GAP iNTERDISCIPLINARITIES
A Global Journal of Interdisciplinary Studies
(ISSN – 2581-5628)
Impact Factor: SJIF - 5.047, IIFS - 4.875
Globally peer-reviewed and open access journal.

A CHALLENGING ROLE OF INDIAN JUDICIARY AT CYBER SPACE TO CURB CYBER CRIME AGAINST WOMEN

Neha K Bhatt, Dr Pareshkumar D. Dobariya

Pursuing PhD in Law.

Assistant Professor, Smt. V.D. Gardi Law College, Wadhwan.

"Laws are a dead letter without courts to expound and define their true meaning and operation." ~Alexander Hamilton[1]

Abstract

The world has entered into a new millennium, but from the dawn of civilization till date, the woman of the patriarchal society of India continues to be oppressed and ill-treated.[2] Crime against women have been increasing in all fields. In the era of digital revolution women are not safe at cyber space. In India cybercrime against women have been rapidly increasing in spite of special legislations to protecting women netizen. Judiciary *played a vital* role *in the implementation of the law and its constitutional role to protecting the human rights as per the legislation. The most important duty of the court is to protect human rights, and to give relief to the victim.[3]The main object of this paper is to analyse the role of Judiciary at cyber space to curb the cybercrime against women in India. This paper is commence with cyber crime's definition and brief view about that. It also focus on kinds of cybercrime against women in India and brief view on cyber legislation.*

Key words: *Crime, Cybercrime, Digital revolution, Cyber legislation, Judiciary, women's rights.*

INTRODUCTION

Technology not only has the power to connect people, but also the power to reinforce and disseminate social and cultural structures and help normalize gender roles.[4] But it has dark side also and strongly impact on our lives as well. In 21st century Cybercrimes the new form of crimes and which are most challenging crimes to curb it. It is more challenging in India as legal awareness regarding cybercrime is very poor. Gender based violence at cyber space some like Cyber harassment, Cyber stalking, Cyber pornography, Cyber defamation, Morphing, Email Spoofing etc. have been increasing due to digital revolution. In the era of digital revolution Women and children have been softly targeted and victimised easily at cyber space.

The changing nature of the society increases the role of the adjudicatory authority in the present days. In the era of Information and technology, the criminals are using new technology to commit the crime. Therefore, appropriate judicial approach towards the technological offences is required for prevention of the crime. For the proper working of the judiciary the rules of jurisdiction plays an important role. Effective legal machinery can be identified on how properly rules and regulations are drafted by legislation and more importantly how precisely principles of jurisdiction are laid down. A court must have jurisdiction, venue and appropriate service of process in order to hear a case and render an effective judgment.[5] So Judiciary has been playing crucial role to protect the rights of women. This research paper is giving brief view about cybercrimes against women and cyber law along with the role of judiciary in today's context the new form of crimes against women at cyber space which need to be combat effectively.

[1] Available on, http://www.inspirationstation.info/1-law-quotes/law-quotes.html, accessed on 12th July 2019.
[2] Available on, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4462781/, accessed on 20th July 2019.
[3] Available on, http://www.legalserviceindia.com/legal/article-244-criminal-judiciary-reforms-in-india.html , accessed on 12th July 2019.
[4] Available on https://www.ictworks.org/gender-violence-2-0-the-digital-safety-gap-for-women/#.XTFIhH9S_cc , accessed on 19th July 2019 at 10.09am.
[5] Available on https://shodhganga.inflibnet.ac.in/bitstream/10603/203654/12/12_chapter%207.pdf, accessed on 20th July 2019 at 6.40pm.

GAP iNTERDISCIPLINARITIES
A Global Journal of Interdisciplinary Studies
(ISSN – 2581-5628)
Impact Factor: SJIF - 5.047, IIFS - 4.875
Globally peer-reviewed and open access journal.

DEFINITION OF CYBER CRIME

There are so many definition which given by different author. In common parlance **Cybercrime** or **Computer-oriented crime**," is a crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target".[6]

The Council of Europe Convention on Cybercrime, to which the United States is a signatory, defines "Cybercrime as a wide range of malicious activities, including the illegal interception of data, system interferences that compromise network integrity and availability, and copyright infringements. Other forms of cybercrime include illegal gambling, the sale of illegal items, like weapons, drugs or counterfeit goods, as well as the solicitation, production, possession or distribution of child pornography".[7]

According to Debrati Halder and K.Jaishankar Cybercrimes can be defined as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS)".[8]

There are also problems of privacy_when confidential_information is intercepted or disclosed, lawfully or otherwise. **Debarati Halder and** K. Jaishankar_further define **Cybercrime** from the perspective of gender and defined 'cybercrime against women' as "Crimes targeted against women with a motive to intentionally harm the victim psychologically and physically, using modern telecommunication networks such as internet and mobile phones".[9] So as per the common understanding cybercrime is such crime that involved "Computer" and "Network".

"Cyber Crime" has not been clearly defined in India's any statute and not even in Information Technology Act 2000. That is the main lacuna of Information Technology act 2000. However in general the term cybercrime means any illegal activity which is carried over or with the help of internet or computers.[10]

CLASSIFICATION OF CYBER-CRIME AGAINST WOMEN

Crimes are classified as "crimes against the human body"," crimes against property " and "crimes against the nation". Cybercrime, like traditional crime, can be broadly classified in to three categories namely "Cybercrime against persons"," Cybercrime against properties" and "Cybercrime against the nations". Cybercrime against person include Internet grooming, Stalking, Harassment, Extortion, Paedophilia, Facebook stalking, Internet troll, Pyramid scheme fraud, Credit card fraud etc. Cybercrime against property include Illegal Access-Hacking and Cracking, Illegal Data Acquisition- Data Espionage, Illegal Interception, Data Interference, System interference, Copyright and Trademark- related offences and Computer-related offences etc. Cybercrime against Nation like Cyber terrorism, Cyber warfare, Cyber laundering etc.[11]

Women especially young girls inexperienced in cyber world, who have been newly introduced to the internet and fail to understand the vices of internet, and hence are most susceptible to falling into the bait of cyber criminals, cybercrimes and cyber bullying are various types. [12] Generally major Cybercrime against women in India are:

1. **Cyberstalking**: Cyberstalking is the use of the Internet or other electronic means to stalk or harass an individual, group, or organization. It may include false accusations, defamation, slander and libel. It may also include monitoring, identity theft, threats, vandalism, solicitation for sex, or gathering information that may be used to threaten, embarrass or harass. Cyberstalking is often accompanied by real time or offline stalking. A stalker may be an online stranger or a person whom the target knows. They may be anonymous and solicit involvement of other people online who do not even know the target.[13]
2. **Cyber Harassment**: Cyber Harassment is characteristic repetitive behaviour intended to disturb or up rest a person though use of internet. A particular class of harassment which is sexual in nature is known as sexual harassment, among several other things it majorly includes persistent and unwanted sexual

[6]Cybercrime, https://en.wikipedia.org/wiki/Cybercrime, accessed on 9th August, 2019 at 6.03pm.
[7]Cybercrime, https://searchsecurity.techtarget.com/definition/cybercrime, accessed on 10th August, 2019 at 2.12pm.
[8]Cyber-crime, https://searchsecurity.techtarget.com/definition/cybercrime, accessed on 10th August 2019 at 5.39pm.
[9] Cyber-crime, https://searchsecurity.techtarget.com/definition/cybercrime, accessed on 10th August 2019 at 5.41pm.
[10] Available on, https://shodhganga.inflibnet.ac.in/bitstream/10603/130487/8/08_chapter%202.pdf, accessed on 4th September 2019 at 05.10pm.
[11] Dejey and S. Murugan IPS, Cyber Forensics, 2018, Oxford University Press, p 47-53.
[12] Misra, Rajat, Cyber Crime against Women (April 10, 2013). Available at SSRN: https://ssrn.com/abstract=2486125 or http://dx.doi.org/10.2139/ssrn.2486125 .
[13] Cyberstalking, https://en.wikipedia.org/wiki/Cyberstalking, accessed on 6th September, 2019 at 4.16pm.

advancement. Under Indian law Sexual harassment has newly been defined under this Criminal Law Amendment (Bill) 2013.[14]

3. **Defamation**: The term defamation is used to define the injury that is caused to the reputation of a person in the eyes of a third person. The injury can be done by words oral or written, or by signs or by visible representations. The intention of the person making the defamatory statement must be to lower the reputation of the person against whom the statement has been made in the eyes of the general public.
   Cyber defamation is a new concept but the traditional definition of the term defamation is application to the cyber defamation as it involves defamation of a person through a new and a virtual medium. "Cyber defamation is publishing of defamatory material against another person with the help of computers or internet."[15]Generally Cyber defamation which has been done by the Internet or Computers. Person's intentions to defame the other person's image or personality through any statements or comments by Computer or Digital media or Internet. The harm caused to a person by publishing a defamatory statement about him on a website is widespread and irreparable as the information is available to the entire world.[16]Penalties for "cyber defamation" vary from country to country, but the fundamental rights covered in the UN Declaration of Human Rights and European Union Fundamental Human Rights.[17]
4. **Morphing**: Morphing is a special effect in motion pictures and animations that changes (or morphs) one image or shape into another through a seamless transition.[18] In this digital era Morphing is also rapidly increasing and women are softly targeted. Internet users can easily download the women pictures from the Facebook, WhatsApp and Instagram. Within few second they can edited pictures and easily able to upload pictures on social media to intent to damage the image of women. So it is also one of the threat to women netigen at cyber space. **Air Force Balbharti School Case (Delhi)** is Morphing's case. This kind of act can be penalised under Sec. 43 and Sec. 66 of the IT Act 2000. This act also can be punishable under Sec. 509 of IPC.
5. **Cyber pornography**: *Violence against Women in Pornography* illuminates the ways in which adult pornography hurts many women, both on and off screen. A growing body of social scientific knowledge shows that it is strongly associated with various types of violence against women in intimate relationships. Many women who try to leave abusive and/or patriarchal men also report that pornography plays a role in the abuse inflicted on them by their ex-partners.[19] In Mumbai, a Swiss couple gathered slum children and then forced them to appear for obscene photographs, which they took and then uploaded those photographs to websites specially designed for pedophiles. The Mumbai police arrested the couples for pornography.[20]
6. **Cyber flirting**: Generally cyber flirting may be considered very minimal petty offence that starts when perpetrator force the victim to hear obscene songs, messages and it may consequently result in cyber sexual defamation and breach of thrust. Again this can be treated as the flip side of IT Act that except Section 72 which deals with the breach of confidentiality and privacy there is no other support that can be offered by the Act to the victim. [21]
7. **Email Spoofing**: E-mail spoofing is a term used to describe fraudulent email activity in which the sender address and other parts of the email header are altered to appear as though the email originated from a different source; it is done by properties of the email, such as the From, Return-Path and Reply-To fields, ill-intentioned users can make the email appear to be from someone other than the actual sender.[22] Criminals at cyber space taking personal information and images from women are used to blackmail those women. Gujarat Abuja's Executive case is very famous cyber spoofing's case.

---

[14] Misra, Rajat, Cyber Crime Against Women (April 10, 2013). Available at SSRN: https://ssrn.com/abstract=2486125 or http://dx.doi.org/10.2139/ssrn.2486125
[15] Cyber defamation in India, http://www.helplinelaw.com/employment-criminal-and-labour/CDII/cyber-defamation-in-india.html on 12th September 2019 at 6.33pm.
[16] Cyber defamation in India, http://www.helplinelaw.com/employment-criminal-and-labour/CDII/cyber-defamation-in-india.html on 12th September 2019 at 6.52pm.
[17] Cyber Defamation Law, https://en.wikipedia.org/wiki/Cyber_defamation_law,accessed on 12th September 2019 at 5.41pm.
[18] Morphing, https://en.wikipedia.org/wiki/Morphing, accessed on 16th September Now2019 at 4.38pm.
[19] Violence against women in Pornography, https://www.taylorfrancis.com/books/9781315652559, accessed on 16th September, 2019 at 6.42pm.
[20]Shobhna Jeet(2012), Cybercrimes against women in India: Information Technology Act, 2000, https://www.elixirpublishers.com/articles/1351168842_47%20(2012)%208891-8895.pdf, accessed on 9th October 2019 at 06:57pm.
[21] Shobhna Jeet(2012), Cybercrimes against women in India: Information Technology Act, 2000, https://www.elixirpublishers.com/articles/1351168842_47%20(2012)%208891-8895.pdf, accessed on 9th October 2019 at 07:05pm.
[22] Misra, Rajat, Cyber Crime against Women (April 10, 2013). Available at SSRN: https://ssrn.com/abstract=2486125 or http://dx.doi.org/10.2139/ssrn.2486125 accessed on 17th September,2019 at 3.32pm.

GAP iNTERDISCIPLINARITIES
A Global Journal of Interdisciplinary Studies
(ISSN – 2581-5628)
Impact Factor: SJIF - 5.047, IIFS - 4.875
Globally peer-reviewed and open access journal.

8. **Trolling**: Trolling is also one of the threat against women netizen at cyber space. Trolls spreads conflict on the Internet, criminal starts quarrelling or upsetting victim by posting inflammatory or off-topic messages in an online community with the intention to provoke victims into an emotional, upsetting response. Trolls are professional abusers who, by creating and using fake IDs on social media, create a cold war atmosphere on the cyber space and are not even easy to trace.[23]
9. **Hacking**: Hacking means unauthorized access to computer system or network, and it is the most predominant form of cybercrime. It is an invasion into the privacy of data, it mostly happens in a social online community to demean a woman by changing her whole profile into an obscene, derogatory one. The reasons vary from personal hatred, revengeful mind to even just for fun. Even though some social networking communities like Orkut, Facebook have the option of reporting profiles as bogus, Photo-Video lock, special tools for reporting, still, many women are kept in dark, when their email IDs or even websites are hacked.[24]
10. **Cyber Bullying**: To define bullying the most acceptable definition of cyber bullying which has been used is "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 cannot easily defend him or herself." There have been variations to this definition explaining meaning of bullying but cybercrime experts has accepted this definition. Place of occurrence of cyber bullying are Social Media (Facebook, Instagram, Snapchat, Twitter, etc.), SMS (text messages from the cellular network), Instant Message Services (WhatsApp, Facebook messenger, I message, etc.), Email etc. There is no specific legislation which provides for the specific cyber bullying laws in India however provisions such as Section 67 of the Information Technology Act deals with cyber bullying in a way. Other than Section 67 and Section 66 E of the IT Act following are the provisions of the cyber bullying laws in India that Indian penal code's Section 354A, Section 354D, Section 507, Section 509 and POSCO act etc..[25]

CYBER LEGISLATION IN INDIA

Cybercrime against women is on at alarming stage and it may pose as a major threat to the security of a person as a whole. In India the term "Cybercrime against women" includes sexual crimes and sexual abuses on the internet. In 1996 the United Nations Commission on International Trade Law has adopted the model law on E-commerce. India is considered as one of the very few countries to enact IT Act 2000 to combat cybercrimes. This Act widely covers the commercial and economic crimes which is clear from the preamble of the IT Act.[26] The act deal with legal recognition of electronic documents and digital signatures, Offenses and contraventions and justice Dispensation Systems for cybercrime. Because of some loopholes in the IT Act, the investigation still relied on the Indian Penal Code, 1860 even in technology based cases. Hence, after careful discussion with various advisory groups and bodies, the amendment act came in force on 27th October, 2009. A major amendment was made in 2008. It introduced Section 66A which penalized sending of "offensive messages".[27] Sections 66A to 66F has been added to section 66 prescribing punishment for offences such as obscene electronic message transmissions, identity theft, cheating by impersonation using computer resource, violation of privacy and cyber terrorism. Section 67 of the IT act 2000 has been amended to reduce the term of imprisonment for publishing or transmitting obscene material in electronic form three years from five years and increase the fine thereof from rupees 100,000/- to rupees 500,000/-. [28]It also introduced Section 69, which gave authorities the power of "interception or monitoring or decryption of any information through any computer resource". It also introduced provisions addressing child porn, cyber terrorism and voyeurism.[29]

[23] Cyber Crimes against Women and Laws in India, https://www.livelaw.in/cyber-crimes-against-women-and-laws-in-india/, accessed on 18th September 2019 at 6.49pm.
[24]https://www.elixirpublishers.com/articles/1351168842_47%20(2012)%208891-8895.pdf, accessed on 9th October 2019 at 06:54 pm.
[25] Mehak Sharma, What is Cyber Bullying or Anti-Bullying Laws in India (29th September 2019), **https://www.myadvo.in/blog/must-read-what-is-cyber-bullying-or-anti-bullying-laws-in-india/**, accessed on 11th October 2019 at 05:22pm.
[26]Cybercrimes against women in India: Information Technology Act, 2000, https://www.elixirpublishers.com/articles/1351168842_47%20(2012)%208891-8895.pdf, accessed on 6th September, 2019 at 1.30pm.
[27] Information Technology Act 2000, https://en.wikipedia.org/wiki/Information_Technology_Act,_2000, accessed on 25th September, 2019 at 3.42pm.
[28] Garima Tiwari, Understanding Laws: Cyber Laws and Cyber Crimes, 1st Edition, 2014 ISBN: 978-93-5143-163-3 pp-11.
[29] Information Technology Act 2000, https://en.wikipedia.org/wiki/Information_Technology_Act,_2000, accessed on 25th September, 2019 at 3.43pm.

GAP iNTERDISCIPLINARITIES
A Global Journal of Interdisciplinary Studies
(ISSN – 2581-5628)
Impact Factor: SJIF - 5.047, IIFS - 4.875
Globally peer-reviewed and open access journal.

MEASURES BY GOVT. OF INDIA

On 23.07.2014, National Commission for Women has submitted a report on "Ways and Means to Safeguard Women from Cyber Crimes in India" which inter-alia recommended for stringent law, Policy to discourage hacking activities, dedicated helpline numbers, opening of more cyber cells, and imparting of proper legal, setting up forensic labs and technical training law enforcement agencies like police& judiciary etc. to combat cybercrime. The Information Technology Act, 2000 together with Indian Penal Code have adequate provisions to deal with prevailing Cyber Crimes. It provides punishment in the form of imprisonment ranging from two years to life imprisonment and fine / penalty depending on the type of Cyber Crime. However, Government has taken a number of legal, technical and administrative measures to prevent incidents of cybercrimes.

1. Cyber Police Stations and Cyber Crime Cells have been set up in each State for reporting and investigation of Cyber Crime cases.
2. Ministry of Electronics & Information Technology (Meity) has setup Cyber Forensics Training Labs in north-eastern States and cities such as Mumbai, Pune, Kolkata and Bangalore to train State police officials and judiciary in cybercrime detection and collection, preservation and seizing of electronic evidence and dealing with cybercrime.
3. Various steps have been taken by Ministry of Home Affairs, Meity and State Government to modernise the setup and equip police personnel with knowledge and skills for prevention and control of cybercrime through various national and State Police academies/judicial academies and other institutes.
4. Ministry of Electronics & Information Technology has issued an advisory on functioning of Matrimonial website on 6thJune, 2016 under Information Technology Act, 2000 and Rules made thereunder directing the matrimonial websites to adopt safeguards to ensure that people using these websites are not deceived through the means of fake profiles or misuse/wrong information posted on the website.
5. The Government has circulated Computer Security Policy and Guidelines to all the Ministries/Departments on taking steps to prevent, detect and mitigate cyber-attacks.
6. A portal namely www.cybercrime.gov.in has been developed by Ministry of Home Affairs to allow public to report cybercrime complaints.[30]

So above mention steps have been taken by Indian government to curb the rapidly increasing cybercrime against women in India. India has also a National Cyber Security Policy, 2013 which provides the legal basis for promoting the cause of cyber security in India. It will cater to the cyber security requirements of government entities at the national and international levels. The policy will help in safeguarding the critical infrastructure like Air Defence system, nuclear plants, banking system, power infrastructure, telecommunication system and many more to secure country's security.[31]

ROLE OF JUDICIARY AT CYBER SPACE

In every legal system, which accepts the democratic form of government, the Judiciary plays an important role. It is most important wing of the government, which resolves the conflicts among the parties. For the development of the society, the smooth and powerful adjudicative authority is required. The changing nature of the society increases the role of the adjudicatory authority in the present days. In the era of Information and technology, the criminals are using new technology to commit the crime. Therefore, appropriate judicial approach towards the technological offences is required for prevention of the crime. For the proper working of the judiciary the rules of jurisdiction plays an important role. The main problem that is going to face in case of cybercrime is concern with the jurisdiction.[32] In India judiciary is an independent machinery. It has been playing very effective role in all laws. However the basic problem arise when the offences are of that nature which require the technical knowledge to understand the nature of the act whether it is an offence or not. Due to this nature of cybercrime, the legal system is facing various problems. The laws are insufficient but the policy and the operative system facing the difficulty of lack of knowledge. In case of judicial perspective, the basic question arising regarding the jurisdiction. The conventional law as like Indian Penal Code and the procedural law that Code of Criminal Procedure has provide provisions regarding the territorial and extra territorial

[30] Laws to Safeguard Women against Cyber Crimes in India, **https://legaldesire.com/laws-to-safeguard-women-against-cyber-crime-in-india/**, accessed on 20th September 2019 at 11.04pm.
[31] Garima Tiwari (2014), Understanding Laws: Cyber Laws and Cyber Crimes, 1st Edition, 2014, pp 13-14.
[32]ROLE OF JUDICIARY IN REGARD TO THE LAW RELATING TO CYBER CRIME https://shodhganga.inflibnet.ac.in/bitstream/10603/203654/12/12_chapter%207.pdf, accessed on 4th October 2019 at 11.03pm.

GAP iNTERDISCIPLINARITIES
A Global Journal of Interdisciplinary Studies
(ISSN – 2581-5628)
Impact Factor: SJIF - 5.047, IIFS - 4.875
Globally peer-reviewed and open access journal.

jurisdiction, but the basic nature of the cybercrime somewhere require something more than the provided rules therefore some reformations are required.[33]

1. **State of Tamil Nadu vs. Suhas Kutti**, It was the first conviction case under the Information technology Act, 2000. Indian court firstly convicted for the offence of cybercrime. The judgment was pronounced in the year 2004, within the seven month after filling the FIR, which brings the conviction for the cybercrime. The Honourable Judge of the Additional Chief Metropolitan Magistrate has passed the order of conviction. In this case, the victim was a divorcee who constantly harassed by annoying phone calls presuming that she would solicit them because of a massage posted on yahoo message group followed by forwarding emails. The massage was extremely obscene, defamatory and annoying. The accuse turn out to be her family friend and interesting in marrying her. The accused held guilty of offences under Section 469, 509 IPC and 67 of IT Act 2000. The accused had convicted and sentenced for the offence to undergo RI for 2 years. Under section 469 IPC to pay fine of Rs.500/-and, for the offence u/s 509 IPC sentenced to undergo 1 year Simple imprisonment and to pay fine of Rs.500/-, and for the offence u/s 67 of IT Act 2000 to undergo rigorous imprisonment for 2 years and to pay fine of Rs.4000/- All sentences to run concurrently.[34]
2. **Ritu kohli's case,** in 2001 first time cyber stalking's case had been reported in India. Manish Kathuria was stalking an Indian lady, Ms. Ritu Kohli by illegally chatting on the web site, www.mirc.com using her name; and used obscene and obnoxious language, and distributed her residence telephone number, invited people to chat with her on the phone. As a result, Ms. Ritu Kohli was getting obscene calls from various states of India and abroad, and people were talking dirty with her. In a state of shock, she called the Delhi police and reported the matter. The police registered her case under Section 509 of the Indian Penal Code, 1860 for outraging the modesty of Ritu Kohli. But Section 509 refers only to a word, a gesture or an act intended to insult modesty of a woman. But when same things are done on Internet, then there is no mention about it in the said section. This case caused alarm to the Indian government, for the need to amend laws regarding the aforesaid crime and regarding protection of victims under the same. So in 2008 Indian legislature has amended the IT Act 2000 and made provisions for cyber stalking. The IT Act, 2008 does not directly address stalking. But the problem is dealt more as an 'intrusion on to the privacy of individual' than as regular cyber offences which are discussed in the IT Act, 2008. Hence the most used provision for regulating cyberstalking in India is Section 72 of the IT Act, 2008[35]
3. **Avinash Bajaj vs. State (N.C.T) of Delhi,** the famous Bazee.com case, the CEO Avinash Bajaj was arrested for an advertisement by a user to sell the DPS sex scandal video. The video was not uploaded on the portal, despite that Avinashwas arrested under Section 67 of the Information Technology Act.It was subsequent to this case that the Intermediary guidelines were passed in 2011 whereby an Intermediary's liability would be absolved if they exercised due diligence to ensure obscene content is not displayed on their portal.[36] The court granted bail to Mr. Bajaj subject to furnishing two sureties of Rs.1 lakh each. The court ordered Mr. Bajaj to surrender his passport and not to leave India without the permission of the court. Court also ordered Mr. Bajaj to participate and assist in the investigation.[37]
4. **Fatima Riswana v. State Rep. by ACP., Chennai & Ors AIR 2005 712,** both the public prosecutor and counsel for the petitioners applied to the court for transfer to another (male) judge, to save the district lady judge from embarrassment of having to view certain CDs that are part of the evidence. The order for transfer was passed and the justification for this was that the "said trial would be about the exploitation of women and their use in sexual escapades by the accused, and the evidence in the case is in the form of CDs. and viewing of which would be necessary in the course of the trial, therefore, for a woman Presiding Officer it would cause embarrassment[38].
5. **Shreya Singhal vs. Union of India, criminal no 167 of 2012**, in this case, S.66A of the Information Technology Act 2000 (inserted vide amendment in 2008) was struck down by the Supreme Court as

[33] ROLE OF JUDICIARY IN REGARD TO THE LAW RELATING TO CYBER CRIME https://shodhganga.inflibnet.ac.in/bitstream/10603/203654/12/12_chapter%207.pdf, accessed on 4th October 2019 at 11:15pm.

[34] ROLE OF JUDICIARY IN REGARD TO THE LAW RELATING TO CYBER CRIME, https://shodhganga.inflibnet.ac.in/bitstream/10603/203654/12/12_chapter%207.pdf, accessed on 4th October 2019 at 11:27pm

[35]Dr. Sapna Sukrut Deo,sssCYBERSTALKING AND ONLINE HARASSMENT: A NEW CHALLENGE FOR LAW ENFORCEMENT, http://docs.manupatra.in/newsline/articles/Upload/FDF5EB3E-2BB1-44BB-8F1D-9CA06D965AA9.pdf, accessed on 5th October 2019 at 01:21pm.

[36] V.M. Eshwar,Aswathy Rajan, A Critical Analysis on Judicial Activism in Relation to Cyber Law-An Indian Perspective, https://acadpubl.eu/hub/2018-119-17/2/123.pdf, accessed on 5th October 2019 at 01:42 pm.

[37] Garima Tiwari (2014), Understanding Laws: Cyber Laws and Cyber Crimes, 1st Edition, 2014, pp 135.

[38] Nidhi Arya "Cyber Crime Scenario in India and Judicial Response" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 |Issue-4, June 2019,pp.1108-1112, URL:https://www.ijtsrd.com/papers/ijtsrd24 025.pdf

'unconstitutional.' The court took this historic decision after the petition alleged that the said provision is extremely vague and it is being misused grossly for curtailing freedom of speech in the cyber space in India. But while it is accepted that the provision may be a draconian law, could the Supreme court use this opportunity to re-frame and reproduce the provision for regulating certain types of speech which may be termed as 'bad talk' in the internet? It may be noted that in India cyber bullying and trolling, online gender harassment, smishing and vishing are becoming rampant. The court could have considered the Therapeutic Jurisprudential value of S.66A to recreate a better law.[39]

6. **State vs. Ts. Balan and Aneesh Balan**, the Additional District Court and Sessions Court here was upheld a lower court's verdict in the first cyber case **State vs. Ts. Balan and Aneesh Balan**filed in the State sentencing a Pentecostal Church priest and his son to rigorous imprisonment in 2006.Disposing of the appeal filed by the priest T.S. Balan and his son, Aneesh Balan, against the order of the Chief Judicial Magistrate. Additional District Judge T.U. Mathewkutty said it was time the government took effective measures to e court check the growing trend of cybercrimes in the state. The court upheld the magistrate's order sentencing the two to three-year rigorous imprisonments and imposing a fine of Rs/- 25,000 under section 67 of the Information Technology Act; awarding six months rigorous imprisonment under section 120(B) of the Indian Penal Code; and ordering one year rigorous imprisonment and imposing a fine of Rs/- 10,000 under section 469 of the code. The court revoked the sentence under Section 66 of the IT Act. Cyber case dates back to January-February 2002 and the priest and his son became the first to be convicted of committing a cybercrime. The two were found guilty of morphing, web-hosting and e-mailing nude pictures of Pastor Abraham and his family. Balan had worked with the pastor until he fell out with him and was shown the door by the latter. Balan joined the Sharon Pentecoastal later. The prosecution said the duo had morphed photographs of Abraham, his son, Valsan Abraham, and daughter, Starla Luke, and e-mailed them from fake mail IDs with captions.The morphed pictures were put on the web and the accused, who edited a local magazine called The Defender', wrote about these photos in his publication.Valsan received the pictures on the Internet and asked his father to file a complaint to the police. A police party raided the house of Balan and his son at Perumbavoor and collected evidences. The magistrate's verdict came after a four-year trial, for which the court had to procure a computer with Internet connection and accessories. The police had to secure the services of a computer analyst too to piece together the evidence. Twenty-nine witnesses, including the internet service provider and Bharat Sanchar Nigam ltd., had to depose before the court.[40]
7. Sreekanth C.Nair vs Licensee/Developer (2008):
   A student of ASCL, came across the website "www.incometaxpune.com", and on visiting the said site, the complainant was taken to a pornographic site and move the court for blocking order against the website. The court ordered that only when the authorities enumerated under Clauses (i) to (vii) when moved were either not inclined or had refused to prefer a complaint to the Director, CERT-In, then the court could be moved for a direction to the officer concerned.[41] The DPS MMS scandal is also very famous school girl case. In this case offender made compromising video clip and air on internet. One more famous Swiss couple gathered slum children case, at Mumbai, in that case couple used children for pornography. Mumbai police detained couple for pornography.
8. A **PIL** filed based on a letter from an NGO named **Prajwala** dated 18.02.2015, the Hon'ble Supreme Court's **Suo moto**, in order to curb circulation of child pornography, rape, gang rape videos on the Internet through social media websites, had directed the central government to create an online portal and hotline number where anonymous complaints can be filed against those responsible for uploading such offensive videos. When the matter came up for hearing on 18.05.2018, a status report was filed by the ASG that the Cyber Crime reporting portal is in its final form and shall be launched on or before July 15, 2018. Further, the Hon'ble Supreme Court had also sought from the parties before it, i.e., Yahoo, Facebook Ireland, Facebook India, Google India, Google Inc., Microsoft, and WhatsApp, to give a report on the recommendations of the Ajith Kumar Committee on measures taken to stop the uploading and sharing of such videos on the Internet, and since the entities had not furnished any affidavit detailing the same, they were fined `1,00,000/- (Rupees One Lakh) each for their apathy in not complying with the directions of the Hon'ble Supreme Court.[42]

[39] Halder Debarati, A Retrospective Analysis of S.66a: Could S.66a of the Information Technology Act Be Reconsidered for Regulating 'Bad Talk' in the Internet? (August 1, 2015). Indian Student Law Review (ISLR), Vol. 3, pp. 91-118, 2015. Available at SSRN: https://ssrn.com/abstract=2687381 , accessed on 7th October 2019 at 07:31pm.
[40]https://shodhganga.inflibnet.ac.in/bitstream/10603/120167/7/chapter%205.pdf,accessed on 7th October 2019 at 08:01pm.
[41] Information Technology, https://www.itlaw.in/judgements/, accessed on 10th October 2019 at 06:35pm.
[42]**Shweta Krishnappa, Cyber-Bullying And The Related Laws In India (5th July 2018),** http://www.legaleraonline.com/articles/cyber-bullying-and-the-related-laws-in-india, accessed on 11th October 2019 at 05:43 pm.

9. In her **Facebook post, Dhada** had lamented the on 18th November 2012 shutdown due to. Shrinivasan had 'liked' the post. Both were arrested by the police on 19th November 2012 on a complaint lodged by a local Sena leader. They were produced before a court in Palghar, which granted them bail. They were booked under IPC's Section 295 (A) deliberate and malicious acts, intended to outrage religious feelings or any class by insulting its religion or religious beliefs), Section 505(2) (statements creating or promoting enmity, hatred or ill-will between classes) and also IT Act. A closure report is usually filed in the court when investigators conclude that no case is made out against the accused. [43]
10. **SMC Pneumatics (India) Pvt. Ltd vs. Jogesh Kawatra[44]**, in this case company's employee sent defamatory and obscene e-mails about its Managing Director. Frequently they sent anonymous e- mails and also sent to many of their business associates to damage their image and goodwill of the plaintiff company. The plaintiff was able to identify the defendant with the help of a private computer expert and moved the Delhi High Court. The court granted an ad- interim injunction and restrained the employee from sending, publishing and transmitting e- mails, which are defamatory or derogatory to the plaintiffs.

CHALLENGES FACED BY INDIAN JUDICIARY AT CYBER SPACE

At Cyber space Indian Judiciary faced number of challenges due to traditional criminal justice system. I have reviewed key challenges that faced by Indian Judges to curbing Cybercrime against women are as follow:

1. Digital Evidentiary Challenges: The main challenge is in computer crime mostly all evidence in digital form. It has been very complicated for investigators to find, preserve digital evidence and also difficult for judges and lawyer to address court. S.65 (B) of the Indian Evidence Act is also create problems in the case of Foreign Service provider sharing evidence. As foreign company generally do not provide certificate, due to that Court has to reject evidence so Indian legislature has to take cognizance and has to made necessary amendment in the said section as per necessities of the digital era.
2. Traditional way of investigation: which is failed in cybercrime. Due to increasing use of ICT, need the new investigations instruments. So for that special technological knowledge and skill should be required in investigation, prosecution and conducting cybercrime trial.
3. Jurisdiction: To decide Jurisdiction is also main challenging point for judiciary while deal the cyber offences. Cybercrime basically borderless crimes. In such kind of specific crime to decide jurisdiction is very complicated issue for the criminal justice system. United nation has also identified jurisdiction in cybercrime as major challenge. Even Indian government has also acknowledged that to decide jurisdiction in cyber offences as major challenge for Judiciary. In this kind of matter Supreme Court has directed to the government to create common portal for reporting cybercrime.
4. No specific Legal Provision: for the protection of individual rights at cyberspace. IT Act 2000 give general protection to the women victim at cyberspace. In 2008 Indian law makers has amended IT Act 2000 but still new form of cybercrime still not covered. Which also create problems in cyber trial for judiciary. Criminal justice has taken cognizance in while drafting national policy and directed the Indian legislature to reclassification of the existed cyber code.
5. Operational challenges: As per the Sec.78 of the IT Act 2000 only inspector rank police officer do investigation in cyber offences. This section has created major challenge at practical level and indirectly affecting in judicial process. Which increasing pendency of court cases and create hurdles in speedy trials. Apart from that non-cooperation from service provider is also major challenge as state has not had control over the Internet.
6. Paucity of technical tools and skilled human resources: Judiciary face the root cause problem due to lack of technical tools, shortage of technical skilled manpower and infrastructure which increase hurdles in court proceedings. In 2017 Indian parliament has also rectified the problem of training of human resources who deal with cybercrime and also suggested nodal agency for cybercrime.
7. Gap between Technology and Knowledge: There is gap between developing technology and traditional knowledge for new emerged cybercrime with the traditional criminal justice system. There are no settled legal procedure standards for dealing new form of cyber offences and no legal specific provisions for specific crime. So during cyber trial judges faced lots of problems in trial and to deliver the judgment.

CONCLUSION

In India Judiciary is playing crucial role in the protection and safety and right of the women at cyberspace. Indian Judiciary has been trying to fill up the loopholes of Information Technology Act 2000. In so many cases

[43]https://www.livemint.com/ accessed on 11th October 2019 at 07:40 pm.
[44]Misra, Rajat, Cyber Crime against Women (April 10, 2013). Available at SSRN: https://ssrn.com/abstract=2486125 or http://dx.doi.org/10.2139/ssrn.2486125 accessed on 15th October 2019 at 04:03pm.

GAP iNTERDISCIPLINARITIES
A Global Journal of Interdisciplinary Studies
(ISSN – 2581-5628)
Impact Factor: SJIF - 5.047, IIFS - 4.875
Globally peer-reviewed and open access journal.

judiciary has protected the right of women at cyberspace. But in changing scenario various kind of new developments at cyberspace lead to different kinds of cybercrimes and which are unnoticed. So in India needed such cyber savvy judges who can easily handle and fairly justified cybercrimes. Apart from that social awareness and advancement regarding individual's cyber rights is very poor, which need of the time to create awareness among society. So all the Constitutional machinery has to try their level best for the social awareness regarding cybercrimes and to take measurements to curbing the cyber issues and cybercrimes.