

# Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

#### **DISCLAIMER**

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Editor-in-chief of White Black Legal

— The Law Journal. The Editorial Team of White Black Legal holds the

- The Law Journal. The Editorial Team of White Black Legal holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of White Black Legal. Though all efforts are made to ensure the accuracy and correctness of the information published, White Black Legal shall not be responsible for any errors caused due to oversight or otherwise.

### **EDITORIAL TEAM**

#### Raju Narayana Swamy (IAS ) Indian Administrative Service officer



professional diploma Procurement from the World Bank.

Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is All India Topper of the 1991 batch of the IAS and is currently posted Principal as Secretary to the Government of Kerala . He has accolades as he hit earned many against the political-bureaucrat corruption nexus in India. Dr Swamv holds B.Tech in Computer Science and Engineering from the IIT Madras and a Cyber from Ph. D. in Law Gujarat National Law University . He also has an LLM (Pro) with specialization IPR) in well as three PG Diplomas from the National Law University, Delhi-Urban one in Environmental Management and Law, another in Law Environmental and Policy and third one in Tourism and Environmental Law. He also post-graduate holds diploma IPR from the National Law School, Bengaluru and a **Public** in

## Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB, LLM degrees from Banaras Hindu University & Phd from university of Kota.He has successfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.



## **Senior Editor**



#### Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

#### Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi, Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.



#### Dr. Navtika Singh Nautival

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.





Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

#### Dr. Nitesh Saraswat

#### E.MBA, LL.M, Ph.D, PGDSAPM

Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.

More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.



# TIDRILLIA DE LA CALLACTA DEL CALLACTA DE LA CALLACTA DEL CALLACTA DE LA CALLACTA

#### Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

#### ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

LEGAL

# CYBERSTALKING AND ITS IMPACT ON WOMEN AND CHILDREN

AUTHORED BY - LAKSHANA. K & NAGASUNDARI SHRUTI. K

#### **ABSTRACT:**

This research paper aims to discuss the offense of cyber stalking, especially deals with the impact such an offense has on the vulnerable groups i.e. women and children. Cyber stalking is the practise of following or harassing someone online or through other technological channels. Evidently, cyber stalking was at its peak during the covid outbreak and with the tremendous growth of the internet, the physical stalking was transformed into cyber stalking as a whole due to the convenience due to the availability of unlimited information just spread outacress the social media pages and the high chances of evading the law and order without an consequences due to the difficulty in detecting such offenders. The lethargicness of the offenders has grown due to the ineffective and improperly implemented legislation and the inadequate penalties when it comes to cybercrimes. The scope of this paper also extends to covering the cases and the news reports of women and children being the victims of cyber stalking and it also intends on covering the international conventions and makes a comparison with that of the Indian legal framework governing cybercrimes. This paper offers a special attention to the IT Act, 2000 and IPC as the cybercrimes are compound offenses which requires governance by both these significant legislations which has a major part to play in the process of trying and penalizing the offenders. As far as international conventions are concerned the USA's and the Europe's have been specifically analyzed due to their standardized method of setting up councils and committees to deal with the issues closely and adequately. The paper also recommends the precautions that are to be taken in order to avoid such offenses such as the non-disclosure of sensitive information, resetting the passwords time and again, concealing the IP address etc. The offense of cyber stalking not only affects the victims physically but also gives them mental trauma and agony and causes damages to them even though there is an absence of evident, physical injury and the violation of the right to privacy, which is constitutionally guaranteed fundamental right, are irreversible.

#### **BACKGROUND OF THE STUDY:**

The term "cyber stalking" refers to a type of cybercrime in which a stalker uses various online platforms or digital media to track or harass a victim in an electronic manner. "Cyber stalking is the practise of unwelcome and persistent internet communication. Any number of incidents, such as threats, libel, slander, sexual harassment, or other attempts to intimidate or control their victim, may be involved." Cyber stalking is a psychological and neurotic behaviour in which the stalker unlawfully and persistently monitors the target's online activity. Cyber stalking is often referred to as "online harassment" and "online abuse," among other terms. Cyber stalking the word is entirely is such a recent phenomenon, neither the media nor law enforcement have been able to fully define or quantify cyber stalking. There is little information for victims or for professionals who work with victims because there sources available are so scarce and constrained according to the Useful service providers. According to statistics, there are millions of prospective users expected future instances. The rise in identity theft was a sign of technology abuse is among the criminal activity's fastestgrowing subsets. According to a 2006 National Crime Prevention Council poll, around 40% of Teenagers had experienced cyber bullying, thus the issue was very serious and widespread. The problem of cyber stalking is widespread and has negative effects. Consequences on teenagers, including elevated levels of sadness, suicide ideation, and anxiety heightened propensity for drug usage and aggressive behaviour.

#### LITERATURE REVIEW:

In 2011, Dinakar K. et al.<sup>2</sup> proposed employing binary and multi-class text classification approaches to categorize textual cyber bullying. The authors conducted their experiment on 4500 YouTube comments and discovered that binary classifiers perform better for individual labels than a multi-class classifier. By Kelly Reynolds et al.<sup>3</sup>, a different machine learning-based approach for cyber bullying detection was put into practice. The authors conducted questionnaires on the Form spring. Me website, and utilized other training datasets to count and standardize the results.

<sup>1</sup> https://www.sciencedirect.com/topics/computer-science/cyberstalking

<sup>2</sup> Dinakar, K., Reichart, R. and Lieberman, H. (2021) 'Modeling the Detection of Textual Cyberbullying', ICWSM Workshop Technical Report WS-11-02 (The Social Mobile Web), Vol.5(No.3). doi:https://doi.org/10.1609/icwsm.v5i3.14209.

<sup>3</sup> Gautam, A.K. and Bansal, A. (2022) 'A Review on Cyberstalking Detection Using Machine Learning Techniques: Current Trends and Future Direction', IJETT Journal, Volume-70(Issue-3). doi:https://doi.org/10.14445/22315381/IJETT-V70I3P211.

In 2012, Dadvar M. et al. <sup>4</sup> proposed an improved model for cyber bullying detection using a hybrid approach that combined the substance, sentiment, and logical components. According to the authors, its detection technique is capable of identifying online bullies and stalkers.

Accuracy using guided machine learning techniques for identifying. A new methodology was put forth by Dadvar M. et al.<sup>5</sup> to deal with gender-based cyber bullying detection using web-based media networks.

A support vector machine was used to appraise the work. Authors have noted that men use more negative and derogatory language than women do. They use the MySpace dataset for trial work, which includes a few comments that target young people and women. A model for the detection of cyber bullying that makes use of two feature selection strategies has been put forth by Vinita Nahar et al<sup>6</sup>. Standard traits were extracted from offensive and non-offensive comments using the BOW approach. It's interesting to note that the probabilistic dormant semantic evaluation technique only extracted emotive highlights from oppressive messages.

#### **RESEARCH PROBLEM:**

The research problem at hand revolves around the pervasive issue of cyber stalking, with a specific focus on its impact on women and minors during the COVID-19 pandemic. In an increasingly digital world, cyber stalking has emerged as a concerning threat, one that can have profound implications for the safety, mental health, and emotional well-being of its victims. This research seeks to address three key research questions. Firstly, it aims to investigate the prevalence and nature of cyber stalking incidents directed at women and minors during the pandemic, shedding light on the unique challenges and vulnerabilities faced by these demographics. Secondly, it delves into the legal frameworks in place to combat cyber stalking, comparing the Information Technology Act of 2008 in India with various penal laws in the United States, and evaluating their effectiveness in safeguarding the rights and security of women and minors. Lastly, this research seeks to uncover the underlying motives and factors driving cyber stalking incidents and proposes a range of recommendations and preventive

<sup>5</sup> MaralDadvar, Franciska de Jong, Roeland Ordelman, DolfTrieschnigg, Improved Cyberbullying Detection Using Gender Information, 12th -Dutch-Belgian Information Retrieval Workshop, paper (2012) 693–696.

<sup>6</sup> Vinita Nahar, SayanUnankard, Xue Li, Caoyi Pang, Sentiment Analysis for Effective Detection of Cyber Bullying, Proceedings of the 14th Asia-Pacific international conference on Web Technologies and Applications, paper (2012).

measures to mitigate these risks, ensuring a safer digital environment for women and minors in both countries. By addressing these questions, this study aims to contribute to a deeper understanding of the issue and inform the development of more effective strategies for prevention and intervention.

#### **RESEARCH METHODOLOGY:**

The form of research methodology that has been utilized in this research paper is the doctrinal methodology of research. This type of research methodology restricts the researcher to use the resources available within the four walls of library. This type of research methodology is also known as the arm chair research. This type of research methodology involves primary and secondary resources. Casual discussion with some professors and lecturers who are capable of answering questions related to the above mentioned the above provided topic served as the primary source. Moreover, it also aided for the increase of knowledge and understanding of the researcher on this topic. The various secondary sources that were put in use for the purpose of research are articles, books, journals, magazines, e-books from the portals such as Jstor, hein online etc. In short, both primary and secondary sources were used. Analytical and comparitive methodology of research methodology was also inculcated as there are sub-headings under which the researcher compares the international conventions on protection against cyber stalking to that of India's framework.

#### **RESEARCH QUESTIONS:**

- RQ: 1 What is cyber stalking and how did it specifically affected women and children during the COVID times?
- RQ: 2 Whether Stalking under Information Technology Act, 2008 and various Penal Laws in India and United States of America has an impact on women and minors?
- RQ: 3 What are the reasons of cyber stalking and what all could be the suggestions and preventive measures to avoid cyber stalking?

# REASON FOR CYBER STALKING AND ITS IMPACT IN WOMEN AND CHILDREN:

Cyber stalking has become one of the most serious crimes in today's world. Experts believe that sexual harassment is often the main motivation behind cyber stalking, and that around 90% of victims are

female. Unfortunately, the anonymity of the internet allows peoples' true behaviors and feelings to be reflected online. Sometimes the stalker's target has done nothing to provoke feelings of hatred or desire for revenge, yet they still become the object of the stalker's fixation.

There can be various reasons someone engages in cyber stalking. For example, the stalker may feel intellectually, physically or sexually attracted to their victim in an unhealthy way. Jealousy over a past or current relationship could also be a motivator. Some cyber stalkers are driven by a desire for vengeance or hatred against their target. Their behavior falls into categories like obsessive, delusional or criminal depending on their specific motivations.

The COVID-19 pandemic led to increased internet usage among teenagers and youth. With more activities moving online, this opened the door for certain cybercrimes to rise, such as cyber stalking. Research shows that women and young adults between 18-24 are more commonly targeted. Statistics indicate around 20% of teenagers have experienced being cyber stalked. Studies also link higher rates of cyber bullying to greater time spent gaming online, more confidence using mobile devices, and preexisting mental health issues in certain individuals. Overall, the growth of technology has allowed cyber stalking cases to multiply exponentially in recent years according to data and experts.

# CASES AND NEWSREPORTS OF CYBERSTALKING ON WOMEN AND CHILDREN:

Cases of cyber bullying and stalking were reported in India in 2020 by the top state. The majority of cyber stalking and bullying occurrences against women and children occurred in the Indian state of Maharashtra in 2020, with roughly 388 cases reported to the police.

In the case of Manish Kathuria<sup>7</sup> The Manish Kathuria case concerned the stalking of a woman by the name of Ritu Kohli. It was the first known instance of cyber-stalking in India and the impetus behind the 2008 amendment to the IT Act. Following Kohli on a chat platform, Kathuria verbally insulted her before giving out her phone information to other individuals. Later, he started chatting on the website "www.mirc.com" while assuming Kohli's identity. As a result, over the course of three days,

<sup>&</sup>lt;sup>7</sup>Manish Kathuria v. State of Punjab, (2018) 1 JT 286

she began to get nearly 40 obscene phone calls at strange hours of the night. She was compelled by this circumstance to inform the Delhi Police about the incident. Following the filing of the complaint, the Delhi Police tracked down the IP addresses and detained Kathuria in accordance with Indian Penal Code Section 509. Since the IT Act had not yet become effective when the complaint was submitted, it was not used in this case. Although there is no evidence of any further action, this instance alerted Indian legislators to the necessity for laws to deal with cyber-stalking. Even then, Section 66-A wasn't introduced until 2008. As a result, cases are now being reported under this section of the Indian Penal Code rather than Section 509, as was the case with the Delhi University student who was detained for stalking a woman from Goa by creating fictitious profiles on social networking sites, uploading pictures to them, and claiming she was his wife. It is hoped that the decision in this would favour the victim. 1. About 20 people are arrested by city police each month for harassing and eve-teasing women, 30% of which involve stalking. Over 1,500 persons were detained by SHE Teams last year in all three commissionerates for harassing women in the city. Hyderabad SHE Teams made the most eve-teasers arrests with 644, including 122 juveniles. Rachakonda made the second-highest harassment arrests with 581, including 26 children. "The majority of stalking cases involve social media, phone calls, and other forms of cyber stalking. Minors make up a large portion of cyber stalking victims "a source for SHE Teams said.

#### **INDIAN LEGISLATION:**

According to Section 67 of the IT Act<sup>8</sup>, anyone who publishes or transmits, or causes to be published or transmitted in electronic form, any material that is lascivious, appeals to the prurient interest, or if its effect is such as to tend to deprave and corrupt persons who are likely, taking into account all relevant circumstances, to read, see, or hear the matter contained or embodied in it, shall be punished may include a prison sentence of up to five years and a fine of up to ten lakh rupees.

Punishment for posting or transmitting content involving sexually explicit acts, etc., in electronic form is outlined in Section 67A of the IT Act. Following the 2008 Amendment, Section 67A was inserted to the IT Act.<sup>9</sup> The stalker will be subject to penalty under this section, according to this section, if he posts any "sexually explicit" material in "electronic form" via any online social media,

<sup>&</sup>lt;sup>8</sup> Information Technology Act,2000, s. 67

<sup>&</sup>lt;sup>9</sup> Information Technology Act, 2000, s. 67A

messaging, or email. *Shreya Singhal v Union of India*<sup>10</sup> on the basis of the ambiguity and chilling impact theory might have been useful in dealing with stalking concerns. It notably addressed the penalties for communicating offensive remarks.

Punishment for posting or transmitting material depicting children in sexually explicit acts, etc., in electronic form, according to Section 67B of the IT Act. The 2008 Amendment introduced Section 67B for the first time into the Act. This section has a focus on stalkers that target minors, or children under the age of 18, and "engage in sexually explicit act or behaviour" in an effort to frighten them.

The "voyeurism" offence is covered by Section 66E of the Information Technology Act of 2000<sup>12</sup> and Section 354C of the Indian Penal Code<sup>13</sup>, respectively.

According to data issued by the National Crime Records Bureau, the number of cybercrime occurrences in 2021 has increased by 18.4% since 2019, but the number of instances involving women has increased at a far faster 28.4% rate. Data showed that 10,730 events, or 20.2% of the 52,974 incidents registered in 2021, were reported as crimes against women. Cyber bullying, cyber pornography, broadcasting obscene sexual content online, cyber stalking, defamation, morphing, and the creation of false profiles are the most common cybercrimes committed against women.

The Indian Penal code, 1860 Section 354D of IPC<sup>14</sup> 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".

"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." <sup>15</sup>

<sup>&</sup>lt;sup>10</sup> Shreya Singhal v. Union of India, AIR 2015 SC 1523.

<sup>&</sup>lt;sup>11</sup> Information Technology Act, 2000, s. 67B

<sup>&</sup>lt;sup>12</sup> Information Technology Act,2000, s. 66E

<sup>&</sup>lt;sup>13</sup> Indian Penal Code, 1860, s. 354C

<sup>&</sup>lt;sup>14</sup> Indian Penal Code, 1860, s. 354D

<sup>&</sup>lt;sup>15</sup> https://blog.ipleaders.in/virtual-reality-cyberstalking-india/

Here the section itself specifically talks about "women" and clearly states that women are considered as the victim bringing in the fact that men is also affected in either way so here in even the section talks about women because of the rate of crime they undergo but considering men on the equal scale wouldn't be the major drawback of this section.

#### **LEGAL SCENARIO OF FOREIGN COUNTRIES:**

The majority of countries use general laws (as appropriate in cases of blackmail, extortion, threats, defamation, outrage of modesty, harassment, theft, invasion of privacy, online impersonation, hacking, etc.) to prosecute those who engage in cyber stalking instead of having any specific legislative provisions to address the issue. However, the following analysis mainly considers the positions of industrialized nations such as the United States

• Legal Status in the United States: Under the federal statute of the United States of America (USA), Title 18, United States Code (U.S.C.), section 2261-A sub-section 1 deals with traditional stalking and sub-section 2 specifically criminalised 'cyber stalking,' and section 2261 (b) provides penal consequences for offenders of cyber stalking with several slabs of imprisonment ranging from life to no more than 20 years or 10 years in prison, or 5 years in prison, with a fine depending on the victim's injury. Aside from this specific law for 'cyber stalking,' there are a number of additional prohibitions that may apply to cyber stalkers, such as threats and extortion<sup>16</sup>, obscene or abusive telephone calls<sup>17</sup>. Obscene or abusive phone calls, the creation of child pornography.<sup>18</sup>

The Budapest Convention is the first legally enforceable global pact focused at addressing cybercrime. The agreement establishes a framework for international collaboration among treaty signatories. It is the only substantive international agreement with the declared goal of combating cybercrime through convergent, harmonized laws and capability development.

Because of the rise in cybercrime, India's Home Ministry is rethinking its decision to join the Budapest Convention.

<sup>&</sup>lt;sup>16</sup> 18 United States Code § 875, 876 (U.S.).

<sup>&</sup>lt;sup>17</sup> 47 United States Code § 223 (U.S.).

<sup>&</sup>lt;sup>18</sup> supra note 25 § 2251 (U.S.).

The Budapest Convention has a significant disadvantage in that the Convention on Cybercrime has also received harsh criticism for both its particular provisions that fail to safeguard the rights of persons and states, as well as its general insufficiency to maintain a free internet.

The Council is undoubtedly addressing these issues. of Europe's Cybercrime Convention Committee, which respects the Budapest Convention on Cybercrime's parties The Committee prioritises solutions to provide criminal justice access to cloud-based evidence. of Europe's Cybercrime Convention Committee, which respects the Budapest Convention on Cybercrime's parties The Committee prioritises solutions to provide criminal justice access to cloud-based evidence. Overall, it appears that India's participation in the Budapest Convention has been mostly influenced by diplomatic and foreign policy reasons, rather than true judicial cooperation on cybercrime and e-evidence. From the latter's point of view x The challenges addressed by the convention's parties through the Cybercrime Convention Committee are highly relevant to India as well. x The Convention provides a legal basis and practical framework for police-to-police and judicial cooperation on cybercrime and evidence with an increasing number of other parties. This framework is constantly being revised to improve its effectiveness. x As the Convention evolves, India would be able to contribute to shaping future solutions if it were a party. x India would become a priority country for capacity building. x Given the Prime Minister's vision of a "Digital India," and given the rise in cybercrime, India would benefit from joining this Treaty. The emphasis on cyber bullying and cyber stalking has mostly resulted from the perceived inadequacies of existing laws, typically by lawmakers and parents of bullying victims, whether those existing laws include stalking, illegal use of computer resources, or the like. The motive for the measure in 1990 that was enacted by 50 U.S. states and the federal government to "criminalise" stalking was due to incidences of stalking against celebrities. <sup>19</sup> For example, in the case of United States v. Lori Drew<sup>20</sup>, in which Megan Meier committed suicide after being bullied on Myspace, three of the four charges brought against the defendant (Drew) were actually in response to alleged violations of the Computer Fraud and Abuse Act, because specific statutes against cyber bullying did not exist at the time. Drew was finally declared free of the charges (but convicted of a misdemeanor) by the jury, but the conviction was later overturned by the court. In this case, Missouri legislators, at

10

<sup>&</sup>lt;sup>19</sup> Spitzberg & Hoobler, 2002

<sup>&</sup>lt;sup>20</sup>United States v. Drew (2009).

the insistence of the public and Meier's parents, created "Megan's Law," which primarily targeted the offence of a person above the age of 18. State legislation in the United States of America: Some states in the United States have begun to address the issue of c/yber bullying. States that have passed legislation have often done so in reaction to instances inside their state, to address what they perceive are flaws in federal laws, or to provide further protection to victims above and beyond current provisions. There are laws that handle solely online harassment of minors or child predators, as well as laws that protect adult cyber stalking victims or victims of any age. While other sites focus in laws that protect victims under the age of 18, Working to Halt Online Abuse is an assistance resource that lists existing and pending cyber stalking-related federal and state legislation in the United States. 18 It also includes a list of those states.

#### SCOPE AND LIMITATION OF THE STUDY:

The scope of this research paper extends to cover in detail the impact cyber stalking causes on women and minors by providing special reference to the effect it had on such vulnerable groups during the covid times. It also provides references to various cases and news reports of cyber stalking on women and children, especially the case of Manish Kathuria which is the impetus behind the 2008 amendment of the Information Technology Act. Further, the research paper dwells into the depths of various international conventions and cyber stalking and compares it to that of the Indian framework. The paper concludes itself by providing the suggestions and preventive measures that are to be taken by the government and the individual citizens in order to prevent themselves from being the victims of cybercrimes.

#### **CONCLUSION:**

Technology development has resulted in an upsurge in crime. Technology and crime are inextricably linked. Technology had a significant influence in the numerous bomb incidents that happened throughout the world. Computers were a major medium in all of these crimes. Computers have shown to be adaptable. It aids with everything from communication to the propagation of horrible infections. The latter element, and more to it, is currently gaining popularity. Computer crimes, sometimes known as cybercrime, have skyrocketed in recent years. Under it, many categories are investigated, one of which being internet stalking. Stalking occurs every day in the physical world, but it has

escalated at twice the rate in the virtual world because stalkers can easily target victims. The internet allows victims to remain anonymous. It is safer than stalking in the real world. The improvement of technology has also resulted in a rise in crime rates. In this digital age, it is possible to say that technology and crime go hand in hand. Technology has played an important role in various crimes that have occurred in and across the world. The prevalence of cybercrime has skyrocketed, and cyber stalking has been identified as one of them. Physical stalking was a common occurrence, but with the advancement of technology and criminals being given the benefit of anonymity via the internet, there has been a doubled rate of cyber stalking because stalkers are difficult to track. For the emerging trend of cybercrime, it is important to have a cyber law enforcing momentum because cybercrime has the potential to destroy each and every one of us. Every facet of life, since it is simple to commit yet extremely difficult to detect. Though India has an exceptionally thorough and well-defined legal system, all extant laws in effect in India were formed with the relevant political, social, economic, and cultural circumstances of the period in mind. Nobody could imagine the internet back then. With the advent of the Internet, a slew of delicate legal concerns and ills arose, necessitating the adoption of Cyber laws. Because cyber stalking is primarily an emotional crime, it must be addressed via a rehabilitative process as well as a therapeutic legal strategy. If restorative justice is included in cyber stalking regulations, victims may be stopped from causing greater harm in the process of escaping their stalkers. Furthermore, the restorative process may seek ways to repair the victim's harm by including not just the offender but also the online service providers. The laws that criminalise online stalking may make the offender feel repentant by making him aware of the illegality of his behaviour during cyber stalking. The victims may not only be cured of their psychological trauma, but they may also be healed of their physical trauma.

#### **DIRECTIONS AND RECCOMENDATIONS:**

#### **Suggestions for Cyber stalking Prevention:**

There is no one-size-fits-all method for preventing cyber stalking. As a result, one must take certain precautionary precautions to avoid being stalked and being a victim of such crimes.

Personal information is limited: One should avoid disclosing more personal information online than is absolutely necessary. Personal information should never be disclosed online, with strangers, or in chat rooms.

Password resets: Passwords should be reset on a regular basis. The password should be strong enough and should not be tied to any person, date, or anything else that stalkers may readily guess.

Sensitive information should not be disclosed: Sensitive information should not be shared outside of social media. Many of us reveal personal information by filling out numerous surveys, but we should be cautious.

Keep an eye on your privacy settings: We should all keep an eye on our privacy settings on various social networking sites. We must make informed decisions about which settings are appropriate for which platforms.

Hide IP address: We must ensure that our IP address is concealed because many programs and websites show our IP address to those with whom we communicate. As a result, in order to avoid becoming a victim of cybercrime, we need conceal our IP address.

