Page 556 - 574 **DOI:** *https://doij.org/10.10000/IJLSI.111342*

INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION

[ISSN 2581-9453]

Volume 4 | Issue 1

2022

Social Media: Regulatory Challenges in Present Scenario

MAHESH KUMAR MEENA[1] AND DR GOVIND SINGH RAJPUROHIT[2]

ABSTRACT

The present study deals with the regulation of that communication medium, which has pushed the speed of communication into a new era. Internet, which was impacting many things, has revolutionized the information era with the introduction of social media. The development of the Internet was in many ways radically different from the advent of any previous sets of innovative communications technologies. It brought new features that not only broke down a host of boundaries between forms of personal and mass communication but also overturned a mass media model that had endured for centuries. The current communications revolution gave content recipients the opportunity to be their own content producers. From simple beginnings, such as the ability to post text or images on personal web pages, user-generated content has become an extraordinary global flood of mixed original and reused content that appears in a multitude of forms and manners. These now notably include video posting, social networking, blogging, tweeting etc. Collectively it has been termed social media. Social media exhibits unique characteristics when compared to 'traditional' media forms. Its speed and scope mean that once content is published, it is available instantaneously to a potentially global audience—the use of social media spans across all professions and ages. Social media is not only changing the way we communicate with friends but dramatically changing the way we work as well.

I. INTRODUCTION

The greatest gift to mankind from the scientific community has been the invention of information technology and the associated communication technologies in the last decade of the 20th century. This technology is of such monumental importance that it has been rightly termed as InfoTech revolution. These technologies have put the entire human civilization on a fast forward mode by introducing unprecedented speed in information & communication via social media.[3] Social media, in particular, has greatly impacted political dynamics on a global scale by enabling users to express themselves publicly in

[1] Author is a Research Scholar at Department of Law, University of Rajasthan, India.
[2] Author is an Associate Professor at University of Rajasthan, India.
[3] Ajay Yadav, 'The Legal Complexities of The Digital World' (2012) 18 Lex Witness 1

 [ISSN 2581-9453]

ways previously unavailable to them[4]. This very shift in communicative power has spawned greater efforts to restrict and control the use of the Internet for information and communication on political, moral, cultural, security and other grounds[5]. This effort of controlling the Internet has led to legal and regulatory initiatives to mitigate risks associated with this new medium, ranging from the privacy of users, intellectual property, national security to frauds, pornography and hacking. Regulatory challenges of social media can be broadly addressed under two heads, namely:

- Legal Regulation
- Moral and Ethical Regulation in the form of guidelines by various statutory authorities like the election commission.

The chapter heavily focuses on the legal, regulatory regime, which constitutes the bulk of regulation in India & other legal systems. It identifies the various problems generated by social media. The chapter also critically analysis the relevant laws and functioning of regulatory authorities in addressing these problems. An additional narrative discusses the moral and ethical guidelines for regulating social media.

II. PROBLEMS POSED BY SOCIAL MEDIA

The basic architecture of social media platforms provides a unique opportunity for interaction with the common masses, which have resulted in great problems for society. The overthrow of autocracy in the Arab world (mainly Egypt, Libya and Tunisia) has demonstrated that the connectivity of Facebook and Twitter can foment revolution.[6] It showed that while social media may unite those who challenge a system such as Egypt`s where the people`s voice was not heard, they can fragment a society such as the United States where every voice is heard. With its proliferation, social media has generated a lot of complicated social and legal regulatory issues, which are as follows:

(A) Pornography and Obscenity

Sexual depictions which constitute "pornography" or "obscenity" are regulatory concerns by the government in both the offline and online world. Social media, in particular with its fast circulation of obscene and pornographic materials, has made regulation more difficult. Various social media websites like YouTube, MySpace and Facebook are loaded with these materials, causing public authorities to work hard to stop this. The difficulty in regulation was well

[4] Wolfgang Danspeckgruber 'Introduction' in Princeton University' (eds.), '*Social Media Revolutions: All Hype or New Reality?'* (Spring, 2011)

[5] William H. Dutton, Anna Dopatka et. al, 'Report on Freedom of Connection Freedom of Expression: The Changing Legal and Regulatory Ecology Shaping the Internet', UNESCO 2011

[6] The Arab Spring, also known as the Arab Revolution is a revolutionary wave of demonstrations and protests occurring in the Arab world that began on 18 December 2010. The importance of the role of social media on the Arab uprisings has been largely debated. Some say that social media was the main instigator of the uprisings; while others claim that it was merely a tool. Either way, the perception of social media has changed; its role in the uprisings has demonstrated to the world its power. Such information allowed the world to stay updated with the protests and facilitated organizing protests. Nine out of ten Egyptians and Tunisians responded to a poll that they used Facebook to organize protests and spread awareness.

evident when Govt. of India filed a counter before the Supreme Court showing its inability to prevent pornographic and obscene materials on the Internet and social media pages.[7]

Though there is no specific provision in any statute that directly deals with pornography, it has been brought within the purview of Sec. 292, which deals with obscenity in the

Indian Penal Code, 1860 ('IPC'). The Section imposes criminal liability for sale, distribution etc., of obscene material.

Sec. 292 (1) of the Indian Panel Code defines obscenity:

"For the purposes of subsection (2), a book, pamphlet, paper, writing, drawing, painting, representation, figure or any other object, shall be deemed to be obscene if it is lascivious or appeals to the prurient interest or if its effect, or (where it comprises two or more distinct items) the effect of any one of its items, is if taken as a whole, such as to tend to deprave and corrupt person, who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it."

The definition is very similar to that found in the English Obscene Publications Act, 1959.

Sec. 292 (1) is based on an 1868 English decision (Hicklin Case)[8] where the test for obscenity was laid down by Cockburn, C.J as follows:

"....the test of obscenity is this, whether the tendency of the matter charged as obscenity is to deprave and corrupt those whose minds are open to such immoral influences, and into whose hands a publication of this sort may fall..... it is quite certain that it would suggest to the minds of the young of either sex or even to persons of more advanced years, thoughts of a most impure and libidinous character."

Under Indian law though watching pornography is not illegal but sharing or disseminating obscene content has been made punishable under Sec. 67 of the Information Technology Act. The Act provides a penalty of imprisonment up to three years for publishing and transmitting obscene content. There are stricter rules against child pornography.

Supreme Court in *Ranjit D. Udeshi vs the State of Maharashtra*[44] defined obscenity as 'the quality of being obscene which means offensive to modesty or decency; lewd, filthy and repulsive.' In this case, the court drew a difference between obscenity and pornography. It [9]was held that while pornography denotes writings, pictures etc., intended to arouse sexual desire, obscenity may include publications not intended to do so but which have that tendency. While both offend against public decency and morals, pornography is obscenity in a more aggravated form.

The impact of obscenity laws in India can be seen in the unfettered discretion exercised by the government to ban films, books and other materials on the pretext of immoral or

[7] *Kamlesh Vaswani v. Union of India* [W.P.(C). No. 177 of 2013 (Supreme Court)], This writ petition was filed before the Supreme Court under Article 32 of the Constitution of India challenging Sections 66, 67, 69, 71, 72, 75, 79, 80 and 85 of the Information Technology Act, 2000 as unconstitutional on the ground that they are inefficient in tackling the rampant availability of pornographic material in India.

[8] *R.* v. *Hicklin*, (1868) LR 3 QB 360

[9] AIR 1965 SC 881, Para 7, p. 885

objectionable content in the offline world.[10] The approach of the govt. Dealing with obscene content on Internet cannot be equated with the offline world. The transnational character of the Internet provides limited scope and jurisdiction to the govt—authorities in regulation.

In the case of *Kamlesh Vaswani vs Union of India and Others*[11], the petitioner challenged Sections 66, 67, 69, 71, 72, 75, 79, 80 and 85 of the Information Technology Act 2000 as unconstitutional, as they are inefficient in tackling the rampant availability of pornographic material in India. It was demanded by the petitioners that viewing pornography be made a non-bailable offence and pornographic content on the Internet be blocked. Internet Service Providers Association of India (ISPAI) has submitted that they cannot block such sites, and they can only do so only on the direction of the govt. The government submitted that it was struggling to block pornography sites because there were around four crore websites, and when they block one, a new one is created. The govt. has further submitted that it has constituted a Cyber Regulation Advisory Committee under Sec. 88 of the IT Act and one of the briefs assigned to that Committee is with regard to the availability of Pornography on the Internet.

Although there can be no difference of opinion on this point that a state should control the possession and dissemination of obscene and indecent material in its territory, there is no consensus on what type of content should be considered obscene or indecent. The sharpest disagreements lie in the field of nudity and depictions of sexuality. Thus, for example, in Scandinavia, there is a general perception that images of naked adults are entirely acceptable, whereas, in countries whose law or culture is based on strict orthodox principles, such as Saudi Arabia[12], depictions of mere nudity may well be unlawful per se. The states are facing a dilemma as to how to prevent pornographic materials on the Internet, which is transnational in character and possessing powers to defy state framed rules and regulations.

The test for determining the standard of obscenity also varies widely and intensifies the problems in regulating obscenity on the Internet. In the UK, e.g. the definition of obscenity is based on the potential effects of the material on its readers or viewers. In Sec. 1(1) of the Obscene Publications Act 1959, obscenity is defined as follows:

"an article shall be deemed to be obscene if its effect or the effect of any one of its terms is, if

[10] In judging as to whether a particular work is obscene, regard must be had to contemporary mores and national standards. While the Supreme Court in India held Lady Chatterley`s lover to be obscene, in England the jury acquitted the publishers finding that the publication did not fall foul of the obscenity test. This was heralded as a turning point in the fight for literary freedom in UK. Perhaps 'community mores and standards' played a part in the Indian Supreme Court taking a different view from the jury. The test has become somewhat outdated in the context of internet age which has broken down traditional barriers and made publications from across the globe available with the click of a mouse. See; Ram Jethmalani & D S Chopra, 'Media Law' (Second Edition, Vol.-I, Thomson Reuters 2014) 942

[11] (2014) 6 SCC 705 (Till the time of writing of this thesis the case was still pending before the Supreme Court)

[12] Faiza S Ambah, 'An Intruder in the Kingdom' (1995) 21Business Week 40

taken as a whole, such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it."

In the case of *DPP vs A and BC Chewing Gum Ltd,*[13] it was held that the abovementioned definition is not limited to sexually explicit material, and a depiction of violent activity has also been held to tend to deprave or corrupt, and thus to be obscene.

(B) Hate Speech

The subject of hate speech has gained significance with the increase in communal conflagrations mainly caused by communal hate campaigns over social media websites. In North-Eastern Mass Exodus[50], Muzaffar Nagar Riots[51], investigations revealed that hate content circulated by social media had sparked communal clashes. Behind nearly half-a-dozen communal clashes in the country, the reason was the content on social media that insulted or humiliated communities.[52] According to a report[53,] there is a surge of 25 per cent on the growth of "problematic" social networking groups on the Internet. The report was based on "over 10,000 problematic web sites, social networking groups, portals, blogs, chat rooms, videos and hate games on the Internet which promote racial violence, antisemitism, homophobia, hate music and terrorism."[54]

Hate speech can be understood as "antisocial oratory that is intended to encourage persecution against people because of their race, colour, religion, ethnic group, or nationality, and has a substantial likelihood of causing harm".[55] It has several dimensions, e.g. context/content/targets/tone and potential implications of speech.

In a landmark American Judgment, the expression 'hate speech' was described by Justice Murphy as:

"fighting words including those which by their very utterance inflict injury or tend to incite an immediate breach of peace to a person or a group of persons. It has been observed that such utterances are no essential part of any exposition of ideas and are of such slight social value as a step to truth that any benefit that may be derived from them is clearly outweighed by the social interest in order and morality."[14]

In India, hate speech does not find a place under Article 19 (2) of the Constitution and, therefore, does not constitute a specific exception to the freedom of speech and expression under Article 19 (1) (a). However, it is read under other specified exceptions under Article 19 (2) such as 'sovereignty and integrity of India', 'security of the State', 'incitement to the offence ', 'defamation' etc.

Hate propaganda is controlled by a wide range of Indian statutes. Some of the provisions which will apply in hate speech over social media platforms are-

- The Indian Penal Code, 1860 contains provisions that prohibit hate propaganda. Section 153-A penalizes the promotion of

[13] *DPP vs. A and BC Chewing Gum Ltd* (1968) 1 QB 159

[14] *Chaplinsky vs. New Hampshire* (1942) 315 U.S. 568

class hatred. Section 295-A penalizes insults to religion and to religious beliefs. Section 505 makes it a penal offence to incite any class or community against another.

- The Information Technology Act, 2000 contains several provisions which will apply to mitigate hate campaigns on the Internet. It includes Sec. 66-A (now unconstitutional), Sec. 69 etc. [15]

Removing hatred materials on social media pages is a difficult task. It is easy for one to upload but hard for others to take it down. At the user's end, Facebook provides an option that enables a user to mark something as obscene/inflammatory/hateful etc., but it then leaves it, at the uploader`s choice, to remove the hateful content. Even after receiving notification of hateful content, most social media platforms take an unreasonably long time to remove it.

At the international level, The International Network against Cyber Hate (INACH), which was started in 2002, is significantly working against cyberhate. INACH Foundation was established under Dutch law and is seated in Amsterdam. The mission of the foundation is to unite and empower organizations across the globe to promote respect and responsibility by countering cyberhate and raising awareness about online discrimination. INACH works for human rights and mutual respect between internet users.

(C) Identity Theft

Identity theft is another problem generated by social media. Since social media websites generate revenue with targeted advertising based on personal information, they encourage their users to provide maximum personal/professional information. With limited regulatory oversight by government, industry standards or incentives to educate users on security, privacy and identity protection, they are exposed to identity theft. Phishing on social media websites is being used to trick individuals into providing sensitive information that can be used to steal their identities. The trick may be delivered through the networking website's messaging system or through an application designed to look like a harmless quiz, survey, or product giveaway.

Many of the users normally post more than enough information about their personal and work lives. The identity thieves could easily compile that information in order to create a fake profile that looks authentic to people who know the user. A fake profile, similar in appearance to the original one, may provide ample opportunity for a fake profile creator to gain information about the user and his/her friends. And because people often believe that they are sharing the information only with the people they already know, they often publish plenty of details that hackers (fake profile creators) can use to harass.

In India, Information Technology Act provides punishment for identity theft. According to 66-C of the Act-

"Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other

[15] These provisions have been discussed later in this chapter.

person shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh."

There is little evidence that users of social networking sites are taking full measures to protect themselves from identity theft. For example, numerous celebrities have claimed their Twitter accounts have been hacked, and there are various profiles by their name.[16,17] According to the Huffington Post, Bulgarian IT consultant Bogomil Shopov claimed in a blog to have purchased personal information on more than 1 million Facebook users for the frighteningly low price of $5.00. The data reportedly includes users' full names, email addresses and links to their Facebook pages.[18]

(D) Intellectual Property Issues

- Trademark infringement and dilution
- Copyright infringement
- Trade secret disclosure

1) Trade Mark Infringement and Dilution

On social media platforms, users discuss, create content and interact with brands more than ever before. Most often, it results in harmful information about goods/services, which injure a brand mark's strength/reputation/goodwill. A quick search for any major brand name on Facebook will often reveal hundreds of results, which typically include some official results (often labelled 'official') and many unofficial results. The prevalence of various contents/pages in the same name often attempts to tarnish the image of famous brands. For example, news of fried rats served instead of chicken in KFC (a famous non-veg food chain) has made a top trend in Facebook after the California based man complained about this.[19] But later, it was found to be a deliberate attempt to tarnish the KFC image.[20]

There are very few measures to prevent an individual or entity from adopting a user name or sub-domain name that incorporates a third party's registered trade mark. Taking remedial action can often be problematic for the trade mark owner, both from the sheer scale of the problem, to considering issues of adverse publicity that may make a bad situation worse.[21]

[16] Alex Myers, 'After a Twitter hack, 'biebermyballs' becomes a popular hashtag' (daily caller, 28 March, 2012) <http://dailycaller.com/2012/03/28/after-a-twitter-hack-biebermyballs-becomes-a-popular-hashtag/> accessed on 02 May 2013

[17] Facebook has deleted the original profile of Dr. Subramanyam Swamy, when he demanded for removal of fake profiles in his name. See; FP Staff, 'Oops! Facebook accidentally deletes Subramanian Swamy's real account, parody page lives on' (First Post, 19 Dec 2014) <http://www.firstpost.com/living/oopsfacebook-accidentally-deletes-subramanian-swamys-real-account-parody-page-lives-on-1857147.html> accessed on 20 Dec. 2014

[18] Ryan Grenoble, 'Bogomil Shopov, Bulgarian Tech Consultant: 1 Million Users' Private Facebook Data Available Online For $5' (The Huffington Post, 27 Oct. 2012) http://www.huffingtonpost.com/2012/10/26/bogomil-shopov-facebook-data_n_2024133.html accessed on 02 May 2013

[19] Emily Smith, 'Time For A Lawyer': KFC Customer Claims He Was Served Fried Rat' (Opposing Views, June 16, 2015) http://www.opposingviews.com/i/health/kfc-customer-claims-he-received-fried-rat-notchicken accessed on 17 June 2015

[20] Shikha Sharma, 'KFC Fried Rat Story Turns Out to be a Deliberate Attempt to Tarnish KFC Brand' (10pointz, 18 June 2015) <http://www.10pointz.com/internet/kfc-fried-rat-story-turns-deliberate-attempttarnish-kfc-brand/> accessed on 19 June 2015

[21] Georgie Collins, 'UK: Social Media – The IP Angle' (Mondaq, 17 November 2010) <http://www.mondaq.com/x/115844/Trademark/Social+Media+The+IP+Angle> accessed on 14 Nov. 2013

Further, Improper dilution of famous marks is another area of concern regarding trademark infringement. It can be done in two ways:

Blurring – occurs in social media when a user uses a famous mark in connection with other goods/services. For example

- Users may use its postings for advertising luxurious BENTLEY clothing, jewellery
- The owner of the famous BENTLEY mark for automobiles does not want to permit usage of its famous mark on such goods

Garnishment – occurs in social media when a user associates a famous mark with substandard goods/services, which results in damage to a famous mark's reputation and injury to famous mark's goodwill

Apart from it, improper comparative advertising can result in trademark misuse on social media platforms. For example

- False/misleading advertising
- Competitors may use each others' trademarks to compare goods/services to divert sales

In addition, there is a lot of uncertainty over the use of trademarks in social media, and there is uncertainty as to whether current trademark laws and enforcement techniques adequately address the trademark issues presented by social networking sites. Both Twitter and Facebook have trademark policies, but they are not well-drafted when it comes to dealing with trademark infringement issues and the practical enforcement of those policies.

Twitter's trademark policy provides:

"Using a company or business name, logo or other trademark-protected materials in a manner that may mislead or confuse others or be used for financial gain may be considered to be trademark infringement. Accounts with clear INTENT to mislead others will be immediately suspended; even if there is no trademark infringement, attempts to mislead others are tantamount to business impersonation".[22]

Twitter has also adopted a specific impersonation policy, stating that: *"non-parody impersonation is a violation of the Twitter Rules...An account may be guilty of impersonation if it confuses or misleads others –accounts with the clear INTENT to confuse or mislead will be permanently suspended."*[23]

Facebook's IP infringement policy provides:

"Facebook is committed to protecting the intellectual property of third parties. On this page, rights owners will find information regarding how to report copyright and other intellectual property infringements by users posting content on our website".

The practical operation of Twitter's policy was put to the test in a US case.[24] Natural gas

[22] Twitter, 'Trademark Policy'(Trademark, 03 Oct. 2012) <https://support.twitter.com/articles/18367trademark-policy> accessed on 05 May 2014

[23] Twitter, 'Impersonation Policy'(Trademark) <https://support.twitter.com/articles/18366-impersonationpolicy> accessed on 05 May 2014

[24] *Oneok vs Twitter*, 4:09-cv-00597-TCK-TLW, case summary available at

distributor Oneok Inc. sued Twitter, Inc. in Federal Court in Oklahoma for direct and contributory trademark infringement. The petitioner, in this case, claimed that Twitter has wrongfully allowed an unauthorized third party to adopt its username "ONEOK", which was not just its corporate name but also a registered trademark. The unauthorized user-posted tweets about ONEOK, which ONEOK Inc said, were misleading as they had the hallmark of appearing like an official statement from ONEOK Inc. when they were not. ONEOK Inc sought to resolve the issues directly with Twitter and asked Twitter to invoke its trademark policy and terminate or transfer the offending account to them. ONEOK Inc's direct correspondence with Twitter was unsuccessful, but after it issued proceedings for trademark infringement, the account was then transferred to ONEOK Inc.

2) Copyright Infringement

The Copyright Act, 1957(Act No. 14 of 1957) governs the laws & applicable rules related to the subject of copyrights in India. The Copyright Act is compliant with most international conventions and treaties in the field of copyrights. India is a member of the Berne Convention of 1886 (as modified at Paris in 1971), the Universal Copyright Convention of 1951 and the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) Agreement of 1995. Though India is not a member of the Rome Convention of 1961, WIPO Copyrights Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT), the Copyright Act is compliant with it.

Copyright is a right given by the law to the creators of literary, dramatic, musical and artistic works and producers of cinematograph films and sound recordings. In fact, copyright is a bundle of rights that includes rights of reproduction, communication to the public, adaptation and translation of the work. The law permits that; there can be slight variations in the composition of the rights, depending on the work.

The growth of the Internet and the increasing popularity of social media have resulted in an increase in copyright infringement. The multimedia world of the social web is littered with copyright materials, which may or may not be reproduced with the consent of the right owners. Photographs posted to Facebook and Flick, films and music posted to YouTube and materials posted on a blog or on wikis may not always be a matter of copyright protection. Users infringing the rights of copyright owners are liable to be sued for infringement.[67] But there are two challenges in this respect-

- Determining ownership of User Generated Content
- Determining liability

3) Trade Secret Disclosure

Social media and trade-secret protection represent a new frontier – one with relatively little case law but with substantial implications. A customer list is the most notable area in which

<http://www.dmlp.org/threats/oneok-inc-v-twitter#description> accessed on 10 Nov. 2014

social media can affect a company's protection of its confidential information.

Employers often encourage their sales personnel to use LinkedIn or other social media platforms to establish and strengthen relationships with actual and potential customers. But sometimes, this relationship raises a question regarding ownership of that social-media account when salespeople leave and go to a rival company? The sales personnel leave the company with a de facto customer list. It is likely that the names and contact information of some or all of a salesperson's key client relationships will reside on that social media account.[25][26]

Sasqua Group, Inc. vs Courtney[72]

In this case, an Executive search firm sued a former employee for misappropriation of trade secrets. The employee was charged for misappropriating the client list of the company.

The court observed that

"A customer list developed by a business through substantial effort and kept in confidence may be treated as a trade secret provided the information it contains is not otherwise readily ascertainable."

But because the information could be pieced together from LinkedIn and other Internet sites, the court held it did not constitute a trade secret.

PhoneDog LLC vs. Kravitz [27]

In this case, the petitioner claimed that its former employee stole trade secrets by keeping and using a Twitter account opened while the employee worked for PhoneDog. Ex-employee has changed the name from @PhoneDog_Noah to @noahkravitz but continued to use the following built up under prior name. Accepting the arguments of the company as substantial, the court has allowed the case to go further.

Another associated legal issue is the disputes regarding the ownership of social networking accounts after an employee who maintains the account leaves the company? Three lawsuits highlight the challenges an employer may face in seeking to gain control of work-related social media accounts maintained by current or former employees.

Eagle vs Edcomm[28] In the present case, the Linkedin password of the former CEO of a company was changed by the company when she left the company. The ex-employee has filed a suit before the court.

The court has made two orders. First-order says that "LinkedIn connections were not a trade secret because they are either generally known in the wider business community or capable of being easily derived from public information." Secondly, "plaintiffs apprehension of 'reputation' 'goodwill' and 'business opportunity' are insufficient to satisfy the 'loss' element of the company."

Blands vs. Roberts[29]

Former employees of an office, who were fired, sued the office, claiming that they were fired for

[25] Michael Elkon, 'Social Media And Trade Secrets' (labour lawyers, 1 July, 2013) <http://www.laborlawyers.com/social-media-and-trade-secrets> accessed on 01 Dec. 2014

[26] WL 3613855 (E.D.N.Y. Aug. 2, 2010)

[27] case no. 3:11-cv-03474

[28] Case 2:11-cv-04303-RB

[29] No. 12-1671 (4:11-cv-00045-RAJ-TEM)

having supported an opposing candidate in a local election. Both the plaintiffs had "liked" the opposing candidate's Facebook page, which they claimed was an act of constitutionally protected speech. A federal district court in Virginia, however, ruled that a Facebook "like" ". . . is insufficient speech to merit constitutional protection"; according to the court, "liking" involves no actual statement, and constitutionally protected speech could not be inferred from "one click of a button."

This case explored the increasingly important intersection of free speech and social media, with the court finding that a "like" was insufficient to warrant constitutional protection**.**

In early 2012, the New York City District Attorney's Office subpoenaed Twitter to produce information and tweets related to the account of the defendant. Twitter first sought to quash the subpoena, but the court denied the motion, finding that it had no proprietary interest in the tweets and therefore did not have the standing to quash the subpoena. Twitter then filed a motion to quash, but the court also denied its motion, finding that the present defendant had no reasonable expectation of privacy in his tweets and that, for the majority of the information sought, no search warrant was required.

This case set an important precedent for the production of information related to social media accounts in criminal suits. According to the court's decision, in certain circumstances, a criminal defendant has no ability to challenge a subpoena that requires a particular social media account information and details of its contents.

These legal complexities have taken many forms. There are three notable examples in the United States which the first one is the Jake Baker incident[30], second is the controversial distribution of the DeCSS software code[3132], which decodes the content-scrambling system used for DVD licensing enforcement, and third is *Gutnick vs Dow Jones*[79], in which libel laws were considered in the context of online publishing. The last example was particularly significant because it epitomized the complexities inherent to applying one country's laws (nation-specific by definition) to the Internet (international by nature).[33]

(E) Defamation

A major issue in the social media context is defamation. Generally speaking, a defamatory statement is a false and disparaging statement about another that causes injury to the reputation of the person to whom it refers and exposes him to hatred, ridicule, or contempt, or which causes him to be shunned or avoided. The Indian Penal

[30] It concerns the alleged obscene internet postings by a student at the University of Michigan to express his fantasies regarding a female student of his acquaintance. His actions and the response by the university authorities and ultimately by the FBI raise interesting questions about the status of electronic postings in the whole domain of freedom of expression and even more on the control required by those who operate newsgroups.

[31] James Danison, 'The DeCSS controversy, both sides' (CNET, 29 May 2004) <http://forums.cnet.com/7726-6130_102-265452.html> accessed on 12 Feb 2014

[32] (2002) HCA 56

[33] Zittrain, Jonathan, 'Be Careful What You Ask For: Reconciling a Global Internet and Local Law' (Harvard law School Public Law) <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=395300> accessed on 17 Oct 2014

Code makes it a punishable offence.[34] The Section requires three essentials:

- Making or publishing any imputation concerning any person
- Such imputation must have been made by (a) words, either spoken or intended to be read, (b) signs, or (c) visible representations.
- Such imputation was made with the intention of harming or with knowledge or reason to believe that it will harm the reputation of the person concerning to whom it is made.

The unmediated character of social media increases its potential for defamatory use. When we consider the essential elements of defamation in the context of defamation on social media pages, the following questions arise:

- When does a publication take place?
- How does a publication take place?
- Where does the publication take place?
- Who is liable for the publication?

Publication-

For the offence of defamation, publication of defamatory matter is essential. In other words, the defamatory matter must be communicated to some person other than the person to whom it concerns. Publication of the defamatory statement takes place when the content of a statement is seen or heard by the reader or the hearer. An electronic publication could take place through email, online bulletin board messages, chat room messages, music downloads, audio files, streaming videos, digital photographs and so on. Section 499 of the Indian Penal Code, 1860 expressly provides that defamation could take place not only by words but also by signs or visible representations. This would mean that even dissemination of defamatory material through the SMS, MMS, Photographs and Videos or mobile phones would constitute an actionable claim.[35]

Place of publication and jurisdiction-

An online defamatory statement can be published anywhere in the world where the Internet is available. This raises jurisdictional issues since, technically, a suit would be maintainable in any jurisdiction in the world where the statement has been accessed. Therefore, a defendant could be dragged to any jurisdiction where the statement is accessed, notwithstanding where he had posted the information. The place of publication that is the place where the material is read, heard or seen is the basis of the cause of action for defamation.

Liability determination-

Fixing the liability for defamatory material between ISPs & information publishers is another important aspect of online defamation. At first, the information publisher would like him held liable, but the role of ISPs in promoting defamatory material shall also be considered. Failure of ISPs in removing the defamatory material on the demand of the victim would be a ground to establish the liability of ISPs. The

[34] Section 499 of Indian Penal Code defines defamation and Section 500 provides punishment for defamation.

[35] Madhavi Gordian Divan, '*Facets of Media Law'* (Reprint, EBC, 2010) 109

liabilities of the ISPs have been discussed later in this chapter.

(F) Privacy Violation by Social Media

While the idea of 'privacy' is venerable, modern obsessions with privacy are largely rooted in the twentieth century.[36] The unprecedented level of information dissemination on social media websites invariably has implications for users' personal privacy. A vast majority of social networking sites set a particular privacy setting as default so that anyone can see a person's information unless privacy settings are actively changed. As a result, a considerable number of the users inadvertently allow public access to parts of their personally identifying information merely by failing to actively change their privacy settings.[37] This criticism is vindicated by a study that points out that 41 per cent of child and 44 per cent of adult Facebook users have open privacy settings, mostly arising out of a failure to change the default settings.[38]However, the problem of privacy violation persists for technology aware users also who have actively changed their default settings because a lot of their information may be available on their friend's social media page. For instance, a user may be tagged in a photograph or comment posted by a friend and is unable to exercise any control over how that data is presented and what privacy settings are applied by the friend.

Websites and advertising companies are able to track the user as they travel on the Internet to assess their personal preferences, habits and lifestyles. It is possible because every time a user logs on to the Internet, he leaves behind an electronic trail. This information is used for direct marketing campaigns that target individual customers. For example, if a user spares little time at some online shopping store like myntra.com, then he will automatically start getting suggestions of new offers from myntra.com on his social media pages. This situation leads only to a logical conclusion that somewhere social networking sites are sharing personal information of the user for revenue purposes.

Another area of privacy violation in social networks is the permanent availability of users' information to others. For example, Facebook does not delete the complete information of the user even if he permanently deletes his account. Facebooks` data use policy says:

"When you delete your account, it is permanently deleted from Facebook. It typically takes about one month to delete an account, but some information may remain in backup copies and logs for up to 90 days. You should only delete your account if you are sure you never want to reactivate it. You can delete your account.

[36] Andrew T. Kenyon & Megan Richardson (eds.), *'New Dimensions in Privacy Law'* (Reprint, Cambridge University Press 2007) 1

[37] Helen Anderson, 'A Privacy Wake-Up Call for Social Networking Sites?' (2009) 20 Entertainment Law Review 7, 245

[38] Office of Communications, Government of UK, *Social Networking* (Research Report, 2008) <http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/report1.pdf> accessed on 11 Aug. 2014

Certain information is needed to provide you with services, so we only delete this information after you delete your account. Some of the things you do on Facebook aren't stored in your account, like posting to a group or sending someone a message (where your friend may still have a message you sent, even after you delete your account). That information remains after you delete your account."[39]

Any picture captured during video chat in Gmail is automatically saved in Google plus, which is Google's social media platform. The user is never informed about the automatic save function of Gmail to Google plus. Thankfully the stored album is set 'private' by default. The permanent availability and saving without the knowledge/consent of the users is a gross violation of the user's right to know. Ironically, the policy of Google-plus says that even if the user deletes his account, the pictures will not be deleted. Further, it takes 60 days for Google plus to permanently delete any material from the trash.[40]

Another major concern is the complexity and incomprehensible nature of the privacy policies and terms of use of most social networking sites. Among other victims of this problem was the winner of an American beauty pageant- Miss New Jersey, 2007. Under the impression that her album was restricted to her Facebook friends only, she posted some racy photographs on the site. To her utter surprise, she was soon blackmailed by another Facebook user who gained access to the album.[41] While the fault, in this case, maybe attributed to the victim, it is not difficult to imagine that a larger number of users are left in the dark owing to the complexities of the websites complex privacy controls. Facebook itself, in a blog post, admitted that most new users of Facebook had their privacy setting set at "public", which have resulted in some users accidentally sharing information with too many people.[42] In the same post, Facebook revealed its plan that now privacy settings for news users would be set 'friends only' by default.

(1) and the right to free speech

The right to freedom of speech and expression and the right to privacy are two sides of the same coin. One person`s right to know and be informed may violate another`s right to be left alone. Just as the freedom of speech and expression is vital for the dissemination of information on matters of public interest, it is equally important to safeguard the private life of an individual to the extent that it is unrelated to public duties or matters of public interest—the law of privacy endeavours to balance these competing freedoms.[43]

[39] Facebook, 'Data Policy' (Facebook, 30 January 2015) <https://www.facebook.com/about/privacy/yourinfo > accessed on 10 March 2014

[40] Google, 'Delete Your Google Plus Profile' <https://support.google.com/plus/answer/1044503?hl =en> accessed on 10 Feb. 2015

[41] Austin Fennier & Post Wires, 'N.J. Miss in a Fix over Her Pics' (nypost, 06 July, 2007) <http://www.nypost.com/p/news/regional/item_u9E3 QCTLwd5sD0Wz7Zb0MO> accessed on 12 July

[42] Facebook, 'Making It Easier to Share With Who You Want' (Newsroom, 22 May 2014) <https://newsroom.fb.com/news/2014/05/making-it-easier-to-share-with-who-you-want/> accessed on 23 May 2014

[43] Madhavi Gordian Divan, '*Facets of Media Law'* (Reprint, EBC 2010) 113

(2) and the law

Article 12 of Universal Declaration of Human Rights and Article 17 of International Covenant on Civil and Political Rights, 1966 reads:

"No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

Article 8 of the European Convention on Human Rights, 1950 reads:

"Everyone has the right to respect for his private and family life, his home and his correspondence.

There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary for a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

There are also a few statutory provisions contained in the Code of Criminal Procedure, 1973 [Sec. 327 (1)], the Indecent Representation of Women (Prohibition) Act, 1980 (Section 3 & 4), The Medical Termination of Pregnancy Act, 1971 (Section 7 (1) (c)), The Hindu Marriage Act, 1955 (Section 22), The Special Marriages Act, 1954 (Section 33), The Children Act, 1960 (Section 36), and the Juvenile Justice Act, 1986 (Section 36) which seek to protect women and children from unwarranted publicity.

In India, Article 19 (2) does not expressly enumerate 'privacy' under 'reasonable

restrictions' but this lacuna has not prevented the courts from carving out a constitutional right to privacy by a creative interpretation of the right to life under Article 21. Supreme Court of India has developed the law on privacy in a series of cases. The surveillance power of state police was first considered in *Kharak Singh vs State of UP*[44] The Court has struck down a regulation that authorized domiciliary visits as being unconstitutional. After this case, the police power of surveillance has been settled by Supreme Court in *Govind vs State of MP*[45] & *Malak Singh vs. State of P & H*[46]. However, to date Supreme Court has not discussed privacy issues in the cyber world.

(G) Cyber Bullying and Harassment

According to the US National Crime Prevention Council, cyberbullying happens when the Internet, cell phones or other devices are used in cruelty to others by sending or posting text or images intended solely to hurt or embarrass another person.

Cyberbullying allows the offender to conceal his identity behind a computer. This anonymity makes it easier for the offender to act against the victim without having to see the victim's physical response. The distancing effects provided by technological devices have an impact on offenders, and it often leads them to

[44] AIR 1963 SC 1295
[45] (1975) 2 SCC 148
[46] (1981) 1 SCC 420

say and do crueller things compared to a traditional face-to-face bullying situation.

Online publication of personal information on social media pages is prone to bullying because it can lead to the disclosure of those information's also are kept private in real life. This vulnerability puts many users in a position as either the victim or active offender partaking in cyberbullying actions**.** Another aspect of social media that can be misleading and hazardous is the ability to create fake profiles. Fake profiles provide an opportunity to say anything to another individual without the worry of any repercussions.

Anonymous blogging has also fostered cyberbullying and fuelled ethical debate. In the US, websites such as College ACB and Juicy Campus both have faced tightened regulations due to their verbally abusive nature. The forum in these sites included various harsh topics for debate/discussion. The equal feature is provided by various other social media websites most often results in abusive comments.[47]

(H) Social Media & Freedom of Speech and Expression

Through social media, the monolith of speech has infiltrated all forms of space. In a democratic country like India, where the Right to Freedom of Speech and Expression has been expressly guaranteed as a fundamental right under the constitution, it is terribly clear that this right cannot be taken away except under the situations mentioned in Article19(2).[48]

Time and again, this fundamental right has taken a course that may well be counted as a threat to laws and policies initiated by the govt. And have resulted in a debate whether these rights can be curtailed. The advancement of technologies, particularly in the social media arena, has added fuel to the fire because it has provided common masses to have to say on a public platform.

Freedom of expression is the most cherished right in our constitution as protected under Art. 19 (1) (a), which is also restricted by what is set out in Art. 19 (2), empowering the state to make appropriate law in that regard. However, even when the state does not interfere, the Freedom of Expression is not as free as it should be. As suggested by Dr Justice Rajendra Babu, market forces and controls by society or the public at large restrict such rights.[96] For example, banning Salman Rushdie book 'satanic verses', banning Mani Ratnam`s film 'Bombay' in Bombay and when film director Deepa Mehta could not show several of her movies, including 'fire' and 'water' in India. These incidences show the curtailment of freedom of expression in India without any legal backing. Such incidences are clearly in violation of Supreme Court judgment in *LIC vs. Manubhai D. Shah*[97]*& Ministry of Information and Broadcasting, Government of*

[47] Richard Donegan, 'Bullying and Cyber bullying: History, Statistics, Law, Prevention and Analysis' (Spring 2012) 3 The Elon Journal of Undergraduate Research in Communications 1

[48] Article 19 (1) (a) of the Constitution of India also confers on the citizens of India the right "to freedom of speech and expression". The freedom of speech and expression means the right to express one's convictions and opinions freely by word of mouth, writing, printing, pictures or any other mode. It also includes the right to propagate or publish the views of other people.
Article 19 (1) All citizens shall have the right—
(a) to freedom of speech and expression;

India vs. Cricket Association of Bengal[98]. These above-discussed judgments say that the right to freedom of speech and expression would include the freedom of a citizen as a viewer/listener/reader to receive and to communicate or disseminate information and ideas without interference. It is the constitutional obligation of the state to ensure

a To speech and expression
b to assemble peaceably and without arms;
c to form associations or unions;
d to move freely throughout the territory of India;
e to reside and settle in any part of the territory of India; [and]
f to practise any profession or to carry on any occupation, trade or business.

2) Nothing in sub-clause (a) of clause (1) shall affect the operation of any existing law, or prevent the state from making any law, in so far as such law imposes reasonable restrictions on the exercise of the right conferred by the said sub-clause in the interests of the sovereignty and integrity of India, the security of the state, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence.

- Conditions in which these rights can be meaningfully and effectively enjoyed by all citizens and prevent their monopoly or dominance by a few.

It is very interesting to note that the Supreme Court in *Tata Press Ltd. Vs. Mahanagar Telephone Nigam Ltd*[99] held that commercial speech is a part of freedom of speech and expression guaranteed under Article 19 (1) (a). Therefore, commercial advertisement is a form of commercial speech and is protected under Article 19 (1) (a) subject to Article 19(2). A very interesting situation arises when we extend this ruling to advertisements over social media websites.

- May commercial speech as a fundamental right of one subjugate the other`s fundamental right to freedom of what to see and what not?
- How can one claim the freedom of speech and expression against the social media web when it is enforceable only against the state? [In India, internet service providers are both state-owned (BSNL and MTNL) and privately-owned (Airtel, Spectranet, Reliance, Sify etc.). Given that most of the ISPs are privately owned, how does the constitution even come into the picture? Our fundamental rights are enforceable vertically, that is, between individuals and the state, and not horizontally – that is, between two individuals or two private parties.

In the first situation, it appears that the actual problem lies with 'terms and conditions stipulated by social networking sites and due regard should be paid to the contractual clause which mentions the advertisements. Most social networks offer their services free of cost. They make money with advertisements. In the process, they allow the bulk of advertisements to be shown on their pages without any involvement of the user. People who use social networks store

various information about themselves, including, but not limited to, their age, gender, interests, and location. This stored information allows advertisers to create specific target groups and individualize their advertisements. While it is clear that social media websites feature advertisements according to the interest of users, it also raises the question of sharing users' personal information with the advertising companies.

Coming to the second situation, it would be pertinent to analyze Article 12 of the Indian

Constitution which says-

"In this part, unless the context otherwise requires, the State includes the Government and Parliament of India and the Government and the Legislature of each of the States and all local or other authorities within the territory of India or under the control of the Government of India."

The Supreme Court has struggled with the issue of defining "other authorities" for the purposes of Part III of the Constitution, with the pendulum swinging wildly at times. In the case of *Pradeep Kumar Biswas v. Indian Institute of Chemical Biology*[100], a 2002 judgment by a Constitution Bench, the court settled upon the following definition:

"The question in each case would be whether in the light of the cumulative facts as established, the body is financially, functionally and administratively dominated by or under the control of the government. Such control must be particular to the body in question and must be pervasive. If this is found, then the body is a State within Article 12. On the other hand, when the control is merely regulatory whether under statute or otherwise, it would not serve to make the body a State."

There is no way to argue that ISPs are under the pervasive financial, functional and administrative domination or control of the state. The test laid down by the court, in this case, seems to be radically under-inclusive. For example, if the government decides to privatize the nation's water supply to private company X., Company X is the sole distributor of water in the country. On gaining control, it decides to cut off the water supply to all households populated by members of a certain religion. There seems something deeply wrong in the argument that there is no remedy under discrimination–law against the conduct of the company.

III. CONCLUSION

The present research paper was conceptualized in the wake of challenges posed by social media in the late twenties. Various countries, along with India, have witnessed a number of social media mischief and the inability of respective regulatory mechanisms ineffective handle the situation. The compelling circumstances after mischief have guided this research in framing and conceptualizing contemporary challenges posed by social media. The perennial failure and overthrowing/suppressive response of regulatory mechanisms have been central points of this paper.

The research for the sake of simplicity was broadly divided under the various heads/chapters. Firstly, the regulatory challenges of social media have been discussed and

analyzed from the perspective of legal and regulatory measures. While doing so, the role and responsibilities of the authorities concerned have also been discussed.

The examination of legal and regulatory issues indicates that the challenges posed by social media are unlikely to be solved merely by adapting and extending existing legal concepts. The new ways of communicating via social media raised legal questions which are fundamentally different for one of the two reasons. Firstly, the concept of freedom of speech and expression in the online era is entirely different in contrast to the offline world. Secondly, the online world demands a new set of rules to be governed. Both of these propositions have been highlighted in the Shreya Singhal case. It can also be concluded that India's Information Technology Act, hurriedly amended in 2008 and updated with rules for Internet intermediaries in 2011, is ill-suited to deal with ICT innovations such as social media and user-generated content, with negative consequences for intermediaries and users alike.

This is also noted in the article that hate speeches on social media platforms are the biggest problem for social unrest, and they need to be addressed on a priority basis. However, to date, there are no effective mechanisms to deal with it, neither at the international level nor at the national level. Though few mechanisms are working very hard in the absence of a proper institutional setup and funding, they are facing problems in implementing their policies.

This is also clear that any attempt by the government to filter online content before it is posted, will not only be against the principles of free speech but also impractical to implement. Pre-publication crackdown is difficult, even unwarranted and, instead, efforts should be made to strengthen the existing IT laws.

*****

 [ISSN 2581-9453]