International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 8 Issue 6, Nov-Dec 2024 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Cyber Stalking: Comprehensive Legislative Framework in India

Sivanesh. T, Sridhar. R. C. S, Renganathan. V

Student, SASTRA Deemed University, Thanjavur, Tamil Nadu, India

ABSTRACT

This article mainly comprise of newly emerging grave offence in Indian society for which we don't have any specific provision for few decades. In the current legislation which came into the effect on 1st July 2024, that is Bharatiya Nyaya Sanhita, 2024(BNS). We have included a specific provision for that new offence, cyber stalking. Since the bill was introduced very recently to analyze the impact or applicability of this provision we need some waiting. Before the introduction of these bill the offence of cyber stalking old code and information technology act was used where there were no clear definition of cyber stalking, which made it difficult for the cyber stalking to be enforced on the offences and with no proper punishment. In this paper we have given our own suggestive ways in eradicating the offence of cyber stalking.

KEYWORDS: *legislation, cyber stalking, offences, punishment, definition*

How to cite this paper: Sivanesh. T | Sridhar. R. C. S | Renganathan. V "Cyber Stalking: Comprehensive Legislative Framework in India" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-8 | Issue-6, December 2024, pp.691-693, URL: www.ijtsrd.com/papers/ijtsrd72660.pdf

IJTSRD72660

INTRODUCTION

Cyber stalking is a major offence rising in contempory India. The growth of technology and media has promoted this offence. The IT act 2000, section 354D and section 67 of IPC were existing legislative before BNS with respective to this kinds of offence. These laws however not complete solving with such complexities existing with cyber stalking. The introduction of BNS specifically Section 78 of the act penalties cyber stalking and provided the more comprehensive framework however it has not completely eradicated the challenges curtaining long the enforcement.

Comparison of IPC and BNS:

- Cyber stalking is a newly coined offence in India, we have cybercrimes mentioned in information technology act and old penal code. The legislation don't have any specific provision which is exclusively mention about cyber stalking offence. Cyber stalking is proved to be a grave offence. The impact of cyber stalking will affect mental and physical health of victim. Many developed countries have specific legislation on cyber stalking subject. The latest criminal legislation passed by the parliament named Bharatiya Nyaya Sanhita, 2023, section 78 of this act deals with stalking and clause (1) (ii) says that "monitors the use by a woman of the internet, e-mail or any other form of electronic communication, commits the offence of stalking"[2], this might express the term cyber stalking because the essential elements of cyber stalking are partially fulfilled. when we compare the provision of Indian Penal Code and newly introduced Bharatiya Nyaya Sanhita, there are few provisions in Indian Penal Code which is related to stalking but no express provision for cyber stalking in Indian Penal Code, those provisions are;
- Section 354D: This section specifically deals with stalking, the term cyber stalking was not expressly mentioned in the old Indian Penal Code. It defines stalking as any act of watching or following a person, contacting them repeatedly, or monitoring their activities, causing fear or alarm. So previously, if any cyber stalking cases was filed it was registered under this IPC provision.

[2] https://www.indiacode.nic.in/show-data

Also this provision is gender biased as it focus only on female victims.

- Section 509: This section pertains to word, gesture, or act intended to insult the modesty of a woman. It can be applied to online harassment where offensive or derogatory messages are sent.
- Section 67 of the Information Technology Act, 2000: This section addresses the publication of obscene material in electronic form. It can be used to prosecute cyber stalkers who send explicit or offensive content. But, this provision was also not clearly mentioned about cyber stalking.

When we analyze the Bharatiya Nyaya Sanhita provision that provide us clear definition of the term cyber stalking in this section 78 of this act. The punishment for the cyber stalking was clearly mentioned in clause 2 of section 78, "(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. In the Indian Penal Code we don't specifically have any express provision for the punishment for the offence. So, Bharatiya Nyaya Sanhita have given us an express punishment provision for cyber stalking reflecting the severity of the offence. Hence the Bharatiya Nyaya Sanhita offers more comprehensive and nuanced approach. The main reason for making express provision for cyber stalking as the technology continues to evolve as an effect, everybody started using internet , mobile and other form of electronic items, there might be a chance for the misuse for which in the Bharatiya Nyaya Sanhita express provision for cyber stalking was introduced.

Enforcement problems on cyber stalking laws in India:

"Even with the most carefully crafted legislation, enforcing a law in a virtual community creates unique problems never before faced by law enforcement agencies"[3]. These problems pertain mainly to international aspects of the Internet. It is a medium that can be accessed by anyone throughout the globe with a computer and modem. This means, as explained below, that a potential offender may not be within the jurisdiction where an offence is committed. Anonymous use of the Internet, though beneficial in many instances, also promises to create challenges for law enforcement authorities[4].An important issue of territorial jurisdiction has not been highlighted in Information Technology Act, 2000. The matter of jurisdiction has been given in the sections 46, 48, 57 and 61 is where the appellate procedure and adjunction process is mentioned. Section 80 which explains the power of a police officer with respect to its jurisdiction that is the power to conduct search in a public area for cyber-crime etc. Cyber-crimes are crimes done by persons using modern technology through a system and internet from any state or country across this world. So it is obvious that cyber-crimes are not bound by geographical limits for better enforcement of cyber laws there should be clear and proper elaboration to be made as to which state will have the power to deal those cases.The main problem arises when there are two different legal provisions for that crime which will result as a problem which will need time to solve it .for example if the stalker is in country a and the victim is in country b . The country b has severe punishment for that particular crime but country a has no provisions regarding that crime. If there is an arrangement where both the countries would cooperate and form an extradition like if the same crime is committed internationally then it can be easily sorted out. In India the Information Technology act has clearly stated the extraterritorial jurisdiction affairs in section 75 says that whether he is a citizen of India or not it mainly related with the offences related to computer systems. Article 14 of the Indian constitution mandates equality before law we can see that even though constitution provides these the constitution on its own has provisions inclined more on women as they are the weaker section of the society .The section 345D of IPC clearly evident that it more inclined towards women's safety where as in this present generation men also need provisions related to cyber law.

Recommendation:

some suggestive recommendations to reduce the offence of cyber stalking they are:

1. Self-regulation:

Self-regulation is a best method to control anything. As a citizen of India everybody must have self-regulation in them and as per article 51-A of Indian constitution it says "to develop the scientific temper, humanism and the spirit of inquiry and reform" and the same article is also speaking about common brotherhood so it is a fundamental duty of every

[3] B. Jensen, Cyberstalking: Crime, Enforcement and Personal Responsibility in the Online World, http://www.law.ucla.edu/Classes/Archive/S96/340/cyberlaw.htm (last visited May 1, 2013).

[4] L. Ellison & Y. Akdeniz, Cyberstalking: The Regulation of Harassment on the Internet, CRIMINAL LAW REVIEW-CRIME, CRIMINAL JUSTICE AND THE INTERNET 7 (Special ed. Dec. 1998).

citizen not to do any of the wrong related to cyber stalking. Everyone should choose a username that is gender neutral or the e-mail ids should be a combination of characters and phrases that are meaningless. The passwords should contain some digits or letters.[5]

2. Use of new software:

The implementation or the use of new software can make sure the restriction of the cyber offence as effective. For example the software like Truecaller can help us to detect and restrict the anonymous threat from reaching our foot.

3. Role of internet service provider(ISP):

The ISP plays an important role in monitoring the network, mainly the offender use ISP source to track the victim, thus using the most latest and secure ISP make it difficult for the criminal to reach the victim.

These are some suggestions that might help to control the cyber stalking.

4. Dedicated cyberstalking law:

Drafting a dedicated cyberstalking law with defined definitions, penalties and victim protection procedures to cover all forms of online abuse. Creation of cybercrime cells in all states with specialized training to handle cyber stalking cases like digital forensics and victim assistance.[6]

Conclusion:

It is very truly said that to change the current scenario, we must change the old out dated model of dealing with the situation with the new effective and enhanced model. As cyber stalking an emerging grave offence, which needs an effective provision and mechanism to curb the crime. The recommended suggestion must be taken placed and enforced, as the world evolve with new crime we need to make sure to get rid of the offence with better modern solutions, like enhanced legislation. It is a call to action for lawmakers, educators, and citizens alike to unite against the changing scenario. The time for change is now—let us all unite to bring a conclusion of the challenge and forge a path toward a brighter, safer digital world for generations to come.

[5] Working to Halt Online Abuse, http://www.haltabuse.org/resources/online.shtml (May 13, 2017, 7:15AM)

[6] https://www.legalserviceindia.com/legal/article-17736