastic increase in Bengaluru.

This is an outcome of awareness and higher crime incidents in the city. Former DG and IGP of Karnataka ST Ramesh stated that Bengaluru was the first in India to get a cybercrime police station in 2001. Bengaluru is an IT hub and the number of IT companies here is high. People with awareness of filing complaints against cybercrimes are also high in number. This indicates that there are a greater number of cyber literates in Bengaluru.

But these approaches were merely noticed. The high reports of these complaints with the lone and unstaffed station have led to poor disposal of such cases. While there was a drastic increase in the rate of crime within a year, the number of charge sheets filed dropped marginally.

2. WOMEN AND CYBERCRIME LAWS - WEST BENGAL:

The legal structure of the Republic of India and the enforcement agencies don't seem to be however well-equipped to touch upon cyber violence or cybercrimes. Crimes against women type a vital a part of cybercrimes in the Republic of India and the on-line platform is currently the new platform wherever women's dignity, privacy and security area unit progressively being challenged each moment. In cybercrimes against women, the impact is additional mental than physical whereas the main target of the laws making certain women's security is additional on physical than mental damage. A recent study found 40 % of adult net users have tough harassment online, with young women enduring notably severe kinds of it. In the case of India, cyber violence against women is increasing and taking various forms as evident from

 [ISSN 2581-5369]

completely different on-line platforms and media reports. However the official crime information in India, the National Crime Records Bureau (NCRB), offers some figures that don't mirror the very fact properly and it conjointly focuses on the problem that there are some gaps within the accessible laws addressing cybercrimes and also the acts of cyber violence and it's additional evident in cases of cybercrimes against women. According to the information tracked by Indian Computer Emergency Response Team (CERT-In), a complete range of 44,679, 49,455, 50,362 and 53,081 cybersecurity incidents were discovered throughout the year 2014, 2015, 2016 and 2017, severally. The NCRB report 2016 states that in 2016 there have been 48,31,515 incidences of crime India below IPC additionally as Special and native Laws, which is 2.9% over the crime incidences of 2015. Of those total crimes, the number of cybercrimes is 12317 that is 0.25% of the full crimes. This is often comprehensive of cybercrimes against women. The law-breaking incidences have raised at a rate of 6.3% throughout 2015-16 and 20.5% throughout 2014-15. The number of cybercrimes in India in 2014 and 2015 is 9622 and 11592 severally. There's no parity within the proportion variation of rate generally and law-breaking rate with cybercrimes increasing at a far quicker rate and still forming a miserable proportion of total crimes in India. The subsequent table can show the individual rates at the national level.

TABLE:1

Table 1 shows cybercrimes type a negligible proportion of total crimes in India though the cases registered have raised quick. It shows either there doesn't seem to be adequate laws to hide all incidences or there's a lack of awareness of what constitutes law-breaking and seeking the assistance of the law. The standing of cybercrimes at the national level is mirrored in Table No.1. Table no. 2 can give us an idea of status in West Bengal.

TABLE 2:

The number of cybercrimes in the state in 2016 is 478 that is simply too low as compared to

different crimes below IPC and SLL. This figure is comprehensive of cybercrimes against women. The percentage of cybercrimes p.a. is lower or same thereto we've got found at the national level. At the national level, this proportion has been largely 0.2% for the last 3 years. Until 2011 the cybercrimes according to the state we tend tore abundant under what we witness these days. In 2011, there were solely forty-three according to instances of cybercrimes, that raised to 196 in 2012, a jump of 355 %. once more in 2014, there has been a rise of101% from that of 2012. From 2014 forwards it's not raised in this rate. Increase in the news of crimes and awareness concerning what constitutes crime area unit reasons behind this huge rate of increase. However, despite this increase, the proportion of cybercrimes remains remarkably low as compared to different crimes in state conjointly.

VIII. GAPS IN CYBER LAWS

The cybercrimes against women are unit gender-specific crimes that affect sole women. The SLLs that cowl cybercrimes against women are Indecent illustration of women (Prohibition) Act,1986 and the Information Technology Act,2000. However, this SLL has not been a widely used legal provision by victims of indecent illustration as this law doesn't offer for victims seeking justice; rather it empowers the state to require initiative to ban indecent illustration of women's body in print or visual media and take penal action if needed. The inadequacy of this law is additional evident if we glance at the number of cases registered below this law. The amount of cases registered below the law has shown a decline of forty 6.1% over the common of 5 years (2008-12) and a rise of 156.7% over the year 2012. Once more a decline of 14.9% was registered within the same crime head throughout 2015 as compared to 2014 when it had been 47. In 2015, 40 cases were registered, and it became 38 in 2016. In West Bengal, no cases were registered below this Act in 2016. Cybercrimes against women are a unit largely registered there under Act, 2000. Specifically, Section 66 A,66E,67 and 67 A touch upon crimes that affect women additionally. The conviction rate of the IT Act isn't in the least spectacular. In-a state, the number of cases registered below this section in 2016 was solely 6 and also the metropolitan town of the metropolis has no registered cases. Lack of awareness of the existence of laws, protective privacy of body or physical acts is a crucial reason behind this low range of registered cases. If the task of the enforcement agencies is restricted to registering cases and creating investigations, then this state of affairs goes to continue. Police and native administration should take measures to sensitize folks on the horizon of laws and civil society has to be concerned.

 [ISSN 2581-5369]

IX. Conclusion

Cybercrime news in Bharat is still in its aborning stage although cyber violence is quick growing. We've found the abnormally low figure of reported cybercrimes in the state that is once more comprehensive of cybercrimes against ladies. Cyberstalking is incredibly common unless a lot of severe violations like rape threat or revenge pornography aren't taken as a significant criticism. Our laws ought to be modified to form them cyber-sensitive also as gender sensitive. The attitude of the laws ought to confirm the dignity of ladies and not do a paternal role. Laws in this area are still inadequate and therefore the IT Act has to be amended to form it well-coordinated with IPC. A lot of IPC provisions ought to be amended to form them cyber-friendly. There ought to be one comprehensive law covering all aspects of cybercrimes against ladies. The police, the judiciary and the native administration should be cyber-friendly and well-equipped to handle shreds of evidence judiciously. Cybercrimes against ladies want a holistic approach with an amendment in laws, change in the approach of officers and a lot of intense sensitization campaigns involving different sections of society.

*****

 [ISSN 2581-5369]