Jus Corpus Law Journal
Open Access Law Journal – Copyright © 2022 – ISSN 2582-7820
Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

Cyberbullying of women

Shreyas Mishra[a]

[a]University of Lucknow, Lucknow, India

Received 25 June 2022; *Accepted* 19 July 2022; *Published* 21 July 2022

"You cannot go home from the Internet,"

A civilized society always wants to protect the modesty of women at any cost, perhaps this was the reason behind the insertion of Section 509 in the Indian Penal Code, 1860. Bullying is not a new phenomenon, but yes cyberbullying is a new evil. Children, women, and other vulnerable sections of our society are the prime target and easy targets of Cyber Bullying. Last year, we witnessed how two online platforms harassed women of a particular religion. Although this is not the first incident of online harassment of women happening in India, however, this was the first time when in an organized manner online harassment of women took place. Ministry of Information Technology had introduced a new IT Rule 2021 to fix the responsibility of the social media intermediaries, unfortunately, this new rule is also inefficient to curb online bullying because of its inherent lacuna. The time has arrived the government should take some stringent measures against the accused of online bullying and harassment so that women should feel safe not only in physical but also in the virtual world.

Keywords: *bullying, women, internet.*

INTRODUCTION

Who does not want reputation, identity, and prestige in society? Among all the intangible assets, if there is one most valuable asset that is nonetheless reputation or goodwill. Especially, when you are female. In the legal world, everyone has a certain reputation but in the real-

world male have to prove their reputation for women, it is presumed by society. Perhaps this might be a reason when one civilization conquers the other, their first and foremost target is the women of the conquered nation. Women are the mirror and lamp of any society. In participatory democracy women are not just a voter rather they are the key player in this game. In the last decade in India, we saw how women come to the centre of the policy making of the government. There is no doubt that the socio economic condition of women especially in India drastically improved. Now they are much more self-independent and vocal about their rights. This all happen because in the last decade they become more aware and more conscious about their civil and political right due to rapid development and easy accessibility of the internet.

The present world is an internet-world' where virtually everyone is your neighbour. For example, the Me to the movement started in the United States of America but it spread across the globe, and in India, we witnessed the resignation of a cabinet minister due to this movement. Here the term virtual neighbour means persons you know through social media sites such as Facebook, Instagram, WhatsApp, and Twitter as well as Dating apps also. Through these platforms, we can connect with others and share our emotions as well as with them. Hence indirectly because of the internet, our social life has become bigger and wider.

Nevertheless, whatever is mentioned in the above paragraph is only one side of the coin. Another side of the internet, or a more specifically social media site, is it gave the birth of a new monster named 'cyber-crimes'. The term "cyber-crimes" is not defined in any statute or rulebook. The word "cyber" is slang for anything relating to computers, information technology, the internet, and virtual reality. Therefore, it stands to reason that "cyber-crimes" are offences relating to computers, information technology, the internet, and virtual reality. So, identity theft, cheating through the internet, online fraud, and pornography are a few examples of cyber-crime. However, among all these offences offence of cyberbullying is a major cyber-crime whose prime victim is a woman. All these offences are happening just because in an internet world creating a fake identity and fake e-address is very easy and unregulated. Here anyone can hide or make his fake identity, and ultimately this is the biggest sin of the internet.

The recent controversy about Bulli Bai App and Sulli Deals is just an alarm call for us to wake up and understand the fact that such kind of cyber world where no laws and regulations will turn this invention into a curse for the whole society. In this article, we will explore the term cyberbullying, the controversy of the Bulli Bai App, and attempt to find out what are the possible regulation and measures which need to be taken to prevent of commission of such offences. As well as what are the best and speedy measures for the conviction of the accused of such offences. For understanding purposes, this article is classified in the following heads: -

- **Meaning of bullying and cyberbullying**
- **Types of cyberbullying**
- **Laws on cyberbullying**
- **The controversy of the Bulli Bai App**
- **Suggestion and conclusion**

MEANING OF BULLYING AND CYBERBULLYING

The term *bullying* can be described as harassment. Bullying tends to become more dangerous as it continues over time and is equated with violence as well as harassment. Accordingly, Erling Roland states that bullying is "longstanding violence, physical or psychological, conducted by an individual or a group directed against an individual who is not able to defend himself in the actual situation."[1] As per Scandinavian researcher Dan Olweus, bullying is "aggressive behaviour that is intentional and that involves an imbalance of power. Most often, it is repeated over time."[2] The Minnesota Department of Education states that "definitions of bullying vary, but most agree that bullying includes the intent to harm repetition….."

From the above definitions it would be appropriate to describe bullying as not only limited to harassment or violence rather it must be having nature of continuity and it may be physical as well as psychological.

[1] Erling Roland, "Bullying: The Scandinavian Research Tradition" (Delwyn P. Tattum & David A. Lanw) *Bullying in Schools* (Stroke-on-Trent, UK: Trentham, 1989) 21–32
[2] Dan Olweus, "Bullying Among School Children" *Health Hazards in Adolescence* (Berlin: De Gruyter, 1990) 259-297

CYBERBULLYING

The term Cyberbullying was given by Bill Belsey. Cyberbullying is defined as, using both information technology and communication technology beyond the limit in order to harm a person's reputation, or state of mind, or humiliate a person. It is an act by which the person being bullied suffers an adverse effect. The often used definition of cyberbullying is '*an aggressive, intentional act or behaviour that is carried out by a group or an individual, using electronic forms of contact, repeatedly and overtime against a victim who cannot easily defend him or herself.* Therefore, Cyberbullying can be referred as bullying or harassment through electronic or communication devices. It may be in the form of posting hurtful words, derogatory comments, or fake information on public forums. It can also be in the form of developing a website and posting obscene photos or defamatory text on it.

TYPES OF CYBERBULLYING

Cyberbullying has different forms and manifestations. It is, therefore, required to appreciate the different types of cyberbullying to report cyberbullying and take preventative measures against cyberbullying. Cyberbullying can take place in the following way[3]:

Exclusion

Harassment

Outing/doxing

Cyberstalking

Trolling

LAWS ON CYBERBULLYING

In India, there is no specific piece of legislation that penalizes cyber-bullying. The Information Technology Act, 2000, as well as the Indian Penal Code, 1860, deal with the issue of cyber-bullying but not in the direct sense.

Remedies under Indian Penal Code 1860 (hereinafter called "Code")

[3] Tae Hoon Kim, '5 Different Types of Cyberbullying' (*End to Cyberbullying Organisation,* 23 December 2013) <http://www.endcyberbullying.org/5-different-types-of-cyberbullying/> accessed 25 June 2022

In the original code and even in the present code no direct section deals with cyberbullying. Ministry of Women and Child Development consider section 354A, 354C, and 354D[4] of the Code for the purpose of cyberbullying and stalking. 2013 Amendment introduced these sections in the Code.

Under section 354C[5], a person who takes pictures of a woman, or watches her where she expects privacy or when she is indulged in some private activity and expects no one to be observed, shall be punished with imprisonment between one year to three years and also liable to fine under first conviction. For the second or subsequent conviction, there is imprisonment between the terms of three to seven years and also a fine. Under this section, a cyberbully can be punished for taking pictures and can be held liable under this section along with other sections if he transmits or publishes the same.

Section 354A[6] provides punishment for sexual harassment. Section 354D[7] provides punishment against stalking. If a man contacts a woman or attempts to even after she expressed disinterest, or monitors her activities on the internet, shall be liable for punishment of imprisonment up to three years and a fine under the first conviction. Under second or subsequent conviction, he shall be punished with imprisonment up to five years and a fine.

Besides these sections a cyberbully may also be prosecuted under the following sections;

Section 499[8] which deals with Defamation, can be committed through electronic means also.

Section 503[9] talks about the offence, where the person sends threatening messages through the mail.

Section 507[10], criminal intimidation through any unidentified communication or means is prohibited.

[4] Indian Penal Code, 1860, ss 354A, 354C,and 354D
[5] Indian Penal Code, 1860, s 354C
[6] Indian Penal Code, 1860, s 354A
[7] Indian Penal Code, 1860, s 354D
[8] Indian Penal Code, 1860, s 499
[9] Indian Penal Code, 1860, s 503
[10] Indian Penal Code, 1860, s 507

According to Section 509[11] of the Indian Penal Code, offenders who intend to disrespect the modesty of a woman by words or gestures can also be done through electronic means, by invading the privacy of the woman.

Remedies under Information technology act 2000

Section 67[12] of the Information Technology Act,2000 deals with cyberbullying in a way. This section prescribes punishment for publishing or transmitting obscene material in electronic form. Along with this section, Section 66E[13] states that any person who intentionally violates privacy by transmitting, capturing, or publishing private pictures of others shall be punished with up to three years' imprisonment or a fine of up to three lakhs.

CONTROVERSY OF BULLI BAI APP

"Bulli Bai" is a derogatory phrase reserved for Muslim women. The Bulli Bai app was created by a group of students who were pursuing engineering and management from different universities. They used the platform to upload doctored photos of prominent Muslim women and auction their sales. These prominent women were journalists and activists from different fields all over India. It was a shocking moment for all of them when they found their photos on Twitter with an offensive caption – "Your Bulli Bai of the day"[14]. Basically, this app did not actually sell anyone but harassed and humiliated these women. Here before going into the details of the controversy of "Bulli Bai" it is required to mention here that this is not the first incident of cyberbullying. In July 2021, several pictures of Muslim women were posted on social media platforms and they were described as "Sulli deals of the day". The common factor in both bullying is that both are against women of the particular community. However, after filling several complaints and taking cognizance by government authorities GitHub blocked this site and at present, it is not in operation. Hence for a better understanding of these

[11] Indian Penal Code, 1860, s 509
[12] Information Technology Act, 2000, s 67
[13] Information Technology Act, 2000, s 66E
[14] Sneha Saha, 'Your Bulli Bai of the day is ….': Woman shares how she was put on sale online' (*BGR*, 3 January 2022) <https://www.bgr.in/features/your-bulli-bai-of-the-day-is-woman-shares-how-she-was-put-on-sale-online-1033024/> accessed 25 June 2022

offences, we have to understand the modus operandi of these offences. Meaning thereby, how suspected persons were doing such kind of activity?

First of all, although the name of the platform is Bulli Baiapp, it is not the kind of app which is can be downloaded from the Apple iOS App Store or Google Play Store. It is not even a traditional computer app (aka application) because it could not be downloaded or installed on a computer. Basically, Bulli Bai was a piece of code hosted on GitHub. It was executable, like a gallery would be, so it did function like an app. But it was also fairly basic code.

Now the next question is what is this term 'code' means and whether anyone can create it or edit it? To answer this question, we have to explore the functioning of Git Hub. GitHub is an open-source platform where app or software developers upload their program code as well as store it and share their projects. It provides a free platform to engineers and software developers so that they can save money and present their programs before the world. Hence technical field experts believe that the Bulli bai app source code is the same code that was used for Sulli deals.[15]

Therefore, the major issue with Git Hub is that its headquarter are located in the United State of America and they have a privacy policy that they will not share the information of users.[16] What they can do in such cases they remove all the content and block that user for future uses. So in this case also GitHub refused to hand over information on the suspects and they remove all the content of Bulli Bai. GitHub's argument for denial of sharing of information is that there is a legal way i.e. Mutual Legal Assistance Treaty 2005 between India and USA and they will give information only upon receiving valid legal process under the treaty. Hence it would be correct to say that the internet has no boundary but the offender of the internet has the indirect defence of territorial boundary.

---

[15] Swathy Moorthy, 'Sulli deals and Bulli Bai | How much responsibility should GitHub take?' (*News 18,* 7 January 2022) <https://www.news18.com/amp/news/tech/sulli-deals-and-bulli-bai-how-much-responsibility-should-github-take-4633694.html> accessed 25 June 2022

[16] Ankita Garg, 'What is Bulli Bai app, what is its link to Sulli Deals, and how GitHub is involved: Story in 10 points' (*India Today,* 10 January 2022) <https://www.indiatoday.in/technology/features/story/what-is-bulli-bai-app-what-is-its-link-to-sulli-deals-and-how-github-is-involved-story-in-10-points-1898365-2022-01-10> accessed 25 June 2022

SUGGESTION AND CONCLUSION

- The mutual Legal Assistance Treaty (MLAT) between US and India is a formal agreement that ensures Legal Assistance between these countries. Data about a criminal investigation can be retrieved by India through this framework. Requests made by India to the US are entertained only after it has passed the test of Probable cause and gone through a multi-layered procedure. Thus, it is a lengthy and mesmerizing process. Hence after these two incidences, there is an urgent need to relook this treaty and make suitable amendments, especially with reference to cyber offences.
- Under Information Technology Act 2000, there is an authority Computer Emergency Response Team[17]whose work is to prevent the spreading of such information, and officers of this authority may file a complaint before Court as well as regulate the functioning of VPN in India. Unfortunately, in both incidences, they woke up very late and Despite having such wide powers, there has been no news of action taken by CERT-IN or any direction issued by it to the hosting website or even to Twitter.
- We do need better police infrastructure and policing, more special cyber cells, and police stations. There is as such no regular training and collaboration with cyber experts on a continuous basis. We have a poor quality of forensic laboratories which eventually help the accused to take the defence of lack of evidence. Hence solidification of the capability of forensic laboratories can lead to timely collection of evidence of cyberbullying, threatening, morphing, and profiling. It is a highly technical job requiring sharp skills as the virtual world is constantly changing at an unimaginable speed. The central government has given funds to states and Union territories under the Cyber Crime Prevention Against Women and Children (CCPWC) scheme to start "cyber forensic-cum-training laboratories". But many state labs do not have sufficient numbers of cyber experts to seize, preserve and store images of digital evidence essential for securing a conviction in courts. Considering the gravity of the issue, states need to allocate similar resources for their forensic units.

[17] Information Technology Act, 2000, s 70B

- Another major problem is time-consuming trials which ultimately result in the failure of justice. Data of NCRB discloses that during 2020, court trials were completed in only nine cases of cyber blackmailing and threatening with a 66.7 percent conviction rate — 393 such cases are pending in courts. Similarly, 29 cases of cyberstalking and bullying of women and children were completed with a 27.6 percent conviction rate — 1,508 cases are pending in courts. A trial has been completed in only two cases of fake profiling while 148 cases are pending. The lack of systematic training of prosecutors and judicial officers in dealing with cyber-crimes are one of the major reason behind such data.
- Almost after one-decade new Information Technology Rule 2021 was laid down by Information Technology Ministry, which covers all the significant social media intermediaries and compels them that they should have to appoint a grievance, compliance, and zonal officer in India. From Facebook to local social media apps, they all now have local officers to cooperate with the government, and users can approach grievances. But GitHub does not have similar officers posted in India and victims have to take the legal route to get information from the platform. Git hub contention in their defence is that they are not social media intermediaries and they are bound only by the laws of the United States of America. Hence there is an urgent need to control such kinds of social media intermediaries and for this end, the ministry has to either amend the rules or existing laws.[18]
- Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021[19], rules do not make mandatory the deployment of technology-based measures such as automated content filtering tools to curb hate speech. These tools do not only curb hate speeches' rather it protects the dignity of women in certain cases. For example, if Git Hub used this tool then definitely after the incidence of sulli deals it can be repeated under the Bulli bai app because the 'Bulli Bai' app is a spin-off of 'Sulli Deals app. GitHub and Twitter are Significant Social Media Intermediaries (SSMIs) under the rules, meaning that they might not entail a penalty for non-observance, since it is not mandatory for

[18] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021
[19] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, s 4

these companies to deploy automated content filtering tools in India. However, as a matter of public policy, it is imperative that they do. Even if these SSMIs do not necessarily use such technological measures to stop hate speech, the Government must be made to *amend* the rules to make the deployment of such technological tools mandatory to stop this form of hate speech that violates one's right to a dignified public forum.

- Section 79[20] of the Information Technology Act 2000 provides a safety wall to social media intermediaries so that they are not liable for third-party content. Whereas under the new rule publisher of content is liable to a third party. The basic difference between publishers and intermediaries is that the former is supplying information unilaterally there is no role of the reader, whereas under latter is not supplying any information but only provides the platform to supply information. The new rule divided social media intermediaries into two groups e.g. significant social media intermediaries which cover WhatsApp, Telegram, and other platforms, the other group is non-significant social media intermediaries which have less than 5 million users. The irony is that in the rule government made a distinction among intermediaries and fixed the liability of publishers but they forget to fix the liability of significant social media intermediaries, which is part of the recommendation of the Joint Parliamentary Committee on the Personal Data Protection Bill, 2019. Therefore this is the right time for the government to take action so to avoid future conflict between these two laws.
- Bombay high court in Muncherji Nusserwanji Cama's judgment[21] held that a third party may be responsible for illegal, defamatory content if they have 'personal knowledge about the content'. Thus, it is proposed that GitHub and Twitter in addition to the authors/originators of the hateful posts must be *jointly* held liable for the damage done to the women who were 'auctioned' and this will set a good precedent for future cases.

[20] Information Technology Act, 2000, s 79
[21] *Muncherji Nusserwanji Cama* (2019) Criminal Application No. 97/2019

Lastly, no matter how much effort the government makes, the reform starts first at the level of society. Bulli Bai and Sulli Deals is not just an app that defames women rather it targeted one religion women who are more dangerous and disgusting. Henceforth Schools, colleges, universities, and communities must take an active role in educating their wards about the rampant cyber abuse and safety measures/avenues available. We also need to involve social media platforms and encourage them to monitor and check abusive traffic and create more safeguards for users, especially women and children.