INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Managing Editor of IJLRA. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of IJLRA.

Though every effort has been made to ensure that the information in Volume II Issue 7 is accurate and appropriately cited/referenced, neither the Editorial Board nor IJLRA shall be held liable or responsible in any manner what sever for any consequences for any action taken by anyone on the basis of information in the Journal.

ISSN: 2582-6433

EDITORIALTEAM

EDITORS

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

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

ISSN: 2582-6433

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.

ISSN: 2582-6433

"A DOCTRINAL ANALYSIS OF CYBERSTALKING LAWS IN INDIA: INTERPLAY BETWEEN THE BHARATIYA NYAYA SANHITA AND THE INFORMATION TECHNOLOGY ACT, 2000."

AUTHORED BY - DHANARAJ.V

Introduction

Cyberstalking sometimes referred to as online stalking or internet stalking is a form of cybercrime in which an individual uses digital means, often the internet, to harass or monitor another person. This electronic harassment can take many forms, including tracking someone's online activities, issuing threats, committing identity theft, stealing personal data, or fabricating information about the victim.

In essence, cyberstalking involves the unlawful and repeated targeting of an individual through online interactions.

Stalking, whether physical or virtual, is a clear infringement of Article 21 of the Indian Constitution, which safeguards the right to privacy. This principle was reaffirmed in the landmark case Justice K.S. Puttaswamy and Others v. Union of India and Others. The primary intent of such acts is often to instill fear in the victim, while an additional consequence can be social isolation.

Different types of psychological motives

Cyberstalking can stem from a variety of negative psychological states, including extreme narcissism, anger, jealousy, obsession, mental disorders, desire for control, sadomasochistic tendencies, sexual deviance, internet dependency, or even religious extremism. Different psychological motives can lead to such behavior, for example:

Jealousy: A powerful and uncomfortable emotion that can drive a person to monitor or harass someone, often in connection with a past or current romantic relationship.

Obsession and attraction: In some cases, the stalker develops an unhealthy fixation or desire toward the victim, blurring the line between admiration and harassment.

ISSN: 2582-6433

Erotomania: A delusional belief that the target, often a celebrity or stranger, harbors romantic feelings for the stalker, typically with a sexual component.

Sexual harassment: For many perpetrators, sexual motives form the primary driving force behind cyberstalking, reflecting the parallels between virtual and real-world misconduct.

Revenge and hatred: A stalker may direct their anger or resentment toward a victim who was not the original cause of those feelings, using the internet as a tool for retaliation.

A real-life example highlights the dangers of cyberstalking. “Seema Khanna” (name changed), an employee at the American embassy in New Delhi, became the target of persistent online harassment. In November 2020, she began receiving threatening emails from a man demanding that she either undress for him or pay ₹1 lakh. The messages warned that her altered photographs and personal information—including her phone number and address—would be published on explicit websites and circulated in her local community.

Initially, Khanna ignored the threats. However, the harassment escalated when she began receiving letters by post with the same menacing tone. The situation compelled her to file a police complaint. The stalker later sent her private photographs via email—images she had stored in her own email account. Investigators concluded that the perpetrator had gained access by hacking her password.

Tracing the emails led police to a cyber café in South Delhi. Deputy Commissioner of Police Dependra Pathak stated, “We aim to identify and apprehend the offender at the earliest.” Authorities also suspected that the stalker had prior acquaintance with the victim, given his level of personal knowledge about her life.

Cyberstalking Definition

Cyberstalking is a type of online harassment in which a person threatens, intimidates, or upsets another individual or group via electronic contact. This conduct, which can be challenging to trace, often includes continuous unwanted contact via phone calls, texts, emails, social media posts, or other online channels. In order to obtain victims' personal information or keep tabs on their internet activity, stalkers may also employ spyware or hacking.

In many countries, including India, cyberstalking is prohibited by the Indian Penal Code (IPC) and the Information Technology Act of 2000. In a particular case, a Delhi woman was subjected to persistent harassment by an acquaintance via fake online profiles and threatening emails. After employing malware to track her online activities, the stalker was ultimately taken into custody, demonstrating India's increasing efforts to stop cyberbullying.

ISSN: 2582-6433

STALKING DEFINITION UNDER BHARATIYA NYAYA SANHITA (BNS)

SECTION 78 STALKING

1. Any man who,
    1. 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
    2. monitors the use by a woman of the internet, e-mail 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,
        1. it was pursued for the purpose of preventing or detecting crime and the man accused of stalking had been entrusted with the responsibility of prevention and detection of crime by the State; or
        2. it was pursued under any law or to comply with any condition or requirement imposed by any person under any law; or
        3. 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.[1]

INFORMATION TECHNOLOGY ACT 2000

- **SECTION 67 Punishment for publishing or transmitting obscene material in electronic form. -**

  Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in

[1] Indiacode https://www.indiacode.nic.in/handle/123456789/20062

ISSN: 2582-6433

it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

- **Section 67A: Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form**

  Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

  Exception: This section and section 67 does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form-

  (i) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting, representation or figure is in the interest of science,literature,art,or learning or other objects of general concern; or

  (ii) which is kept or used bona fide for religious purposes.[2]

- **67B. Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form.**–Whoever,–

  (a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct; or

  (b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or

[2]indiacode https://www.indiacode.nic.in/handle/123456789/20062

ISSN: 2582-6433

(c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or

(d) facilitates abusing children online, or

(e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children,

shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees

Provided that provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting representation or figure in electronic form–

(i) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting representation or figure is the interest of science, literature, art or learning or other objects of general concern; or

(j) (ii) which is kept or used for bona fide heritage or religious purposes.

LEGAL PERSPECTIVE OF CYBERSTALKING

In India, the legal enforcement community first realized the existence of cyberstalking crime much later than in other nations such as the US, UK, Canada, and Australia, where cyberstalking is criminalized. Even though stalking cases in India were first documented twenty years ago, the IT Act, 2000, which was later revised in 2008, established the laws pertaining to cybercrime. The IT Act is deemed insufficient and addresses "intrusion on the privacy of individual" rather than cyberstalking directly. Women's safety has become a top priority following a number of unsettling and extensively publicized incidents, including the "Delhi gang rape and murder" that occurred in December 2012 and the cybercrime-related incident that occurred at the Delhi Metro station in 2013.

There aren't many studies from an Indian perspective that address how cyberstalking is enforced legally in India. For instance, the rise of the Internet is seen in Kashmiria as a catalyst

ISSN: 2582-6433

and opportunity for cybercrimes. She concludes that the Indian cyberstalking laws are insufficient for deterring crime and punishing offenders after contrasting them with regulations from the UK and the USA. In a similar vein, Halder & Jaishankar's comparative analysis of cyberstalking laws in the UK, USA, and India has brought attention to the significance of secondary victimization and denial of justice as the primary causes of the crime's spread. The paper by Sadotra and Kour illustrates the different ways that cyberstalking and harassment in India can be addressed using the common law and existing legislation**.**

TECHNICAL ASPECTS OF CYBER STALKING

The use of cyberstalking techniques is both encouraged and discouraged by technology. Stopping the stalker's actions to prevent the crime from occurring and assisting law enforcement are the challenges.

The stalker is located and identified by law enforcement. ICT, internet technology, IP-connected devices such as computers, smartphones, and tablets, as well as communication tools like SMS and instant messaging, have all been linked to an increase in cyberstalking crimes, according to a small number of research conducted from an HCI perspective. Technical methods to prevent the crime and assist the victim and law enforcement in locating and apprehending the stalkers have also been made public by these investigations. Face-to-face encounters and text-based technology-mediated communications, such as email and instant messaging, are not the same.

Kinds of Cyberstalking

Cyberstalking can be classified into three different types, which are as follows:

Email stalking has grown in popularity in the real world, much like other stalker techniques like phone calls, letters, and physical surveillance. Cyberstalking, on the other hand, can take many different forms. Unwanted electronic mail, which can contain insulting, hazardous, or hostile messages, is one of the most common forms of harassment.

Sending the victim too much junk mail or malware are examples of other types of online harassment. Keep in mind that telemarketing calls or virus distribution are not stalking in and of themselves.

Internet stalking

Stalking on the Internet It is conceivable that stalkers would make considerable use of the int

ISSN: 2582-6433

ernet to disseminate false information about their victims and endanger them. Cyberstalking f requently turns into a public problem rather than a personal one. Because it appears to have th e greatest potential to spread into real life, this type of online stalking is particularly concerni ng. Cyberstalking can occasionally be accompanied by more conventional stalking tactics, su ch as frequent phone calls, threatening letters, graffiti, and even physical assaults. People who are frequently within bullet range of their stalker and others who are stalked from 2,000 mile s away have quite different experiences.

Computer stalking

Cyberstalking Last but not least, computer stalking is a subset of cyberstalking that entails usi ng the victim's web browser to access their Windows computer. The fact that every Windows computer with an active Internet connection can be located and remotely connected to anothe r computer is probably not well known. This connection allows the hacker to take over the vi ctim's computer without interference from third parties. The cyberstalker can usually start a di rect conversation with the victim once their machine connects to the Internet in any way. The victim's sole defence if a stalker gains access to their computer is to change their IP address a nd cease accessing the Internet.

How to identify Cyberstalking

Sometimes it might be hard for the victim of harassment or stalking to understand that what they are experiencing is illegal and needs to be reported to the police. When determining whether a circumstance qualifies as stalking, the victim should think about whether the offender is acting intentionally and maliciously. A persistent, obsession-driven grudge that is aimed directly at the victim is frequently the basis for stalking behavior. Even after the victim has directly warned the offender to cease, this practice continues.

Key indicators for spotting incidents of cyberstalking include:

False accusations.

A cyberstalker frequently posts misleading information on blogs or social media sites in an attempt to harm his victim's image. To disseminate false information and accusations about the victim, a perpetrator may even set up fake websites or other accounts. collecting data on the victim. A cyberstalker may engage with the victim's friends, family, and coworkers in an effort to learn as much as they can about them. A cyberstalker may engage a private investigator in extreme circumstances.

ISSN: 2582-6433

Monitoring the victim's activities.

To find out about his online activity, a cyberstalker can try to track down his victim's IP address or break into his emails and social media accounts.

encouraging the victim to be harassed by others.

The offender may encourage the involvement of third parties to harass the victim.

False victimization.

It is not uncommon for a cyberstalker to claim the victim is harassing him, taking the position of victim in his own mind.

Is cyberstalking is crime?

In many nations, including the US, cyberstalking is illegal. However, laws differ greatly:

United States:

Cyberstalking is covered under state and federal legislation, including the Violence Against Women Act. Fines and jail time are examples of penalties.

United Kingdom:

Protected by theMalicious Communications Act of 1988 and the Protectionfrom Harassment Act of 1997.

European Union:

Article 8 of the European Convention on Human Rights is violated by the practice of doxing.

Other Countries:

To protect their citizens, countries like Singapore, Australia, Canada, and India have put anti-cyberstalking legislation into place. Due to jurisdictional concerns in cross border cases and the anonymity of offenders, implementation of current legislation might be difficult.

Legal Framework Around the world

Ubited kingdom

The United Kingdom does not have a dedicated statute exclusively addressing cyberstalking. Instead, the issue is dealt with under three primary legislations that target harassment in general, which are also applied to online stalking cases. These are the Telecommunications Act, 1984, the Malicious Communications Act, 1988, and the Protection from Harassment Act, 1997.

Under the Telecommunications Act, 1984, it is a criminal offence to send messages that are indecent, threatening, or otherwise inappropriate. The Malicious Communications Act, 1988,

ISSN: 2582-6433

which has a broader scope, criminalizes the sending of letters or the delivery of articles intended to cause distress or anxiety to the recipient.

If you'd like, I can also rephrase the next country's legal framework in the same clear and academic style so the whole section is consistent.

Strengthening Legal Frameworks: Suggestions and Recommendations

At present, India does not have dedicated legislation to specifically tackle online hate speech. Although certain provisions under the Indian Penal Code (IPC) and the Information Technology (IT) Act provide some avenues for legal action, these measures face notable limitations. For example, Section 153A of the IPC prohibits promoting hostility between different communities, while Section 295A criminalizes deliberate acts intended to insult

Case Study – Cyber Stalking Incident

Seema Khanna (name changed), employed at an embassy in New Delhi, never anticipated that her routine internet browsing would turn into a serious breach of her privacy.

In what appears to be a case of cyber stalking, she began receiving a series of threatening emails from a man demanding that she either pose nude for him or pay ₹1 lakh. According to her complaint filed with the Delhi Police, the harassment started in the third week of November.

The offender warned that if she did not comply, he would upload morphed images of her to adult websites, along with her phone number and address. He also threatened to circulate these images in her local neighbourhood in southwest Delhi.

At first, Seema ignored the messages, but soon similar threats began arriving by post. This escalation left her with no choice but to approach the police, according to an officer from the cybercrime cell.

The situation worsened when the stalker emailed her some photographs, which she recognised as the same ones stored in her private email folder. Investigations revealed that her email account had been hacked, giving the accused access to her personal pictures.

Preliminary police inquiries traced the emails to a cyber café in South Delhi. Deputy Commissioner of Police (Crime), Dependra Pathak, stated that efforts were underway to locate the perpetrator, who might be someone familiar with the victim due to his detailed knowledge about her.

The accused faces potential charges under Section 509 of the Indian Penal Code, for insulting the modesty of a woman, as well as relevant provisions of the Information Technology Act, 2000.

ISSN: 2582-6433

Case Law:

Aditya Alias Manoj Soni v. State of Madhya Pradesh (22 February 2017)

In this matter, Mr. A.K. Jain appeared as counsel for the applicant, while Mr. Vijay Soni represented the State. The application was filed under Section 439 of the Code of Criminal Procedure, 1973, seeking bail for the applicant, Aditya alias Manoj Soni, in connection with Crime No. 671/2016 registered at Police Station Kotwali, District Damoh. The case involved offences under Sections 384, 386, 452, 420, 467, 471, and 509 of the Indian Penal Code, along with Section 67 of the Information Technology Act.

According to the prosecution, the applicant allegedly engaged in cyberstalking a married woman via Facebook. It is claimed that he created a fake profile under the name "Kunal Adhiraj Singh," using the photograph of the Superintendent of Police, Sagar, as the display image. Through this false identity, he allegedly initiated online communication with the complainant via Facebook Messenger.

During these interactions, the complainant reportedly sent her photographs to the applicant upon his request. The applicant is then accused of sending her obscene images, which prompted her to object and delete them from her account. Subsequently, he is alleged to have demanded ₹5,000 from the complainant, threatening to defame her on social media if she refused. The prosecution asserts that the applicant not only made the demand but also personally collected the money

Strengthening Legal Frameworks: Suggestions and Recommendations

At present, India does not have dedicated legislation to specifically tackle online hate speech. Although certain provisions under the Indian Penal Code (IPC) and the Information Technology (IT) Act provide some avenues for legal action, these measures face notable limitations. For example, Section 153A of the IPC prohibits promoting hostility between different communities, while Section 295A criminalizes deliberate acts intended to insult religious beliefs. Despite their intent, these provisions are frequently criticized for their broad and ambiguous wording, which can lead to misuse and the suppression of legitimate expression.

Similarly, Section 66A of the IT Act, which once permitted the removal of "offensive" online content, was invalidated by the Supreme Court in 2015 for infringing on the right to free speech.

ISSN: 2582-6433

Conclusion and Suggestions

The most appropriate way to report incidents of cyberstalking or related offences is through an online help desk or by approaching the local cybercrime cell. In line with Rule 2(b) of Chapter II of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, online platforms are obligated to remove flagged content within 24 hours of receiving a complaint. Apart from filing a report with the police, victims can also approach the Indian Computer Emergency Response Team (CERT-IN), the nodal agency appointed under Section 70B of the IT Act. Another convenient option is to lodge a complaint through the National Cyber Crime Reporting Portal.

On an individual level, preventive measures can significantly reduce the risk of cyber offences. These include setting strong, complex passwords containing both letters and numbers, and avoiding the disclosure of excessive personal details on social networking sites. From a legislative standpoint, amendments to the Information Technology Act are necessary to strengthen enforcement mechanisms. Additionally, expanding the scope of existing laws to include extraterritorial jurisdiction would enhance the ability to combat cybercrimes committed across borders.