International Journal of Engineering Research and General Science Volume 3, Issue 2, Part 2, March-April, 2015
ISSN 2091-2730

CYBER BULLING – THE REPERCUSSION OF LACK CYBER GOVERNENCE IN INDIA

DR.AARTI TOLIA

B.COM.,M.A.,LL.M., PhD (through National Law School of India University) Practicing law and Professor of Law in Mumbai.

Abstract: From the pre-technology age explicating ethics has always attracted the attention of philosophers globally. With distinct decipherment in various nations and cultures throughout the globe the field of ethics involves organizing, safeguarding, and advocating theories to evaluate and bisect right and wrong behavior. The rudimentary interpretation of online dictionary elucidates ethics to be the body of moral principles or values governing of a particular culture or group reflecting dharma. From the birth the parents, the schools & the statute incorporate ethical standards to which all individuals abide and draw line between the limits and boundaries to adhere.

Post technology the basic human needs have seen a radical change where 'food, clothing and shelter' have now an added element to its definition as in 'food, clothing, shelter and internet'. The internet has enveloped every phenomenon in all walks of life, from banking to shopping, from education to projects and research. The paper accentuates the incompetency of the parents, teachers and statute to incorporate online ethical standards in children thereby escalating the chances of reckless use of the cyber space. Internet savvy users are also in dilemma on analyzing what amounts to ethical on the World Wide Web. Parents, educators, administrators across the globe are struggling to explore appropriate approaches to demonstrate and inculcate cyber ethics in the new generation.

Keywords: Cyberbullying, Cyberspace, Ethics, Social Networking Sites, Indian Penal Code 1860, Information Technology Act 2000.

INTRODUCTION

Preclude:

The development of information technology escalates oodles of issues like computer intrusion, security, privacy infringement, intellectual property legitimacy, defamation, cheating, fraud and impersonation and so on. The innate feature of anonymity comforts the perpetrator to behave unethical on internet with no cyber-censorship. In short the cyber ethics may be defined as a responsible use of internet or responsibilities for information on internet. This paper is divided into two sections where part one highlights on the careless & bold access of Social Networking Sites (SNS) by children and youth on internet the second part illuminates the role of statute i.e. pitfall in the cyber governance of India to inculcate cyber-ethics in the pre-stages.

Part I

Logical interpretation of cyber ethics means principles or standards of human conduct thereby obeying laws applicable to online behavior for a safe and healthy browsing. It may be addressed with different names like cyber citizenship or netiquettes and sheds light on what user does online when no one is watching. The moral behavior and true virtues that one follows offline in the real world on daily basis when practiced online it defines cyber ethics. It is very essential for a user to understand what are the causes and consequences of accessing technology in haphazard manner.

New generation-children and teens who otherwise may think several times before committing an offence offline like pick pocketing, robbing etc. don't take a second to cross the cyber ethical boundaries and being accountable to a cybercrime due to lack of cyber regulations. The availability of internet on cheap and handy devices round the clock supplemented with anonymity is no less than 'genie and the magic lamp' for children and teens to fulfil their unlimited wishes at a click of the mouse. Technology continuous to change rapid than a blink of eye as such it brings new dimensions to the responsibilities of parents, teachers and legislation. Today the education system is reliant on internet for projects, homework, research and filling of online forms is a part of routine work. Children use a computer and internet at very early stage of education, maybe on their own, or through the educational institutes where schools provide free access to internet in the libraries or on cell phones, as such practically what steps have been adapted to coach ethical use of technology in schools.

Bullying has been a concern in schools and colleges for ages but the pre-technology period saw innocent peer-to-peer harassment or mischief within the control of the teacher but the post technology has marked a violent online behavior creating totally a new subject of concern, study and research coined as 'cyberbullying.' Bullying may be verbal, physical, sexual, prejudicial, and emotional and when all this is done using technology it is cyberbullying the demon form of bullying. Cyberbullying can be briefly defined as "sending or posting harmful or cruel text or images using the Internet or other digital communication devices" (Willard, 2004b, p. 1).

The free access to Google and unmonitored profile creation on social networking sites has led children to use internet recklessly. Playing mischief and posting remarks on peers profiles have become a customary obsession in children and youth. The soft and light remarks advance to be heavy and harsh when children form hate groups and target a single victim with abusive messages and online comments. A person is judged on how many friends he or she has on SNSs or how many likes & comments one receive on the SNSs. In the bid to add and increase the friend-count online children have accepted and added strangers to their profile. They do not hesitate to chat and give out all the personal information to such strangers escalating unknown dangers to them or their family and friends. The weak and shy child in the class or society is the target of such bullying. Many children join the group with the fear that they may be secluded from the group if they don't join their peers, while others are those who themselves have been a victim to cyberbullying in their past.

The aftereffects of cyberbullying show psychological irreparable harm and may ruin the future of the victim, he may show poor results in studies and inflict in low self-esteem, school failure, anger, anxiety, depression, school avoidance, school violence, and suicide. The victim has no escape as the abusive content posted takes no time to reach multitudinous online audience leaving the child with a fear, insult, defamation & drive to suicide. A survey conducted by Patchin and Hinduja (2006) of under 18, highlighted various forms of bullying including being ignored (60.4%), disrespected (50.0%), called names (29.9%), threatened (21.4%), picked on (19.8%), made fun of (19.3%) and having spread rumors about them (18.8%). A study conducted by McAfee states that 52% of school going children in India have an account on SNS wherein 50% have experienced cyberbullying, 92% children have done something risky online, and 70% have posted their personal information online. The SNSs have set 13 years of age as criteria to open an account but as per The Social Age Study by knowthenet.org.uk- 59% have an account on SNSs before the age of 10. The 13 years of age limitation is set according to the Children's Online Privacy Protection Act (COPPA) 1998 which restricts online service providers from collecting personal information and protects against collecting and sharing information of children with third parties.

The Anti-bullying charity's findings in 2013 states that 69% young people have been victims of cyber bullying-a number much higher than its previous reports, young children are likely to be bullied as twice on Facebook as on any other social networking

site.[1] A survey report of NSPCC states 93% of users in 2013 were between the ages 5-15 years, 82% were of 5-7 years, 96% were 8-11 years and 99% were 12-15 years old.[2]

Creating of fake profile by children under 13 is an offence as per the COPPA. As per the Indian Act 18 years is considered as the age of majority, with innumerous clan of children opening an account below 18 years of age is against the Indian Majority Act, the Indian contract Act, and also the Information Technology Act thereby coming into the gamut of cybercrime, accounting to punishable offences. A Public Interest Litigation (PIL) was filed by the former Bhartiya Janata Party ideologue K.N.Govindacharya in concern of an incident where several minors involved in 'sex and smoke' party in Gurgaon gathered through Facebook. The Delhi High Court through a division of bench directed Facebook and other SNSs to put a disclaimer in bold letter stating children below 13 years of age cannot open an account on it. Senior advocate appearing for the Facebook assured that Facebook will upload a disclaimer for the same. YES- All is assured- all are directed but - *WHERE IS THE MECHANISM TO VERIFY THE AGE OF THE USER?* In practical bureaucracies and their norms are necessary for implementation of the law without which law remains inadequate and crippled. The synergy between the normative order of law and the normative order of bureaucratic norms is mandatory on global platform for cyber-safety.

Part II

The European Union[3] has taken outstanding initiative and is the only international Council that has framed guidelines for cyber ethics i.e. protect online -freedom, security and human rights, and aids to protect societies worldwide from the risk of cyber-crimes. The draft TWO of the EU Human Rights Guidelines on Freedom of Opinion & Expression Online and Offline in its clause A(6) states that every signatory state member of the EU are committed to protect and ensure freedom of opinion and expression, within their boundaries and all over the world. India, United Kingdom (UK) & USA has ratified the treaties and various global documents to administer cybercrimes in their local Legislations. The discussion of online offences related to children always directed to cyber child pornography, but thanks to the legislation of India for its initiative in bringing child pornography under statute. Child Pornography has been addressed wisely in Information Technology Act 2000 (ITA-2000) as amended in 2008 wherein first time the Act has used and introduced the word children in Section 67B which read as:

67 B Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form. Whoever,-

(a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct or

(b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner or

[1] CYBERBULLYING STATISTICS: THE ANNUAL CYBERBULLYING SURVEY 2013 http://www.ditchthelabel.org/cyberbullying-statistics/accessed on 18/3/2014.

[2] Statistics on online safety http://www.nspcc.org.uk/Inform/resourcesforprofessionals/onlinesafety/statistics-online-safety_wda93975.html, accessed on 18/3/2014.

[3] You are here: Home » National » India, allies to combat cybercrime India, allies to combat cybercrime Anirban Bhaumik, New Delhi, May 16, 2012, DHNS:Website: http://www.deccanherald.com/content/249937/india-allies-combat-cybercrime.html, last accessed on 24/3/2014.

(c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource or

(d) facilitates abusing children online or

(e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, ……

This Section has addressed online child pornography and is welcome amendment to the ITAA 2008. The same concern towards children can be noticed by the Government of India's ratification of the Convention on the Rights of children leading administration of conventional laws to boost the new landmark legislation - Protection of Children from Sexual Offences Act, 2012 (POCSO). POCSO is the outcome of the basic fundamentals enshrined in the UNCRC whence the appropriate national, bilateral and multilateral measures to encourage protection of children from sexual offences and assaults is addressed. The Act has no mention of bullying or cyberbullying and online offences related to children. In India the Information Technology Act and the Indian Penal Code are the legislations under which cybercrimes are addressed. If the perpetrator is an adult then criminal and civil laws attracting punishment and compensation to the victim child and aggrieved family members is the relief. But if the wrong doer and the target both are children then along with the IT Act & IPC the Juvenile Justice (care and protection of children) Act, 2000 has to be looked into. The Amendment of the Information Technology Act in 2008 has put efforts to combat cyber-crimes but if seen through the children protection perspective it does not have much to offer other than Sec 67 B as discussed above. No other offences related to children have been addressed in the IT Act in spite of child cases been brought to notice before the amendments and online mischief been played by children prior to 2008.

The following table shows the legislations in India that attract cyber-crimes

Information Technology Act-2008	Section	Indian Penal Code	Section
Tampering with computer source documents	Sec. 66	*Sending threatening messages by email*	Sec. 503
Punishment for sending offensive messages through communication service, etc.	Sec. 66 A	*Sending defamatory messages by email*	Sec. 499
Publishing obscene information	Sec. 67	*Forgery of electronic records-*	Sec.463
Un-authorized access to protect system	Sec. 70	*Bogus websites, cyber frauds*	Sec 420
Breach of Confidentiality and Privacy	Sec. 72	*Email spoofing& Web-Jacking*	Sec 383
Publishing false digital signature certificates	Sec. 73	*E-mail Abuse-*	Sec. 500

The Information Technology Amendment Act has some eminent elements as follows:

- Data privacy
- Information Security

- Defining cyber café
- Making digital signature technology neutral
- Defining reasonable security practices to be followed by corporate
- Delineating the role of intermediaries
- Defining the role of Indian Computer Emergency Response Team
- Inclusion of some additional cybercrimes like child pornography and cyber terrorism
- Authorizing an Inspector to investigate cyber offences

Technology changes at a rapid pace, cybercrimes emerge with new ways to fraud and play with the law, unfortunately the online victimization of users is on rise. Undoubtedly the Information Technology Amended Act of 2008 is a masterpiece compared to its antecedent the Information Technology Act 2000 but the Amendment has overlooked concrete tough measures for inculcating cyber ethics and creating awareness. The Amendment has focused more on e-commerce while other issues like defamation, privacy infringement and torts have been overlooked. India has no statute directly addressing the guarantee to privacy of an individual but ingredient of right to privacy as traditionally contained in the common law and in criminal law is recognized in courts which include defamation, harassment, nuances and breach of confidence. The Juvenile Justice (Care and Protection of Children) Act 2000 prohibits the publications of names and other particulars of children involved in the proceeding under the Act thereby managing to secure the privacy of the child in the trial. Article 21 of the Indian Constitution has a provision which reads *'No person shall be deprived of his life or personal liberty except according to procedure established by law'* this Article is deemed to have within its ambit inter-alia- the Right to Privacy'- the right to be left alone[4]. Where the Supreme Court laid down that right to privacy is implicit in the right to life and liberty guaranteed to a citizen under Article 21 of the Constitution, which guarantees the citizen the right to safeguard the privacy of own life, family, marriage and procreation, motherhood, childbearing and education among others. As such children in India being the citizens of India are at risk of their privacy being infringed online and target to online bullying, with no special law addressing the 'invasion of online privacy' of children to mitigate the inadequacies in the IPC & IT Act.

Cyberbullying is a new area of concern bothering the parents, teachers and the society an initiative in the Act with provisions of awareness would go far long creating cyber ethics as technology has to be understood and learnt by all the stalk-holders like the parents, teachers, educational institutes, Non-Government Organizations, Judicial officers, legal professional, litigant public and the society at large. Lack of tech-savvy staff and knowledge of the adjudication process including the investigating agencies further widens the issue. India needs to strengthen the high-tech crime units and incident response teams, with more effective interagency. A joint effort of public-private and international cooperation on local, national and international level will surely help to curb the menace of cyberbullying and strengthen a healthy online experience. An amendment in The Juvenile Justice (Care and Protection of Children) Act 2000, to discipline and counsel the juvenile on cyber ethics and cyber in the reformative term has to be added. The child offender may or may not have been booked for online offences, but maybe online or offline-the Act needs to have counselors to coach the use of cyber space as it is very likely that once released the child will have a cell-phone with an internet from tomorrow.

Conclusion:

'***ignorantia legis neminem excusat'* –** A simple rule of ignorance of law excuses no one thereby not knowing the laws and limits on internet does not make a wrong doer skip liability of law merely on the basis of its unawareness of the content.

A mixed percentage of children and adult user's access internet, it is impractical to teach cyber ethics to adults' elders but to washout the cyberbullying and other offences from the grass root level steps should be taken to implement rules and regulations in schools and institutions. Cyber ethics should form a compulsory part of the curriculum without which schools and colleges should not receive their grants and aids. The childish nature of child if molded in a proper direction in proper time-there are fair and full chances

[4] (Rajgopal v State of TN, 1994 (6) SCC 632)

of a safe online future with moral cyber ethics. An emphasis on the role of the local educational institutes to draft policies and guidelines to create cyber ethic awareness for effective implementation of the international human rights norms will surely prove to be gainful. The Government also needs to set proficient curator organizations and not rules and regulations in schools for the name sake. Stringent pre-school and school awareness, safety policies and guidelines will surely prove to be effective tools to establish and ensure a child friendly cyber space with healthy browsing experience.

REFERENCES:

1) ETHICS AND THE HISTORY OF INDIAN PHILOSOPHY, SEE- HTTP://BOOKS.GOOGLE.CO.IN/BOOKS/ABOUT/ETHICS_AND_THE_HISTORY_OF_INDIAN_PHILOSO.HTML?ID=X89I_ZEGPHKC
2) The Handbook of Information and Computer Ethics.
3) *EU External Freedom of Express Policy- see- F]EU External Freedom of Expression Policy - WikiLeaks*
4) Cyberbullying Among Adolescents: Implications for Empirical Research- Journal of adolescence health.
5) The edition of Commentary on Information Technology Act by Apar Gupta, 2nd edition 2011