IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

GENDER, SHAME AND TECHNOLOGY- CYBER CRIMES AGAINST WOMEN

Ananya Chakravarti

Abstract: The incident of cyber-stalking has come into the fore since the 19th century. Exponential advances in the development and use of computer and other technologies have provided exciting, constructive opportunities for advancement, productivity, and enjoyment. However, these remarkable advancements also have generated new arenas and tool for victimization. A crime only recently identified by the government agencies and the news media is cyber-stalking, the use of any number of electronic communication to stalk or harass any person.

1.INTRODUCTION

With advancement of technology and Internet, crimes or offences like cyber-stalking and other technology related crimes have increased and it is a major issue. Most discussions on internet enabled crimes focus on financial crimes, i.e. crimes against property. "Cyber-stalking is therefore unique, because internet has enabled a new form of crime against person, much like cases of distribution of child pornography or the use of encryption technology by members of organized crime to communicate privately". As per the "Working to Halt Online Abuse", "a volunteer organization fighting against online harassment, 50-75 cases of online abuse are reported every week alone in the U.S.A". This has only increased with the multiplication of social media platforms such as "Face book, MySpace, Orkut"[1] which has facilitated the commoditization of social relations and personal information. Such websites, by providing an insight into the fantasies, insecurities and alter egos of people, create a fertile ground for crimes such as cyber-stalking. Imagine discovering a message in your inbox that reads:

"I am your worst nightmare. Your troubles are just beginning"

Such kind of message creates a fear of being watched and harassed not just mentally but even physically.

[1] B.A. White, Second life: a guide to your virtual world, Que Publication house, 1st edition Page 416, 2007.

Stalking is when a person or a group of persons follows and watches another person, or set of persons to the point of obsession for reasons known or unknown. The exact reason for this behaviour is rooted in more than one factor, and the outcome of stalker's targeting isn't revealed until the victim is hurt or the stalker is apprehended. So, in the same way stalking is being done in the cyber world, by the medium of internet. Cyber-stalking is a crime in which the attacker harasses a victim using electronic communication, such as email or instant messaging (IM), or messages posted to a Web site or a discussion group. A cyber-stalker relies upon the anonymity afforded by the Internet to allow them to stalk their victim without being detected. Cyber-stalking messages differ from ordinary spam in that a cyber-stalker targets a specific victim with often threatening messages, while the spammer targets a multitude of recipients with simply annoying messages[2].

Stalking is not a new form of crime, however cyber-stalking is of recent origin as it has come into existence after the advent of modern technology such as the Internet. However, it is only recently that it has received attention as a serious crime. Till then the activities that characterized stalking were dismissed as minor and not deserving any State invention. Actions such as harassing phone calls, unsolicited gifts, persistent following and domestic assaults were either not covered by legislation or simply could be dealt with other provisions under criminal law. But the term stalking acquired broad public recognition in the west during mid -1990s when a number of criminal cases were widely reported in the media in which the offenders had repeatedly subjected his or her victims to either criminal behaviour or forms of harassment which fell short of being criminal. Initially, stalking was considered as a phenomena associated with celebrities, with obsessive fans following or trying to contact their idols. In response to the increasing number of incidents of stalking coming to attention of criminal justice system, new legislation were introduced in countries like UK. Model Anti-stalking code by the National Institute of justice of USA, for the adoption by its States[3], is an example of these efforts.

As technology advances, society is becoming increasingly reliant on computers and the Internet. The sphere of cyberspace facilitates information to be transferred over data lines and the anonymity which cyber-world provides, leaving millions of people vulnerable to cybercrimes. Big corporations, private industries, businesses, government agencies as well as individuals and children are at risk of privacy loss, harmful viruses, child pornography, sexual predators and stalkers. The field of stalking has experienced a great deal of refinement over the last decade; however its online counterpart is still barely understood.

In spite of the overwhelming attention that the phenomenon of stalking has received over the decades, cyber stalking remains the step child of the Criminal Justice System, functioning as a mere branch of stalking". Cyber stalking occurs when a person is persistently pursued online. This online harassment invades the victims' privacy in that their every online move is monitored. It disrupts the lives of victims as they feel afraid and threatened. The phenomenon of cyber stalking is intensified as cyber stalkers do not have to leave their homes to find or pursue

[2] http://searchsecurity.techtarget.com/definition/cyber-stalking

[3] As many as 17 states in the US have adopted Anti-stalking legislation.

their targets. The cyber stalking behaviour is further fuelled as the cyber stalker fears no physical violence based on the reliance of anonymity within the realms of cyber space. Cyber stalking can be just as threatening as stalking, leaving the victims vulnerable to a variety of aspects including anxiety, mental anguish and even physical harm. In this way, cyber stalking proves itself to be a menace in a technological world.[4]

Jurisdictions across the globe are now beginning to take legal action against cyber stalking behaviour, recognising it as a public problem which merits attention. The effects of cyber stalking upon an individual may have behavioural, psychological and social consequences.

2. NATURE OF CYBER-STALKING

There are various ways of committing cyber-stalking: One of the ways is computer stalking coupled with e-mail stalking where the perpetrator exploits the cyber-world and computer operating-system in order to hamper the user and takes control over them.

Cyber-stalking can be explained as a tool bound crime, its use of the Internet and cyber-space is essential.

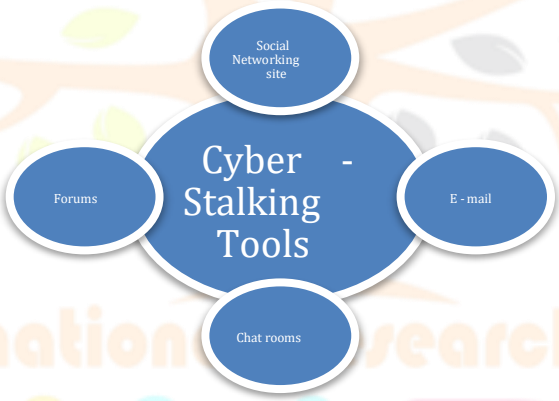

Fig 2.3.1 shows Cyber-Stalking tool and places for crime.

3. CYBER CRIME

The conceptualisation of cybercrimes emerged from the inception of the Internet and the consistent expansion of cyber technology. Cyber-crimes have thus resulted in challenges of addressing old and new crimes facilitated by the use of cyber technology. As clarified by Schell and Martin, cyber-crimes are crime allied to technology, computers and the Internet that causes harm to property and/ or persons.

[4] S. Basu, Stalking the Stranger in Web 2.0: A Contemporary Regulatory Analysis, European Journal for Law & Technology Vol.3 No.2, 2012.

The market for cybercrime is extended across the globe. The Internet makes provision for the creation and maintenance of illicit markets. Users can easily conceal their identities and be in various locations to create and participate in illicit online markets and activities. The nature of cybercrimes therefore creates opportunities for the relatively effortless commission of covert illicit online activities.

Cybercrimes can be divided into two broad categories: (i) cybercrimes resulting in harm to property, and (ii) cybercrimes resulting in harm to persons. The former category is commonly carried out using cracking techniques and includes various crimes such as flooding, virus attacks, spoofing. These types of crime have a primary goal which is to cause harm and damage to property by means of destruction, infection, corruption, fraud and theft. The latter category deals with the direct harm caused to persons through the commission of illegal activities. These crimes are more personal and often have lasting consequences. In essence, all that is required for the commission of cybercrime is an Internet connection and an individual with criminal intent.

.

4. THE SIGNIFICANCE OF CYBER SPACE

The Internet possesses innovative techniques that are significant to the sphere of cyber space. Computer culture allows its user a world of freedom, in that they can go anywhere and do anything within the realms of cyber space. Furthermore, cyber space has become an environment characterised by uninhibited consumption, voyeurism and fantasy. Within the realms of cyber space, new cultures are developed and practised. The Internet is a convenience for cybercrime communities to cohabit and flourish. These citizens are not alienated, rebuked or ostracised based on sex, age, race or marital status. They are accepted and, in some instances, supported and even encouraged. Thus, in cyber space, anybody can be whoever they want to be.

5. STALKING VERSUS CYBER STALKING

The concepts of stalking and cyber stalking are often confused, misunderstood and misinterpreted. Stalking is a crime but only as far as the anti-social behaviour meets the legislative criteria qualifying it as a crime. Although stalking had not been defined as a crime in India earlier, stalking was being addressed as an anti –social behaviour. Similarly, cyber stalking is distinguished as a crime through legislation and is defined in Indian Penal Code, 1860.

In general sense terms, stalking refers to harassing or threatening behaviour that an individual engages in repeatedly towards another person. It is a pattern of goal-oriented behaviour, both lawful and unlawful, promoted by a delusional and narcissistic perception of a relationship and intended to empower the 'predator' to feel omnipotent and in control, while reducing the prey's emotional stability to a state of vulnerability and fear. In quasi-legal

terms[5], stalking can be defined as a 'wilful course of conduct' involving' repeated or continuing harassment of another individual' that 'actually cause' the victim to feel terrorized, frightened, intimidated, threatened, harassed or molested and that would cause a 'reasonable person' to feel so.[6]

6. CYBER STALKING

The term cyber-stalking relates to the stalking taking place in the cyberspace. It's a non-physical jurisdiction in which information is exchanged and interactions occur, with the Internet being the avenue to reach this place. Cyber stalking can be defined as: behaviour in which an individual, group of individuals or organisation, uses information and communications technology to harass another individual, group of individuals or organisation. Such behaviours may include, but are not limited to, the transmission of threats and false accusations, damage to data or equipment, identity theft, data theft, computer monitoring, the solicitation of minors for sexual purposes and any form of aggression. Harassment is defined as a course of action that a reasonable person, in possession of the same information, would think causes another reasonable person to suffer emotional distress."

While this is only one of the several definitions propounded by criminologists, one factor that is accepted universally is the fact that the behaviour of stalking can range from the sending of a non-threatening e-mail to a more serious encounter between the stalker and his target and generally involves behaviour and action that is premeditated, repetitious, aggressive and vengeful.[7]

7. SOCIAL NETWORKS AS A COMMON PATH TO CYBER STALKING

Contemporarily, online social networking has transformed from a niche phenomenon, in that it was only used by few people, to mass consumption. The massive increase in participation within these social networks has also seen a development of variation and sophistication of function and usage patterns across various social networking sites. Millions of users adapt social network sites into their daily lives as it has become a lifestyle trend.

Through social networking technology, a social, collaborative and interactive platform has been created for Internet users to interact and communicate with each other by creating online profiles. As social networks advance and expand, so too, does the level and intensity of socialisation among Internet users. Users tend to become more open and candid, even desensitised, when expressing their personal thoughts and sharing information and thus become vulnerable to Internet violations.

[5] As distinguished from the literality of a statutory definition.

[6] Nandan Kamath, Law relating to Computers Internet & E-commerce, (5th ED. 2012) Universal Law Publication Co., Pg. 247264.

[7] ML Pittaro, Cyber Stalking: An Analysis of Online Harassment and Intimidation, 1(2) International Law Journals CYBER CRIMINOLOGY 180, 181 (2007).

Hill explains that a social networking web site is a virtual environment where people can connect with each other.[8] "Users can customise their profiles with pictures, details about their personal interests and values and they can provide contact information. An e-mail address is the only requirement needed to set up a profile on a social networking web site". Social networks allow their members to create a profile, a representation of themselves for others to follow with the intention of contacting or being contacted by others, to meet new friends or romantic interests and find new jobs.

Cyberspace has multidimensional implications for an individual's social identity. An individual enters cyber space in many different ways – "by entering a newsgroup or e-mail discussion group, playing an online virtual game or even just browsing social network sites. The management of identity is linked to the management of cyberspace. In this way, users become their own promoters through the media as they gain the public's interest and response". They promote themselves by sharing their opinions publically through status updates, debating on subjects or matters, communicating with authors other as well as publishing personal experiences through blogs.

People do not realise how much information they post on the Internet, leaving trails or significant information for cyber stalkers. Cyber stalkers use e-mail addresses, phone numbers, street addresses or even instant messaging to stalk their victims. In addition, provocative and recognisable photos on online profiles increase individuals' vulnerability to cyber stalking. They are viewed as easier targets than those who do not have photos of themselves. There appears to be general consensus among researchers that although social networks cannot be identified as the sole cause of cyber stalking; they do facilitate and help fuel cyber stalking as a deviant behaviour.[9]

Smith (2011) indicates that according to research conducted by the British "Electronic Communication Harassment Organization (ECHO), social networks are often used as a channel for harassment and intimidation".[10] More victims reported to having been tracked down through social networks than on dating sites. The research also concluded that in the case of cyber stalking, perpetrators were likely to be strangers, resulting in unclear motives for the harassment. Although social network sites are rated as the most common medium used in cyber stalking, victims are also located through search engines, online forums, message, boards, chat rooms or electronic mail.[11]. As Internet is a universal enabler, it is not only providing an opportunity for research and development of mankind

[8] Hill, S. 2010. *Social networking websites encourage stalking*. Available at: http://cyberpaths.blogspot.com/2009/02/socialnetworking-web-sites-encourage.html.

[9] Smith, C. 2011. *Cyber stalkers take to social networks over dating sites: Study*. Available at: http://www.huffingtonpost.com.

[10] Ibid

[11] www.apc.org/en/projects/mdg3-take-back-tech-end-violenceagainst- women accessed, cited at: www.genderit.org/es/node/2212.

but also providing a wide platform for criminal activity.[12] Offenders or people who want to pursue criminal activities find internet as a safe and fertile ground for their effort.

As technology is advancing with every second, on one hand it will bring development to society as new aspect of world will be explored and world will come close while on the other hand, issues like cyber-crimes, lack of privacy and terrorism will increase tremendously. The world is just one click away but it makes us technologically vulnerable and an easy means to those who want to pursue criminal activity. For example- a delusional lover who is fascinated by one person can easily extract all the information about that person by searching him/her online through information portal sites or social media,

"The issue of technology and its misuse by criminals increasingly runs like a golden thread through all discussions of the new security threats that face the contemporary world."[13] The growth of the internet – a key symbol of globalisation and the domain for the spread of information and the conducting of legitimate business transaction, equally, provides significant new opportunities for cyber-crimes such as fraud, cyber stalking, spread of pornographic material, the misuse of personal data and sabotage. Technology has facilitated terrorist organizations for making explosives or communicating in between themselves by using encrypted e-mails. Traffickers now not only transport tangible goods such as drugs or weapons by using advance technology but also facilitate their underground trade in 'intangible commodities such as child pornography.

The information technology is a double-edged sword, consistently presenting us with benefit and disadvantages. Today, internet utility and '.com' has become a household expression. The reliability and availability of the internet are critical operational considerations. Activities that threaten these attributes like spamming, spoofing, stalking have grave impact on its user community. Two important dimensions to be considered for the accelerated expansion of the technology that are- (i) Firstly, the use of technology has broadened from wealthy and sophisticated users to the wider population.[14] (ii) Secondly, even in the developing world the benefits brought by technological advances are not insignificant. Best example of this is that in many poor and even war-torn states, where official systems of governance have all but collapsed, the mobile phone and e-mail are ubiquitous symbols of technological penetration.[15] This dual shift of the use of technology- both downward and upward provides a critical space for the development of criminal opportunities that national frontiers can do little to contain. The best example to explain this is the speciality of West African criminal groups, which generally involve the request for an upfront payment on the promise of a greater financial reward, which never used to happen. Originally such letters were

[12] Peter R. Stephenson & Richard D. Walter, Annual symposium of Information Assurance (ASIA), June 7-8, 2011 Albany New York.

[13] Antonio M. Costa, emerging challenges Crime: New Frontiers for Regulation Law Enforcement and Research, 1st edition 2004 printed in Netherland.

[14] Ernesto U. Savona, Crime & Technology New Frontiers Research for Regulation and Law Enforcement, 1st edition 2004 Springer publication house.

[15] Ibid.

faxed to a few hundred possible victims; now the internet has been used as a resource to identify likely targets, with electronic mail providing an ability to make contact with thousands of possible victims simultaneously.[16]

Criminals are using technology to maximize their opportunity and minimize the risk of being detected and caught. In today's time, Information and communication technology (ICT) is used to maximize the possibility of crime by the means of technology. Increased attention is being paid to information and communication technology- related crimes as by the help of Information and communication technology criminals are communicating, to organise themselves better, widen the spectrum of their business, update their modus operandi and techniques and avoid law enforcement risk.[17]

The conception of cyber stalking evoked much international interest during the development of technology, thus generating an extensive body of work about it. Despite this wealth of knowledge there are still no clear universally accepted guidelines pertaining to the nature and extent of cyber stalking, as research is often confined to small-scale studies which cannot be generalised. In many countries, there is no specific anti-stalking legislation. A variety of research studies conducted internationally on cyber stalking and the dangers of social networks targeted students, as respondents, in a university environment. It may well be that the ever increasing use of the Internet by students is resulting in their amplified vulnerability to cyber victimisation.

In an informative cybercrime book by Hitchcock[18] the "author shares her own personal experience of cyber stalking victimisation". She recalls it as "commencing with receiving countless spam emails from an unknown individual. It later started to progress to abusive e-mails being sent out to the victim's colleagues from the assailant, posing as the victim. The perpetrator would also harass the victim by imitating her online persona and posting offensive comments about certain groups of people. The cyber stalking escalated when online advertisements were placed on the Internet, suggesting sexual innuendos from her. Her home address and phone number were provided. The harassment climaxed when the perpetrator threatened harm by means of rape and death to her. Due to intense fear and discomfort, she decided to relocate with her family. The perpetrators were apprehended and criminal and civil charges were laid against them". This account portrays a detailed description of the experience of a cyber-stalking victim depicting the escalating harm they endure.

[16] Ibid
[17] Ibid.
[18] J.A. Hitchcock, Net Crimes & misdemeanours: Outmanoeuvring web spammers, stalkers and con artists, 2nd edition, 2006, Information today Inc.

8. LEGAL ACTS, PROVISIONS AND PROTECTION

Law enforcement agencies in current scenario knows that cyber-stalking is a real issue which need to be dealt in a proper manner with the contribution of local police, state police, inspection service agencies, among others. It is the need of the hour and local citizens of respective countries are demanding these officers dealing with cyber-stalking and other such related offences to be well versed with technologies in order to tackle such offences.

In the 49th year of Indian independence, internet was commercially introduced in India. The beginnings of Internet were small and the growth of subscribers was slow. However, within a short time, internet grew exponentially and there was no stopping it. India has an extremely detailed and well defined legal system, where numerous laws have been enacted and implemented. But, there was a vacuum when it comes to cyber-space. In order to fill that vacuum, the Information Technology Act, 2000 was enacted. The reason for that was because
existing laws of India could not be interpreted in the light of the emerging cyber-space, to include all aspects relating to different activities in cyber-space. None of the then existing law gave any legal validity or sanction to the activities in cyber-space. There was no law or enactment to give legal validity to e-mails. The judiciary in our country was reluctant to give legality to e-mails. Internet requires an enabling and supportive legal infrastructure in tune with the times. Mobile laws, E-commerce laws, the future of Internet, can only be possible if necessary infrastructure complements the same to enable its vibrant growth. Thus it was felt that it was time to enact a cyber-law.

Meanwhile, the General assembly of the United Nation adopted the United Nation Commission on International Trade Laws (UNCITRAL) Model law on Electronic Commerce on January 30, 1997. Inspired by the UNCITRAL Model law n E-commerce, Government of India decided to enact a law that would make cosmetic changes to some other existing laws.

The Parliament of India under Article 253 of the Constitution, relying on the resolution of General Assembly of the United Nation passed India's first Cyber law. Information Technology Act, 2000 got assent from the President on June 9 and was implemented on October 17, 2000.

9. INFORMATION TECHNOLOGY ACT, 2000

Digital technology and new communication systems have made dramatic changes in our lives. The Indian parliament enacted in the fifty-first year of the republic of India, an act called the Information Technology Act, 2000. The problem with the Act lies in the Preamble itself where the statute adopts a more commercial outlook and does not even attempt to recognize in the Preamble, the intention of the statute to regulate non-commercial criminal behaviour perpetrated through an electronic mode.

[1] Legal Solutions

Nonetheless, the provisions of the IT Act do attempt to penalize acts of cyber-stalking. Prior to the 2008 amendment, the first section that dealt with the issue is Section 67, which made the publication of any material that is "lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons" punishable with imprisonment up to five years and fine up to one lakh rupees which may increase to ten years and fine of two lakh rupees if the offender is convicted for the second time.[19] The second provision on cyber-stalking is Section 72, which penalizes the disclosure of information obtained from "electronic record, book, register, correspondence, information, document or other material" without the consent of the concerned person with imprisonment up to two years and a fine up to one lakh rupees. The generality of these provisions cannot be over-emphasized and it is quite evident that a number of issues such as the use of innocent third-persons of the sending of e-mails which may nonetheless amount to harassment remain unaddressed by these provisions.

The amendment of 2008 has been an attempt to model India's act according to the laws of United Kingdom. Therefore, under Section 67A, the publication or transmission of material containing sexually explicit act or conduct in an electronic form has been made punishable with imprisonment up to five years and fine up to one lakh rupees. This provision only makes specific what was already covered under Section 67 of the pre-amendment Act. Section 66A is more specific to cyber-stalking. In this section, the sending of messages that are "grossly offensive or has a menacing character" or the sending of information that the sender knows to be false with the intention of "causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will" is punishable with imprisonment of three years. While the incorporation of this provision is commendable, it suffers from the same problems that have been outlined above with respect to the laws in UK and USA and require immediate rectification.

However this effective Section of Information technology Act 2000 was struck down in Shreya Singhal vs. Union of India[175], as it was creating problems and turning out to be troublesome for the society. As section 66A was too vaguely worded and would cover any opinion on any subject, the Court observed that the 'freedom of Speech and expression' is not absolute but it was necessary that one has to tolerate unpopular views of people. Reasonable restrictions which are given in article 19(2) of the Constitution of India can only be attracted when discussion and advocacy, the two basic foundations of Article 19(1) (a) reaches the third foundation of the said article that is, incitement.

After the particular section got struck down there was no other sections that dealt with cyber-stalking particularly, thus there is a need for proper legislation which deals with it.

[19] Section 67, IT ACT 2000.

10. THE WAY FORWARD

With the advent of technology, offences like cyber-stalking are extending their base. Therefore there is a requirement of dynamic provisions to tackle this issue.

The very first step in order to curb cyber-stalking is an amendment of Information Technology Act and bring back the particular Section 66A which was struck down by Supreme Court in Shreya Singhal vs. Union of India (2015). A new provision to tackle the issue will be an ideal solution. It can be incorporated within the Indian Pena Code (IPC) or shifted to Information Technology Act (IT Act).

Secondly, the offence of cyber-stalking should be amended in the Indian Penal Code, 1860 and be brought as gender-neutral offence rather than gender centric offence as laid down under Section 354D of the Indian Penal Code, 1860. Further, cyber-stalking should be defined from the point of view of victim's experience. So that all the aspects related to cyber-stalking can be covered. Those aspects are as follows –

(i) Malice
(ii) Premeditation,
(iii) Repetition
(iv) Distress
(v) Obsession
(vi) Vendetta
(vii) No Legitimate Purpose
(viii) Personally Directed
(ix) Disregarded Warnings to Stop Harassment and
(x) Threats

These aspects should be covered under one particular legislation so that it can deal more effectively and all the aspects by which stalking can be defined come within one fold.

[2] Non-legal Solutions

In addition to the recommended amendment, it is important for the Internet users to adopt some non-legal provisions. Following are certain non-legal provision that should be adopted:

1.Self-Regulation

In this, Internet users should be aware of the facts that many stalkers are out there so in order to save themselves Internet users should select gender-neutral username or id and form a meaning less password which will be difficult to crack. Internet users, mainly those who are active on social media sites should avoid putting personal information or post intimate or personal photos.

2.Use of Software Programs:

There are a number of software programs available on Internet which can control the content received. For example, there are many e-mail services providers, who provide services where certain mails will get deleted automatically from a specific e-mail address.

3.Regulation of Social Media Sites:

Internet users should properly go through the regulations given on these social media sites and keep their respective profile blocked from viewing by unknown people. All these social media sites have various options by which Internet users can restrict unknown people to view any photos and any other information contained there.

4.Role of Internet Service Providers (ISPs)

Certain steps have been taken by ISPs to restrict harassing behaviour. Therefore, most providers have specific addresses to report abuses, including social networking websites such as Facebook, which allows its users to report obscene content and abusive behaviour. In addition, ISPs also control unwanted e-mails by automatically sending to the "spam" folder. Holding ISPs accountable for dissemination of information will also come handy.

- **Measures from Government's End**

In order to curtail the offence, government should take some adequate measures, some of which are as follows –

1.Proper identification of the individuals, groups logging into the system which should be stored.

2.More static IP's should be made mandatory at users end to investigate Cyber-stalking offences

Government should ask residential places and all corporates business houses to have a static IP.

- **Victimization Surveys**

The availability of authentic data is an important factor in formulating criminological responses for the offence of cyber-stalking. India is still strategizing and making criminological inferences on the basis of foreign data which

limits the effectiveness of the efforts of criminal justice system. So to get to know the exact nature and extend of the problem, we must undertake authentic cyber-stalking victimization survey. These surveys can help our system to make sound and effective criminological response for the particular offence.

REFERENCES

[1] Anvar P. V. vs. P. K. Basheer (2012) Civil Appeal 4226 of 2012.

[2] Denzyl P. Dayal, *Spams Attacks, Cyber-stalking & Abuse* (Dominant Publisher & Distributors, 1st edition, (Page 145-204)2005).

[3] Eshan Salimi, Abbas Mansouabadi, "The criminology of Cyber-Stalking: Investigating the Crime, Offenders and Victims of Cyber-Stalking" (2014) International Journal of Criminology and Sociological Theory Vol. 7, No.2, Pg. 1-9.

[4] FBI 'Landmark Cyber stalking Case Results in Life Sentences for Three Family Members ' (*FBI*, 12 April 2016) <https://www.fbi.gov/news/stories/2016/april/landmarkcyberstalking-case-life-sentences-for-three-family-members/landmark-cyberstalking-case-life-sentences-for-three-familymembers> accessed 6 September 2022.

[5] Karan Girotra vs. State, (2012) VAD (Delhi) 483

[6] Laura F. Curtis, *"*Virtual vs. Reality: An Examination of the nature of Stalking and Cyber-stalking*" (2012)* San Diego State University

[7] Pavan Duggal, Textbook on Cyber Law, Universal Law Publication. (2nd Edition, 2016)

[8] Prasanto, K Roy 'Why online harassment goes unpunished in India' (BBC, 17 July 2015) < http://www.bbc.com/news/world-asia-india-33532706 > accessed 6 August 2022.

[9] S. Basu, "Stalking the Stranger in Web 2.0: A Contemporary Regulatory Analysis" (2012) European Journal for Law and Technology Vol. 3 No. 2

[10] Shreya Singhal vs. Union of India (2012) Criminal Writ Petition No. 167 of 2012.

[11] SV JOGA RAO, Law of Cyber Crimes & Information Technology Law (1st edition, Wadhwa & Company, Nagpur, India 2007).

[12] The Constitution of India, 1950

[13] The Information Technology Act, 2000

[14] The Indian Penal Code, 1860

[15] The State (cyber cell) Vs. Yogisha @ Yogesh Pandurang Prabhu (2009) 37th court, ESPLANADE, MUMBAI, C.C. NO. 3700686/PS.

[16] United States of America vs. David Thomas Matusiewicz et al. Criminal action No. 13- 83 United States District Court, D. Delaware.

[17] Vaishali Bhagwat 'The chilling effect on freedom of speech and expression' (Vaishali Bhagwat 1 April 2015) <https://vaishalibhagwat.com/2015/04/01/the-chilling-effect-on-freedom-of-speech-and-expressionin-cyberspace/ > accessed 7 August 2022

[18] Vishaka & Others vs. State of Rajasthan & (1997) Others JT 1997(7) SC 384