

WHITE BLACK LEGAL LAW JOURNAL ISSN: 2581-8503

3.424 . (3.63

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.

WWW.WHITEBLACKLEGAL.CO.IN

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 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.

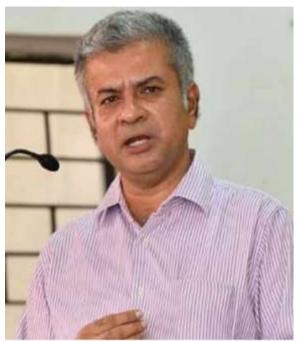
LEGAL

EBLA

I T

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer



a professional Procurement from the World Bank.

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

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 succesfully 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 Nautiyal

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.

Dr. Rinu Saraswat



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.





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

<u>CYBER STALKING- WAY FORWARD</u> <u>TOWARDS A NEW LEGISLATION</u>

Authored By -Adv. Aanchal Rathore

Abstract

The advent of technology has led to the cyber space becoming the new preferred environment. Accordingly, new issues in the form of various cyber crimes have also cropped up. Cyber stalking is one such cyber crime that has emerged in our society. While many countries have anti stalking legislations already in place, in India there is no standalone provision to punish cyber stalking. Section 66A of the Information Technology Act, 2000 dealing with punishment for sending offensive messages through communication service, was struck down by the Supreme Court in 2015. Since then, cases are filed under the relevant sections of the Indian Penal Code, 1860 particularly Section 354D and Section 509 both of which are gender specific provisions. Through this article the author has tried to highlight the need for a separate provision for cyber stalking in the Information Technology Act, 2000. The article discusses the legal position with respect to cyber stalking in India and also discusses the psychological and mental impact of stalking on the victims. The author has also suggested a draft of the provision on cyber stalking which can be taken into account by the legislators while drafting a provision that punishes cyber stalking.

INTRODUCTION

According to Merriam-Webster Dictionary, crime is defined as "an illegal act for which someone can be punished by the government". As per Halsbury's Laws of England, "A crime is an unlawful act or default which is an offence against the public and renders the person guilty of the act and liable to punishment". A crime is thus an act or an omission rendered punishable by the state. A crime creates a sense of societal fear and it adversely affects the societal conscience. It is inequitable and unjust if such a situation is allowed to perpetuate and continue in the society. A crime is something that shakes the societal conscience. A society in which human dignity is of paramount importance cannot allow such things to continue to exist which shake the societal conscience. This is where criminal law comes into action.

The state representing the people and the society has its prime duty to protect the people against such wrongs. It is important that in a civil society like ours, the faith of people on each other as well as on the legal system is maintained. The concept of a crime is a creation of the state and is based on the idea of protecting the interests of the society as well as that of the individuals. It is the duty of the state to safeguard against exploitation, oppression and aggression; particularly the vulnerable sections of the society.

There is no one complete definition of cyber crime. Simply put, a cyber crime is any crime which is committed using a computer. Cyber law is thus law governing the crimes related to the cyberspace. The ultimate purpose of criminal law as well as that of cyber law is to protect individual dignity and to restore societal stability, decency and order and to create faith and cohesion in the society. It is the collective societal judgment or the societal abhorrence which pre determines the acts which will be considered as criminal and thus punishable. The legislature merely being the representative is the body to make such laws and is ultimately guided by societal conscience.

Since what would constitute a crime and what would not constitute a crime is dependent upon societal perception; it is determined by a spatio-temporal variation or dynamism. Thus, what might be a crime in a society might not be crime somewhere else. Also, what might not be an offence at present can be an offence tomorrow. In context of cyber crimes, since the advent of technology and internet in itself is a relatively newer phenomenon, cyberspace is becoming the new preferred environment. It is said that technology is a double edged sword. It can potentially be a boon as well as a bane depending on its possible use or misuse. With the advent of technology, cyber crime cases such as online bank frauds, cyber terrorism, identity theft, cyber pornography, hacking and many others are on a rise with each passing day. All legal issues related to internet crimes are usually dealt with through cyber laws.

In light of the recent COVID-19 pandemic and the imposed lockdowns, there has been an increase in the usage of internet and computer systems by people especially in 2020 since people were confined to their homes and were essentially working from home as well. As a necessary corollary, considering that everything has its flipside, there has also been an increase in cyber crimes throughout the country with various instances of phishing, stalking, identity theft or other frauds have been committed. As per the Crime in India 2021 Statistics¹ published by the National Crime

¹ Crime in India 2021 Statistics, NCRB, available at: https://ncrb.gov.in/sites/default/files/CII-

^{2021/}CII_2021Volume%202.pdf

Records Bureau under the Ministry of Home Affairs, there were 52,974 cyber crimes across India in the year 2021 and the rate of total cyber crimes in India was 3.9%. On a bare perusal of the data of previous years it can be seen that this figure has consistently been on a rise and has now reached alarming levels.

INFORMATION TECHNOLOGY ACT, 2000 AND ITS RELATION WITH INDIAN PENAL CODE, 1860

The Information Technology Act, 2000 (hereinafter 'IT Act') was brought into effect on 17th October, 2000 and was primarily enacted in India in compliance of the Model Law on Electronic Commerce adopted by The United Nations Commission on International Trade Law in 1996. The Act sought to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce". The Act also provides for certain offences under Chapter XI and as per Section 75 of the Act, the IT Act applies also to any offence or contravention committed abroad by any person regardless of the person's nationality, in case the act or conduct involves a computer, computer system or computer network located in India.

It is a basic principle in every society which is governed by the rule of law that every law that is made should be in line with the spirit of the Constitution. All laws have to act subservient to the Constitution and have to abide by the essential principles of the Constitution and its basic structure. Consequently, the constitutional essence of The Information Technology Act, 2000 also lies in the fact that it has to subscribe to the basic principles of equity, justice, good conscience, reasonableness and non-arbitrariness. These principles are the essential governing principles of the Constitution and there cannot be any provision in the IT Act which goes against these principles and the principle of fairness.

Section 40 of the Indian Penal Code, 1860 (hereinafter 'IPC') defines an "offence" as an act punishable under the IPC or under any special or local law. The IT Act being a special law is read in conjunction with the provisions of IPC as well as the Code of Criminal Procedure which forms the general law. In fact, the provisions of the IT Act have effect notwithstanding anything inconsistent therewith contained in any law for the time being in force.²

² The Information Technology Act, 2000, Section 81.

The IT Act as amended in 2008 added many new offences and one of such offences was Section 66A. As per the amended IT Act³, an officer not below the rank of Inspector is empowered to investigate offences under the Act. Thus, it is the state which prosecutes under the IT Act.

CYBER STALKING AND ITS IMPACT ON THE VICTIM

Cyber stalking has not been defined in any particular legal provision in India. It can include following or pursuing a person online with a view to harass or embarrass them, watching their every move, stalking someone on social media or other platforms, continuously contacting them through emails or text messages or phone calls etc despite their disinterest and can even include cases of hacking into their profiles and interfering with their data and personal information or creating fake accounts. It may include posting private information or spreading rumours online about somebody or their family members. The list is therefore not exhaustive and covers a wide spectrum of activities. As per Merriam Webster Dictionary, cyber stalking is defined as the use of electronic communication to harass or threaten someone with physical harm.

Cyber stalking or even stalking in general is an act which causes fear or annoyance to the other person. It can also intimidate the other person and can potentially impact the person's mental frame of mind as well. The fear of constantly being followed in the physical world is scary but so is constantly being watched online. The same act of stalking and harassment in the physical world can rather be done online with much more ease and convenience.

One of the major reasons why cyber crimes thrive is that the perpetrator has an advantage of anonymity⁴. This encourages more and more of such crimes being committed in today's world because the perpetrator feels that his identity is not revealed since he is not physically doing the offence potentially leaving no trace of any evidence. There are increasing numbers of cases where the stalkers have installed location tracking devices such as GPS⁵ on the car of the victim to track their real time movements. The stalker can get it done for really cheap prices and its effects as can then be far reaching.

Furthermore, it is not always necessary that the person stalking is unknown to the victim and there could be cases where the perpetrator is in fact known to or is even an intimate partner of the victim

³ The Information Technology Act, 2000, Section 78.

⁴ Heena Keswani, Cyber Stalking: A Critical Study, Bharti Law Review, April- June, 2017.

⁵ Cynthia Fraser, Erica Olsen, Keofeng Lee & Cindy Southworth, The New Age of Stalking: Technological Implications for Stalking, 61 JUV. & FAM. CT. J. 39 (2010).

but despite that he or she engages in cyber stalking. In the National Violence Against Women Survey⁶ conducted in 2000, it was found that in the USA approximately 4.8% of the surveyed women and 0.6% of the surveyed men were stalked by a current or former intimate partner at some point in their lifetime.

The harm that can be caused by simply a touch of a button is something that nobody could have possibly fathomed when technology was making its way into our lives. Stalking interferes with the peaceful enjoyment of one's life and liberty. It instils torment, fear, uncertainty and causes emotional harassment to the person and may also seriously impact their mental health in the long run. It may lead to destroying the peace of mind of the victim and not just that, he or she may be driven into emotional distress and may actually fear for his or her life and safety since there are chances of cyber stalking spilling over and being carried on physically as well. Stress and anxiety have been medically identified as causing physical health issues as well. Since the person being stalked may have thoughts of self-doubt and may in extreme cases also lead to thoughts of self-harm or even thoughts of committing suicides.

In a study⁷ conducted on 100 victims of stalking with a 50 item questionnaire to examine the social and psychological impact of stalking on them, it was found that majority of the victims were subjected to multiple forms of harassment including being followed, repeatedly being approached and bombarded with letters or phone calls for periods ranging from a month to 20 years. 58 of them had received threats and 34 were physically or sexually assaulted. Almost all of them had to make changes in their lives to deal with it wherein 53% of them had to change or cease their employment and 39% had to move their homes. A whopping 83% had reported increased levels of anxiety and 55% had intrusive recollections and flashbacks with nightmares, appetite disturbances and depressed mood. Suicidal feelings were acknowledged by 24% of victims and 37% of them fulfilled the criteria for being diagnosed with post-traumatic stress disorder. This shows the seriousness of the impact of stalking on the minds of the victims.

It is a general perception that women are more likely to be victims of cyberstalking. However, it has been found that over all, men are somewhat more likely than women to experience at least one of the elements of online harassment, 44% vs. 37%. In terms of specific experiences, men are

⁶ Patricia Traden & Nancy Thoennes, Full Report of the Prevaluce, Incidence, and Consequences of Violence Against Women, Nov 2000, NCJ 183781.

⁷ Michele Pathé & Paul E. Mullen, The impact of stalkers on their victims, 170 British Journal of Psychiatry , 12-17 (1997).

more likely than women to encounter name-calling, embarrassment, and physical threats. Among all internet users, 6% of men and 9% of women have experienced being stalked⁸.

In the National Violence Against Women Survey⁹, it was found that 8.1% of surveyed women and 2.2% of surveyed men reported being stalked at some point in their life. This also highlights that it is not just women who are victims of cyber stalking. Though in comparison to women, the proportion of men is less, however, they do account for a good chunk of the society which certainly cannot be ignored.

LEGAL PROVISIONS REGARDING STALKING IN INDIA

The law regarding stalking in India is primarily contained under Section 354D of IPC which states that "any man who 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 monitors the use by a woman of the internet, email or any other form of electronic communication, commits the offence of stalking". The said section was added by the Criminal Law Amendment Act, 2013 which was passed in response to the outrage following the Delhi gang rape case. In this light, it is noteworthy that the said section is gender specific. It only punishes a man for stalking and thus in cases where the same act is committed by a woman she would not be held liable for the same.

Apart from Section 354D IPC, in cases of stalking, the act of an offender may also attract punishment under other provisions of IPC if the particular ingredients of those sections are fulfilled. For instance, Section 503 IPC dealing with criminal intimidation may be attracted where a person threatens another with any injury to his person, reputation or property; or Section 507 dealing with criminal intimidation by an anonymous communication may be attracted in cases where the name or abode of the person is concealed. Section 509 may be indirectly made applicable where words said, gestures or acts are done in order to outrage the modesty of a woman. In the year 2001, the first case reported on cyber stalking was reported in India. Ritu Kohli was stalked by Manish Kathuria who followed her on a chat website and abused her. He began using the website in her name to invite people for chatting and then gave away her phone number to

⁸ Pew Research Center, October 2014, "Online Harassment".

⁹ Supra point 5.

people. As a result, Ritu Kohli started receiving obscene calls at odd hours in the night which led her to report the matter to the Delhi Police. A case was registered under Section 509 of IPC. However, since Section 509 could not squarely cover with Ritu Kohli's case being one committed online and through the use of internet, a need was felt to bring about a law dealing with the same. Accordingly, an amendment in the IT Act was brought about in the year 2008 which inserted Section 66A dealing with the punishment for sending offensive messages through communication service etc. In the year 2003, another case was reported¹⁰ where Seema Khanna (name changed) received emails from a man asking her to pose nude or to pay him Rs 1 lakh. She was also threatened of her morphed pictures being released on adult websites along with her personal details. The accused had hacked into her mail and accessed her pictures from there. A case was later lodged under Section 509 IPC and also under IT Act. The police later admitted that the IT Act is not enough to deal with cyber stalking.

The IT Act did not (and still does not) contain any separate provision dealing with cyber stalking and the same was covered under Section 66A of the Act which prescribed a punishment for cases "where any person who sends, by means of a computer resource or a communication device,-:

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

However, the Hon'ble Supreme Court in the landmark case of Shreya Singhal v, Union of India¹¹ struck down Section 66 A of the IT Act in its entirety being violative of Article 19(1)(a) and not being saved under Article 19(2) of the Constitution. Justice R. F. Nariman, speaking for the two judges' bench, agreed with the petitioners that the said Section suffers from the vice of being open ended, undefined and vague since none of the terms given in the Section like "grossly offensive" or "menacing character" have been defined. The court considered the chilling effect of Section 66A upon the freedom of speech and expression so much so that virtually any opinion would be covered under its ambit.

¹⁰ Sachin Prashar, Cyber pal demands nude pics, Times of India, December 2003, available at: https://timesofindia.indiatimes.com/city/delhi/cyber-pal-demands-nude-pics/articleshow/381426.cms.

¹¹ Shreya Singhal v. Union of India AIR 2015 SC 1523.

Since the striking down of Section 66A of the Act by the Supreme Court, there is no particular law dealing with cyber stalking under the Indian law. Thus, invariably, for cases involving cyber stalking reliance is made on the various provisions of IPC. However, it is clear that the various provisions of IPC are not sufficient to deal with the cases of cyber stalking. Section 354A of IPC is gender specific and thus does not cover cases where the perpetrator is a woman. In a PIL¹² filed in 2018 to make crimes like rape, sexual harassment, outraging modesty, stalking and voyeurism as gender neutral, the Supreme Court dismissed the PIL holding that it was open to the Parliament to amend the law. The PIL questioned constitutional validity of all these provisions including Section 345D however the court observed that these are very well protected by Article 14 and 15 of the Constitution of India. It is clear that even though Section 354A of IPC is gender biased, it is still constitutionally valid and therefore it does not make it punishable where the same is committed by a woman. Though there have been repeated demands of making these laws gender neutral either by mentioning the misuse¹³ of them by women or otherwise.

Apart from this, other provisions of IPC can be attracted for committing such activities only if the particular ingredients of those provisions are attracted like Section 503, 507, 509 IPC. In this light, the author feels that it is imperative to have a standalone provision dealing with cyber stalking under the IT Act.

Furthermore, stalking is invariably an attack on the Right to privacy of the individual. The Constitution of India guarantees the Right to life and personal liberty to every person¹⁴. The Supreme Court of India has unanimously held that the Right to Privacy is a Fundamental Right under Article 21 of the constitution of India¹⁵. Stalking as a crime infringes upon the victim's privacy and safety and thereby violates Article 21 of the Constitution of India.

The Universal Declaration of Human Rights, adopted by the UN General Assembly, enshrines the inalienable rights and freedoms of all human beings. It expressly provides that no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, or to attacks

¹² Satya Prakash, *SC rejects PIL to make rape, sexual harassment cases gender neutral*, Tribune India, February 2,2018, New Delhi.

¹³ PIL in Supreme Court seeks directions to Centre to consider misuse of laws under IPC Sections 354A-D, 506, 509, 376,498A, Indianlegallive (August 16, 2021), <u>https://www.indialegallive.com/top-news-of-the-day/news/pil-in-supreme-court-seeks-directions-to-centre-to-consider-misuse-of-laws-under-ipc-sections-354a-354d-506-509-376-498a/.</u>

¹⁴ Constitution of India, Article 21.

¹⁵ Justice K.S. Puttaswamy (Retd) vs. Union of India, AIR 2017 SC 4161.

upon his honour and reputation¹⁶. As is clear, stalking is one of the forms of arbitrary interference upon the privacy of an individual. India, being actively involved in the drafting of the Universal Declaration of Human Rights, has always sought to make its laws in conformity with the same. The present anti-stalking laws in India also seek to abide by these basic principles. It is the view of the author that it is in this background that a new law on stalking needs to be framed.

SUGGESTIONS FOR AN ANTI STALKING LEGISLATION IN INDIA

In India, there is no standalone provision for which makes stalking as a punishable offence. Especially after Section 66A of the IT Act has been declared ultra vires by the Supreme Court, there is a need for a new, separate law to be framed in this regard. On the one hand it can be done while improving on the language of Section 66A of the IT Act to make it less vague and open ended while on the other hand, an inspiration can be taken from the legal position in other nations which have anti- stalking laws in place. It is on this basis that the author would like to suggest the framing of a new law on stalking in India which can be framed on the following lines:

Punishment for Cyber Stalking- Any person who

-sends or disseminates by means of a computer resource or a communication device, any message, picture, video, or any other information to any person, after repeatedly being denied contact by that person, with a view to harass, demean, embarrass, intimidate or cause fear to them, whether or not it is with a sexual connotation; or

- Constantly and repeatedly monitors the use of internet or email or any other form of electronic communication by any person except where it is reasonable or justified by law; or

- installs any GPS or similar device on the automobile of any person or downloads any other similar application in any electronic device of any person in order to acquire information about the location or other personal information of such person, without such person's consent; or Shall be punished with rigorous imprisonment as well as fine.

The section can further provide an explanation stating the definition of "information", "electronic mail", "GPS device", "automobile" and "application".

The author feels that stringent punishment for the offence of cyber stalking needs to be provided in order to ensure that deterrence is created in the society against the commission of such crimes. Thus, the state can prosecute the offender for the cyber stalking by providing for the first conviction, a simple imprisonment for a term of minimum 3 years and upon a subsequent

¹⁶ Universal Declaration of Human Rights, Article 12.

conviction, rigorous imprisonment for a term of minimum of 5 years. This shall be in addition to a fine.

Apart from this, a speedier trial can be afforded for the prosecution of offences under the IT Act so as to enable the victims to prosecute the offenders of cyber crimes. The judges can also consider the impact of stalking on the mental and psychological health of the victims and accordingly make use of their inherent powers to conclude the trial of offences related to cyber crimes at their earliest without unnecessary delays. Efforts can also be made to generate awareness regarding the legal recourse available to the victims of cyber stalking.

CONCLUSION

The very aim of any Anti-stalking legislation should be to effectively deal with the mischief of stalking. Stalking of any kind has deeply penetrative and irreversible damage on the mental health of the victim. In absence of a separate provision, presently resort is had to Section 354D and other sections of IPC. However, section 354D only deals with cases where the perpetrator is a male thus leaving out any remedy to an entire set of cases of where the victims are male. In this light it becomes important that there should be a separate provision in India under the IT Act dealing with cyber stalking. A careful perusal of the anti-stalking legislation of other nations can be relevant in preparing our own separate provision for cyber stalking. Through this article, the author has tried to fill the gaps in the existing literature on the subject by suggesting a possible draft of a new legislation which will be in tune with the present technological advancements.