*Page 668 - 687* **DOI:** *https://doij.org/10.10000/IJLMH.111976*

# INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

**Volume 4 | Issue 5**

**2021**

© 2021 *International Journal of Law Management & Humanities*

Follow this and additional works at: https://www.ijlmh.com/
Under the aegis of VidhiAagaz – Inking Your Brain (https://www.vidhiaagaz.com/)

This Article is brought to you for "free" and "open access" by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in International Journal of Law Management & Humanities after due review.

In case of **any suggestion or complaint**, please contact **Gyan@vidhiaagaz.com**.

**To submit your Manuscript** for Publication at **International Journal of Law Management & Humanities**, kindly email your Manuscript at **submission@ijlmh.com.**

# An Exploratory Study on the Concept and the Form of Stalking as a Cyber Crime

ARNAB KUMAR GHOSH[1]

## ABSTRACT

*Social networking technology provides a collaborative and interactive platform for Internet users to socialize. Users are more open to expressing their thoughts and sharing information, increasing internet violations in the process. Cyber stalking is a violation faced by internet users. Cyber stalking is a real stalk evolution. It is like stalking others through communication technology. Some overt methods of cyber stalking and digital harassment include "attacks" by unwelcome friends requesting or sending messages, spam, and the transmission of viruses. Behaviors such as sending abusive, threatening, or obscene emails to the victim or the victim's family are likely to be further exacerbated. According to a survey those who uses the Internet for more than three hours a day, they were vulnerable to online stalking. Additionally, those who used the Internet for more than five hours a day were faced with cyber stalking. 50% of these cases are not even reported to the police. This cyber stalking has a great psychosocial impact on individuals. Victims report many serious consequences, including increased suicidal thoughts, fear, anger, depression, and post-traumatic stress disorder (PTSD) symptoms. Faced with this phenomenon, they devised strategies such as family-friendly and asking for help from trusted friends. The positive effect of cyber stalking exposure is that they tend to be careful and cautious about sharing personal information through social networking sites, depending on whether they are online or not. In order to assess these social issues, we need to look at various aspects of cyber stalking.*

***Keywords:*** *Internet, Communication, Psychological, Victimization, Information.*

## I. INTRODUCTION

The old adage, “sticks and stones may break my bones but words will never harm me” does not apply in the worlds of Internet technology, where false, hurtful or humiliating comments can go viral and global in just seconds. It is needless to repeat and will always hold true that- Nothing ever goes away once it is posted online. With the advent of the Information and Communications Technology, Cyber stalking has grown to become a big concern for law

[1] Author is a student at KIIT School of Law, India.

© 2021. International Journal of Law Management & Humanities [ISSN 2581-5369]

enforcement and anyone engaged in online activities[2]. Cyber stalking is a relatively new terrorist. Often, priority is lower than Cyber terrorism, which is a global important topic. It quickly spreads out due to the anonymity and confidentiality of the Internet. Legal advances to protect people from Cyber stalkers are limited to the geographer in the relevant state or the country. This chapter describes online actions of the effects and steps that you need to stop it. India not only grabbed one of the first ranks to swallow the highest number of internet users, which we also know as global sexual harassment statistics. The scale with online women who reflect harassment images that they are in the material scale. A poll conducted by the feminism in India has emphasized that 50% of women are confronted in large Indian cities online abuse. What an excellent surge in the cases of Cyber stalking against men on a mutation. Experts are finished that this rate is 50:50 cyber stalking cases that face men and women[3]. As a result of the pandemic, physical stalkers have certainly been replaced by virtual stalkers. With so many applications, stalker, spyware, social networking tools and other technologies available, stalking people has never been easier. "Cyber stalking" is defined as a stalking crime in which a stalker uses the Internet or other electronic devices to stalk someone. Online harassment and online abuse are used synonymously with cyber stalking. The Internet has opened up a medium for faster communication and data sharing. People can interact with each other and access each other's information with the click of a social media site. Meanwhile, technology includes loopholes that allow criminals to abuse the freedom of such an approach, and cybercrime is on the rise in India. Stalking is related to a phenomenon referred to as Obsessive Relational Intrusion (ORI), designed for the development of intimacy. ORI is an undesirable desire for intimacy by repeated intrusion into a person's physical or symbolic individual senses. This chapter ends with the application of social learning theory, many of which act as both bullies and targets. For example, children exposed to domestic violence at home are more likely to bully others than children who are not exposed to domestic violence[4]. So, in this article we will be discussing all forms of cyber stalking and ways to prevent those cyber stalking through different laws and sections present in India.

## II. METHODOLOGY

This doctrinal study or a non-empirical study performed on cyber stalking by an undergraduate student. A doctrinal methodology was selected for this research project as a means to examine

[2] https://www.risingkashmir.com/-Cyber-Stalking-and-Cyber-Bullying--There-s-someone-watching-you---I-90285

[3] https://vidhisastras.com/cyber-stalking-in-india/

[4] https://www.sciencedirect.com/science/article/pii/B9780128159170000034

people before and after COVID times those who have been stalked, harassed or threatened through the use of the Internet, email or other forms of electronic devices. I have done it with the help of secondary research method. Collectively, I have tried to gathered data from sources including internet, journals, blogs and articles. Qualitative research based on primary data collected from different survey by using an online platform.

## III. LITERATURE REVIEW

### (A) What is a cyber crime?

Cyber stalking is the act of stalking or harassing someone over the Internet. It can be set on individuals, groups, and even organizations, and can contain slander, defamation, and intimidation. The purpose may be to control or intimidate victims, or to obtain information about other crimes such as theft of personal information and online stalking. This happens in places like social media forums, emails, etc. over the internet. It is usually planned and runs for a while. Other forms of cyber stalking can be used to stalk victims and make their lives uncomfortable.

Cyber stalkers may, for example, stalk their victims on social media, trolling and sending threatening comments; they may even hack email accounts to connect with the victim's connections, including friends and employers. Faking photos on social media or sending threatening private messages are examples of social media stalking[5]. Cyber stalking does not always require direct conversation, and some victims are unaware that they are being followed online. Perpetrators might utilize numerous tactics to monitor victims and utilize the information acquired for crimes such as identity theft. Users' personal information, such as images, addresses, contacts, and whereabouts, are accessible via social networking websites and mobile apps. This information can be used by stalkers to threaten, blackmail, or physically contact the victim. Emails are also used by cyber stalkers to track down a target. Hacking can give a stalker access to a person's email account, **(**Haryani & Farahidah, 2010) which they can then use to send threatening or obscene messages. Some emails are infected with computer malware or viruses, rendering the email useless to the sender.

For example, if you've received a few negative comments on Facebook and Instagram, it may upset or annoy you, but this isn't cyber stalking yet. For some people, such as semi-celebrities looking for attention, negative comments are actually welcomed[5].

### (B) What can cyber stalking constitute?

[5] https://www.tripwire.com/state-of-security/security-awareness/what-cyberstalking-prevent/

- False accusations of a defamatory character.
- Hacking or vandalizing the victim's website.
- Making sexual comments.
- Publishing materials so as to defame a person.
- Personally targeting the victims of crime.
- Humiliating someone to form a gang against them.[6]

**(C) Difference between Online and offline stalking:**[7]

| **Cyber Stalking** | **Offline Stalking** |
|---|---|
| Cyber stalking is online threat and there is no direct relationship between the victim and cyber stalker. | Offline stalking is direct physical threat to the victim and there is some relationship between the victim and the stalker. |
| Cyber stalking is universal. | Offline stalking is particular. |
| No prior clear identity about the cyber stalker. | Clear identification about the offline stalker. |
| Cyber stalking is posting a nude or semi nude photo in the internet and using obscene language and verbal intimidation. | Direct physical threat in offline stalking. |
| Enforcement of law is easier in offline stalking. | Cyber stalking sometimes requires extradition. |

**(D) Kinds of cyber stalking**

- *Catfishing* – In Catfishing, Stalkers create a fake profile on social media to approach victims. Sometimes they copy the existing user's profile with photos to look it like a real one.
- *Monitoring location check-ins on social media* - Stalkers keep an eye on the activities of a victim from their check-ins on social media such as Facebook and Instagram. This is an easier job for a stalker to gauge a victim's behavioral pattern quite accurately.

[6] https://blog.ipleaders.in/virtual-reality-cyberstalking-india/
[7] https://www.latestlaws.com/articles/how-to-file-cyber-stalking-complaint-in-india-by-buelah-pranathi-gollapudi/

© 2021. International Journal of Law Management & Humanities [ISSN 2581-5369]

- *Visiting virtually via Google Maps Street View* - If a stalker discovers the victim's address, then it is not hard to find the area, neighborhood, and surroundings by using Street View. Tech-savvy stalkers don't need that too. They can discover the victim's place from the posts or photos posted on social media.

- *Hijacking webcam* - Computer's webcam hijacking is one of the most disgusting methods of cyber stalking to invade the victim's privacy. Stalkers push malware-infected files into the victim's computer which gives them access to the webcam.

- *Installing Stalkerware* - One more method which is increasing its popularity is the use of Stalkerware. It is a kind of software or spyware which keeps track of the location, enable access to text and browsing history, make an audio recording, etc. And an important thing is that it runs in the background without any knowledge to the victim.[8]

**(D) Types of Cyber Stalking**

- *Email Stalking:* Direct Communication through E-mail or electronic mail is the most commonly used network based application. Today, it has become the most common way to harass threat or stalk a person. Stalkers send spontaneous mails in which lead to nuisance, hatred, obscenity or threats. Such stalkers repeatedly send mails to their victims for and try to initiate or fix a relationship or threaten and hurt a person.
- *Internet Stalking:* Global communication through the Internet. Stalkers comprehensively use the Internet to slander and endanger their victims. Cyber stalking takes on a different public dimension. What makes it disturbing is that it appears to be the most likely to spill over into physical space. Generally, cyber stalking is accompanied by traditional stalking behaviors such as threatening phone calls, vandalism of property, threatening mail, and physical attacks. There are important differences between the situation of someone who is regularly within shooting range of her/his stalker and someone who is being stalked from two thousand miles away.
- *Computer Stalking:* Unauthorized control another person's computer. In this type, the stalker, by unauthorized access, controls victims' computer. The stalker can thus communicate directly with his victim when the target computer connects to the Internet. Stalker assumes control of the victim's computer and the only defense left for the victim is to renounce their current Internet "address". (Maahi, 2018)

**(E) Types of Cyber Stalkers**

[8] https://www.lawyered.in/legal-disrupt/articles/what-is-cyberstalking/

© 2021. International Journal of Law Management & Humanities [ISSN 2581-5369]

**1.** *Vindictive Cyber stalker:* This group threatens victims more than other groups, and in most cases also includes offline behavior. One-third of this group is known to have previously had two-thirds of their criminal records at the expense of others. His ability to use computers was highly evaluated by the victims along the way. This group afflicted victims more than any other group using a wide range of Internet tools such as spam, email bomb attacks, and personal information theft. This group was also the only group using the Trojan horse program. Three-quarters of victims in this group reported threatening multimedia images or audio files (skulls and crossbones, corpses, screams, etc.), receiving strange or distorted/irrelevant comments. Mental problems. Two-thirds of these victims knew the stalker before the victim started. Half of the victims said that the bullying started off trivial and flew in all proportions. A third of victims reported no apparent reason for stalking. The remaining victims admitted that they had previously had active discussions with the stalker.

**2.** *Composed Cyber stalker*: This group is made up of stalkers who are not willing to establish a relationship with the victim. The obvious purpose was only to induce and distress the victims with constant annoyance and frustration. This group was presumed to have medium to high level computer skills. This stalker poses a generalized threat to the victim. Only one person in this group had a stalk history before. No one in this stalker group was mentally strong. Nevertheless, he stalked three offline victims.[9]

**3.** *Intimate Cyber stalker*: This group consists of two subgroups, one who is actually close and one who is enthusiastic. Relatives were acquaintances and acquaintances of the victim. Passionate people were individuals who wanted an intimate relationship with their victims. This group was characterized by what interests them or seeks relationships with their victims. Victims also reported that the group possessed a wide range of computer technologies, from a much lower level to a higher level than the other groups. The stalker used e-mail, web discussion groups, and e-dating sites to reveal detailed knowledge of the victim. The intimate subgroup was engaged in online behavior, even intimidating a loved one or friend of the victim, as they seek to restore their relationship with the victim. In some cases, an intimate person pretended to be a victim, pretending to be a partner in a chat room or buying a product online by name. This subgroup had no cases of offline stalkers after cyber stalkers. Often through more intimate communication than other subgroups, passionate people were trying to build a closer relationship with their victims. But when their attempts were rejected, their messages became more threatening. In that unfortunate case, the criminal has stalked the victim offline.

[9] https://www.sciencedirect.com/science/article/pii/B9780124078178000023

© 2021. International Journal of Law Management & Humanities [ISSN 2581-5369]

**4.** *Collective Cyber Stalkers:* This last group involved two or more individuals stalking victims online. They assumed that the stalkers in this group were being treated unfairly by their victims and tried to punish the victims accordingly. The group allowed victims to recruit others to harass offline. The victim rated the stalker's computer literacy from fairly high to high. Online stalking contained threatening multimedia harassing victims of blackmail, spam, email bombing and privacy theft. The group also conducted investigations into their victims. Additionally, (McFarlane and Bocij, 2003) learned that another small group, cyber stalking, could possibly exist. In such cases, organizations can be criticized and insulted for their business practices. As a result, they use bullying to defames or silence victims. The group used theft of personal information to spoof victims and damage their credibility.[8]

**5.** ***Ghost Cyber stalkers:*** Not included in Dr. Mullen's five stalker profiles, the ghost cyber stalker is unique to the Information Age. They are online assailants who their target cannot identify. Using Cyber stealth, the ghost cyber stalker repeatedly makes direct or indirect threats of physical harm and inspires fear. They can represent an amalgamation of the other five types, be a predatory troll or a sadistic online user with no connection to their victim. Ghost cyber stalkers rely upon the veil of anonymity afforded to all online users.[10]

**(F) Steps to Take When Cyber stalked:**

***Step-1: Block the Profile-***

Do you feel that a person disturbs a lot from your messages? The cyber law, as well as web services, gives you the possibility of blocking anyone. You will stop receiving messages from this person. As your first stage of the battle against cyber stalking, block the person and stop receiving your messages. This will guarantee your mental peace.

***Step-2: Report the Profile-***

The whole platform of social media allows you to denounce a profile. Report them as inappropriate. If there is another way to report, you should also use it. However, this may not be the end of the persecution. Sometimes the stalker statements despite reporting, using a different identity. It will take time before knowing that it is the same person. Platform moderators are usually fast to work in this regard and delete their profiles.

***Step-3: File a Complaint-***

Once you have taken the first two steps, you must make a complaint with the police. If you feel that the pursuer may cause damage, you should report immediately to the police. You may not have much information about Stalker. However, when the complaint is archived, you will

[10] https://www.ipredator.co/cyberstalking-facts/

receive advice on how to deal with the best situation. Even with fewer details on the tracker, you may be able to stop the persecution completely.[11]

## IV. CYBER STALKING LAWS ARE DEALT IN INDIA BY THE FOLLOWING ACTS

### (A) Information Technology Act, 2000:

#### 1. Section 66E of Information Technology Act, 2000-

Punishment for violation of privacy- Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.[12]

#### 2. Section 67 of Information Technology Act, 2000-

As per the above mentioned section which is replica of Section 292 of Indian Penal Code, if someone tries to publish obscene material about the victim on social media platforms in order to bully the victim, he shall be punished with imprisonment for a term which may extend to 3 years along with a fine up to Rs. 5Lakhs in case of first-time offenders. In case of subsequent conviction, the term of imprisonment may extend to 5 years along with a fine up to 10Lakhs.

#### 3. Section 67A of Information Technology Act, 2000-

If someone attempts to publish any sexually explicit material in electronic form, he shall be guilty and shall be punished with imprisonment for a term that may extend to 5 years along with a fine up to Rs. 10 Lakhs in case of first-time offenders. In case of subsequent conviction, the term of imprisonment may extend to 7 years along with a fine up to 10 Lakhs.

#### 4. Section 67B of Information Technology Act, 2000-

If someone publishes material in which children are engaged in sexual activities to terrorize the children (less than 18 years of age), such person shall be guilty and shall be punished with imprisonment for a term that may extend to 5 years along with a fine up to Rs. 10 Lakhs in case of first-time offenders. In case of subsequent conviction, the term of imprisonment may extend to 7 years along with a fine up to 10 Lakhs.[13]

#### 5. Section 66A of Information Technology Act, 2000-

It states that a person would be punished with imprisonment for up to 3 years with fine if he uses a computer resource or communication device to send any information that is grossly offensive or has menacing character.[14]

---

[11]https://www.jigsawacademy.com/blogs/cyber-security/cyber-safety-cyberstalking#Steps-to-Take-When-CyberStalked

[12] https://indiankanoon.org/doc/112223967/

[13] https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf

[14] https://www.legalserviceindia.com/legal/article-1048-cyber-stalking-in-india.html

**6. Section 72 of Information Technology Act, 2000-**

Any person who illegally discloses any electronic information or other material which contains personal information of that person without the consent of that person to any other person is liable for the punishment of imprisonment which may extend to 3 years or with fine which may extend to 5 lakh rupees or with both.[15]

**(B) Indian Penal Code,1860:**

**1. Section 354D of Indian Penal Code, 1860-**

This section considers both physical stalking and cyber stalking. The section's scope is defined in terms of the activities that constitute "stalking." The Section expressly states that anyone who attempts to monitor a woman's online activities is guilty of stalking. As a result, if the stalker engages in any of the offences listed in the section, he violates the Indian Penal Code Section 354D.[16]

**2. Section 503 of the Indian Penal Code, 1860-**

Section 503 deals with criminal intimidation as threats made to any person with an injury to their reputation, either in order to cause harm or to make her change her course of action regarding anything she would otherwise do/not do. Punishment involves imprisonment which may extend to 2 years and/or fine.[17]

**3. Section 509 of the Indian Penal Code, 1860-**

Any person who utters derogatory words in order to insult the modesty of a woman shall be punished with an imprisonment of 1 year and/or fine.

**4. Section 507 of the Indian Penal Code, 1860-**

This section punishes criminal intimidation by anonymous communication with imprisonment for a term that may extend up to 2 years.[18]

**5. Section 500 of the Indian Penal Code, 1860-**

It deals with defamation, can be applied in cases of cyber stalking in India if the stalker forges the victim's personal information to post an obscene message or comment on any electronic media. The punishment for any such act with imprisonment up to 2 years, fine, or both.[19]

[15] https://itforchange.net.
[16] https://blog.ipleaders.in/virtual-reality-cyberstalking-india/
[17] https://legislative.gov.in/sites/default/files/A1860-45.pdf
[18] https://www.jigsawacademy.com/blogs/cyber-security/cyberstalking
[19]https://timesofindia.indiatimes.com/life-style/spotlight/beware-cyberstalking-is-on-the-rise-during-the-pandemic/articleshow/81924158.cms

© 2021. International Journal of Law Management & Humanities [ISSN 2581-5369]

## V. INDIAN CASES AND JUDGMENTS RELATED TO CYBER STALKING

### (A) Shreya Singhal vs. Union of India

Decided: 24th March, 2015.

Citation(s): Air 2015 SC 1523; Writ Petition (Criminal) No. 167 OF 2012.

*Facts:*

The Petitioners have raised a substantial number of focuses with regards to the legality of area 66A. In making an offence, area 66A experiences the bad habit of dubiousness on the grounds that dissimilar to the offence made by section 66 of a similar Act, none of the previously mentioned terms are even endeavored to be characterized and can't be characterized, the outcome being that honest people are additionally reserved in. Such people are not told unmistakably on which side of the line they fall; and it is available to the experts to be as self-assertive and eccentric as they prefer in booking such people under the said segment. Actually, a substantial number of honest people have been reserved. The arrested women were released later on and it was decided to close the criminal cases against them yet the arrests attracted widespread public protest. It was felt that the police has misused its power by invoking Section 66A inter alia contending that it violates the freedom of speech and expression.[20]

*Judgment:*

The Court held that the provision of section 66A of the IT Act is derogative to the Article 19(1) (a) and all things considered it is a arbitrary provision which breaks the privilege of national to have the right to speech and expression of their perspectives on web. All things considered the arrangement concerned is unavoidably invalid and accordingly struck down completely.[21]

### (B) State vs. Yogesh Prabhu

Decided: 3rd July 2015.

Citation(s): C.C. NO. 3700686/PS/2009

*Facts:*

Mumbai Cyber Cell secured first ever conviction in Maharashtra under the IT act on Friday. The case was investigated by the cell for online stalking in 2009. Metropolitan Magistrate court convicted Yogesh Prabhu for stalking and sending obscene images to his colleague. The conviction was procured on evidence; including crucial witness statement stating that the crime

[20] http://www.legalservicesindia.com/article/2473/Shreya-Singhal-v-U.O.I.html
[21] www.manupatra.com

© 2021. International Journal of Law Management & Humanities [ISSN 2581-5369]

was committed using a laptop sponsored by office. According to the prosecution's case, the complainant communicated with Prabhu through online networking site Orkut. However, on one occasion Prabhu sent the complainant obscene messages, following which she removed him from her friend list. A few days later, she received an email from an unknown person with "foul and objectionable language". The complainant continued to receive the emails and she eventually sent a complaint to Joint Commissioner of Police (Crime).[22] Following the complaint, the cyber cell traced the IP address and found that it was sent from the same office where she worked and it was the same person the complainant chatted with, Prabhu.

*Judgment*

For this the court sentenced accused Yogisha Prabhu is convicted for offence punishable under section 509 of Indian Penal Code and section 66(E) of Information Technology Act, vide section 248(2) of Code of Criminal Procedure. Accused is sentenced to suffer simple imprisonment for one month for offence punishable under section 509 of Indian Penal Code and to pay fine of Rs. 5,000 (Rs. Five Thousand only) in default to suffer simple imprisonment for one month. Accused is sentenced to suffer simple imprisonment for three months for offence punishable under section 66(E) of Information Technology Act and to pay fine of Rs.10,000 (Rupees Ten Thousand only) in default to suffer simple imprisonment for two months. Both the substantive sentences shall run concurrently.[23]

**(C) Manish Kathuria vs. Ritu Kohli**

Decided: 10th September 2014.

Citation(s): C.C. No. 14616/2014.

*Facts:*

In 2001, India's first cyber stalking case was reported. Manish Kathuria was stalking an Indian lady, Ms. Ritu Kohli by illegally chatting on the web site, www.mirc.com using her name; and used obscene and obnoxious language, and distributed her residence telephone number, invited people to chat with her on the phone. As a result, Ms. Ritu Kohli was getting obscene calls from various states of India and abroad, and people were talking dirty with her. In a state of shock, she called the Delhi police and reported the matter. The police registered her case under Section 509 of the Indian Penal Code, 1860 for outraging the modesty of Ritu Kohli. But Section 509 refers only to a word, a gesture or an act intended to insult modesty of a woman. But when same things are done on Internet, then there is no mention about it in the said section.

[22] https://www.latestlaws.com/wp-content/uploads/2018/08/Cyber-Stalking-Indian-and-International-Perspective
[23] https://www.cyberlawconsulting.com/images/Cyber%20Stalking.pdf

This case caused alarm to the Indian government, for the need to amend laws regarding the aforesaid crime and regarding protection of victims under the same.[24]

*Judgment:*

As a result, cases started being reported under this section as opposed to Section 509 of the Indian Penal Code, as was the case where a Delhi University student was arrested for stalking a woman from Goa by creating fake profiles on social networking websites, uploading pictures on them and declared her to be his wife. It is hoped that the decision in this would favor the victim. However, in 2015, Section 66A was struck down as unconstitutional by the Supreme Court for being violative of Section 19(1) (a) of the Indian Constitution.

**(D) State of Tamil Nadu vs. Suhas Kutti**

Decided: 5th November, 2004.

Citation(s): C No. 4680 of 2004.

*Facts:*

The accused was the family friend of the victim. The accused wanted to marry the victim but the victim refused and married another person. The marriage broke apart. On seeing this, the accused saw this as an opportunity and asked her for marriage. The victim refused again. On being refused, the accused posted obscene and defamatory messages about the said victim on Yahoo messenger groups harming her reputation and insulting her modesty. The accused also forwarded emails received in a fake account opened by him in the victim's name. The posting of messages resulted in annoying calls to the victim. The calls were in the belief the victim is soliciting for sex work. The victim was fed up with the harassment took steps against it and filed a report again him. The accused was arrested and he reiterated that he did not do such a thing.[25]

*Judgment:*

Despite of all such arguments, the proofs were presented before the Court. The IP address belonging to the harasser was same as the accused. The Cyber Café owner, an eye-witness, gave statement against the accused. After relying on the expert witnesses and other evidences produced before Court, the Additional Chief Metropolitan Magistrate held the accused guilty of offences under Section 509 IPC and Section 67 of Information Technology Act, 2000.[26]

[24]http://docs.manupatra.in/newsline/articles/Upload/FDF5EB3E-2BB1-44BB-8F1D-9CA06D965AA9.pdf
[25] https://lawlex.org/case-summary/case-summary-state-of-tamil-nadu-vs-suhas-katti/24568
[26] https://supremoamicus.org/wp-content/uploads/2018/06/33.pdf

**(E) Subramanian Swamy vs. Union of India**

Decided: 13th May, 2016

Citation(s): 7 SSC 221 Writ Petition (Criminal) No. 184 OF 2014

*Facts:*

The petition was filed under Article 32 of the Indian Constitution by Subramanian Swamy along with other petitioners challenging the Constitutional validity of Criminal defamation under Section 499 (defamation) and Section 500 (punishment for defamation) of Indian Penal Code, 1860 and Sections 199(1) to 199(4) of Indian Code of Criminal Procedure, 1973. The petition was filed because the petitioners argued that it curtailed their Fundamental Right of 'Right to freedom of speech and expression' under Article 19(1)(a).In the year 2014, a corruption allegation was made by Dr. Subramanian Swamy against Ms. Jayalathitha in response to this the Tamil Nadu state government filed a defamation case against him. After this Dr. Swamy along with other prominent politicians challenged the constitutionality of criminal defamation laws in India.[27]

*Judgment:*

The court upheld the constitutional validity of Section 499 and 500 of the Indian Penal Code (IPC), 1860. The Court emphasized that the law on criminal defamation is clear and unambiguous and thus distinguished other cases in which it had struck down legislation that infringed freedom of speech, such as Shreya Singhal v. Union of India. Hence, the petitions were dismissed by the Court by upholding the constitutional validity of the Criminal Defamation under Section 499 and 500 of IPC.[28]

**(F) Karan Girotra vs. State & Anr**

Decided: 8th May, 2012

Citation(s): 2012 SCC OnLine Del 2673

*Facts:*

This case was delivered on 8th May 2012 on cyber stalking when the petitioner filed an application to grant anticipatory bail. This case deals with a woman, Shivani Saxena, whose marriage could not be consummated and she filed a divorce with mutual consent. In between, she came across Karan Girotra while chatting on the internet, who told her that he loved her and wanted to marry her. Girotra invited Saxena over to his house to introduce her to his family

[27]https://www.scobserver.in/court-case/defamation-as-a-criminal-offence
[28] https://www.jusdicere.in/subramanian-swamy-v-union-of-india/

© 2021. International Journal of Law Management & Humanities [ISSN 2581-5369]

where he intoxicated her and sexually assaulted her. He started assuring her that he would marry her and began sending her obscene pictures of her assaultation. He also threatened her to circulate the pictures if she would not marry him. As a result, an engagement ceremony was performed after which he continued to assault her and called off his engagement to her. Frustrated out of this, Saxena filed a complaint under section 66-A of the IT Act.[29]

*Judgment:*

By virtue of which the petitioner was restrained to be arrested by the Investigating Agency is recalled and the petition for the grant of the anticipatory bail is dismissed. [30]

**(G) J.S. Chikkannavar vs. Venkatesh**

Decided: 4th November, 1988.

Citation(s): 1989 (1) KarLJ 24

*Facts:*

Referring to the ingredients of the offences of criminal intimidation as enumerated is Section 503 I.P.C., the Court said at para-3 that by such resolution the accused 2 to 54 have prima facie compelled the complainant to do an act "which that person is legally entitled to do."The petitioners have not at all threatened the respondent herein with any injury to his person, reputation or property with intent to cause him to do any act which he is not legally bound to do. He was dismembered from the Association for the reason that he has acted detrimental to interests of Dharwad Bar Association in as much as he has circulated number of pamphlets in the public which defame and lower the dignity of Dharwad Bar Association and its members. They maintained that they have not at all compelled him to do an act which he was legally not entitled to do.

*Judgment:*

The trial Court fell in serious error in issuing process against the petitioners and the impugned order is wholly unsustainable. The petition is allowed and the order of the Court below issuing process against the petitioners is quashed.[31]

**(H) Jayanta Kumar Das vs. State of Odisha**

Decided: 4th November, 1988.

Citation(s): 1989 (1) KarLJ 24

[29] www.thehindu.com
[30] https://indiankanoon.org/doc/107460954/
[31] https://indiankanoon.org/doc/1518413/?type=print

*Facts:*

The accused has been convicted for sending obscene messages to a lady, defaming and causing mental harassment by putting up her personal details and information on a pornographic website. The accused was arrested under section 500 of the Indian Penal Code and 66(C) and 67 (a) of the Information Technology Act. The accused Jayanta Das had uploaded all the personal information of the victim in a bid to take revenge from her husband based in Puri. Crime branch officials said that Das had posted the mobile number, address and private information of the victim on desihunt.com website. Being a pornographic and wife swapping website, the victim received calls from various persons asking more details about her.[14]

*Judgment:*

RTI Activist Jayanta Das has been awarded 6-year jail term and asked to pay Rs 9,000 fine by Puri SDJM Court for defaming a lady on internet in 2012.

## VI. FINDINGS

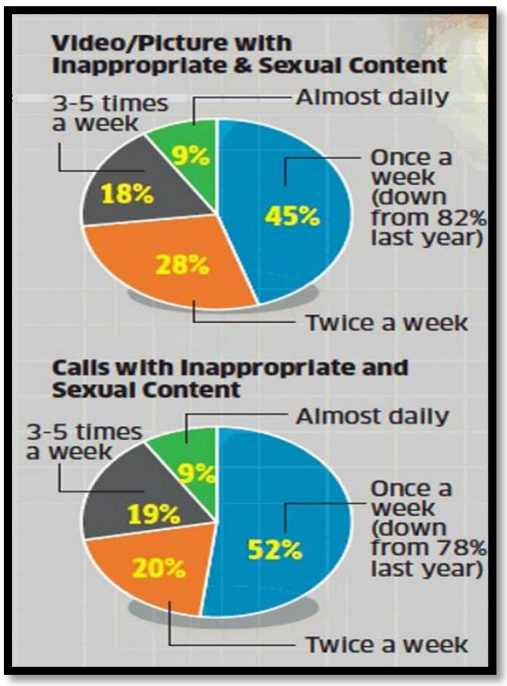


***Figure:*** *https://economictimes.indiatimes.com/magazines/panache/stalker-alert-1-in-3-women-who-use-mobiles-in-india-face-harassment-receive-inappropriate-calls/articleshow/68556513.cms*

- 36% of the online Stalking victims did not take any actions. 28% of them have reported that they have reduced their online presence after being abused.
- 30% of the online Stalking victims who had experienced violence had found it extremely upsetting and 15% have faced serious mental issues like depression and insomnia.

- The mechanisms on social media to report online abuse are ineffective and victims are more likely to block the abusers instead of reporting them.
- 38% of the victims have characterized that the laws are “not at all helpful”.
- According to NCRB, the number of cases registered under the law has shown a decline of 46% in 5 years (2008-2012) and an increase of 156.7% in the year of 2012 under IPC and SLLs.
- A decline of 14.9% was registered in the same crime during 2015. In the year 2015, 40 cases were registered and it became 38 in 2016.
- About 27000+ cybercrimes were reported in the year 2017 with an average of one every ten minutes.[32]

## VII. DISCUSSION

This research part analyzes the jobs of both cybercriminals and digital casualties and how they connect—some of the time in manners that reflect "this present reality" criminal–casualty relationship and now and again in manners that are very unique. It is likewise about individuals. Understanding that you are cyber stalked is the initial phase in fighting it. Understanding individuals on the location of any types of cybercrime—the people who perpetrate it, the individuals who are harmed by it, and the individuals who work to stop it—is the initial move toward getting cybercrime. Understanding the intentions, qualities, and normal practices of crooks in each gathering, alongside breaking down the proof in every specific case, can assist with fostering a criminal profile that will help with recognizing and catching guilty parties. Some portion of the criminal profile includes concentrating on the sorts of individuals lawbreakers pick as casualties. Casualty profiles can likewise be utilized in preparing sting tasks that draw the cybercriminal out of the virtual world and into the genuine one. Examiners of cybercrime need every one of the qualities that are expected of any criminal specialist, in addition to a couple of additional ones for sure. Not exclusively should the internet analysts be shrewd, coherent, level headed, patient, inquisitive, and in great shape, yet additionally they should have some information and comprehension of PCs, organizing, specialized language, the programmer underground, and IT security issues. Understanding the innovation of cyber stalked is simple contrasted and understanding individuals who do the wrongdoings. The human factor is frequently the most mysterious part in an examination.[33]

[32] https://lexforti.com/legal-news/wp-content/uploads/2020/09/Cyber-Crime.pdf
[33] https://www.sciencedirect.com/science/article/pii/B9781597492768000030

**(A) Different ways to guard against cyber stalking include the following:**

- Update all software to prevent information leaks.
- Mask your internet protocol address with a virtual private network.
- Strengthen privacy settings on social media.
- Strengthen all devices with strong passwords or, better, use multifactor authentication.
- Avoid using public Wi-Fi networks.
- Send private information via private messages, not by posting on public forums.
- Safeguard mobile devices by using password protection and never leave devices unattended.
- Disable location settings on devices.
- Install antivirus software on devices to detect malicious software.
- Always log out of all accounts at the end of a session.
- Beware of installing apps that ask to access your personal information.[34]

## VIII. CONCLUSION

Studies are required to improve our understanding of Cyber stalking. The fast pace with which technology changes, as well as the favorable cost of technologies that make a person easier to follow and steal a victim. Studies based on sacrificial experience must be examined at depth, so that the right laws are written to protect victims of cyber stalking. A collaborative effort of victims, law enforcement agencies and private and public areas is required to combat Cyber stalking and develop an effective answer.[35] In 17 years since the Information Technology Act of 2000 was passed, dozens of cyberstalking incidents have been reported, but many more go unreported. The main reason behind this, is that the authorities who are concerned with registering such complaints or taking action in such matters are more comfortable with the traditional laws for the physical world.[25] Section 354D of the Indian Penal Code, covers stalking & not cyber-stalking except for the monitoring of a woman's communications by a man.

The literature about Cyber stalking is still in the child shoes; However, it is expected that the incidence of cyber stalking increase to rise as the internet becomes even more popular than

[34] https://searchsecurity.techtarget.com/definition/cyberstalking
[35] http://iacis.org/iis/2009/P2009_1212.pdf

today, especially under the company of the Company.[36] Only mentioned, a large part of modern life cannot be carried out as effectively, without the consecutive access to the World Wide Web (Hutton 2003). Although prosecution is confronted with a number of obstacles, there is hope. The action on the federal, state and local level must combine, share and distribute intelligence interest formations. With good workout and instructions, law enforcement researchers can often consequences with a certain accuracy of an electronic path that was left by the Cyber Stalker (Reno 1999)[37]. Metaphorically, an electronic path is the equivalent of burglars leaving a fingerprint at the scene. With a small work, the electronic path can often be returned to the original place of origin.

*****

[36] https://www.nw3c.org/
[37] https://www.justice.gov/criminal/cybercrime/cyberstalking.htm

© 2021. International Journal of Law Management & Humanities [ISSN 2581-5369]

## IX. REFERENCES


- Jaishankar, K., & Uma Sankary, V. (2005). Cyber stalking: A global menace in the information super highway. ERCES Online Quarterly Review,2(3), Retrieved May 7, 2007, from http://www.erces.com/journal/articles/archives/volume2v03/v02.htm.
- King, S. A. (1996). Is the Internet Addictive, or Are Addicts Using the Internet? Retrieved February 18, 2006, from Web site: http://webpages.charter.net/stormking/iad.html
- McFarlane, L., & Bocij, P. (2005). An exploration of predatory behaviour in cyberspace: Towards a typology of cyber stalkers. First Monday, 8. Retrieved Feb 18, 2006, from http://firstmonday.org/issues/issues8_9/mcfarlane/index.html.
- McFarlane, L., & Bocij, P. (2003). Cyber stalking: defining the invasion of cyberspace.
- Haryani and Farahidah (2010) Cyber stalking: The social impact of social networking technology.
- McFarlane, L., and Bocij, P. (2003) Cyber stalking: defining the invasion of cyberspace.
- Michael L. Pittaro, (2007) Cyber stalking: An Analysis of Online Harassment and Intimidation. Legal Journal Vol-II Issue- I (2020).
- Manvi-Singh, (2018) Cyber Stalking Indian and International Perspective.
- Molly Ghosh, (Jan 17, 2018) Introspecting the Gaps between Cyber Crimes against Women and Laws: A Study of West Bengal .
- Parag Agarawal, (2018) Precedent: A Publication of Jus Dicere & Co. Volume 2 Issue 1.
- Dr. Sapna Sukrut Deo, (2013) Cyber stalking And Online Harassment: A New Challenge for Law Enforcement.
- Defamation as a Criminal offence, Supreme Court Observer 2020.
- 8 P. Oppili, (Jan 05 , 2002) First case to be prosecuted under IT Act, THE HINDU .
- Maahi, (2018) Stalking: The Stalker Savings the Victim.
- Karen, Daniel and Thomas (2009) Cyber stalking: An Exploratory Study of Students at a Mid-Atlantic University.
- *Goodno, N.H., (2007) Cyber stalking, a new crime: Evaluating the effectiveness of current state and federal laws.*


© 2021. International Journal of Law Management & Humanities [ISSN 2581-5369]

- Paul Bocij, Leroy McFarlane (2003) Cyberstalking: The Technology of Hate.
- Felson, M. (2002) Crime and Everyday Life. 3rd edn. California: Sage Publications.
- Littlejohn and Micheal, (2008) Understanding the people on the scene.
- Hutton, S. (2003). Cyber stalking.
- Reno, J. (1999) Report on Cyber Stalking: A new challenges for law enforcement and industry.


*****

© 2021. International Journal of Law Management & Humanities [ISSN 2581-5369]