



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

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.

WHITE BLACK
LEGAL

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 diploma in Public

a professional 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

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

CYBERBULLYING AND ONLINE HARASSMENT LAWS PROTECTING INDIVIDUALS

AUTHOR - DIKSHA NAUTIYAL
CO-AUTHOR - UJJWAL KUMAR SINGH
LAW COLLEGE DEHRADUN, UTTARANCHAL UNIVERSITY

ABSTRACT- In this article I want to highlight the concept of cyberbullying and online harassment. It is becoming a common crime nowadays, in today's world technology is changing with the needs of society. So cyberbullying and online harassment are taking place each time. The individual harms the dignity of other people through cyberbullying and online harassment. Most people are not aware of cyberbullying and online harassment the victim's mental state is affected and some victims are committing suicide because of this crime. These crimes are getting worse and dangerous all over the world.

KEYWORDS

Cybercrime, Cyberbullying, online harassment, Victim's mental health

INTRODUCTION

In today's world, the speed of technology is increasing with the high rate of changing the needs of society. The internet is present in every sector of our life. But some people use the internet for a wrongful purpose which harms others somehow. The wrongful actions which are prohibited by law include spreading rumours, making fake profiles posting vulgar messages or threatening messages, or threats to child pornography these all come under the category of Cyberbullying. The concept of cyberbullying means harassing or insulting any person through various platforms which are used for communication. Further, the category of cybercrime is divided into various parts such as Cyberstalking, Cyberbullying, Cyber Pornography, Cyber defamation, Online harassment etc. There are so many illegal activities which are committed with the help of the internet by technically skilled criminals. While taking into wider interpretation the cybercrime takes place on the digital platform only.

MEANING OF BULLYING

Bullying is an act which hurts the person physically while on the other hand, cyberbullying takes place only on the digital platform. The term cyberbullying was first coined by Bill Belsey. Cyberbullying is an act where the individual harms the reputation of another person. This can also lead to emotional damage to the victim. Some examples which are very common for cyber bullying

EXAMPLES OF CYBERBULLYING

1. Posting rude comments or rumours which spoil the reputation of the individual
2. Sending or posting vulgar messages
3. Making a fake profile in the name of the victim
4. Making sexually coloured remarks or disclosing private information regarding causing damage to other people.
5. Posting a mean or hurtful picture or video.

Cyberbullying may take place in different groups from one side or another while using digital platforms:

1. The wrongful content is posted online about the victim so that the dignity of the victim hurts.
2. To threaten somebody so that they commit an act of violence.
3. Posting vulgar messages about the victim.

TYPES OF CYBERBULLYING

1. Flaming – Flaming is the type of cyberbullying which includes sending offensive or hurtful texts. Sending vulgar and abusive words which are aggressive. It includes insults and words full of anger. It is important to note that those who engage in flaming use capital letters, images and symbols to add emotion to their argument. Flaming is a dangerous type of behaviour that can lead to serious problems. The perpetrator does the act only with the intent to harm the victim.

2. Harassment – It is the type of cyberbullying, where a person receives threatening or vulgar messages. The messages that are sent to the victim usually follow a pattern with the intent to hurt the dignity of the victim. The perpetrator used only a digital platform to perform this act.

3. Cyberstalking – Cyberstalking is a heinous offence where the victim receives threatening messages. It also includes physical threats to victims. The victim is monitored online by the perpetrator. Cyberstalking is defined under section 354D of the Indian Penal Code, 1860.

4. Outing / Doxing – The term doxing means the act of disclosing personal information without the consent of the person. This can also be extended by spreading personal pictures or videos.

5. Masquerading – Masquerading is an act where the bully creates a fake or unreal identity or profile. The main purpose of the perpetrator is to cause harm to the victim so that the dignity of the victim is spoiled. The bully is done with the intent to harm that person.

THE LEGAL FRAMEWORK

The Internet has many unique qualities. Firstly, it leads to physical/geographical barriers. And therefore the person acting from any part of the world and the internet extends anonymity to the users. It is a comforting feature of many people who use the internet for good faith and on the other hand some people use the internet for wrongful purposes. Two major laws address cybercrime. The Indian Penal Code, 1860 and the Information Technology Act, 2000. The Indian Penal Code defines cyberstalking which is defined in Section 354D. The Information and Technology Act defines punishment which is defined under Section 66 A, Section 66C, Section 66 D, Section 66E and Section 67A, Section 67B.

Sections 67, 67A and 67B these sections are related to the publishing of information which is obscene in electronic form.

Section 66 A This section deals with the punishment for the offence of sending abusive, hurtful messages or any material online through the internet on any social media or any other digital

platform.

Section 66 E This section deals with the punishment for infringement of privacy, if a person violates the privacy of another person by using their images or sharing information, he will be guilty of cyberbullying.

CHARACTERISTICS OF CYBER CRIME

The Concept of cybercrime plays an important role in traditional crime. Due to the growth of internet technology, crime has become a serious crime. So it is necessary to examine the characteristics of cyber crime.

1. People with specialized knowledge – Cyber crimes can only be done by professional people who know about the internet and various other social platforms.
2. Virtual world - The act which takes place in cyberspace and the person who committed that crime is physically outside the cyberspace. Every act which is done by a person takes place in a virtual world.

CYBER PORNOGRAPHY

Cyber pornography means an act of using cyberspace to create, display, distribute, import or publish pornography or obscene materials. With the increase in technology, cyber pornography has taken place online and the act is increasing with the rapid growth in today's world. The person does any wrongful act which leads towards the crime then that person is punished by the law.

The first ever case where the conviction of Cyber pornography took place, was the case of SuhasKatti v. State of Tamil Nadu, decided by a Chennai court in 2004. The woman, a divorcee, complained to the police about a man who was sending her obscene, defamatory and annoying messages in the Yahoo message group, the accused opened a fake email account in the name of the woman, and the messages were from the woman's account. The victim also received phone calls from people who believed that the woman was soliciting sex work. The police complaint was lodged and further, and the cybercrime report was also lodged. Katti was

punished with 2 years of rigorous imprisonment and a Rs 500 fine under Section 469 of IPC (Forgery to harm reputation), under Section 509 of IPC (words, gestures or acts, intended to insult the modesty of the woman) and rigorous imprisonment for 2 years with the fine of Rs. 4000 fine for the offence under the section 67 of Information Technology Act 2000 (punishment for transmitting obscene material in electronic form)

MORPHING

Morphing involves editing the original picture by an unauthorized user - when the unauthorized user with his fake identity downloads the victim's pictures and then uploads them on the digital platform. It is a common phenomenon that women's pictures are uploaded on different websites and their faces or images are used by the person so that the dignity of the woman is hurt. Such an act could attract offences under section 43 (which means any act of unauthorized downloading/ copying/ extracting and destroying/ altering.

SENDING OBSCENE / DEFAMATORY / ANNOYING MESSAGES

Posting a woman's image with her phone number and other personal information, such an act also invades the privacy of the women and their personal information is also disclosed to the public. Sending obscene and annoying messages on the digital platform. The act committed by the person can lead to an offence and that person is charged under Section 354, section 499, and Section 509 of IPC.

REASONS BEHIND CYBERBULLYING AND ONLINE HARASSMENT

Fascination - These are some who are one-sided love. The stalker has love and affection towards the victim and if he/ she refuses to accept the proposal then that person becomes a stalker and starts harassing or bullying her/ him in case of making the victim feel malaise.

Revenge - When the accused has the feeling of revenge for the victim, they can do anything for the revenge and it can be turned into something unpredictable. If the victim refuses to accept his/ her proposal then the accused takes revenge against the victim.

CASES OF CYBERBULLYING

1. VISHAKA V. THE STATE OF RAJASTHAN AIR 1997 SC

Cyberbullying was the first time dealt with as an issue by the Supreme Court in this landmark case. In this case, while dealing with the issue of bullying, guidelines to protect women from sexual harassment were laid down by the court. The Court stated that, “Cyberbullying means bullying which is done through digital devices such as mobiles, computers/ laptops or tablets. SMS, online social media platforms or any online groups where people can share and exchange messages. Sending, sharing or posting false information about someone defines the term bullying.

2. SADDAM HUSSEIN V. STATE OF M.P

In this case, the accused had outraged the modesty of the victim; video recorded the same on his phone and used the same to blackmail the victim. A criminal complaint was lodged under Section 354 of IPC (Stalking), Section 507 of IPC (criminal intimidation by anonymous communication) of IPC and Section 66A of the IT ACT. The petition was filed before the Madhya Pradesh High Court for quashing based on a compromise condition between the victim and the accused. The high court refused to quash the proceedings, stating that the offences were against the society at large and that the personal compromise between the parties would not affect the continuation of the prosecution.

3. MANISH KATHURIA CASE

The first reported case of cyberstalking in India and the reason for the 2008 amendment to the IT ACT, the Manish Kathuria case involved the stalking of a woman named Ritu Kohli. He followed a woman on the chat website, abused her by using obscene language and then disclosed her personal information to her. The accused used her identity and started chatting with another person. Ritu Kohli, a young woman, complained in 2001 that someone was impersonating her identity on social media and the case was charged under section 509 of the Indian Penal Code.

4. Tamil Nadu V. Suhas Katti

The perpetrator was charged with an annoying, obscene and defamatory message in the Yahoo message group. The victim's Email account was used by the defendant. The posting of the message resulted in annoying phone calls to the victim, and the victim's mental state was affected. Then the victim filed a complaint to the police station and police traced the accused. The accused used the internet platform to harass women, so he was charged under Section 67 of the IT Act 2000, Section 469 and Section 509 IPC. Based on expert witness the court held that the crime is conclusively proved and the accused was convicted and sentenced to undergo rigorous imprisonment for 2 years. This is the first case where an accused was convicted under Section 67 of the Information Technology Act, 2000.

5. SHREYA SINGHAL V. UNION OF INDIA

In the Shreya Singhal case, the Supreme Court struck down section 66A of the Information Technology Act, 2000 which provided provision for the arrest of a person who allegedly posted offensive content on social media. The Supreme Court also held that the Section was not saved under being a 'reasonable restriction' on the right of freedom of speech and expression under Article 19 (2).

CONSTITUTIONAL PERSPECTIVE

Freedom of speech and expression is a basic human right which was mentioned under Article 19 of the Constitution. Everyone has a right to freedom of opinion and expression; this right includes the freedom to hold opinions without inference. In the Indian Constitution, article 19 provides for the right to freedom of speech and expression. A person who is a victim of cybercrime can get remedy in the various laws. The restriction of freedom of speech and expression can be found in section 292 and section 294 of the Indian Penal Code, these sections deal with the content that is deemed to be obscene. Some people will use offensive and hurtful language which hurts the dignity of the other person.

VICTIMIZATION OF FEMALES IN CYBERSPACE

India was ranked second among the countries with the most internet users. The number of

internet users increases with the rapid growth in cyberspace. Cyberspace is a digital platform where the person uses the internet for good purposes or bad purposes such as Cyberstalking, online harassment, cyberbullying etc. In the digital age, the internet is a common thing which is used by every individual. Some people use the internet only to hurt the dignity of the person or harass that person so that their mental health is affected.

In today's scenario cybercrime is increasing with the rapid technology change. There are so many cases where cybercrime has taken place, such as Sending or posting messages to the victim, offensive or hurtful messages, and giving threats to the victim. Cyberstalking is also a dangerous crime where the person follows the person online and victim activity is also noted so that the accused can spoil the reputation of the victim.

CYBERSTALKING

Stalking in general means an act of harassing or threatening the other person. Cyberstalking is different from stalking because the accused uses the digital platform to harm the victim. Examples of cyberstalking are email, chat rooms etc.

Cyberstalking is divided into three categories which are mentioned below:

1. Stalking by Email – In this type of stalking the accused directly sends an email to the victim to threaten or harass her. In this type, the sending or posting of vulgar messages were sent to the victim or hateful or obscene messages.
2. Stalking through the Internet – In this type the accused used the online method to threaten or harass the victim. The accused disclosed some sensitive information about the victim to the other person.
3. Stalking through Computers – In this type the accused has noted the activity of the victim. In this type of stalking the stalker can control the account and address of the victim.

PSYCHOLOGICAL EFFECTS OF CYBER-BULLYING

There are so many psychological effects which were suffered by the victim that are discussed below

1. Many of the cyber victims feel angry, frustrated, sad and depressed.
2. They also feel fear, confusion, guilt and shame.

3. It creates the feeling of low self-esteem, and it also creates suicidal thoughts in the victim.
4. In most cases, it creates a high level of social anxiety.
5. Cyberbullying is a dangerous act which can affect the physical health of the victim such as causing weight loss or gain, headaches, breathing issues and sleeping problems.

PREVENTION OF CYBERBULLYING AND ONLINE HARASSMENT

Preventing cyberbullying and online harassment has a comprehensive approach that addresses individual behaviour some important points are discussed below:

1. Educate individuals about cyberbullying because some people do not know about cybercrime.
2. Encourage parents to monitor the activity of children online and guide them about cybercrime.
3. Create a supportive environment in each place so that the individual will freely speak about cyberbullying and online harassment.
4. Effective policies and legislation were implemented that address cyberbullying and online harassment. It should ensure that these policies provide clear definitions of cybercrime.
5. Provide legal awareness in schools, and colleges so that students are aware of cybercrime and its types.

STATISTICS DATA

Cyberbullying and online harassment are significant issues in India, particularly among young people. The National Council of Education Research and Training surveyed in 2019; around 27% of Indian students especially young people, had experienced cyberbullying. These crimes generally occur on digital platforms like Facebook, WhatsApp, and other social media platforms.

Cultural norms and societal attitudes towards gender, caste and religion can also influence the

dynamics of cyberbullying. Many cases of cybercrime are unreported because there is fear in the mind of the victim that her dignity will get spoiled. Secondly, there is a lack of knowledge about cybercrime.

The legal framework also plays an important role in addressing cyberbullying and online harassment, such as the Information Technology Act, 2000 and the Indian Penal Code.

Cyberbullying can affect people of all ages, but young people often get affected by cyberbullying and online harassment.

There are so many different types of cybercrime such as spreading rumours and posting inappropriate or threatening messages.

The data which is reported by the national cyber crime department shows the cases of cyber crime. But those cases are unreported or lack knowledge of the victim, so this crime is a heinous crime which needs to be recorded. So that the person would get punished for his act which he has done.

CONCLUSION

In Conclusion, this article has explored the complex landscape of cyberbullying and online harassment, examining the evolution of legal frameworks, their effectiveness, and challenges. The concept of cyberbullying and online harassment has a wider ambit so each individual should know about cybercrime are consequences of cybercrime in our daily lives and the effectiveness of legal measures in combating cyberbullying. We should understand that cybercrime is dangerous and should be treated as another crime. And everyone should have complete knowledge about cybercrime. Recommendations for enhancing legal protections include promoting digital literacy and empathy-building programs to foster positive online behaviour. In conclusion, addressing cyberbullying and online harassment requires a wider approach.