Internet has touched every aspect of human life, bringing ease in connecting people around the globe and has also made information available to huge strata of the society on a click of a button. With advancement, came unforeseen banes of cyber offences. Cyber stalking, cyber bullying, spoofing, phishing, credit card frauds are a few to name from the possible cyber offences and many are still not predictable. Cyber bullying is a form of electronic communication which harms the reputation or privacy of an individual, or threatens, or harasses, leaving a long lasting impact. It is using beyond the permissible limit or unauthorized use of electronic technology affecting the life and reputation of another.

**Definition of Cyber bullying**

The term Cyber Bullying was coined by Bill Belsey, Canadian educator. Cyber bullying is defined as, using both information technology and communication technology beyond the limits in order to harm a person’s reputation, state of mind, or to humiliate a person. It is an act by which the person being bullied suffers an adverse effect. It is a deliberate attempt which can be continuous or one time. The bully can be a known person or maybe an unknown person or a group. It is done using technologies such as internet, some chat groups, instant messaging, short message service, web pages, e-mails, etc. The intention is to harm a person. It is an act of a person who is either physically powerful or socially powerful over the victim. It can also be in the form of developing a web site and posting obscene photos or defamatory text on it. Some instances of cyber bullying can be a mere e-mail to someone who has expressed his contention of not keeping any contact, posting pictures and sexual remarks.

A frequently used definition of cyber-bullying is "an aggressive, intentional act or behavior 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 are many variations of the definition, such as the National Crime

---

3. Ibid
4. Ibid
Prevention Council's more specific definition: "the process of using the Internet, cell phones or other devices to send or post text or images intended to hurt or embarrass another person".\(^5\)

**Cyberbullying Includes\(^6\)**

- Sending inappropriate text messages.
- Posting statements online that are vulgar or unacceptable.
- Sending or posting pictures that are not permitted by you.
- Making negative comments.
- Blackmailing with certain demands.
- Stalking and use of intimidation.
- Threats of violence or death.
- Sexually explicit photos or descriptions, which are considered pornography.
- Secretly-recorded photos or videos that were taken without the subject’s knowledge.
- Hate-related communications or actions

Cyber bullying or bullying of any type is against the law. It can have horrible outcomes that will hurt others and sometimes it can lead to crimes, revenge, murders or even cause deaths to innocents that had nothing to do with it in the first place.

**Types of Cyberbullying\(^7\)**

Cyber bullying is a term used to define recurrent and sustained verbal and/or physical attacks by one or more children towards another child who is unable or unwilling to deescalate the engagement using information and communication technology. Like classic bullying, cyber bullying is harmful, repeated and hostile behavior intended to deprecate and disparage a targeted child. Bullying use to be confined to schools, neighborhoods or some small geographic location that the bullied child could leave and seek respite. With cyber bullying, the target child has no escape from the taunting and harassment afforded by the internet and mobile digital technology. Given the variety of methodologies cyber bullies use, which continues to expand, provided below are the ten most common:

1. **Exclusion**: Exclusion is a cyber bullying tactic that is highly effective and indirectly sends a provocative message to the target child without the need for actual verbal deprecation. As its well-known children and teens are developmentally fixated on being recognized by their peers, the process of

---

\(^5\) Cyber Bullying, *available at*: https://myfirstblog563.wordpress.com, visited on October 30, 2017 at 9.00 a.m.


designating who is a member of the peer group and who is not included can be devastating to the target child.

2. **Flaming**: Flaming is a term describing an online passionate argument that frequently includes profane or vulgar language, that typically occurs in public communication environments for peer bystanders to witness including discussion boards and groups, chatrooms and newsgroups. Flaming may have features of a normal message, but its intent if designed differently.

3. **Outing**: Outing is a term that includes the public display, posting, or forwarding of personal communication or images by the cyber bully personal to the target child. Outing becomes even more detrimental to the target child when the communications posted and displayed publicly contains sensitive personal information or images that are sexual in nature.

4. **E-mail Threats and Dissemination**: E-mail Threats and Dissemination is a cyber bully tactic used to inspire fear in the target child and then informing other members in the peer group of the alleged threat. The cyber bully sends a threatening e-mail to the target child and then forwards or copy & pastes the threatening message to others of the implied threat.

5. **Harassment**: Harassment is sending hurtful messages to the target child that is worded in a severe, persistent or pervasive manner causing the respondent undue concern. These threatening messages are hurtful, frequent and very serious. Although sending constant and endless hurtful and insulting messages to someone may be included in cyber stalking, the implied threats in harassment does not lead the target child to believe the potential exists the cyber bully may actually be engaged in offline stalking of the target child.

6. **Phishing**: Phishing is a cyber bully tactic that requires tricking, persuading or manipulating the target child into revealing personal and/or financial information about themselves and/or their loved ones. Once the cyber bully acquires this information, they begin to use the information to access their profiles if it may be the target child’s password, purchasing unauthorized items with the target child’s or parents credit cards.

7. **Impersonation**: Impersonation or “imping” as a tactic in cyber bullying can only occur with the “veil of anonymity” offered by digital technology. Cyber bullies impersonate the target child and make unpopular online comments on social networking sites and in chat rooms. Using impersonation, cyber bullies set up websites that include vitriolic information leading to the target child being ostracized or victimized in more classic bullying ways.

8. **Denigration**: Denigration is used in both classic and cyber bullying, denigration is a term used to describe when cyber bullies send, post or publish cruel rumors, gossip and untrue statements about a target child to intentionally damage their reputation or friendships. Also known as “dissing,” this cyber bullying method is a common element and layer involved in most all of the cyber bullying tactics listed.
9. **E-mail and Cell Phone Image Dissemination**: Not only a tactic used in cyber bullying, but a form of information exchange that can be a criminal act if the images are pornographic or graphic enough depicting under aged children. Children can receive images directly on their phones and then send them to everyone in their address books. Of all cyber bullying methods, this tactic, which serves to embarrass a target child, can lead to serious criminal charges.

10. **Image and Videos**: The usage of images and video recording has become a growing concern that many communities, law enforcement agencies and schools are taking seriously.

**Who are the victims of Cyberbullies?**

The term “cyber bullying” is used only when the bully and the victim are both under the age of 18. When one or both parties are adults, it’s called “cyberstalking” or “cyber-harassment.” Cyber bullying has become more common thanks to widespread access to cell phones and the Internet, even among young children. Often, kids who are cyberbullied also are bullied in person. Three elements are found in all forms of bullying, including cyberbullying:

- **Imbalance of Power:**
- **Intent to cause harm:**
- **Repetition:**

Most victims of cyberbullies are children, but there are also adults who are cyberbullying victims. Generally, cyberbullies will know their victim, but occasionally they will pick victims they don’t know. In these situations, the cyberbully is picking on someone based on a type of bias or prejudice. They may pick on people based on religion, race, gender, sexual orientation, or people who are deemed “not cool.” Other times, they will pick on someone based on a message that he/she has posted that the bully doesn’t like.

**Legal Issues relating to Cyberbullying**

Offences of bullying, stalking, terrorism breach of confidentiality, etc. committed in cyberspace were like similar offences in the real world were punishable. The Information Technology Act, 2000 (IT Act) was enacted to deal with e-commerce and electronic records and also to punish e-commerce offences. Offences such as intimidation, insult, annoying, harassment, defamation, etc. in cyber space continued to be punishable only under the IPC till the 2008 amendment to the IT Act.

---

8 End of bullying. available at: http://fundforcivility.org/cyberbullying-2/, visited on January 15, 2018
10 The Indian Penal Code, (45 of 1860).
11 The Information Technology Act, (21 of 2000)
Section 66\textsuperscript{12} deals with actions done through a computer or a computer device that are grossly offensive or menacing, or done to annoy, inconvenience, insult, injure or cause ill will against the person it is directed at. Cyber-bullying may not always involve false statements. It may involve taunts about a person's quirks. S. 66 A\textsuperscript{13} is viewed as a draconian and controversial law which has a very wide scope that confers unbridled discretion in enforcement as the terms “grossly offensive”, “menacing”, “done to annoy”, “inconvenience”, “insult”, “injure”, “cause ill will” are not defined. With the vast socio, economic, regional and cultural disparity in India it is difficult to define these terms in a manner to deal with and satisfy all cross sections of society and this is best left to judicial determination. On the other hand, with the delays in the administration of justice - including criminal justice and absence of police reforms, the vague terms may be tools to harassment of innocent minors.

A picture of the victim may be morphed and shown in a comical or sexually suggestive light. If a girl’s picture is morphed, or sexually coloured remarks made against her, it can be construed as words, gestures or acts intended to insult her modesty and may attract up to 1 year imprisonment and a fine or either one.\textsuperscript{14} Indecent representation of males is not covered under this Section. It could also be transmission of obscene material in electronic form,\textsuperscript{15} attracting a punishment of upto 3 years imprisonment with a fine of upto Five Lakh Rupees for the first offence. The punishment for a subsequent conviction is higher.\textsuperscript{16} Publishing or transmitting content electronically in which children are depicted in an obscene, indecent or sexually explicit manner; or entices a child into an online relationship for the purpose of sexually explicit or otherwise offensive acts or facilitates or records the abuse of children are all actions which result in enhanced criminal liability.\textsuperscript{17}

In the virtual world, people use “user names” which may be fictitious. This is an accepted practice. Where anyone represents himself as another person or another as himself or knowingly substituting one person for another, he commits the offence of cheating by personation which can attract liability for fine and/or imprisonment up to two years.\textsuperscript{18} Once it is detected that someone is using a false identity to cyber-bully or to cheat someone online, this section can be attracted. But a commonly accepted practice online is the use of pseudonyms or fictitious usernames. Impersonation is dealt with in the IT Act.\textsuperscript{19}

\textsuperscript{12} The Information Technology Act, (21 of 2000)
\textsuperscript{13} The Information Technology Act, (21 of 2000)
\textsuperscript{14} The Indian Penal Code,(45 of 1860),S. 509; “Woman” in this section suggests female. It does not exclude minors.
\textsuperscript{15} The Information Technology Act, 2000,S.67. Even sending an obscene message through the mobile is an offence under the act, Rohit Vedpaul Kaushal v State of Maharashtra & Ors, 2008(2) AIR BomR90 (Nagpur Bench)
\textsuperscript{16} The Information Technology Act, (21 of 2000), S.66.
\textsuperscript{17} S. 67A of the Information Technology Act.(21 of 2000)
\textsuperscript{18} S. 416 of the Indian Penal Code, (45 of 1860).
\textsuperscript{19} S.66D of the Information Technology Act,(21 of 2000)
Drawbacks of Applying Statutory approach to Cyberbullies

Cyber bullying is, many a time, not actuated by malice and may be done to “poke fun” at a friend or acquaintance. However, the perpetrator may unintentionally cross the acceptable line or the victim may believe that it is distasteful and hence unacceptable. Sometimes, malice may be present. Further, the statement made may not be “false” as contemplated by the IPC or IT Act. Bullying may also involve repeatedly confronting someone with a truth, or what is believed to be true with a view to ridicule, humiliate or shame that person.

The IPC classifies minors under 3 heads:

1. Children below seven are legally presumed not capable of committing crimes. This legal presumption is irrefutable.
2. Children between seven and twelve are presumed not capable of committing crimes. However, proof that the child had knowledge of the consequences of the action can refute this and make them liable. The standard of proof is high and the law leans in favour of the minor. Establishing that a minor of this age group has committed any form of “cyber crime” in the form of cyber bullying is difficult.
3. Children above the age of 12 who are assumed to be capable of having mens rea and committing such crimes.

From a study of the offences mentioned as components of cyber-bullying, it is clear that they require mens-rea. Minors up to the age of 7 are exempt from liability as they cannot have mens-rea. It is difficult to establish mens-rea of anyone between the ages of 7 and 12. Anyone above the age of 12 is attributed with mens rea if they commit a crime. Thus, the Indian legal system has fixed the age of understanding for the purpose of “mens rea” as 12 years. It is seen from the foreign statutes in pari materia that juveniles are treated and tried as adults in certain cases. Even in India, The Juvenile Justice Act was amended in the year 2015 which allows children aged 16 to 18 years and in conflict with law to be tried as adults in cases of heinous offences While one is for such a provision, particularly for heinous crimes such as rape and murder, juveniles who are first time offenders should have no criminal liability whatsoever for cyber bullying, unless it leads to suicide or death.

If a child above 7 commits cyber bullying in the form of a cyber crime, he will be subject to the Juvenile Justice Act and be put into remand homes or borstal schools or similar facilities to serve time for their crime. This will be too harsh. Firstly, the child

---

20 Knowledge, knowingly, malice, calculated to are words that ascribe mens-rea as a component of an offence.
21 S. 83 of the Indian Penal Code, (45 of 1860).
may understand only the action he commits and not all the consequences. This would lead to punishment being detrimental. Secondly, punishment of a child in such form, which involves displacing him from his place of residence, family and familiar surroundings, may harden him instead of deter from further crimes. Cyber bullying is, arguably, a milder offence when compared to offences such as murder. Thus, if convicted, a cyber-bully would be housed and disciplined with other juveniles in conflict with the law who may be habitual offenders or may have committed heinous crimes. This may jeopardize the cyber bully’s safety or influence him to go deeper into crime and become a habitual offender. Thus, criminalizing minors for cyber bullying can be counterproductive. It is over criminalization.

**Cyberbullying: From Online Suicide Groups to ‘Blue Whale’ Menace**

Internet has changed the way we talk, live, earn, eat and sleep. Thankfully, the change has mostly been for better and internet or web has enriched our lives in the last two decades or so. However, all good things have a bad side, too. So is also the Internet. Cyber bullying, blackmail, data theft and hacking make lives of several people hell. Sadly, web is also being used extensively for the proliferation of terrorism-related ideology, drug peddling, prostitution, child pornography and what not. But the latest fad of inducing young children to suicide through ‘Blue Whale’ challenge game has taken the misuse of internet to a new level. The deadly game which originated in Russia in 2013 prompts children (challengers) to perform a series of tasks given to them by the game administrators for 50 days on mobile app, culminating in the challenger’s suicide. The game reportedly caused first suicide in 2015 and since then, it claimed lives of several youngsters around the world. One Russian Philipp Budeikin, a former psychology student, claimed that he designed the game to purge the society of useless people. Though the megalomaniac was put behind bars, his deadly creation continues to cause harm to youngsters in one country or other.

The notorious online game, Blue Whale, has allegedly pushed three teenagers into committing suicide in India while two were rescued before they could take the extreme step. The number of suicides across Russia and the Central Asian countries of Kazakhstan and Kyrgyzstan where the game is in rage are reported to be over 130. Alarmed by the growing number of suicides caused by the app-based game, software industry body Nasscom and Data Security Council of India (DSCI) issued an advisory for all the stakeholders to check the spread of the game. The Ministry of Women and Child Development to issue alerts to parents, schools and colleges, and recommended that it activates a hotline or web portal to receive tip-offs to identify sources of the game and to bury the Blue Whale once and for all.

---

Judicial Response

The Indian judiciary is playing the important role in dealing with the cyber crimes relating to sending offensive messages through communication service etc. The Additional District Court and Sessions Court was upheld a lower court’s verdict in the first cyber case in *State v. Ts. Balan and Aneesh Balan case* in 2006 and sentenced a Pentecostal priest and his son for morphed photographs and e-mailed to victims from fake IDs with captions under section 67 of Information Technology Act, 2000.

In the light of a series of arrests made under section 66A of the Information Technology Act, 2000, *Shreya Singhal v. Union of India*28 is the case where the writ petition was filed in public interest under Article 32 of the Constitution of India for seeking to strike down Section 66A as unconstitutional by arguing that section 66A is so wide, vague and incapable of being judged on objective standards that it is susceptible to wanton abuse. It was further argued that the terms ‘offensive’, ‘menacing’, ‘annoyance’, ‘danger’, ‘obstruction’ and ‘insult’ have not been defined in the Information Technology Act, General Clauses Act or any other legislation. It has been held in the case of *A. K. Roy v. Union of India*29 that the impossibility of framing a definition with mathematical precision does not justify the use of vague expressions. In the said case, a provision of the National Security Act was held to be violative (due to being capable of wanton abuse) of the Fundamental Right to Life and Personal Liberty guaranteed under Article 21 of the Constitution. Citing the arrests made under section 66A, the petitioner submits that the wide legislative language of the Section severely disincentives citizens from exercising their Constitutionally protected right to free speech for fear of frivolous prosecution (the ‘chilling effect’), which violates the Freedom of Speech and Expression guaranteed under Article 19(1)(a) of the Constitution. Furthermore, whether or not section 66A meets the test of ‘reasonableness’ laid down under Article 19(2), it is nonetheless violative of Articles 14 (Right to Equality) and 21 of the Constitution. The Hon’ SC declared section 66A as unconstitutional in its entirety and against the freedom of speech and expression and struck it down in *Shreya Singhal and others v. Union of India*. This section had been misused by police in various states to arrest the innocent person for posting critical comments about social and political issues on networking sites. This section had led to the arrest of many people’s for posting content deemed to be allegedly objectionable on the internet.

Additionally, in *S. Khushboo v. Kanniammal*,30 the Supreme Court observed that the proper course for Magistrates is required to use their statutory powers to direct an investigation into the allegations before taking cognizance of the offence alleged

---

27 (2006) Additional District Court and Sessions Court, Kerala, for morphed photographs and e-mailed to victims from fake IDs with captions.
28 AIR 2015 SC 1523; (2005) 5 SCC.
29 AIR 1982 SC 710.
30 (2010) 4 SCALE 467.
where the cases involving the fundamental right of Freedom of Speech and Expression. Because in this the petitioner prays that Section 66A of the Information Technology Act shall be struck down as unconstitutional and a guideline must be issued by the Court that offences involving Freedom of Speech and Expression be treated as non-cognizable offences.

In *Rajeev Chandrashekhar v. Union of India*[^31] and *Common Cause v. Union of India*[^32] case, a writ petition was filed in public interest under Article 32 of the Constitution of India by challenging section 66A of the Information Technology Act, 2000 and Rules 3(2), 3(3), 3(4) and 3(7) of the Information Technology (Intermediaries Guidelines) Rules, 2011 as unconstitutional. In this case the Petitioner, a serving Member of Parliament submits that Section 66A contains several words/terms that are undefined, vague, open to misinterpretation, and thus problematic. This imposes statutory limits on the exercise of internet freedom which are well beyond the Constitutional parameters of ‘reasonable restrictions’ enshrined in Article 19(2) and the Intermediaries Guidelines Rules, Rule 3(2) lists the various types of information that ought not to be carried on a computer system which violates Article 14 in being arbitrary and overly broad.

In *Common Cause v. Union of India*[^33] case, Common Cause, a registered society, filed a writ petition under Article 32 of the Constitution of India for the enforcement of Fundamental Rights under Articles 14, 19 and 21 of the Constitution of India by challenging the constitutional validity of Articles 66A, 69A and 80 of the Information Technology Act. In this case it is contended that the restrictions imposed by Section 66A of the IT Act are violative of Article 14 because they restrict free online speech and also the violative of Article 19 because the restrictions on speech causing mere ‘annoyance’ often go beyond the ambit of reasonable restrictions stipulated under Article 19(2) of the Indian Constitution. It is also contended that ‘grossly offensive’, ‘danger’ and ‘annoyance’ are vague, arbitrary and constitutionally undefined terms as found under Section 66A. It is also contended that section 69A of the IT Act is violative of Articles 14, 19 & 21 of the Constitution of India because it neither provides a Redressal machinery after blocking of online information of an entity, nor any provisions for unblocking them while the process of blocking is entirely secret, and fails to meet constitutional safeguards of natural justice. Similarly, section 80 of Act is violative of Articles 14, 19 and 21 of the Indian Constitution because it confers unlimited powers to police authorities to arrest without warrant any person suspected of committing a crime under this Act.

In *Dilip Kumar Tulsidas v. Union of India*[^34], the petitioner has also sought directions against the respondents to carry out widespread awareness campaigns relating to

cyber crime sought to be punishable under Information Technology Act and other penal law. In the prevalent system of cyber crime investigation, there is a lack of procedural safeguards. There are also a number of instances where the police and cooperating private entities have displayed great negligence towards the innocent citizens and the investigative methods are not suited to dealing with complex cyber crimes.

In *People’s Union for Civil Liberties v. Union of India*35, a writ petition was filed in public interest under Article 32 of the Constitution of India regarding the misuse of the Rules framed under the IT Act throughout the country despite the fact that Supreme Court issuing the similar notice in *Shreya Singhal v. U.O.I*36 soon before this. The Information Technology (Intermediaries Guidelines) Rules, 2011 which provide for legal determinations and effective censorship by private on-line service providers are vague and undefined categories and contrary to Articles, 14, 19 and 21. The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 which provides the process of blocking is fully secret and fail to meet constitutional safeguards of natural justice under Article 19 and 21 and the unreasonably restrictive procedure for banning websites in addition does not meet the procedural natural justice standards for book banning, ebooks may thus be banned easily and secretively.

**Suggestion:**

There are precautions everyone can take to prevent cyberbullying. Teens especially should use caution when giving out their mobile phone number or email address, or other social media contact information. The victim should not reply to threatening or disturbing emails, as this will only encourage the bully. If others in a chat or online discussion become unpleasant, leave the conversation. Make use of the privacy and security settings on social networking sites, as this will prevent bullies from seeing information they can use against their victims.

When a teen or anyone is a victim of cyberbullying, there are people they can turn to for help and for recourse against the person abusing them. First, an adolescent should tell someone they trust, whether it is a friend, parent, teacher, or other person who works with youth. They should keep any emails, messages, or texts as evidence of the bullying. They can also block email addresses or specific users on certain social networks, so they do not receive any more messages from the bully. Finally, they should contact their Internet service provider, the bully's Internet service provider or host for any web pages, or the help desk of any social media networks on which the cyberbullying occurs. Harassment of others through such sites is often a violation of the terms of service of the host or provider. As a result, the bully's account or access to the site, forum, or network may be suspended.

36 AIR 2015 SC 1523; (2005) 5 SCC.
If a teenager reports a cyberbullying incident, it is important to remind them that it is not their fault. Bring cyberbullying matters to the appropriate authorities - teachers, principals, Internet service providers, website hosts, etc. - to deal with them. A combination of a safe and sensible approach to Internet safety, with an attitude of no tolerance for bullying, can work hand in hand to prevent cyberbullying.

**Conclusion**

In view of the expanding dimensions of computer-related crimes, there is need for adopting appropriate regulatory legal measures and gearing up the law enforcement mechanism to tackle the problem of Cyber crime with stern hands. That apart, the peculiar nature of Cyber crimes is such that the offender and the victims do not come face to face, which facilitates the criminals to carry on their criminal activities with sufficient sophistication without the fear of being apprehended or prosecuted. It is for this reason that a multi-pronged approach and concerted efforts of all the law enforcement functionaries is much more needed for effective handling of Cyber crime cases. A common Cyber crime regulatory law universally acceptable to all the countries would perhaps provide a viable solution to prevent and control cyber criminality. Therefore, a sound strategy for prevention of Cyber crime necessitates mobilisation of community participation in combating this menace. This calls for participative role of all those who perceive that the growing incidence of Cyber crime is a potential danger to society as a whole. It also calls for self protection initiatives by the people who are vulnerable to Cyber crimes. They must have adequate knowledge and awareness about the nature and gravity of these crimes and the dangers fraught by them. Obviously, media has an important role to play in warning people against the possible dangers and evil effects of Cyber crimes on victims as also the nation and the safety measures which are necessary to combat this hi-tech criminality.