INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

ISSN: 2582-6433

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

www.ijlra.com
Volume 2 Issue 7 | Jan 2024
ISSN: 2582-6433

"EXPLORING THE CORRELATION BETWEEN CYBER STALKING AND SUBSEQUENT ONLINE HARASSMENT"

AUTHORED BY - UTKARSH PANDEY[1] & SWATI BARANWAL[2]

INTRODUCTION

Due to the swift growth that the internet has undergone in this era, it has fostered advances in almost every facet of society thus available and accessible to everyone and in every corner of the Earth. It is largely accountable for the developing and enhancing global commerce, promoting noteworthy progressions in education sector and healthcare, and expediating worldwide communication that was once considered to be restricted and expensive. However, it also has a darker side in that it has unlocked various opportunities for people to commit crimes which were previously unknown to us; such crimes not only challenges but also surpasses all physical boundaries, borders, and limitations to detect, punish, and diminish what appears to be a growing social problem of global proportions. The Internet has literally become a fertile breeding ground for an entirely new and unique type of criminal offender hereafter known as the cyber stalker. The cyber stalker is one who uses the Internet as a weapon or tool of sorts to prey upon, harass, threaten, and generate fear and trepidation in his or her victims through sophisticated stalking tactics, which for the most part, are largely misunderstood and in some cases, legal.

Cyber stalkers' behaviours, patterns, and tactics are largely misunderstood and to a certain extent – unknown. The term cyber stalking generally refers to the use of the Internet, email, or other electronic communication device to create a criminal level of intimidation, harassment, and fear in one or more victims. There is very little known about cyber stalking, but what is accepted is that cyber stalking behaviours can vary from a non-threatening email to a potentially deadly encounter between the stalker and the targeted victim. The obvious key to distinguishing traditional stalking from cyber stalking is that cyber stalkers rely predominantly on the Internet and other electronic communication devices to harass, threaten, and intimidate their targeted

[1] Research scholar, University of Lucknow
[2] Advocate, HC Of Delhi

ISSN: 2582-6433

victims. Most cyber stalking behaviours are premeditated, repetitious, and can be quite aggressive in their approach, but border on being illegal under current statutory law in most states.

CONCEPT OF CYBER STALKING

Stalking generally means a harassing behaviour which one person exhibits towards the other. The Oxford dictionary defines stalking as "pursuing stealthily". Stalking may comprise of following a person, appearing at a person's home or place of business, making harassing phone calls, leaving written messages or objects. At times there may be certain instances which are quite insignificant in themselves but when sufficiently repeated are often likely to provoke feelings of harassment in the victim, like sending letters or flowers to the target or a stranger, engaging the target in an unsolicited conversion in a public place such as at a bus stop, etc. Cyber stalking is a virtual form of physical stalking and can be categorized into two parts:

i. Cyber stalking that starts and continues on the internet and comprises of threatening victims on the internet, sending harassing e-mail or morphed photographs of the victim being displayed on pornographic websites.
ii. Cyber stalking that begins online and then spreads in the real world when the perpetrator finds out about the personal details of the victim and persistently follows the victim and may indulge into sinister behaviour like giving death threats and causing physical assault to the victim. Out of the estimated 79 million population worldwide on the internet at any given time, we could find 63,000 internet stalkers travelling the information superhighway, stalking approximately 4, 74,000 victims.

Nature of cyber stalking

There are myriad ways of committing cyber stalking which can be resorted to by the perpetrators. Computer stalking is one of the very popular means by which the cyber stalker exploits the internet and the windows operating system in order to assume control over the computer of the user. The cyber stalker can communicate directly with the user as soon as the user computer connects to the internet and assume control of the user's computer. An example of this kind of cyber stalking was the case of a woman who received a message stating "I'm going to get you". The cyber stalker then opened the woman's CD-ROM drive in order to prove he had control of her computer. Keystroke logging makes the recording of every keystroke possible and viewing the computer desktop in real time. E-mail account of the user may also be used as a tool for cyber

ISSN: 2582-6433

stalking. Access to an e-mail account of an innocent user may be gained by the hacker and that address may be used to send messages that may be threatening or offensive. Some may send electronic viruses that can infect the victim's files. A person's mailbox may be filled with thousands of unwanted messages in order to make the account useless by the harasser. It is known as mail bombing. Also, a cyber stalker may indulge in spamming.

Online stalkers may post insulting messages on electronic bulletin boards signed with the e-mail address of the person being harassed or statements about the victim to start rumors about him through the bulletin board system which is basically a local computer that can be connected directly with a modem and allows users to leave messages in group forums to be read at a later time.

Many cyber stalking cases begin from arguments that can take place in chat rooms or news groups. While chatting, participants type line messages directly to the computer screens of other participants. Chat-line users may capture, store and transmit these communications to others outside the chat service. Same is the case with the message which is posted to a public newsgroup as it is also available for anyone to view, copy and store and such public messages can be accessed by anyone at any time even years after the message was originally written which can be misused by stalkers. Cyber stalker may indulge in flaming wherein he may engage in live chat abuse of the user.

PROFILE OF VICTIMS OF CYBER STALKING

Those who are emotionally weak or unstable or have family problems and try to search for a sounding board in the virtual world may be an easy target of cyber stalkers. Cyber stalker victimizes a person who is a new user of the net and is inexperienced to the Internet safeguards. Further, the ones who portray no inhibitions and like to reveal personal information to strangers in chat rooms are easily befriended by the cyber stalkers. Cyber Stalking usually occurs with women, who are stalked by men, or children who are stalked by adult predators or pedophiles.

PROFILE OF CYBER STALKER

The first and foremost thing to remember is that anyone can be a cyber stalker. Stalker may be a friend, a neighbour or a relative also. Moreover, a stalker can be of either sex and can come from all backgrounds and life styles. Generally, the stalkers have an average IQ (Intelligence Quotient)

ISSN: 2582-6433

and are unemployed. Being socially incompetent, the stalkers have a profound sense of inferiority and tendency to control the life of others. In some cases, stalkers may be themselves victims of any kind of violence, and hence, they want to take out their frustration on others. Cyber stalkers can be broadly categorized into three types:

1. The delusional cyber stalker

   Schizophrenia, bipolar disorder and other mental illnesses are common in these stalkers due to which they are severely deluded into believing that their victim is in love with them even though they may have never met. The most common type of stalker from this group is the type who pursues a celebrity. This syndrome is better known as the "obsessed fan syndrome". It is a daunting task to get rid of delusional stalkers.

2. The obsessional cyber stalker

   Cyber stalker usually has had a prior relationship with the victim in this case and cannot come to terms with the fact that his or her relationship is over. He or she then tries to coerce the victim into re-entering the relationship or has his or her revenge on the victim by inducing fear and making his or her life miserable. One should not be misled by believing that this stalker is harmlessly in love and incapable of causing real harm.

3. The vengeful cyber stalker

   Disgruntled employees and ex-spouses who develop resent towards their victim as they inculcate a feeling that they were the ones who have been victimized first and now are merely teaching their victims a lesson, are the typical examples of such kind of cyber stalkers. Their actions are similar to that of the obsessional stalker but they differ in motive as, usually, they are desperate to induce fear in their victims by blackmailing or threatening them after taking over their computers.

FACTORS PROVIDING IGNITION TO A CYBER STALKER

Factors that motivate stalkers to commit brutal and barbaric crime of cyber stalking are envy, unemployment or failure in job or life coupled with an intention to intimidate their victims. Sexual harassment is a common experience offline and recent technological advancements have provided more impetus to it online also since internet reflects real lives and people. Pursuing the victim under the garb of anonymity online has made stalking easy for sexual gratification. Feeling

ISSN: 2582-6433

of revenge and hatred may also lead to cyber stalking when something knowingly or unknowingly said or done by the victim online offends someone. Obsession for love may be a pertinent cause for initiating cyber stalking. It can start with an online romance which moves to real life only to break-up once the persons really meet and one of them refuses to take "NO" for an answer. Another case may be when obsessive stalking starts in real life and then graduates to virtual world. Worst part about this kind of stalking is that perpetrator and victim are initially in an intimate relationship so it leads to sharing of personal information which is later on used to harass the victim.

Legal scenario in India

Section 66A of the Indian Information Technology Act, 2008 penalizes sending false and offensive messages through communication services. It reads as follows: "Any person who sends, by means of a computer resource or a communication device, -

a) Any information that is grossly offensive or has menacing character; or
b) Any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently makes by making use of such computer resource or a communication device,
c) Any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages, shall be punishable with imprisonment for a term which may extend to three years and with fine.

Explanation: For the purposes of this section, terms 'electronic mail' and 'electronic mail message' means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message. Section 72 Section 72 of the Indian Information Technology Act, 2008 which deals with breach of confidentiality and privacy, section 72A of the said Act which prescribes punishment for disclosure of information for breach of lawful contract read with section 441 and 509 of the Indian Penal Code (which deal with offences related to Criminal trespass and acts intended to insult the modesty of a woman respectively), were being used to prosecute offenders for cyber stalking before coming into force of the Criminal Law Amendment Act, 2013."

ISSN: 2582-6433

Now such offensive activities are to be dealt with by Section 354D of the Indian Penal Code, (added by the Criminal Law Amendment Act, 2013 with effect from 3rd February, 2013) which specifically makes provision for prosecuting the perpetrator of cyber stalking with harsher punishment. It reads as follows:

1. Any man who-
   i. Follows a woman and contacts, or attempts to contact such woman to foster personal interaction repeatedly despite a clear indication of disinterest by such woman; or
   ii. Monitors the use by a woman of the internet, email or any other form of electronic communication, commits the offence of stalking.

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

   i. it was pursued for the purpose of preventing or detecting crime and the man accused of stalking had been entrusted with the responsibility of prevention or detention of crime by the State; or
   ii. it was pursued under any law or to comply with any condition or requirement imposed by any person under any law; or
   iii. in the particular circumstances such conduct was reasonable and justified.

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

SUGGESTIONS

We strongly believe that in complete darkness we all are on the same footing and it is only our knowledge and wisdom that leads us towards light. Internet users must be proactive towards their safety and must keep in mind is that no one has the authority to harass any other person. To curb cyber stalking, instead of remaining a mute victim, the police must be informed immediately. For the prevention of cyber stalking, we would like to give following suggestions:

1. Real name must never be used as screen name of user ID and also personal information must never be disclosed in public places like chat rooms.

ISSN: 2582-6433

2. ISP and Internet Relay Chat network that have an acceptance use policy which prohibits cyber stalking should be preferably used.
3. Generally, every outgoing mail may have a signature that contains information about the sender such as telephone or fax number which gets automatically added to the end of the mail message by email program. While sending email to unknown persons personal details should be removed from signatures which are attached to the emails.
4. Computer keeps a memory reserve therefore memory catch after surfing internet must be removed so that anyone who accesses the computer cannot see what sites that person visited.
5. Harassment mails must be reported to Internet Service Provider like MTNL etc. and e-mail provider like Gmail, yahoo etc.
6. Advice from technically sound persons must be sought. Even the creator of the rampaging famous "I love you" virus was tracked down by street-smart users as stalker left behind a distinct electronic trail through his I.P. address.
7. Users must behave appropriately and politely while participating in chat room conversations and must never indulge in heated arguments.
8. A person must make sure that virus protection is up to date and passwords must also be changed regularly to keep the stalker away from personal computer.
9. Every now and then people must search for their name or their family members' name online and endeavour should be made to remove private or inappropriate matter.
10. Many cyber stalkers physically attack or rape their victims when they meet them in the physical world. Hence one must never meet an online acquaintance alone in the real world.
11. User can hide his or her identity with anonym misers which are famous for encrypting the URLs that a person visits so that an Internet Service Provider cannot keep a record of them.
12. Screening voice calls, SMS, chat and email may be done. If someone bothers in an online forum often communications from them can be blocked.
13. A person's plan to travel or attend a place must never be disclosed on any online calendars. Not even on social network sites where events are listed. Such disclosures are likely to enable a stalker to know a person's whereabouts.
14. Privacy settings in all online accounts must be used to regulate online sharing with those outside the trusted circle.

ISSN: 2582-6433

CONCLUSION

However, the issue of cyber stalking, being very sensitive, must be addressed immediately as it leaves a deep scar on the victim's psyche if left unaddressed. There is a general ignorance of the masses about cyber stalking. Hence it is imperative that awareness regarding this heinous-online-abuse should be spread amongst the people. Likewise, existence of the legal remedies to curb it must be brought to the knowledge of masses as it is the only silver lining in the dark clouds to dispel the atrocious darkness of cyber stalking.