



INTERNATIONAL LAW  
JOURNAL

---

**WHITE BLACK  
LEGAL LAW  
JOURNAL  
ISSN: 2581-  
8503**

*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](http://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

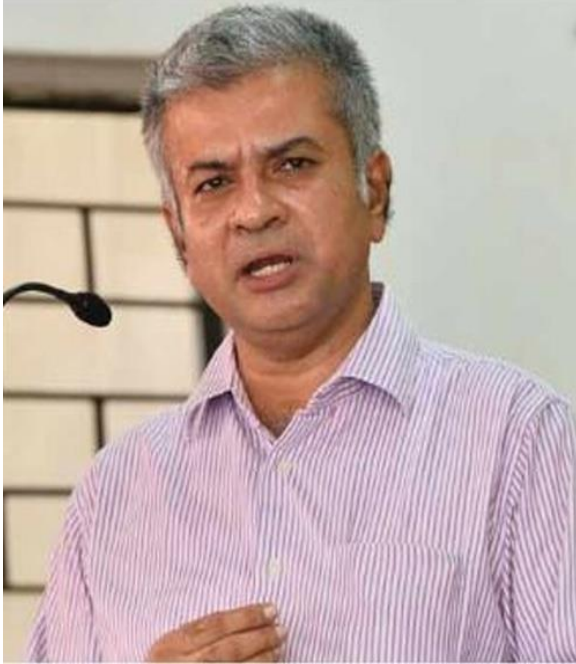
– The Law Journal. The Editorial Team of White Black Legal holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of White Black Legal. Though all efforts 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.

W H I T E B L A C K  
L E G A L



## EDITORIAL TEAM

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



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 is currently 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 University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a

professional diploma in Public Procurement from the World Bank.

### 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.



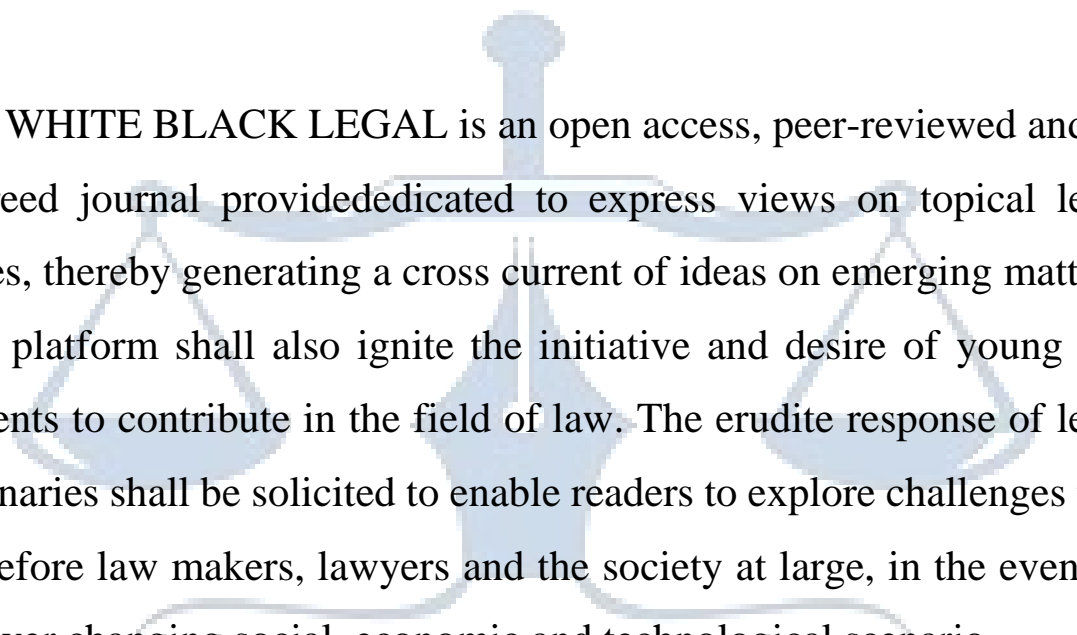
## **Subhrajit Chanda**



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

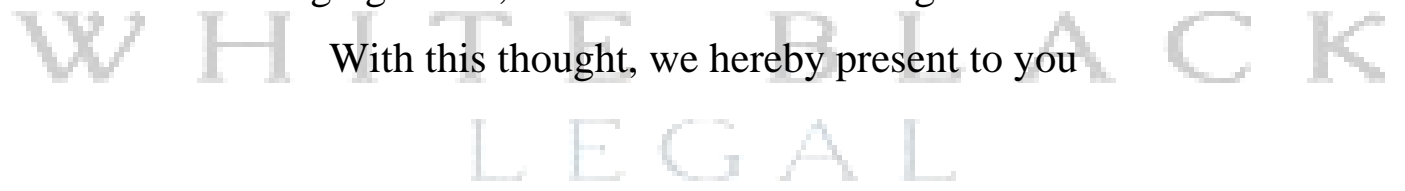
Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International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





# **A STUDY ON CYBER CRIME AGAINST MEN AND RESPONSE OF CRIMINAL JUSTICE ADMINISTRATION IN INDIA**

AUTHOR: PRAGADEESHWARAN B M, BA.LLB (Hons), IV year

CO-AUTHOR: MUKILAN V, BA.LLB (Hons), IV year

CO-AUTHOR: MANOJ PRAKASH S, BA.LLB (Hons), IV year

Designation: Undergraduate Students

Institution: The Tamilnadu Dr Ambedkar Law University (Tndalu),

School Of Excellence In Law (Soel)

## **ABSTRACT**

*India is a place where the patriarchy shows dominance in families. Indian Society always seems to express its concern about Gender Equality but in reality it seems like less emphasis is placed on men than women when they become victims of any crime. Cyber Crime is one such crime where men become victims. It is a malicious and deliberate attempt by an individual or an organization to gain access to another person's private and sensitive information. Usually, the perpetrator seeks to benefit from disrupting the target's network. In recent trends, men have become more vulnerable to cyber threats and the youth of our country have been radicalized to commit terror attacks that threaten India's sovereignty, integrity, and security. They often become victims to cyber harassment, pornography and cyber radicalisation. India's Criminal Justice System provides a list of legislations that provide laws for protection of women who become victims of Cyber Crime but the same laws almost turn a blind eye when it comes to men. The paper focuses on bringing out the kinds of cyber-attacks and the need for statutory provisions to safeguard individuals' privacy. There is an urgent need for improving the Criminal Administration of Justice for victimized men. Major stress is placed on bringing about a strict enforcement of data protection laws like IT Act, IPC and POTA. The cyber laws in India should also be periodically reviewed in order to cope up with emerging trends of cyber-crime and also suggest ways to strengthen the judicial, law enforcement and come up with innovative methods of investigation on par with the emerging new trends of Cybercrime.*

**Keywords:** Gender equality, Cyber Radicalization, Online Pornography, Cyber Harassments

## **INTRODUCTION:**

Internet is fast mode of communication covering all spheres of mankind. The growing ICT have bad and good impact on our society. Law imposes rules and regulations that regulates conduct of people. The law should keep itself updated to tackle new trends of crimes. Emerging rate of cybercrime poses threat to individual's privacy, modesty and threatens the nation's security. The rapid growth of technology leaves the law behind. The Constitution safeguards privacy of an Individual under Article 21, at the same time guarantees Freedom of Speech and Expression under Article 19 (impliedly gives right to express views through social media). The research in our hand make the field under study when we found gender biased issues in Laws. In India, cyber laws like IT act 2000, IPC are enacted to protect the victims of cybercrime and punish the offenders. The time has changed where men are also falling victims for cybercrimes, surprisingly perpetrators are women. A practice of forcing someone to do something, particularly to perform sexual acts or to, extort money, by threatening to publish naked pictures or sexual information about them is sextortion<sup>1</sup>.

The criminal justice administration starts from the Police to the Apex court of India. It is observed that women are given protection for their modesty and privacy. When the same happens to men, criminal justice administration has come blind folded, as there is no separate law for protecting men victims, the reason is stereotype in our country, getting fixed to an abstract idea that women are the victims and men always stand as an offender. This gives advantage to women perpetrators to use the loopholes for their selfish needs.

The IPC Sections 503 (threatening injury, reputation or property), 509 (penal provision for insulting the modesty of a woman) and 354A (sexual harassment), are available to women for their protection. While there is vast majority of sexual harassment cases that are filed by women, yet there are a number of cases involving female on male sexual harassment. This type of harassment also includes rape and death threats, such as those at the heart of an upcoming Supreme Court case.<sup>2</sup> There is a need for law to safeguard the modesty, privacy of men. In accordance with principle of Equality before law and Equal protection by law, the IPC provisions has to be gender neutral, which shall provide same hand

---

<sup>1</sup> Government of India, Ministry of Home Affairs: National Cyber Crime Reporting Portal < <https://cybercrime.gov.in/Webform/CyberAware.aspx> > accessed 26 May 2022

<sup>2</sup> Soraya Chemaly, 'There's No Comparing Male and Female Harassment Online', (SEPTEMBER 9, 2014) < <https://time.com/3305466/male-female-harassment-online/> > accessed on 25 June 2022



of justice and punishment to victims and offenders respectively.<sup>3</sup>

### **OBJECTIVES:**

1. The non-existence of statutory protection for victimized men.
2. Women are given a soft corner when they are committing cybercrime
3. In recent years, cyber stalking against men has increased but has been given lesser importance.
4. The online radicalization of Indian youths is a threat to India's security
5. Strict enforcement of data protection acts is required like the IT act, 2000, IPC and POTA

### **METHODOLOGY:**

This study uses Doctrinal research as there is dearth of publicly available primary documents.

Doctrinal research means research that involves the significant amount of reading and referring text books, articles, journals, dictionaries, encyclopaedia etc., . It involves systematic analysis of statutory provisions, logical and legal reasoning of principles and legal propositions<sup>4</sup>.

This study relies upon the secondary data to assess the study of cyber-attacks on men and the response of criminal justice administration in India. The data sources include reports of crime in India by the National Crime Record Bureau, from newspaper articles like News Indian Express, Times of India and Tribune India. This research also view point of different authors, the reports and papers released by the European Union, United Nations Organisation. Hence it can be concluded that the Doctrinal Research gives a way to understand the study on cyber-attacks on men and response of criminal administration.

### **REVIEW OF LITERATURE:**

The Analysis of Anti-Cyber Bullying Laws in India portrays that cyber bullying is a kind of harassment that involves the usage of electronic devices such as laptops, mobile phones, tablets which involves text messages, voice chats, video chats, social media, where harmful messages ranging from indecent comments to threats to rape and kill are present. It also mentions that with the advent of the

---

<sup>3</sup> Rishi Malhotra v. Union of India, Writ Petition(s) (Criminal) No. 145 of 2017

<sup>4</sup> Sarfaraz Alam, 'Doctrinal and Non-Doctrinal Research Sample' < [www.academia.edu](http://www.academia.edu) > accessed 27 May 2022

internet, more fake identities are created which gives anonymity to the users to help hide their self-identity<sup>5</sup>. Owing to the Global Pandemic of Covid-19, physical stalking is now transformed into Virtual stalking, which is now a form of cyber-crime. Cyber Stalking is harassing a person through the internet and monitoring someone's data, data theft, data forging, and identity theft<sup>6</sup>.

Men in India, especially Muslim youths in Jammu and Kashmir are under extreme radicalization by terror outfits, which prompts them to attack even the armed forces, provoke communal violence and act as a sleeper cell. The terror outfits like Lakshar e Taiba, Jaish e Mohammad, ISIS are using technology to change their modus operandi to cyber radicalization that holds another threat of terrorism financing. They create dark webs and use social media to spread extremist ideology to youths for radicalizing them. Relying upon the European Commission report,<sup>7</sup> it says that the trends, means and patterns of radicalization evolves as time passes and adds that internet platform, including the social media, is paving new opportunities for terrorist groups and their sympathizers to communicate mobile and recruit among themselves.

## **I. CYBER HARASSMENT**

Cyber Harassment is form of bullying or harassment using electronic forms of contact. Cyber Harassment has become increasingly common, especially among teenagers. Harmful bullying behaviour can include posting rumors about a person, threats, and sexual remarks, disclose victim's personal informations or hate speech. The person indulged in harassment have clear intention to harm and repeated behaviour. Result of which, victims who are lower self-esteem increases suicidal ideation and a variety of emotional responses like retreating, being scared, frustrated, angry, and depressed.

The terms Cyber Harassment and Cyberbullying are sometimes used synonymously, though some people use cyberbullying specifically to refer to harassment among minors or in a school setting. Cyberbullying is defined as, an aggressive, intentional act or behaviour that is carried out by a group or an individual, using electronic forms of contact, repeatedly and over time against a victim who

---

<sup>5</sup> Vinod Joseph and Mitali Jain, 'India: Anti-Cyber Bullying Laws in India - An Analysis' < <https://www.mondaq.com/india/crime/989624/anti-cyber-bullying-laws-in-india--an-analysis> > accessed 26 May 2022

<sup>6</sup> Vanya Verma, 'The virtual reality of cyberstalking in India' < <https://blog.ipleaders.in/virtual-reality-cyberstalking-india/> > accessed 27 May 2022

<sup>7</sup> European Commission, Migration and Home Affairs: Prevention of Radicalisation

cannot easily defend him or herself.<sup>8</sup> On the other hand, Internet Trolling is a common form of bullying over the Internet in an online community in order to elicit a reaction, disruption, or for their own personal amusement.

### **I.1. General Aspect**

Cyber Harassment is being cruel to others by sending or posting harmful material using a cell phone or the internet. Today Harassment has moved from the printed page to cyberspace. This can include repeated e-mail or text messaging contact with an individual who wants no further contact, spreading malicious information about that person on social networking sites, threatening others, and revealing personal and confidential information about that person, including his or her contact information. Whether or not this can legitimately be considered a crime is hard to determine. Unlike in the past, the Internet has made it easier for Cyber Harassment to remain anonymous.

In Vermont 2003, 13 – year old boy Ryan Patrick Halligan hung himself after being subjected to repeated instant messaging and Internet Bullying. Over a period of a year, Halligan received taunts that made fun of his learning disorder and implied that he was a gay. One perpetrator, in particular, created an intricate plan that involved a girl whom Halligan liked, pretending to be interested in him, only to later publicly embarrass him. The bullying seemed to ebb and flow for a time but increased in the summer of 2003 just before Halligan took his own life.<sup>9</sup>

### **I.2. Cyber Harassment incidents in India**

As the research focus is on the men population; universe of the study being India, we have fetched some cyber bullying and harassment incidents. Issues about Cyber Harassment on men has got attention recently, when media spoke about criminal administration system and society failing to deliver justice to victimized men. Has trend grows, the cyber harassments are accompanied by cyber stalking. Malad suicide case would be a suitable example, the following information was extracted from the Indian Express,

---

<sup>8</sup> Jason Wayne, Cybercrime and Digital Forensics, first published 2018

<sup>9</sup> Ryan Halligan, Suicide of Ryan Halligan < <https://en-academic.com/dic.nsf/enwiki/11625772> > accessed 28 May 2022

### **Facts of case study no. 1:**

A 38 year old man committed suicide in Malad on May 4 2022 who was the sales executive.<sup>10</sup>

### **Problem**

The victim was harassed by cyber fraudster who sent his nude photos with indecent messages to his friends and colleagues saying him to repay his online loan through a mobile app “Call Hello Gash”.

### **Police action:**

The victims elder brother went to the police station when his brother started to receive these kind of messages where the police give him an acknowledgement of his complaint but no FIR was filed. Only after the suicide of the victim, Police filed a FIR.

### **Who is convict?**

There is no information regarding the convict and police were searching for them

### **Observation:**

There are many similar incidents like the one mentioned above:

- 1) In Mumbai, Police failed a FIR on cyber fraudsters for targeting a 33 year old man they gave him a loan amount of rupees 7000 through online transactions and acquired his contact list on his phone. When he failed to repay it, they threatened him with the pornographic video marked with his face and sent it to his 12 family members including four women.
- 2) The Bandra police station in Mumbai, filed a FIR against cyber fraudster, when 23 year old man was threatened by a morphed nude photo and the photo was circulated to 6 of his family members to repay his loan amount with more interest.

The next incident was reported by the same printed media, about cyber bullying done by known organisations, and one such was Rupee Bazaar, a money lending app.

### **Facts of case study no. 2:**

A 23-year-old Sai Aravind committed suicide by hanging in Chennai.<sup>11</sup>

---

<sup>10</sup> Jayprakash S Naidu, Mumbai: Man ends life after cyber fraudsters circulate morphed nude photos, harass him over online loan < <https://indianexpress.com/article/cities/mumbai/man-suicide-cyber-fraudsters-harassment-online-loan-7903003/> > accessed 29 May 2022

<sup>11</sup> The New Indian Express, ‘Bullied online by money-lending app company, Chennai man kills self’ (Chennai, 25



**Problem:**

Sai Aravind got money as debt from a money lending app called “**Rupee Bazaar**” and unfortunately, he could not return the debt as per the time fixed. Since the app got permission to access his contact list in his mobile, the money lenders started cyber bullying the victim and sent messages titled ARAVIND IS A FRAUD to members in his contacts list. Frustrated by these messages, he filed a complaint in Arumbakkam Police Station, but no action was taken. Depressed, victim committed suicide.

**Police action:**

The victim filed a complaint in nearby Police station but no action was taken by the police. After the victims’ suicide, the police filed his death as a case of suspicious death which was neither satisfactory nor accepted by relatives of the victim.

**Convict:**

The convict is a 23-year-old male working as an IT professional in Chennai.

**Observation:**

When there is an unknown perpetrator who haven’t revealed his/her identity till now, the police, who is the part of criminal administration fail to take the complaint seriously. More or less, actions are taken by police only when any suicide or injury occurs to the victims. In recent year, Digital Bullying is a threat to kids and their privacy and liberty. It is extremely invasive and upsets kids very much. Before the situation turns out of control, parents need to urge their kids to report all instances of digital bullying so that they can deal with the bullies and stop the nuisance<sup>12</sup>. Moreover during pandemic, the surge of cyber harassments has increased, over 900 complaints were filed from 257 cities in India. According to the report published by Cyber Bullying Action Awareness Program (CWAAP), most of the complaints were about sextortion and trolling<sup>13</sup>.

**Inferences**

In cyberspace, modesty of men is at stake, when laws to protect the modesty and privacy of women

---

November 2020

<sup>12</sup> G. Ram Kumar, Cyber Crimes: A Primer Internet Threats and Email Abuses

<sup>13</sup> The Times of India, ‘Cyber Harassment cases see upswing in pandemic’ (Mumbai, 12 January 2022)

exist, the same does not back the modesty of a men. There has always exist the disparity in criminal justice administration system due to the fact that, Women are expected to follow all the social traditions, customs, and norms, be submissive, passive, and compassionate just to maintain the family as a unit. This has also been used to mitigate a woman's liability of a crime and justify the low female criminality rate as compared to men. There are various reasons to explain the logic behind this pattern. One can be that, criminal justice administration system is being too chivalrous and is stuck to a stereotype which portrays that women need protection.<sup>14</sup>

## **II. CYBER RADICALIZATION**

Radicalisation refers to the process of an individual's transformation from a moderate, law-abiding citizen into an active, anti-state, violent extremist<sup>15</sup>. Radicalisation, if unchecked can lead to extremist discourse of society, recruitment by terrorists, aggravate communal violence and fuel extremism among other group. The major outcome of Cyber Radicalisation is Cyber Terrorism.

Online radicalisation and recruitment of the Indian youth by ISIS is a major threat to Nation's Sovereignty, Security and Integrity, but with the advent of increasing Internet penetration and social media, the problem has got compounded. It is difficult to regulate social platforms due to their inherent advantages on one hand and greater anonymity and transnational reach on other hand. Cyber terrorism is the act of causing fear in people's thinking through the use of the internet as a medium. Cyber Terrorism is mentioned in Section 66-F of the Information Technology Act of 2002.

### **2.1 - GENERAL ASPECT**

Not only in India, All over the world most of the Terrorist Organisations like (Al Qaeda, ISIS, Taliban) uses Cyber Radicalisation as the major tool for attracting more peoples to add in their groups and convert them to an Extremist.

Once the President of US Barack Obama said, Terrorist organisations such as Al-Qaeda and the Islamic State, are exploiting the Internet and social media platforms to radicalise and attract young

---

<sup>14</sup> Niharika Tiwari, 'Gender Disparity in the Criminal Justice System of India' < <https://blog.iplayers.in/gender-disparity-criminal-justice-system-india/> > accessed 28 May 2022

<sup>15</sup> Drishti IAS, 'Status of Radicalisation in India'(2020) < <https://www.drishtias.com/daily-updates/daily-news-analysis/status-of-radicalisation-in-india> > accessed 29 May 2022

Muslims to their ranks:

“The high-quality videos, the online magazines, the use of social media, terrorist Twitter accounts – it’s all designed to target today’s young people online, in cyberspace”<sup>16</sup>.

In **Netherland**, the Government says that, Terrorists undergo radicalised before resorting to violence, so the Government made the Teachers and youth workers attempt to detect this and, if required, submit their concerns to the police and criminal justice authorities. It is feasible to halt radicalization and prevent it from turning to terrorism in this way.

To counter-radicalisation, the European Commission proposed a **Radicalisation Awareness Network (RAN)**, an EU-wide umbrella network uniting essential first-line practitioners and field specialists. The major aim is to create awareness to the peoples and states regarding the Radicalisation process of the Terrorist Groups. It established Commission for the making of policies for Counter-Radicalisation.

## 2.2 - INDIAN ASPECT

India's Constitution, being a secular republic, clearly specifies the right to be regarded as equal citizens regardless of religion, caste, or gender. The mainstream Indian National Congress and regional groups, on the other hand, have used minorities to achieve political advantage in India's secular politics. In fact, Hindu nationalism is sometimes considered as a direct response to the fractiousness that has contributed to the violent strain of identity politics that exists today. From 1980 to the present, the BJP's emergence as a national party has been distinguished by its devotion to religion-based 'Hindu' nationalism, which tries to define Indian identity and culture only in terms of 'Hindu' ideals, leaving no place for other religions. According to Union Defence Minister, today, the enemy no longer needs to enter the border. He can also target our security apparatus from outside the border. Alignment and realignment of global powers have added to the already changing security challenges. The State Administration issued a social media ban in the Kashmir Valley in April 2017. Despite the fact that more than 20 social media sites were shut down, young people quickly returned to the internet by utilising VPNs, which improve the user's secrecy and privacy.

---

<sup>16</sup> European Foundation For South Asian Studies, Cyber-Radicalisation: Combating Terrorism in the digital era (2018)

### **2.3 - INITIATIVES TAKEN BY THE INDIAN GOVERNMENT**

When terror outfits started to use ICT for radicalisation, there is shift in the modus operandi of terror outfits in the way of recruiting, training, and deploying the cadre. From Recruitment to money transfer takes place in online which is far dangerous than the ISI modus operandi which usually trains people across the border. There is need for de-radicalisation and counter radicalisation process from government side.<sup>17</sup>

- 1. Counter Radicalisation:** It is the process through vulnerable persons are prevented from getting radicalised. In the Kashmir Valley, the majority of Muslim youth are rapidly gravitating toward radical political, social, and religious ideologies that reject and challenge the status quo. In Kashmir's Muslim society, there has been a dramatic increase in Pan-Islamism, steadily marginalising an early pro-nationalist insurgency ideology. Young people are being indoctrinated with Wahhabi ideology, which rejects the historic Kashmiri tradition of people visiting and paying reverence at the shrines of popular saints (Sufis and Rishis), calling it a breach of Islam's precepts.
- 2. Counter Violent Extremism:** were developed in Indian states in 2019: Andhra Pradesh, Kerala, Maharashtra, and Telangana. India's law enforcement personnel met with representatives from global social media corporations on a regular basis to examine emerging dangers and methods to prevent online terrorist recruiting and radicalization. Throughout the year, Indian officials observed online terrorist radicalization in conflict-free zones, mainly in the southern Indian states. India's strategy emphasised content suppression, including cutting down internet access in some areas.
- 3. International and Regional Cooperation:** India is a founding member of the Global Counter-Terrorism Forum (GCTF) and participated in the GCTF, the ASEAN Regional Forum, and other UN counter-terrorism fora in 2019. In ASEAN conferences, India also continues to lead efforts to denounce terrorism and call for concrete actions to combat the danger. India held the first Quad-country (the United States, Australia, India, and Japan) on Counter-Terrorism.
- 4. CERTs (Cyber Emergency Response Teams)** have been formed. With the formation of the National Cyber Coordination Centre (NCCC), the Indian government made a giant step forward combating cyber-threats and terrorism. The Ministry of Home Affairs (MHA) has also established the Indian Cyber Crime Coordination Centre (IC4) to tackle cybercrime and cyber terrorism.

---

<sup>17</sup> Ashok Kumar IPS, Vipul Anekat IPS , “Challenges to Internal Security of India”, 4<sup>th</sup> Edition



### **III. SCRUTINY ON LEGAL STATUTES**

#### Need for Gender Neutral provisions.

In one of the incidences, Vijay Nair, a businessman from Mumbai and the founder of a media company, was interrupted in any of his discussions and harassed by a woman who was commenting on his Twitter account and making sexually explicit comments. She claimed to be the victim alongside Nair and said that a couple in Delhi was stalking them both. But as time went on, it became clear that she was the one who had actually done all of this because she liked Nair. This had an impact on Nair's mental health and created embarrassing situations at work because all of her female friends had received emails about it. Section 354D of the IPC, 1860, which primarily punishes female victims, does not define cyber stalking as a crime. She has not yet faced charges for the wrong she did. The Criminal Law Amendment Act, which was based on Justice Verma's committee's recommendation for gender neutralisation, inserted Section 354(D) in 2013, the committee was concerned over the gender neutralizing of the sexual harassment law.<sup>18</sup> Article 14 of the constitution of India strikes at arbitrariness in State action and ensures fairness and equality of treatment.<sup>19</sup> The category of people, sex, or who is typically the victim are not topics of discussion when it comes to laws. In a given culture, laws are mandated to apply to every person equally without causing any injustice to any gender. However, the Indian Penal Code, 1860's Section 354D does not guarantee everyone's safety. Although there are fewer male than female victims of cyber stalking, this does not give us the licence to victimise men.<sup>20</sup> Men have experienced major stalking situations by female stalkers in a number of instances. It is necessary for the legislation to be gender-neutral since it is not just about men and women but also about the other gender, which is already a vulnerable group in society. We ignore the violence experienced by the community of the other gender because we believe that human bodies can only be either male or female.

#### Online Pornography

Online Pornography is a serious threat in the cyber space. Section 67 of the IT Act speaks indirectly about online pornography and makes the publication and distribution of obscene scenes as illegal,

---

<sup>18</sup> Mayank Bhandari, 'Gender Neutralizing of India's Stalking Laws', (June 4, 2020)

< <https://www.jurist.org/commentary/2020/06/mayank-bhandari-gender-neutral-stalking-laws/#> > accessed on 25 June 2022

<sup>19</sup> *Maneka Gandhi v. Union of India* AIR [1978] SC [597]

<sup>20</sup> Section 354D: 'Steals lips on male stalking', < <https://www.lawcommunity.in/articles/section-354d-sealed-lips-on-male-stalking> > accessed on 25 June 2022

which is slightly gender biased towards women.<sup>21</sup> Though the word, whoever in that section refers to everyone including men, but the IT Act provides maximum support to women and carefree the victims of male society.<sup>22</sup> Section 292, 293 and 354 of IPC is also gender biased and has no provisions for a male victim abused by women. Some aspects of section 354 of IPC was introduced by the Criminal Law Amendment Act, 2013 after the Nirbhaya case, which gives only about the protection of women through her web history and it silently implies that men will be the wrongdoer. There is ample need for a law that will be not only free from gender biased like men or female, but it should also be available to third genders, LGBTQ community.<sup>23</sup> The Indecent representation of women act has to be replaced with gender neutral law which provide punishment of wrongdoer irrespective of gender. Although, this research portrays less number of cases where men is victim of pornography, reason behind this that non reported cases of sexual abuse, harassment, men being blackmailed with nude photos by his fellow beings, under these circumstances, the victim is left empty handed with no legal protection. There is Section 377 of the IPC criminalizes sodomy without consent, the act comes into force only after the occurrence, women can approach police station even if she thinks eminent danger for her modesty or privacy in cyberspace, the same protection is NOT available for men.

#### Cyber Radicalisation:

A minute analysis of the Information Technology Act, 2008 would show that the language of the provisions, especially section 69 F, fails to recognize the inherent meaning of terrorism through cyber space. Vandalizing the cyber space could definitely be termed as cyber terrorism, but cyber communication carried out to vandalize the peace of civil society must not be ignored.<sup>24</sup>

The IT Act was enacted in the year 2000 with a view to give a fillip to the growth of electronic based transactions, to provide legal recognition for e-commerce and e-transactions, to facilitate e-governance, to prevent computer based crimes and ensure security practices and procedures in the context of widest possible use of information technology worldwide.

---

<sup>21</sup> Aarshi, "Pornography As Cyber Crime", < <https://www.legalserviceindia.com/legal/article-914-pornography-as-cyber-crime.html> > accessed on 27 June 2022

<sup>22</sup> Nidhi Chhillar, "Cyber Pornography" (iPleaders, July 19, 2019) < [https://blog.iplayers.in/cyber-pornography/?amp=1#Information\\_Technology\\_Act\\_2000](https://blog.iplayers.in/cyber-pornography/?amp=1#Information_Technology_Act_2000) > accessed on 27 June 2022

<sup>23</sup> Mayank Raj Maurya, "Obscenity laws in India" (iPleaders, January 05, 2021) < <https://blog.iplayers.in/obscenity-and-its-laws-in-india/?amp=1> > accessed on 27 June 2022

<sup>24</sup> P. Madhava Soma Sundaram, Syed Umarhathab, "Cyber Crime and Digital Disorder"

Section 66F of IT act only mentions about terror at that threatens the nation but does not talk about Cyber radicalisation which also impose threat to the country and individuals. Section 69 speaks about powers to issue directions for interception or monitoring or decryption of any information through any computer resource; section 69A and 69B speaks about issuing directions for blocking for public access of any information through any computer resource, and authorize to monitor and collect traffic data or information through any computer resource for Cyber Security. All these sections may signify the communicational aspect of cyber terrorism, which is missing in the definition of cyber radicalisation in section 66F. Though amended Act in 2008 had included provisions, which would protect personal data, prevent financial frauds and restrict offensive communication, the purpose of preventing extremist usage of the cyber communications was not properly satisfied.

A law meant for safeguarding electronic commerce could go to save the personal data of the individuals, but it may not successfully envelop the issues of terrorism, even though such terrorist move could disrupt the commercial transactions through cyber space and thereby cause financial loss to the nation.

The UAPA, 1967 covers the aspects of terrorism, focuses only on events that would occur during terrorist act or post terror act. Sec 15 says about any act that threatens the Nation's integrity, security. It punishes individuals for organising camps (Sec18A) and recruiting any persons for terrorist act (Sec 18B). Prevention is better than cure, the legislations failed to address the causes that leads to the crime. Radicalisation is one such cause, which enables the Indian youths to indulge in terror acts. The Cyber space has given greater advantage to terror outfits to radicalise the youths. Cyber radicalisation can happen trans-borders to any targeted citizens in India, by any terror outfits. Radicalisation is initial step to recruitment, thus it becomes necessary for the law to punish individuals who radicalise other and provide counselling to radicalised youths as a step towards de-radicalisation.

Section 121 of IPC talks about terrorism which contains main ingredients such, Accused or Attempt or Abet to wage war against the Government of India. This section, does not includes person inflicting radicalisation, punishment for forceful radicalisation. Any terrorist who are mostly arrested are charged under section UAPA act or under sec 120 and section 121 of IPC. To terminate the terrorism from our country, the law must prohibit the intending act at the beginning stage, once radicalisation is criminalised in IPC, there is chance of decrease in youths involving in terror act that will shield the

citizens from getting exposed to terror outfits. IT Act, 2008 is the only cyber law available in India, and it has to get amended for introducing a Cyber radicalisation. The modes operandi of terrorist are physical radicalisation, once which was happening by trafficking men across borders, training them and sending them back as sleeper cells threatens the Nation's security as well as youths of India are misguided from their ordinary course of life.

### **RECOMMENDATION:**

1. Section 67 of IT act, is over-used and exhausted in all online crimes against women. In fact, many crimes do not fall under the scope of the Act since offences like cyber-stalking and defamation, email-spoofing and morphing are not included in the legislation and therefore do not carry penal punishment.
2. There are no. of statutes, which rely only on the offences to women's, like Indecent Representation of Women (Prohibition Act) 1986, National Commission for Women, etc. In the same way, men should also be safeguarded under these acts (or) the government should make some adjustments in the gender specific acts like Indecent Representation of Women (Prohibition Act) to as Indecent Representation Prohibition Act, then the rule and the punishment under this act passes to every affected person whether it is men or women or children or LGBTQ25 and act as a light in the dark room.
3. Section 377 of IPC states that men who have undergone sexual abuse or any other kind of sexual violence, can find recourse under Section 377 against any gender. Section 377 is one of the few gender neutral provision that India. Taking this as an example, the laws for cyber laws should be made gender neutral, though the few gender neutral law exist, it's not known to police officials, who are the primary face of criminal justice administration system. They simply mediate the cases where women is an offender and let them free without filling any charges. The gender neutral law implementation becomes possible only when these kind of stereotype behaviour changes.
4. Men are equally responsible as the government. Only when a social evil comes into light, steps can be taken by the government to institute laws for uprooting it, but in this scenario, men are too shy to even report it. Then how can we solely blame the government for having not passed a single legislation that safeguards men. Only when men report their abusement

---

<sup>25</sup> *Navtej Singh Johar vs Union Of India* (2018) 10 SCC 1



boldly, the abuse of men in online pornography and child pornography can be controlled by the government by making legislations that can help men too.

5. Radicalisation should be designated as terrorist act under Sec.15 of UAPA act and Cyber Radicalisation shall be added to Sec.66F. A New chapter dedicated for cyber terrorism, Cyber radicalisation, and extremist speeches in the main legislation.
6. The language of Section 66F must be stretched to cover cyber communication that is carried out with intent to fulfil terrorist missions. Section 69, which speaks about power to issue for interception or monitoring or decryption of any information through any computer resource, must be included in the ambit of section 66F.
7. Sec. 121 of IPC must include the ambit of radicalisation

### **LIMITATIONS**

There are certain limitations upon this research which are as follows:

- 1) This research studies about the nature of cyber-attacks against men and response of criminal administration in India, and so the study is limited to men in certain aspects.
- 2) This study focuses on criminal administration in India. Hence, it cannot be applied universally.
- 3) This research is made through secondary data like Books, newspaper journals, articles, online journals, online articles and research papers of various authors. It lacks the genuineness of primary data and therefore lacks quantitative analysis.
- 4) The data source is too compact to find. There are only a very few data in this field of cyber-space. There are little surveys in this cyber-space field and data is difficult to find. This may also be the major limitation in this study.