

Social Media Crime In Digital World – A Critique Through Law, Policy and Practice

*Dr. Narender Nagarwal**

I. Introduction

From the last decade of 2005-2015, we have been witnessing to a number of “social media revolutions,” from Anna Hazare’s Lokpal movement¹ to Occupy Wall Street movement² to the sensational Delhi’s Nirbhaya rape case³. In the foretasted incidents, the common man wholeheartedly supported the struggle through different form of social media i.e. Facebook, Twitter, YouTube, Instagram and WhatsApp etc. It is an undeniable fact that whole movement fuelled by social media by the masses especially the youth of this country. Understandably, it can

*Dr Narender Nagarwal, Assistant Professor (Law), Campus Law Centre, Faculty of Law, University of Delhi. The view expressed herein are personal in nature, the author can be contacted at his e-mail: narender.nagarwal@gmail.com.

¹ Anna Hazare is a renowned social activist who spearheaded the anti-corruption movement in 2011. Hazare started a [hunger strike](#) on 5 April 2011 to exert pressure on the Indian government to enact a stringent anti-corruption law, [The Lokpal Bill, 2011](#) as envisaged in the [Jan Lokpal Bill](#), for the institution of an [ombudsman](#) with the power to deal with corruption in public places. The fast led to nationwide protests in support. The fast ended on 9 April 2011, a day after the government accepted Hazare’s demands. The anti-corruption movement wholly fueled by different modes of social media.

² The Occupy movement is the international branch of the Occupy Wall Street movement that protests against social and economic inequality around the world, its primary goal being to make the economic and political kindred in all societies less vertically hierarchical and more evenness strewn. The first Occupy protest to receive sweeping attention was Occupy Wall Street in New York City’s Zuccotti Park, which began on 17 September 2011. By the Oct 09, 2011 this protests had taken place in over 951 cities across 82 countries, and over 600 communities in the United States. This movement had also availed different modes of social media platforms to spreading their messages.

³ The 2012 Delhi gang rape case involved a [rape](#) and fatal assault that occurred on 16 December 2012 in Delhi. The incident took place when a 23-year-old female [physiotherapy](#) intern, Jyoti Singh was beaten, [gang raped](#), and tortured in a private bus in which she was traveling with her friend. As a result of the massive people protests in Delhi, in December 2012, a judicial committee headed by J. S. Verma, former Judge of Supreme Court, was set up to study and take public suggestions for the best ways to amend laws to provide quicker investigation and prosecution of sex offenders. After considering about 80,000 suggestions, the committee submitted a report which indicated that failures on the part of the government and police were the root cause behind crimes against women. In 2013, the [Criminal Law \(Amendment\) Ordinance, 2013](#) was promulgated that led to enactment of several new laws, and six new fast-track courts were created to hear rape cases. This movement too used social media for spreading messages to escalate pressure upon the government.

safely be stated that the social media has been playing a significant role in shaping people's opinion and developing their views on any particular issue that has social relevance. It is hard to disagree to conclude that there is no impact of social media upon the minds and thoughts of youth (the largest users of social media i.e. Facebook and Twitter).

An analysis of advantageous and disadvantageous part of social media confirms that despite many benefits, some of the menace and other concomitant ill-effect cannot be sidelined. The news and views spread so rapidly through social media that may cause turbulence and social disharmony. The social media topic contained pertinent pluses but on the same tone while recognizing the multiple merits of social media, the perils too needs to be tackled prudently. The people's ability is immature to coordinate with massive information sent in text messages, Facebook posts and tweets as they imbibe them without verifying the contents and it could be harmful.⁴ There have been numerous instances wherein the social media has created the social turbulence if we regard the recent Muzaffarnagar experience in which a fake video uploaded by a local politician escalated the communal tension and the act has been done aiming to target minority community of the area. Hence, creating social unrest through social media and sudden rise of online crimes poses a grave threat to the contemporary Indian society. The online harassment of women, eminent citizens and political personalities through various modes of social media exemplifies the behaviour and social sickness of a society.. It has been observed that the online harassment by trolls⁵ on social media often remains unnoticed and hardly discussed as a serious web based crime.⁶ This sort of online pestering comprises rape threat, caste and religious based abusing and sometime uploading morphed pictures of women etc. By overlooking the consequences and supposed harm that may affect the basic freedom of individuals especially the women, we trivialise the serious issues that must be tackled through law and stringent policy and roadmap.

In light of this, the present paper deals with two significant issues surrounding the social media, firstly the problem of online abuse and the role of the legal machinery; secondly the rampant misuse of social media to fulfill political interests of a political class. The main thrust of the paper is to recognise the cyber harassment and gender-based discrimination through social media. It is crucial to educate, propagate and sustain an awareness campaign of gender related harassment, to

⁴ Clay Shirky, *The Political Power of Social Media*, Foreign Affairs (Jan/Feb2011), available at: <http://www.cc.gatech.edu/~beki/cs4001/Shirky.pdf> (last visited Aug 06, 2016).

⁵ See, Oxford Dictionaries Online definition of "troll": a person who makes a deliberately offensive or provocative online post, available at: <http://www.oxforddictionaries.com/definition/english/troll> (last visited Aug 02, 2016).

⁶ Daniel K Citron, "Laws Expressive Value in Combating Cyber Gender Harassment", 108 Michigan Law Review 402 (2009).

ensure that women's complaints to be heard if she faces such online abuses through trolls or if she complained about exceeding her privacy. Further, the perpetrators of online abuses must remember that attack through social media now will not remain unheard and any deliberate misadventures of misogyny through social media will be dealt severely.

II. Social Media: The Transformation of Traditional Media

Sharing information through social media is imperative to accomplish digital citizenship which undeniably opened fresh avenues to share and spread information and knowledge and services, to more and more people in short span of time that too at nominal cost.⁷ The dawn of social media is transforming the way in which people connect with each other and the manner in which information is shared and distributed. It is different from traditional media such as print, radio and television.⁸ In this context, it would worthwhile to mention the assertion made by Andreas Kaplan and Michael Haenlein⁹ about the social media and they opined that "it is a faction of internet-based application that are erect on the intellectual and technological foundation of Web 2.0, that allow the creation and exchange of user generated content".¹⁰ Today, there are numerous social networking websites over the internet like Facebook, WhatsApp, You tube, Twitter, Instagram etc, which have been playing a dominating and decisive role to influence public opinion.¹¹

The most appreciable thing of the social media is that the new generation has now variety of preferences to choose from what they should read, like and most importantly contribute. The list of social media tools could probably run on for paragraphs, and today's technology changes so rapidly that many industries, including corporations and news media, can barely keep up. In the traditional

⁷Sumit Chaturvedi and Dr. Sachin Gupta, *Social Media Promotions- Can We Restrict It Under Law?*, 1(1) International Journal of Research-Granthaalayah 43-50, (2014), available at: http://granthaalayah.com/Articles/Vol1Iss1/06_IJRG14_A08_11.pdf (last visited July 27, 2016).

⁸Department of Electronics & Information Technology, Government of India, Framework & Guidelines for use of Social Media for Government Organizations, available at : http://deity.gov.in/sites/upload_files/dit/files/SocialMediaFrameworkDraftforPublicConsultation_192011.pdf (last visited July 27, 2016).

⁹Andreas Kaplan and Michael Haenle in, *Users of the World, Unite! The Challenges and Opportunities of Social Media*, 53 Business Horizons 59-68, (2010).

¹⁰Dr. Kiran Bala, *Social Media and Changing Communication Patterns*, 5(1) Global Media Journal-Indian Edition (2014) available at: http://www.caluniv.ac.in/global-media-journal/ARTICLE-JUNE-2014/A_3.pdf (last visited Aug 28, 2016).

¹¹Megha Gaur, *Role of Media in Public Opinion Formation*, 2(2) Masters International Journal of Management Research and Development (2014), available at: <http://docplayer.net/22930708-Role-of-media-in-public-opinion-formation.html> (last visited Aug 01, 2016).

world, newspapers, corporations, governments, or other types of leading organizations simply had to give out information, and people would consume it by reading or looking at it. But this seemingly tried-and-true method is transforming. In other words the present generation is just not relying on traditional media to get latest information and news. Today's audiences expect to be able to choose what they read, and most believe they should be able to contribute content and opinions, too. This shift, sometimes called the social media revolution, is not the death of journalism as America always knew it; it's the birth of a democratic movement that emphasises some of journalism's key factors: transparency, honesty, and giving a voice to the person who doesn't have one. The major reason of sudden rise of social media is that the mainstream media i.e. newspapers and electronic media have been currently facing a kind of credibility crisis as they have been suffering with profitable syndrome i.e. how to make money in in the digital age. The said crisis is man-made and natural due to sidelining the journalistic ethos in the race of profit-making media houses. The main advantage of social media is that anybody can run his own news through hashtag. The direct reporting through smartphone is more authentic and credible than traditional newspaper briefing mostly inadequate and curtailed. It is admitted that there are some factors that are contributing to the social disharmony through social media but present generation is educated enough to differentiate between factual news and false propaganda.

III. Social Media in Indian Scenario: Abrupt Ascend

With the progression of social media revolution, India too could not remain isolated from its influence. Presently, about 300 million¹² people have been using different forms of social media. The way social media has transformed the way of communication have received a lot of media attention in the past few years. In India, no other media has befallen as well-liked in such a short span of period as social media. The applause of this terrific feat goes to user friendly features of social media that facilitates them to share and contribute of any post or video they like.¹³ Moreover, it has the potential to fundamentally change the character of our social lives, both on an interpersonal and a community level. Sometimes, such tools are misused by a person which leads to interference into one's privacy.¹⁴ Thus it is almost impossible to remain aloof from these forms of communication by the present generation as it is nascent quicker with the availability of cheaper broadband

¹² 11th Annual Report, Internet and Mobile Association of India (IAMAI) 2014-15 Available at: http://www.iamai.in/sites/default/files/annual_report/AnnualReport2014-15.pdf (last visited July 25, 2016).

¹³ *Supra* note 11.

¹⁴ Trisha Dowerah Baruah, *Effectiveness of Social Media as a Tool of Communication and its Potential for Technology Enabled Connections: A Micro-Level Study*, 2(5) International Journal of Scientific and Research Publications (2012), available at: http://www.ijsrp.org/research_paper_may2012/ijsrp-may-2012-24.pdf (last visited Aug 01, 2016).

or Wi-Fi connection and smartphone at very low prices.¹⁵ The expansion of this above form of the social media in India is basically due to the thriving economy, inexpensive latest technology, telecom expansion, and internet expansion in the recent year and it also had a wide impact on the inter-personal and intra-personal communication, group and public communication, and mass communication. It can be seen that most of the established newspapers, TV and radio channels observe the content of favored social networking sites like Facebook and Twitter to have the newest update of incident around the world.¹⁶

Apart from this, social media in India is *pro tem* as a “watchdog of watchdogs” in the sense that when something contentious does not find room in the traditional media, then public highlights it on social media sites and as a result of which the traditional media has to cover the issue under the public pressure. Such control upon conventional media from the public side should be welcomed as public reaction is not based on corporate compulsions but the real facts and events happening in our society.¹⁷ It also shows that social media uses the “wisdom of crowd” to connect information in a collaborative manner. These characteristic denote the paradigm shift from Web 1.0 technologies that enabled simple information sharing and basic two-way transactions to Web 2.0- where literally everyone can be a user as well as generator of content.¹⁸

IV. Social Media and its Perils: An Explanation

Since the rise of internet freedom in the early 1990s, the Indian networked population has grown from millions to billions.¹⁹ Over the period social media have become a fact of life for civil society worldwide, involving many actors-citizens, groups, political parties, government and even certain dissent groups viz. extremists, terrorists and separatists’ organizations. The crucial issue is despite considerable benefits how does the ubiquity of social media affect India’s interest, how should the Indian government and its policies to respond it? The distressing situation is that government has no control to restrain social media sites except the complete shutdown of internet. Presently, different groups who have strong anti-India stand too working through social media spearheaded the hate campaign against India. Hence the medium of social media has regularly been employed by adversaries-state as well as non-state actors- to create misinformation, fictitious narratives, hate propaganda, inciting fear, false alarm, infuse mutual distrust, which started to impact the various facet of human life and day to day functioning of societies,

¹⁵ *Supra* note 11.

¹⁶ *Id.*

¹⁷ *Id.*

¹⁸ Sisira Neti, *Social Media and Its Role in Marketing*, 1(2) International Journal of Enterprise Computing and Business System (2011), available at: <http://www.ijecbs.com/July2011/13.pdf> (last visited July 25, 2016).

¹⁹ *Supra* note 13.

which further destabilizes national integration and security of India.²⁰ The succinct analysis of sundry social media menace is herewith discussed below:-

- a) Virtual Violence on Social Media through Cyber-Trolling:** The notion of virtual violence in form of cyber-trolling is often enacted against dissent, voices and spreading communalism on the social media platform, such as Facebook, Twitter, WhatsApp and akin social networking sites, as means of limiting or undermining freedom of speech and expression in the virtual space. It is a form of targeted gender and symbolic violence which can be viewed as “silence planned tactics”²¹ against those individuals who disagree (whether physically, mentally, orally, writing acts) with the ideologies of the present government. Surprisingly the major victims of social media trolling are vulnerable section minorities, women and marginalized sections of society, who just exposed the real perpetrators of cyber-criminal world. It also becomes brutal, when involving the online threats of sexual violence, gang rape using highly filthy languages aiming to offend the dignity of women.²² In 2014, the cases registered for cyber trolling in Mumbai has tremendously increased to 133 from 33 in 2013, as founded in reply to an application filed against police authorities under Right to Information Act 2005.²³ Trolling leaves its victims in a powerless position as freedom of expression for perpetrator are defended by the so called BJPs social media army. The book “*I Am a Troll: Inside the Secrete World of the BJP’s Social Media Army*” which was authored by Swati Chaturvedi, plainly exposed the horrific world of social media campaign being run by BJP wherein paid trolls officially propagate their hate campaigns, that too from plush political offices. In an interview to the caravan magazine, Sadhavi Khosla, a former BJP volunteer depict the ‘dark side’ of social media and uncovered the hidden agenda of the National Digital Operations Centre (i.e. the BJP Digital Campaigning Wing) in spreading hatred and communal disharmony through social media. She

²⁰ Kirti Singh, “Fake News and Social Media Nexus: A New Challenge for National Security” Centre for Air Power Studies, *available at:* http://www.academia.edu/36741642/FAKE_NEWS_and_SOCIAL_MEDIA_NEXUS_A_NEW_CHALLENGE_FOR_NATIONAL_SECURITY (last visited June 06, 2018).

²¹ Karan Lumsden and Heather M Morgan, *Cyber Trolling as Symbolic Violence: Deconstructing Gender Abuse Online* *available at:* https://www.researchgate.net/publication/317551298_Cyber-trolling_as_symbolic_violence_deconstructing_gendered_abuse_online (last visited June 06, 2018).

²² L. P. Sheridan and T. Grant, *Is Cyberstalking Different?*, 13(6) *Psychology, Crimes and Law* 627-640, (2007).

²³ Prasant Mali, *Troll Trolling and Law in India*, Academia, (2015) *available at:* http://www.academia.edu/10237949/Troll_Trolling_and_Law_in_India_By_Prashant_Mali (last visited May 02, 2016).

further said that BJP's IT Cell ran targeted campaign over platform such as WhatsApp and Twitter against those who were pretty critical about present regime.²⁴ These trolls have not spared even some famous journalists e.g. Rajdeep Sardesai, Barkha Dutt, Siddharth Varadrajan, Nikhil Waghle and Rana Ayyub.²⁵ Recently, UN Human Rights wing issued an advisory to the Indian authorities to take appropriate measure to protect senior journalist Rana Ayyub, as she has been getting death threats following an online hate campaign.²⁶ Apart from that, NDTV news anchor Ravish Kumar too have been subjected to frequency of abusive calls and deaths threats via social media, that he has received since 2015 have increase manifold in last two months i.e. April and May 2018.²⁷ However, there is some ray of hope to contain online criminal activities of trolls as recently the Hon'ble High Court of Punjab and Haryana has held that propaganda and incitement to violence on social media is equivalent to collecting men for waging war against the Government of India, as defined under IPC section 122. High Court made this observation while ruling against the bail plea of Arvinder Singh, member of terror group Babar Khalsa, who was arrested in May 2016.²⁸

- b) Disseminate Communal Hatred through Fake News:** The dispersal of communal stuff under the gloom of fake news and hate propaganda on social media is emerging as one of the new challenges towards the democratic principles and secular ethos of the nation. The social media users are recurrently exposed to a surfeit of fake news concerning communal hatred propaganda, which they often believe as real news and without authenticate the same they share it on their social media platforms, which undoubtedly had a great repercussions on the behaviour of individuals and mould their minds towards schism in the society. This gloomy side of social media, which act as powerful and swift vehicle to circulate the

²⁴ Kedar Nagarajan, "I Am Against Any Kind of Hatred Being Spread: Sadhvi Khosla, A Former BJP Volunteer, Discusses the Party's Social Media Campaign, Online Trolls and Why She Left" *The Caravan Magazine* available at: <http://www.caravanmagazine.in/vantage/sadhvi-khosla-bjp-social-media-trolls> (Last visited on July 07, 2018).

²⁵ Sunetra Choudhary, *In War Against Trolls, Maneka Gandhi Sets Up Cyber Cell*, NDTV, (July 08, 2016), available at: <http://www.ndtv.com/india-news/in-war-against-trolls-maneka-gandhi-sets-up-cyber-cell-1429411> (last visited July 18, 2016).

²⁶ For details, please see <https://www.firstpost.com/india/un-experts-call-on-indian-government-to-protect-journalist-rana-ayyub-from-online-hate-campaign-4481595.html> (last visited on June 06, 2018)

²⁷ See, NDTV Ravish Kumar says death threat have increased, *The Hindu*, May 28, 2018 available at: <http://www.thehindu.com/news/national/ntdvs-ravish-kumar-says-death-threats-have-increased/article23989047.ece> (last visited on June 06, 2018).

²⁸ Sofi Ahsan, *Incitement To Violence, Propaganda On Social Media Akin To Investigate War Against Govt.: High Court*, *The Indian Express* New Delhi edn. July 06, 2018.

fake news, has been misused by anti-social elements for disturbing communal harmony. The Muzaffarnagar riot of 2013 incident has shown how social media can be manipulated so as to increase and escalate communal tensions and violence.²⁹ The mass exodus of northeastern student from Bangalore in 2015, shows how digital sphere of social media groups circulating and promoting false information to hoodwinking the consumer of that information. It is been witnessing that in 2015, a FIR has been registered against Ritu Rathur, under section 505(1)(c)³⁰ of Indian Penal Code, 1860 for 'spreading rumors' to disturb communal harmony through sensational and controversial posts on social media.³¹ The plague of fake news on social media is so perilous that in 2012; a viral video of violence against Muslims in Burma has spontaneously triggered violence in Ahmadabad. Likewise the rumors on Twitter maliciously tinted Dr. Pankaj Narang murder, as a communal incident and astonishingly the dangerous falsehoods continued even after the police and press, continuously avowed that there was no communal slant to the murder.³² Hence the danger of fake news is a product of a human mind, not a machine or software, and the answer lies with the human themselves, by speeding up the counter narrative in order to bulldoze the impact of fake news through legislation, indeed needs a practical and holistic approach.³³

- c) **Anti-India Propaganda through Social Media:** Since the advancement of new social media revolution, it has been observed that the maximum number of social networking sites have turned out as effective and non-risky medium for India baiters to pour out their venom against the nation. The sites have been ruthlessly misused in Kashmir and North Eastern states to unleash disinformation campaign by twisting the facts. The main idea is to mobilize the international support for so-called 'independence' movement and to malign the Indian state and security forces for violating human rights of the citizens. Since these sites have wide outreach, the

²⁹ *Supra* note 8.

³⁰ Section 505(1)(c) of Indian Penal Code, 1860 (45 of 1860): "whoever makes, publishes or circulates any statement, rumors or reports with intent to incite, or which is likely to incite, any class or community of persons to commit any offence against any other class or community shall be punished with imprisonment which may be extent to three years or with fine or with both".

³¹ Mohammad Ali, *Ritu Rathaur book for 'spreading rumors'*, *The Hindu* Oct 05, 2015), available at: <http://www.thehindu.com/news/national/other-states/ritu-rathaur-booked-for-spreading-rumours/article7723408.ece> (last visited July 27, 2016).

³² Scroll Staff, *How Rumors on Twitter Maliciously Painted the Delhi Murder as a Communal Incident*, Scroll. In March 26, 2016 available at: <http://scroll.in/article/805717/how-rumours-on-twitter-maliciously-painted-the-delhi-dentist-murder-as-a-communal-in> (last visited Aug 02, 2016).

³³ *Supra* note 21.

vicious propaganda is being undertaken in an organized manner. If reports are to be believed, most of the sites remain the handiwork of ISI of Pakistan. Their stooges in Kashmir and around the world have been systematically painting India as a demon. The role of social media in Kashmir and other parts of the country has been devastating in promoting hatred and spreading anti-national sentiment.³⁴ Undoubtedly, care must be taken as we travel down the information in superhighway, but terrorization of what ahead should not force us into the breakdown lane.

V. Tackling Social Media related Cyber Crimes: Some Progressive Steps

Social media is used as a means for communication and interaction among people across the globe, but the cyber criminals are using it as a medium to commit offences related to privacy, defamation, and misrepresentation of identity or cheating by personation, obscenity, sending offensive messages and some time against state i.e. promoting anti-national activities, spread hate so on and so forth. Many people have fallen prey to these offences due to lack of awareness and overuse of these social networking websites. The fear of lagging behind in this technology race has led to the increase in the statistics of these crimes. According to Pavan Duggal, Cyber Lawyer and Advocate with Supreme Court of India, for every 500 instances of cyber crimes that takes place in India, only 50 are reported and out of that 50, only one is registered as an FIR or criminal case.³⁵ Giving an insight into the reasons for low reporting, Nand Kumar Sarvade, Former Director, Cyber Security and Compliance at NASSCOM,³⁶ argue that very often, people are not aware whether an incident is a cyber-crime or not; there is also lack of awareness on where to lodge a complaint or another issue is whether the police will understand the complainant's grievances or not.³⁷

³⁴Dost Khan, *Social Media emerges New Weapon of India Bashers in Kashmir*, State Times, Nov 02, 2015) available at: <http://www.news.statetimes.in> (last visited July 28, 2016).

³⁵M. Neela Malar, *Impact of Cyber Crimes on Social Networking Pattern of Girls*, 1(1) International Journal of Internet of Things 9-15, (2012) available at: <http://www.sapub.org/global/showpaperpdf.aspx?doi=10.5923/j.ijit.20120101.02> (last visited Aug 02, 2016).

³⁶The National Association of Software and Services Companies (NASSCOM) is a trade association of Indian Information Technology (IT) and Business Process Outsourcing (BPO) industry. Established in 1988, NASSCOM is a non-profit organization registered under Indian Society Act, 1860.

The main vision of NASSCOM is to help the IT and IT enabled products and services industry in India to be a trustworthy, respected, innovative and society friendly industry in the world. Currently, Mr. R Chandrashekar is the President of NASSCOM.

³⁷*Supra* note 31.

So it can be stated that, one of the most important issues concerning cyberspace today is that of cyber-crime through the social media. At the outset cyber-crime can be explained as any criminal violation or an unlawful act taking place on the computer. Cyber-crimes refer to all the activities done with criminal intent in cyberspace. The Information Technology Act, 2000³⁸ does not explicitly define the term cybercrime but it has discussed the issues of cyber-crimes in two broad groups. One is Chapter 9 which deals with penalties and adjudications under section 43 to 47 and another is chapter 11 which deals with offences under sections 65 to 75.³⁹ Cyber-crime through social media is basically divided into 3 major categories i.e. cyber-crimes against persons, property and Government. Cyber-crimes committed against persons include various crimes like cyber stalking, cyber bullying, cyber defamation, cyber forgery and frauds, infringement of privacy, and identity theft. The second categories of cyber-crimes are that of cyber-crimes against all forms of property. These crimes include unauthorized computer trespassing through cyber space, computer vandalism, transmission of harmful programs, and unauthorized possession of computerized information viz. hacking and cracking are amongst the gravest cyber-crimes known till date. The third category of cyber-crimes relate to cyber-crimes against Government. Cyber terrorism is one distinct kind of crime in this category. It marked itself into the so called crime of terrorism when an individual “cracks” into a government or military maintained website.⁴⁰

So far as the issue of tackling the social media related crimes, the government has not come forward with any concrete plan to resolve the pernicious problem of online abuse against women by trolls. In this context, Mr. Arun Jaitley, Minister of Information and Broadcasting (also holding charge of finance and corporate affairs), has expressed his helplessness to contain the rising graph of online abuse by trolls. He stated the government position in the following words, “we do not have control on online trolling and one has to learn to live with it as censorship is

³⁸ At present many legal provisions recognize paper based records and documents which should bear signature. Since electronic commerce eliminate the need for legal changes. The United Nations Commission on International Trade Law (UNCITRAL) adopted a Model Law on Electronic Commerce in 1996. The General Assembly of United Nations by its Resolution No. 51/162, dated 30th January, 1997, recommended that all States should give favorable consideration to all said Model Law when they enact or revise their laws. The Model law provides for equal legal treatment of users of electronic communication and paper based communication. As India being signatory to it has to revise its laws as per the said Model Law. Keeping in view the urgent need to bring suitable amendments in the existing laws to facilitate e-commerce and with a view to facilitate Electronic Governance, the Information and Technology Bill was introduced in the Parliament and received the assent of the President on 9th June 2000 as w.e.f. 17.10.2000.

³⁹ Dr. Abhijeet Deb, *Cyber Crime and Judicial Response in India*, 3(2) Indian Journal of Law and Justice 106, (2012).

⁴⁰ Harpreet Kaur, *Cyber Law: an Overview*, 8(1) Nyaya Deep 87-89, (2007).

not possible on it, by this he suggested that either to digest or just ignored it”⁴¹ which indicate the insensitivity of the government and also shows how the government is serious to contain the online abuse through social media. Remarkably, his cabinet colleague on the other side, Ms. Maneka Gandhi, has firmly believed that online abuse by troll should be treated as violence against the women and punitive measures needs to be taken.⁴² Taking a positive note on legitimate and longstanding demand to initiate punitive measures to contain online trolling and targeted misogyny that is widespread in social media, the Ministry of Women and Child Development, Govt. of India has recently established a dedicated “Cyber Cell” in her ministry which empowered to refer the complaint to concern police station to investigate the matter further with recommendatory remarks and further action thereof. Through this mechanism, the complainant can send her complaint against bullying, stalking, or abusive behavior directed against them online to the Cyber Cell and can redress her grievances. Therefore, in view of above discussion it can safely be stated that despite little efforts of the government, the success of cyber cell constituted by the government is yet to be assessed. But the task of elimination of social media related crimes needs a balancing and determined will as the perils of social media in day to day lives are reaching to an unprecedented level.

VI. Law and Policy to Tackle the Cyber Crimes: An Assessment

In numerous occasions, the existing legal system and framework have revealed meagerness while tackling with emerging cyber-crimes done through social media. Though social media has given people a platform to air their views but it has also left them vulnerable to slander, character assassination, intimidation and defamation. The underlining principle of “freedom of speech and expression” denote “right to hold opinion” which does not mean right to bully, intimidate, or harass others in a public setting, and preventing them from speaking. However, while putting in place the mechanisms to address such harassment online, it is entirely possible to overstep the boundaries and introduce a law that is harmful to free speech. That is exactly what Section 66A⁴³ of the Information Technology Act, 2000 was, until it was

⁴¹Anindita Sanyal, Ignore or digest, Says Arun Jaitley on Online Trolling, NDTV, (May 20, 2016) available at: <http://www.ndtv.com/india-news/ignore-or-digest-says-arun-jaitley-on-online-trolling-1408058> (last visited Aug 02, 2016).

⁴²Sunetra Choudhury, *Online Attacks On Women To Be Treated As Violence: Maneka Gandhi to NDTV*, NDTV, May 18, 2016 available at: <http://www.ndtv.com/india-news/online-trolling-against-women-will-be-considered-violence-maneka-gandhi-1407271> (last visited Aug 04, 2016).

⁴³Section 66A of the Information Technology Act, 2000 (21 of 2000) read as “Punishment for sending offensive messages through communication service, etc”.

eventually struck down⁴⁴ by the Supreme Court in *Shreya Singhal v Union of India*⁴⁵. Section 66A ostensibly intended to deal with messages of a “grossly offensive” or “menacing character,” or circulation of false information with the intent to cause “annoyance, inconvenience, danger, obstruction, insult, injury.”⁴⁶ But, it was so poorly drafted, and with such few procedural safeguards, that it became a tool abused by those in positions of power to stifle dissent or even mild criticism. Section 66A was, thus, invoked against two young women who had criticised the shutdown of Mumbai for Shiv Sena founder Bal Thackeray’s funeral. It was invoked against two men who had circulated an email that incorrectly labelled a mansion as belonging to Kerala Chief Minister Pinarayi Vijayan. It was also used against a professor of Jadavpur University who circulated an email of West Bengal Chief Minister Mamata Banerjee⁴⁷. These are among the many instances where Section 66A was used simply to stifle dissent and debate in a manner that could not have been done were any of these instances related to offline speech. Beside this, Section 66C and 66D of The Information Technology Act, 2000 is purportedly attracted when imposters use the unique identification features of the real person to create a fake profile in order to commit several social media related cyber-crimes. Section 67 of The Information Technology Act, 2000 affirmed that whoever publishes or transmits obscene material in electronic form, will be prosecuted with imprisonment of 3 to 5 years with fine or which may extend to five to ten lakh rupees. In this context the case of Suhas Katti⁴⁸ is noteworthy to mention herein, the conviction was achieved successfully within a relatively quick time of 7 months from the filing of the FIR under section 67 of The Information Technology Act, 2000 along with 469 and 509 of Indian Penal Code, 1860 before the Hon’ble Additional Chief Metropolitan Magistrate, Egmore and moreover it was the first case linking conviction under The Information Technology Act, 2000 allied to the posting of obscene and slanderous messages on the social media. Accordingly the Section 69 and 69A of The Information

⁴⁴ A Division bench of Supreme Court consisting of justices J. Chelameswar and R.F. Nariman decided on 24th March, 2015 in *Shreya Singhal v. Union of India* to struck down section 66A of Information Act, 2000 (21 of 2000) as unconstitutional, as it is violative of Article 19(1)(a) related to freedom of speech and expressions. Now comments on social networking sites will not be offensive unless they came under the provisions of the Indian Penal Code, 1860 (45 of 1860).

⁴⁵ Writ Petition (Criminal) No. 167 of 2012.

⁴⁶ Section 66A, The Information Technology Act, 2000 (21 of 2000).

⁴⁷ Express News Service, *Section 66A: Seven Instances of Alleged Abuse on Social Media*, The Indian Express, Mar 24, 2015 available at: <http://indianexpress.com/article/india/india-others/section-66-a-instances-of-alleged-abuse-on-social-media/> (last visited Aug 05, 2016).

⁴⁸ *State of Tamil Nadu v. Suhaskatti*, 4680 of 2004 Criminal Complaint; and Judgment delivered by Ld. Additional Chief Metropolitan Magistrate, Egmore on 5.11.2004.

Technology Act, 2000 is also more important as it allows government to intercept, monitor and block websites for public access through any computer resources in context of preserving public order and preventing incitement. It is pertinent to note that section 78 of the IT Act, 2000 empowers police inspector to investigate the cases falling under this Act.

The way in which people are generally harassed through cyber bullying, revenge porn, trolling, obscene text messages, virtual mobbing and so on, and adding that these offenders are punishable under the relevant provisions of Indian Penal Code, 1860. The Hon'ble Supreme Court of India has also reiterated in numerous cases that "right to privacy" is a sacred principle under Article 21 of the Constitution of India;⁴⁹ however, its application vis-à-vis internet content has not yet been directly clarified by judicial rulings. Meanwhile, the Article 19(2) of the Constitution of India had doggedly stated that nothing in 19(1)(a)⁵⁰ shall affect the operation of any existing law on imposing reasonable restrictions on the exercise of the right conferred by the said sub-clause in the interest of the sovereignty and integrity of India, the security of the State, public order, decency or morality, defamation or incitement to an offence.⁵¹ In practice, however, the enforcement agencies file the cases invoking the relevant sections from Indian Penal Code 1860 in addition those corresponding with the Information Technology Act, 2000 like offences under Indian Penal Code, 1860 as 463⁵², 464⁵³, 468⁵⁴, and 469⁵⁵ read with the

⁴⁹ Article 21 of The Constitution of India, 1950 guaranteed "Protection of Life and Personal Liberty" which means that No person shall be deprived of his life or personal liberty except according to procedure established by law.

⁵⁰ Article 19(1) (a) of The Constitution of India, 1950 guaranteed that "All citizen shall have the right to freedom of speech and expression".

⁵¹ V. N. Shukla, *Constitution of India* 117 (M. P. Singh ed., 11th ed. 2008).

⁵² Section 463 of the Indian Penal Code, 1860 (45 of 1860) defines "Forgery" as "whoever makes any..... false electronic records with intent to cause damage or injury to public or any persons..... with the intent to commit any fraud, commits forgery".

⁵³ Section 464 of Indian Penal Code, 1860 (45 of 1860): "Making of False Document: a person is said to make a false electronic record who dishonestly and fraudulently..... transmit or alter any electronic records..... with the intention of causing it to be that such electronic record was made by the authority of person by whom he knows".

⁵⁴ Section 468 of Indian Penal Code, 1860 (45 of 1860) "Forgery for Purpose of Cheating: whoever commits forgery, intending that the electronic record used for the purpose of cheating shall be punished with imprisonment of either description for the term which may be extent to seven years and shall also be liable to fine".

⁵⁵ Section 469 of Indian Penal Code, 1860 (45 of 1860) "Forgery for Purpose of Harming Reputation: whoever commits forgery.... intending that the electronic records forged shall harm the reputation shall be punished with imprisonment of description for a term which may extend to three years and shall also be liable to fine".

Information Technology Act, 2000 Sections 43⁵⁶ and 66⁵⁷ to ensure the evidence or punishment stated at least in either of the legislation can be brought about easily. In addition to this, Section 507⁵⁸, 499⁵⁹, 509⁶⁰ and 354 A and B⁶¹ of Indian Penal Code, 1860 allows the victim to lodge a complaint without knowing the true identity of the harasser. It also covers the proliferation of trolls in the virtual world. Recently the offence of Stalking under section 354D has been inserted into Indian Penal Code, 1860 by the Criminal Law Amendment Act, 2013 in which the offender in a first conviction punishes with 3 years along with fine and in second conviction punishes with five years of punishment along with fine.

In this context, the admissibility of electronic records as evidence is enshrined in Section 65B⁶² of Indian Evidence Act, 1872 assumes significance in the area of social media related crime. This is a landmark piece of legislation in the area of evidences produced from a computer or electronic device. Any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer shall be treated like

⁵⁶ Section 43 of The Information Technology Act, 2000 (21 of 2000), “Penalty and compensation for damage to computer, computer system etc.”

⁵⁷ Section 66 of The Information Technology Act, 2000 (21 of 2000) “Computer related offences: if any persons dishonestly or fraudulently does any act referred to in section 43 shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or both”.

⁵⁸ Section 507 of Indian Penal Code, 1860 (45 of 1860) “Criminal intimidation by an anonymous communication”

⁵⁹ Section 499 of Indian Penal Code, 1860 (45 of 1860) “Defamation: whoever by words either spoken or intended to be read.....make or publishes any imputation concerning any person intending to harm, the reputation of such person, is said to defame the person”.

⁶⁰ Section 509 of Indian Penal Code, 1860 (45 of 1860) “Word, Gesture or act intended to insult the modesty of a women: whoever intending to insult the modesty of any women, utters any word, make any sound or gesture or exhibits any object shall be seen by such women or intrudes upon the privacy of such women shall be punished with simple imprisonment for a term which may extend to three years and also with fine”.

⁶¹ Section 354A of Indian Penal Code, 1860 (45 of 1860) “Sexual harassment and punishment for sexual harassment: any act which....., demand or request for sexual favours or showing pornography against the will of a women or making sexual coloured remarks shall be guilty of the offence of sexual harassment and punished with rigorous imprisonment for a term which may extend to three years or with fine or both. Here sadly no punishment has been prescribed for making sexual coloured remarks”. And Section 354 B deal with “

Assault or use of criminal force to women with intent to disrobe”....shall be punished for the term of three to seven years along with fine”.

⁶² Section 65B of The Evidence Act, 1872 (1 of 1872) deals with “Admissibility of electronic records” which has been inserted by The Information Technology Act, 2000 (21 of 2000).

a document, without further proof or production of the original, if the conditions like these are satisfied: (a) the computer output containing the information was produced by the computer during the period over which the computer was used regularly by lawful persons (b) the information ...derived was regularly fed into the computer in the ordinary course of the said activities; (c) throughout the material part of the said period, the computer was operating properly and a certificate signed by a person responsible etc.

Beside the above mentioned framework, the Information and Broadcasting Ministry has planned to expand social media analytics wing of the ministry which currently scrutinises posts on platforms like Twitter and Facebook and generates reports to the Prime Minister's Office, the National Security Advisor's Office and various intelligence bureaus, aside from ministries including home affairs, external affairs and defence.⁶³ But, to fight against these social media related cyber criminals the law enforcement agencies (including the Cyber Cell, Central Bureau of Investigation, National Investigation Agency etc.) will have to enhance their high technology capabilities, including personnel recruitment and retention programmes.⁶⁴ In order to deal with this problem, the Computer Emergency Response Team – India (CERT - In) has been set up which is operational as the national agency for cyber incidents. It operates a 24x7 Incident Response Help Desk to help users in responding to cyber security incidents. It has been issuing regular alerts on cyber security threats and advises countermeasures to prevent attacks. But, unfortunately at present there is no organization in India that can categorically scrutinize trolls or comments posted through social media. If anyone moved a complaint to police or other agencies, then police has the power to approach the court to pass an order directing “CERT-In and Google” to obliterate a set of derogatory blogs or comments. The Police is also empowered to take such an order from the Court as per section 69A of the Information Technology Act, 2000. This particular section also authorises to issue directions for blocking public access of any information through any computer resource. Regrettably, the existing laws are not competent enough and crippled in cases where the person is based on abroad, and not within Indian jurisdiction. The Facebook shares details of its users only in case of national interest like terrorism etc.⁶⁵ Hence it is the high time that law enforcement agencies and supportive groups should come forward to empower and protect individuals from falling prey to these cyber-crimes and

⁶³Government to Monitor Social Media 24X7 to Counter Negative Comments, Blogs, *Hindustan Times* (Feb 24, 2016) available at: <http://www.hindustantimes.com/india/govt-to-monitor-social-media-24x7-to-counter-negative-comments-blogs/story> (last visited Aug 04, 2016).

⁶⁴Vivek. Y. Dhupdale, *Cyber Crimes in India and the Challenges Ahead*, 1(2) Indian Journal of Law and Justice 108, (2010).

⁶⁵ *Supra* note 23.

other online crime committed through social media. Undoubtedly the major challenges to combat social media related cyber-crime through law, policy and practice is that despite having the sufficient national legal framework, the respective authorities have not been able to implement it on the ground level so as to minimize the threat of cyber-crimes which is frequently knocked through different medium of social media in the newer form of threat like online trolling, imitating/fake account, instigating riots, flash mobs, and stern vulnerabilities like victimization of women continue to surface.

VII. Concluding Remarks

Despite mix records, the social media have become coordinating tools for the contemporary digitally equipped societies, as the social media revolution has wrought a new kind of social order by strengthening social network but on the other side it has diminished the inter-personal relations.⁶⁶ The social media tools provide web based practices and services that foster engagement. This shows how the integration of technology makes life smooth for people. This colossal churn-out in the virtual world had unquestionably specified the growing supremacy of this web based social media and its brunt on the masses, particularly the new generation which have a direct or indirect impact on it and in the same way it also draws an imprecise conclusions in the form of various rumours which consistently strikes to cause different forms of bullying, flash mobs, and riots through the social media.⁶⁷ The problem is further aggravated due to disproportional growth ratio of cyber laws in relation to curb the peril in social media. The only promising step is to make people aware of their rights and duties to report cyber-crimes happens through social media in times as and when it occur and recognising it as their duty towards the society.

No doubt that the provisions of penal laws and information technology laws seems to be sufficient to deal with almost all types of criminal activities done through social media, but all that it needed is an effective enforcement of the same by the appropriate authorities at the ground level and to suitably modify at regular interval so as to make it more effective and powerful to combat new cyber-crimes committed through social media. In this connection, the judiciary should also play an important role in order to make the application of laws more stringent to check cyber-crime. In order to do this, the regulatory framework governing social

⁶⁶Supra note 11.

⁶⁷Aatish Prashar, *An Analysis of New Media's Role in Mass Movements (With Reference to Anna Hazare's Campaign 'India Against Corruption')*, 2(7) Journal of Mass Communication Journalism, (2012) available at: [http://www.omicsgroup.org/journals/an-analysis-of-new-medias-role-in-mass-movements-\(with-reference-to-anna-hazares-campaign-india-against-corruption\)-2165-7912.1000118.pdf](http://www.omicsgroup.org/journals/an-analysis-of-new-medias-role-in-mass-movements-(with-reference-to-anna-hazares-campaign-india-against-corruption)-2165-7912.1000118.pdf) (last visited July 27, 2016).

networking sites should also regularly be reviewed. At last, to some extent the Parliament of India has attempted to cover many crimes under The Information Technology Act, 2000 by enacting the Information Technology Amendment Act, 2008, but even then it would be incomplete as new and new cyber-crimes through social media are being sinister at regular interval and it is undeniably one of the greatest challenge to the criminal justice system of India.⁶⁸

⁶⁸*Supra* note 60 at p. 114.