National Journal of Advanced Research
www.thestudiesjournal.com
ISSN: 2455-216X
Received: 27-01-2025, Accepted: 26-02-2025, Published: 15-03-2025
Volume 11, Issue 1, 2025, Page No. 24-31

Regulating freedom of speech and expression in social media: Challenges before the Indian law

Dr. S Krishnan[1], Komal Yadav[2]
[1] Associate Professor, Department of Law, Jaipur National University, Jaipur, India
[2] Advocate, Department of Law, District Court, Saket, New Delhi, India

Abstract
This article is regulation freedom of speech on social media. Freedom of speech is a principle that supports the freedom of an individual or a community to articulate their opinions and ideas without fear of retaliation, censorship, or legal sanction. The term "freedom of expression" is sometimes used synonymously but includes any act of seeking, receiving, and imparting information or ideas, regardless of the medium used. Freedom of expression is recognized as a human right under article 19 of the Universal Declaration of Human Rights (UDHR) and recognized in international human rights law in the International Covenant on Civil and Political Rights (ICCPR). Article 19 of the UDHR states that "everyone shall have the right to hold opinions without interference" and "everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice". Social media platforms have revolutionised our ability to connect across historic social, political and geographic divides. Where previously gatekeepers mitigated and negotiated access to mass media platforms, today potentially anyone and any content can reach millions of individuals in an instant. This development bears great opportunities for the democratisation of expression and the diversification of public discourse but has likewise broadened the impact and harm done through disinformation and hate speech.

Keywords: Regulating, freedom, speech, social, media.

Introduction

"The more time you spend in India, the more you realize that this country is one of the world's greatest wonders- a miracle with a message. And the message is that democracy matters."

-Thomas Friedmann [1]

India is one of such paradises on earth where you can speak your heart out without the fear of someone gunning you down for that, or, it has been until now. Even if the situation of Indians is a lot better than that of their fellow citizens of other nations, the picture is not really soothing or mesmerizing for Indians anymore. This observation is being made with regard to the exercise of the right of freedom of speech and expression in the context of social media and the hurdles placed on that by the arbitrary use of the so called cyber laws of the nation, particularly Section 66A of the Information Technology Act, 2000.

Before delving into the issue in details, it is but desirable to first understand the concepts of social media and freedom of speech and expression.

What is Social Media?

Social media comprises primarily internet and mobile phone based tools for sharing and discussing information. It blends technology, telecommunications, and social interaction and provides a platform to communicate through words, pictures, films, and music [2]. Social media includes web-based and mobile technologies used to turn communication into interactive dialogue [3].

Social media can be defined as any web or mobile based platform that enables an individual or agency to communicate interactively and enables exchange of user generated content [4]. Andreas Kaplan and Michael Haenlein define social media as "a group of internet- based applications that build on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of user- generated content." [5] "Web 2.0" refers to Internet platforms that allow for interactive participation by users [6]."User generated content" is the name for all of the ways in which people may use social media [7]. The Organization for Economic Cooperation and Development (OECD) specifies three criteria for content to be classified as "user generated:" (1) it should be available on a publicly accessible website or on asocial networking site that is available to a select group, (2) it entails a minimum amount of creative effort, and (3) it is "created outside of professional routines and practices [8]."

Another variant of social media is mobile social media *i.e.* when social media is used in combination with mobile devices it is called mobile social media. Due to the fact that mobile social media runs on mobile devices, it differentiates from traditional social media as it incorporates new factors such as the current location of the user (location-sensitivity) or the time delay between sending and receiving messages(time-sensitivity).

Types of Social Media

Social Media can be broadly divided into following categories:

1. Social networking

Social networking is an online service that enables its users to create virtual networks with likeminded people. It offers facilities such as chat, instant messaging, photo sharing, video sharing, updates etc. The most popular are Facebook and LinkedIn.

2. Blogs

Blogs are descriptive content created and maintained by individual users and may contain text, photos and links to other websites. The interactive feature of blogs is the ability of readers to leave comments and the comment trail can be followed.

3. Microblogs
Micro blogs are similar to blogs with a typical restriction of 140 characters or less, which allows users to write and share content. Twitter is a micro blogging site that enables its users to send and read ‘tweets’.

4. Vlogs and Video Sharing sites
Video blogs (Vlogs) are blogging sites that mainly use video as the main form of content supported by text. You Tube is the world’s largest video sharing site. You Tube is a videolive casting and video sharing site where users can view, upload, share videos and even leave comments.

5. Wikis
Wiki is a collaborative website that allows multiple users to create and update pages on particular or interlinked subjects. While a single page is referred to as ‘wiki page’, the entire related content on that topic is called a ‘Wiki’. These multiple pages are linked through hyperlinks and allow users to interact in a complex and non- linear manner.

6. Social Bookmarking
These services allow one to save, organize and manage links to various websites and resources around the internet. Interaction is by tagging websites and searching through websites bookmarked by other people. The most popular are Delicious and Stumble Upon.

7. Social News
These services allow one to post various news items or links to outside articles. Interaction takes place by voting for the items and commenting on them. Voting is the core aspect as the items that get the most votes are prominently displayed. The most popular are Digg, Reddit and Propeller.

8. Media Sharing
These services allow one to upload and share photos or videos. Interaction is by sharing and commenting on user submissions. The most popular are YouTube and Flickr.
There can be overlap among the above mentioned types of social media. For instance, Facebook has micro blogging features with their ‘status update’. Also, Flickr and YouTube have comment systems similar to that of blogs.

Freedom of Speech and Expression
Freedom of speech and expression is broadly understood as the notion that every person has the natural right to freely express themselves through any media and frontier without outside interference, such as censorship, and without fear of reprisal, such as threats and persecutions. Freedom of expression is a complex right. This is because freedom of expression is not absolute and carries with it special duties and responsibilities therefore it may be subject to certain restrictions provided by law.
The term freedom of expression itself had existed since ancient times, dating back at least to the Greek Athenian era more than 2400 years ago. The following are some of the most commonly agreed upon definitions of freedom of expression that are considered as valid international standards:

- “Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.” [Article 19, Universal Declaration of Human Rights, 1948 (UDHR)]
- “Everyoneshallhavetherighttoholdopinionswithoutinterference.Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.” [Article 19 (2), International Covenant on Civil and Political Rights, 1966 (ICCPR)]

Similarly, 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.
The term ‘freedom of speech and expression’ includes any act of seeking, receiving and imparting information or ideas, regardless of the medium used. Based on John Milton’s arguments, freedom of speech is understood as a multi-faceted right including not only the right to express or disseminate information and ideas but also including the right to seek, receive and impart information and ideas.
The notion of freedom of speech and expression is intimately linked to the concept of democracy. Alexander Meiklejohn, one of the proponents of this link argues that democracy means self-government by the people and for the proper functioning of which, an informed electorate is indispensable which, in turn, requires that there be no constraints on the free flow of information and ideas. Democracy will not be true to its essential ideal if those in power are able to manipulate the electorate by withholding information and stifling criticism.
Again, Richard Moon argues that the value of freedom of speech and expression lies within social interactions. He says “[b]y communicating an individual forms relationships and associations with others-family, friends, co-workers, church congregation, and countrymen, by entering into discussion with others an individual participates in the development of knowledge and in the direction of the community.”
In the light of Moon’s argument, the importance of freedom of speech and expression while using social media can be better understood.

Freedom of Speech and Expression and Social Media/Internet
The Internet and Social Media has become a vital communications tool through which individuals can exercise their right of freedom of expression and exchange information and ideas. In the past year or so, a growing movement of people around the world has been witnessed who are advocating for change, justice, equality, accountability of the powerful and respect for human rights. In such movements, the Internet and Social Media has often played a key role by enabling people to connect and exchange information instantly and by creating a sense of solidarity.

Emphasising the importance of internet, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression in his Report, which was submitted to the Human Rights Council, stated that the internet has become a key means by which individuals can exercise their right to freedom and expression and hence, internet access is a human right.Report further stressed that States should ensure that internet access is maintained at all times, even during times of political unrest. The States were also reminded of their positive obligation to promote or to facilitate the enjoyment of the right of freedom of expression and the means necessary to exercise this right, including the Internet. The States were also asked to adopt policies to make the Internet widely available, accessible and affordable to all.

The UN Human Rights Committee has also tried to give practical application to freedom of opinion and expression in the radically altered media landscape, the centre stage of which is occupied by the internet and mobile communication. Describing new media as a global network to exchange ideas and opinions that does not necessarily rely on the traditional mass media, the Committee stated that the States should take all necessary steps to foster the independence of these new media and also ensure access to them. Moreover, Article 19 of the UDHR and Article 19(2) of the ICCPR also provides for freedom of speech and expression even in case of internet and social media.

Thus, it is seen that freedom of speech and expression is recognized as a fundamental right in whatever medium it is exercised under the Constitution of India and other international documents. And in the light of the growing use of internet and social media as a medium of exercising this right, access to this medium has also been recognized as a fundamental human right.

Restrictions on Freedom of Speech and Expression

The freedom of speech and expression does not confer on the citizens the right to speak or publish without responsibility. It is not an unbraided license giving immunity for every possible use of language and prevents punishment for those who abuse this freedom. Article 19(3) of the ICCPR imposes restrictions on the following grounds:

a. For respect of the rights of reputations of others
b. For protection of national security, or public order, or public health or morals.

As per Article 19(2) of the Constitution of India, the legislature may enact laws to impose restrictions on the right to speech and expression on the following grounds:

a. Sovereignty and Integrity Of India
b. Security of the State
c. Friendly relations with Foreign States
d. Public order
e. Decency or morality
f. Contempt of court
g. Defamation
h. Incitement to an offence

Censoring Social Media

Information is a buzz word today. It is essential to march along with the progressive trends in today's world. Technology savvy world with an increasing capacity for communicating, simplifying and storing information with amazing speed has put information at the core of development. There can be no democratic participation in decision making without transparency and sharing information. Social media has the power to reach the masses and distribute information, which in turn has resulted in everyone acting as a watchdog, scrutinizing the powerful and exposing mismanagement and corruption.

Till recently, governments across the globe have tried to withhold information from the common man on one pretext or another. And, now with the advent of social media with immense power of delivering information to the masses, is perceived as a threat by Governments who are carefully trying to regulate it. Internet has become the basis of modern civilization due to its limitless possibilities and widespread reach. As it is quite instrumental in the storage and dissemination of information and opinion, it has acquired a unique role in the functioning of democracies all over the world. Through social media and internet, the citizens can unite despite territorial limitations. Although everyone is not physically present, the force of the protest is not diminished in any way. Thus, it is evident as to why Governments across the world seek to censor the internet.

Again, apart from its beneficial role, Internet is open to misuse as well, which gives the State a justification to regulate online content in the interests of the public at large. Several cyber-crimes, defamation, invasion of privacy, incitement of offences, racist remarks, stalking, abuse, hacking, harassment and many more can be easily committed through social media and once such objectionable content is uploaded, it becomes viral and consequently, very difficult to contain. Hence, the importance of the State regulating social media also cannot be denied.

As long as the interests of people, either individually or collectively are taken care of, there can be no objection to government regulation but the problem arises when, in the name of regulation, it starts censoring i.e. encroaching upon the civil rights of the people *viz*. freedom of speech and expression etc. Although there are safeguards in this regard, every State tends to surpass them in some way though its magnitude may vary from State to State.

China is the leader in Internet censorship. It has an elaborate mechanism in place to effect censorship known as "Great Firewall of China" and officially as "Golden Shield Project". Blocking web- pages with objectionable content is the regular mode of internet censorship.

Coming to India, according to the Freedom House's latest report **'**Freedom on the Net, 2012', India's overall Internet Freedom Status is "Partly Free". India has secured a score of 39 on a scale from 0 (most free) to 100 (least free), which places India 20 out of the 47 countries worldwide that were included in the report.On 12 March 2012, Reporters without Borders published a report titled 'Internet Enemies Report, 2012' **o**n the basis of the growing control over the net by Government [21]. Report contained a list of 'Enemies of the Internet' that restrict online access and harass their netizens; and a second list of 'Countries under Surveillance' for displaying a disturbing attitude towards the Internet. Report put India in the list of 'Countries under Surveillance'. In its seventh transparency report, published on 27th April 2013, Internet giant Google noted that the Indian government has nearly doubled its requests to Google for removal of content in the second half of 2012 as compared to the first six months. The report, further noted that between July and December 2012, Google had received more than 2,285 government requests to delete 24,149 pieces of information. In the first half of 2012, Google received 1,811 requests to remove 18,070 pieces of information. During the same six-month period, the Indian government — both by way of court orders and by way of requests from police— requested Google to disclose user information 2,319 times over 3,467 users/accounts.

Although the Information Technology Act was in force since 2000, India did not police the cyber space with much vigour before the 2008 terrorist attack on Mumbai. After the attacks, the Information Technology Act, 2000 was amended to expand and strengthen the monitoring and censoring capacity of the Government. The cyber law of India now contains provisions relating to blocking of websites, monitoring and collecting internet traffic data, interception or decryption of such data, unhindered access to sensitive personal data, holding intermediaries *viz.* social media websites liable for hosting user- generated objectionable content, etc. In this backdrop, India has been considered as a country engaged in 'selective' Internet filtering.

Pre-Screening Content on Social Media

In December, 2011, the Indian Government asked the internet companies like Google, Facebook, Microsoft, etc. to create a framework to pre-screen the data before it goes up on the website. Some defamatory content was found on a social networking site and on that pretext, Government has asked the companies to chalk out a way to ensure that such content is screened before it goes online.

As a major debate broke out on the matter and it was portrayed in a negative light, Kapil Sibal told media that the Government was not trying to censor the freedom of speech and expression online; it merely wanted to stop offensive material from being uploaded on social networkingsites. Thecompanies also informed that it is not possible to meet with the demand due the volume of user-generated content in India and that they cannot be responsible for determining what is or is not defamatory.

In the *Secretary, Ministry of Information and Broadcasting, Government of India and others vs. Cricket Association of Bengal and others,* the Supreme Court held that "for ensuring the free speech right of the citizens of this country, it is necessary that the citizens have the benefit of plurality of views and a range of opinions on all public issues. A successful democracy posits an aware citizenry. Diversity of opinions, views, ideas and ideologies is essential to enable the citizens to arrive at informed judgment on all issues touching them. This cannot be provided by a medium controlled by a monopoly- whether the monopoly is of the State or any other individual, group or organization."

In the light of the above, it can be opined that rather than censoring of social media, its regulation is desirable in a way which maintains the rights of users and also protects that of the victims simultaneously. This brings us to discussing the cyber laws of India which are intended to regulate social media, albeit in an indirect manner.

Cyber Laws of India and Social Media

Although there is no specific legislation in India which deals with social media, there are several provisions in the existing so-called cyber laws which can be used to seek redress in case of violation of any rights in the cyber space, internet and social media. The legislations and the relevant provisions are specifically enumerated as under:

The Information Technology Act, 2000

a. Under Chapter XI of the Act, Sections 65, 66, 66A, 6C, 66D, 66E, 66F, 67, 67A and 67B contain punishments for computer related offences which can also be committed through social media *viz.* tampering with computer source code, committing computer related offences given under Section 43, sending offensive messages through communication services, identity theft, cheating by personation using computer resource, violation of privacy, cyber terrorism, publishing or transmitting obscene material in electronic form, material containing sexually explicit act in electronic form, material depicting children in sexually explicit act in electronic form, respectively.
b. Section 69 of the Act grants power to the Central or a State Government to issue directions for interception or monitoring or decryption of any information through any computer resource in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States, public order, for preventing incitement to commission of any cognizable offence, for investigation of any offence.
c. Section 69A grants power to the Central Government to issue directions to block public access of nay information through any computer resource on similar grounds.
d. Section 69B grants power to the Central Government to issue directions to authorize any agency to monitor and collect traffic data or information through any computer resource for cyber security.
e. Section 79 provides for liability of intermediary. An intermediary shall not be liable for any third party information, data or communication link made available or hosted by him in the following cases-
   - His function is limited to providing access to a communication system over which such information is transmitted, stored or hosted.
   - He does not initiate, select the receiver and select or modify the information contained in the transmission.
   - He observes due diligence and other guidelines prescribed by the Central Government while discharging his duties.

   Again, an intermediary shall be liable in the following cases:
   - He has conspired, abetted, aided or induced by threats, promise or otherwise in the commission of the unlawful act.
   - He fails to expeditiously remove or disable access to the material which is being used to commit the unlawful act, upon receiving actual knowledge or on being notified by the Government.
f. If any intermediary fails to assist, comply with direction and intentionally contravenes provisions under Sections 69, 69A and 69B respectively, he shall be liable to punishment.
g. Section 43A provides that where a body corporate possessing, dealing or handling any sensitive personal data or information in a computer resource owned, controlled or operated by it, is negligent in

implementing and maintaining reasonable security practices and procedures thereby causing wrongful loss or wrongful gain to any person, it shall be liable to pay damages by way of compensation to the affected person.

h. Section 70B provides for an agency of the Government to be appointed by the Central Government called the Indian Computer Emergency Response Team, which shall serve as the national agency for performing functions relating to cyber security.

The Central Government has also enacted rules to give effect to various provisions of this Act which are as follows:

The Information Technology (Procedure and Safeguards of Interception, Monitoring and Decryption of Information) Rules, 2009

These rules are made by the Central Government in exercise of its powers under Section 87(2) (y) with regard to the procedure and safeguards for monitoring and collecting traffic data or information under Section 69B (3).

Rule 3 provides that the interception or monitoring or decryption of information under Section 69 shall be carried out by an order issued by the competent authority.

Rule 2(d) defines competent authority as the Secretary in the Minister of Home Affairs, in case of Central Government and the Secretary in charge of the Home Department, in case of a State Government or Union territory.

Rule 4 provides for an agency of the Government authorized by the competent authority to carry out the functions.

Rule 10 requires the name and designation of the officer of the authorized \agency to whom such information should be disclosed.

Rule 13 requires the intermediary to provide all facilities, co- operation and assistance for interception or monitoring or decryption of information.

The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009

These rules are made by the Central Government in exercise of its powers under Section 87(2) (z) with regard to the procedure and safeguards for blocking for access by the public under Section 69A (2).

Rules 3, 4, 5, 6, 7 and 8 contain the regular method of sending request for blocking to the Nodal officer of concerned organization who shall examine it and forward it to the Designated Officer of the Central Government who shall further examine it along with a Committee and then, their recommendation shall be sent to the Secretary, Department of IT for his approval, upon which the Designated Officer shall direct such blocking.

However, Rule 9 grants power to the Designated Officer to take a decision regarding blocking in cases of emergency where delay is unacceptable.

Rule 13 provides that every intermediary shall designate a person to receive and handle directions for blocking of information, who shall acknowledge receipt of the directions to the Designated Officer within two hours of receipt through acknowledgment letter or fax or e- mail.

Rule 10 provides that the Designated Officer, on receipt of a court order directing blocking of any information, shall submit it to the Secretary, Department of Information and Technology and initiate action immediately.

The Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009

These rules are made by the Central Government in exercise of its power under Section 87(2) (za) with regard to the procedure and safeguards for monitoring and collecting traffic data or information under Section 69B (3).

Rule 3 provides that directions for monitoring and collection of traffic data or information under Section 69B (3) shall be issued by an order made by the competent authority.

Rule 2(d) defines competent authority as the Secretary of the Government of India in the Department of Information Technology under the Ministry of Communications and Information Technology.

Rule 3 further provides that the competent authority may issue directions for monitoring for purposes related to cyber security.

Rule 4 provides that the competent authority may authorize any agency of the Government for monitoring and collection of traffic that or information who shall designate a nodal officer to send requisition conveying direction under Rule 3 to the Designated Officer of the intermediary.

The Information Technology (Intermediaries Guidelines) Rules, 2011

These rules are made by the Central Government in exercise of its powers under Section 87(2) (zg) with regard to the guidelines to be observed by the intermediaries under Section 79(2).

Section 2(w) of the Information Technology Act, 2000 defines “intermediary” with respect to any particular electronic records as any person who on behalf of another person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service, network service, internet service, web- hosting service providers, search engines, online payment sites, online auction sites, online market places and cyber cafes.

Rule 3 makes it mandatory for the intermediary to inform the users by clearly stating that under the rules and regulations, privacy policy and user agreement, which are published on the website, they are not to host, display, upload, modify, publish, transmit, update or share any information that is objectionable under Rule 3(2).

Once a violation under Rule 3(2) is noticed by or is brought to actual knowledge of any intermediary by an affected person in writing or through e-mail, Rule 3(4) requires the intermediary to remove the objectionable content within 36 hours.

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

These rules are made by the Central Government in exercise of its powers under Section 87(2) (ob) read with Section 43A with regard to the reasonable security practices and procedures and sensitive personal data or information under Section 43A.

Rule 6 provides that the disclosure of sensitive personal data or information by body corporate to any third party shall require prior permission from the provider of such information. However, the information can be shared with Government agencies, without obtaining prior consent, for the purpose of verification of identity, or for prevention, detection, investigation including cyber incidents, prosecution, prosecution, and punishment of offences.

Section66A of the Information Technology Act, 2000

Of all these provisions, Section 66A has been in news in recent times, albeit for all the wrong reasons.

Before discussing the issue in detail, it is desirable to first have a look at Section 66A, the provision itself. Section 66A of the Information Technology Act, 2000 inserted vide Information Technology (Amendment) Act, 2008 provides punishment for sending offensive messages through communication service, etc. and states:

Any person who sends, by means of a computer resource or a communication device,

a. Any information that is grossly offensive or has menacing character;
b. any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently by making use of such computer resource or a communication device,
c. any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages shall be punishable with imprisonment for a term which may extend to three years and with fine.

Explanation: For the purposes of this section, terms "electronic mail" and "electronic mail message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, images, audio, video and any other electronic record, which maybe transmitted with the message.

Section 66A was inserted through an amendment to the Act in 2008. The Amendment Bill, which was introduced in Parliament in 2006, had only the first two sub-clauses under Section 66A. Section 66A was originally intended to tackle spam, defined as unwanted and unwarranted e-mails. The Department of Information Technology told the committee that sub-clause (b) of Section 66A and Clause (i) of Section 43 of the Act sufficiently addressed the issue of spam. However, the Standing Committee on Information Technology, in its 2007 report, recommended that the Bill be made more stringent. Thus, sub-clause (c) was added to the provision, besides increasing the punishment for violation to three years imprisonment from up to two years.

A minute perusal of the provision clearly indicates that there is an inherent inconsistency between the phraseology of Section 66A and Article 19 (1) (a) of the Constitution, which guarantees freedom of speech and expression to every citizen. Under Article 19(2), restrictions on freedom of speech and expression are reasonable if they pertain to any of the listed grounds, such as sovereignty and integrity of India, 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. But under Section 66A, restrictions have been placed on freedom of speech and expression on several other grounds, apart from those mentioned in the Constitution.

There are several anomalies in the provision, which are inconsistent with free speech requirements. Words like “grossly offensive”, “menacing character”, “annoyance”, “danger”, “obstruction”, “insult” and “injury” do not have any precise definition. A prominent question that has been left unanswered is whether these words are to be construed with regard to the sensibilities of the particular person the words are addressed to or as per that of a reasonable man. Going by the sensibilities of particular individuals, it is most likely that even authors of innocent communication through e-mail could be accused of having violated the law.

To add to the fear that this provision could be hugely misused, several incidents in the recent past bear testimony to the same. A chronological order of such events is as follows:

- In April 2012, Ambikesh Mahapatra, a Professor of chemistry in Jadavpur University in West Bengal, was arrested for posting a cartoon on West Bengal Chief Minister Mamata Banerjee on social networking sites.
- In May 2012, two Air India employees were arrested by the Mumbai Police for putting up on Facebook and Orkut content that was against a trade union leader and some politicians. They were in custody for 12 days.
- In October 2012, Ravi Srinivasan, a businessman, was arrested by the Puducherry Police for tweeting that Kartik Chidambaram (son of Union Finance Minister P. Chidambaram) appears to have amassed more wealth than Robert Vadra, son-in-law of Congress president Sonia Gandhi.
- In November 2012, Shaheen Dhada was arrested for questioning the shutdown of Mumbai following the death of Shiv Sena Supremo Bal Thackeray in her Facebook post, which was “liked” and shared by her friend, Renu, who was also arrested by the Thane Police in Maharashtra.

In the face of widespread abuse of Section 66A, a writ petition has been filed in the form of a public interest litigation in the Supreme Court challenging the section’s constitutionality wherein it has been submitted that the phraseology of impugned Section is so wide and vague and incapable of being judged on objective standards, that it is susceptible to wanton abuse and hence falls foul of Article 14, 19 (1) (a) and Article 21 of the Constitution. Admitting the writ petition, Division Bench of Supreme Court, comprising Chief Justice Altamas Kabir and Justice J. Chelameswar, noted that the “wording of Section 66A is not satisfactory. It is made very wide and can apply to all kinds of comments.”

To prevent the misuse of Section 66A, however, Ministry of Communications and Information Technology, Government of India has issued Advisory to State/UT Governments on implementation of Section 66A.They have been advised that with regard to the arrest of any person in connection with a complaint registered under Section 66A, the concerned police officer of a police station under the State’s jurisdiction may arrest any person only with prior approval of such arrest from an officer not below the rank of the Inspector General of Police in the Metropolitan cities or an officer not below the rank of Deputy Commissioner of Police or Superintendent of police at the district level, as the case may be.

Conclusion

It is clearly evident that social media is a very powerful means of exercising one's freedom of speech and expression. However, it is also been increasingly used for illegal acts which has given force to the Government's attempts at censoring social media. Where on the one hand, the misuse of social media entails the need for legal censorship, on the other hand, there are legitimate fears of violation of civil rights of people as an inevitable consequence of censorship.

What is therefore desirable is regulation of social media, not its censorship. However, the present cyber laws of India are neither appropriate nor adequate in this respect. An analysis of the existing IT laws shows that there is unaccountable and immense power in the hands of the Government while dealing with security in the cyber space. Even then, it is not sufficient to check the misuse of social media. Hence, a specific legislation is desirable to regulate social media.

However, there are many practical difficulties which may arise while doing so. There is a very thin line which demarcates the enjoyment of one's right and the violation of the enjoyment of else's right in the process. In social media, the exercise of freedom of speech and expression by one may result in the invasion of privacy and defamation. Again, the idea of objectionable content varies from one person to another. A cartoon is a harmless way of having fun but offence may be taken by the person concerned. Similarly, hate speech, racist remarks, religious sentiments have different meanings for different people.

Keeping all this in mind, it is suggested that the Government should form a Committee including technical experts to look into all the possible facets of the use and misuse of social media and recommend a suitable manner in which it can be regulated without hindering the civil rights of citizens.

References

1. Rohit Raj, "Defining Contours of Press Freedom in Backdrop of National Emergency of 1975", *All India Reporter* (Journal Section), 2008, 155-160, at 160.
2. Paranjoy Guha Thakurta, *Media Ethics* (NewDelhi: OxfordUniversityPress, 2012, 354.
3. "SocialMedia", available on the Web, URL:http://en.wikipedia.org/wiki/social_media,accessedon14/4/13.
4. Social Media Framework Draft for Public Consultation", available on the Web, URL: http://www.indiaenvironmetportal.org.in/files/file/SocialMediaFrameworkDraftforPublicConsultation_192011-2.pdf,accessedon10/4/13.
5. Andreas M Kaplan, Michael Haenlein. Users of the World, Unite! The Challenges and Opportunities of Social Media", *Business Horizons*,2010:53:59-68. at 61.
6. *Ibid.*, at 60–61 (noting that Web 2.0 may be contrasted with Web 1.0 platforms, which simply provide content to users without giving them the opportunity to interact with or modify the information online).
7. *Ibid.*,at61.
8. OECD, Participative Web and User-Created Content: Web 2.0, Wikis, and Social Networking, 2007, 1-74. at 8, available on the Web, URL: http://www.oecd.org/sti/38393115.pdf;*see also* Kaplan & Haenlein, note 5, at 61.
9. In 2010, Kaplan and Haenlein classified social media into six different types:[9]
   a. Collaborative projects (e.g., Wikipedia),
   b. Blogs and microblogs (e.g., Twitter),
   c. Content communities (e.g., YouTube),
   d. Social networking sites (e.g., Facebook),
   e. Virtual game worlds (e.g., WorldofWarcraft), and
   f. Virtual social worlds (e.g. SecondLife). See Note 5, pp. 62-64.
10. UNESCO, Freedom of Expression Toolkit: A Guide Students, 2013, 1-86, at 16, available on the Web, URL: http://unesdoc.unesco.org/images/0021/002186/218618e.pdf., accessed on 14/4/13.
11. Freedomof Speech", available on the Web, URL: http://en.wikipedia.org/wiki/freedom_of_speech, accessed on 21/4/13. In its landmark judgment, the Indian Supreme Court in the case of the Secretary, Ministry of Information and Broadcasting vs. Cricket Association, Bengal with Cricket Association, Bengal vs. Union of India (AIR 1995 SC 1236) has also recognised the 'right to information' as part of the fundamental right of speech and expression under Article 19 (1) (a) of the Indian Constitution.
12. Randal Marlin, *Propagandaandthe Ethicsof Persuasion* (Ontario: Broadview Press, 2002), pp.226-227.
13. *Ibid.*,p.229.
14. "Freedom of Expression Everywhere", available on the Web, URL: http://www.ohchr.org/EN/NewsEvents/Pages/Freedomofexpressioneverywhere.aspx, accessed on 5/4/13.
15. Report of the Special Rapporteur on Key Trends and Challenges to the Right of All Individuals to Seek, Receive and Impart Information and Ideas of All Kinds through the Internet, 2011, UN General Assembly Doc. A/HRC/17/27. This Report is also available on the web, URL: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G11/132/01/PDF/G1113201.pdf?OpenElement.
16. "Freedom of Expression and New Media", available on the Web, URL: http://www.ohchr.org/EN/NewsEvents/Pages/FreedomExpressionandnewmedia.aspx, accessed on 5/4/13.
17. BalMukundVyas(2008),"SharingofInformationwithcitizens",*AllIndiaReporter*(JournalSection), 2008, 171-176,at176.
18. *Ibid.*
19. Justice Rajesh Tandon, "Policing the Web: Free Speech under Attack?", *Lawyers Update*, August 2011, also available on the Web, URL: http://lawyersupdate.co.in/LU/7/65.asp, accessed on 24/5/13.
20. Freedom House, *Freedom on the Net*, 2012, available on the Web, URL: http://www.freedomhouse.org/sites/default/files/India%202012.pdf, accessed on 24/5/13.
21. Reporters without Borders, *Internet Enemies Report***,** 2012, available on the Web, URL: http://march12.rsf.org/i/Report_EnemiesoftheInternet_2012.pdf, accessed on 24/5/13.

22. Google Seventh Transparency Report can be accessed online, URL: http://www.google.com/transparencyreport/, accessed on 01/5/13.
23. See Open Net Initiative Report on India. It describes India as a stable democracy with a strong tradition of press freedom, nevertheless continuing its regime of Internet filtering. Report is available on the web, URL: http://access.opennet.net/wp-content/uploads/2011/12/accesscontested-india.pdf, accessed on 30/4/13.
24. "Indian Government v Social Networking Sites", available onthe Web, URL: http://barandbench.com/indian_government_v_social_networking_sites.html, accessed on 30/4/12.
25. AIR1995SC 1236
26. Censoring the Internet", available on the Web, URL: http://barandbench.com/censoring_the_internet.html, accessed on 30/4/13.
27. India passed the Information Technology Act 2000 in May 2000 in pursuance of the United Nations General Assembly Resolution A/RES/51/162 of 30th January 1997. This Resolution adopted the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law. The Information Technology Act, 2000 came into force on 17th October 2000 and it has been substantially amended through the Information Technology (Amendment) Act, 2008. It got the Presidential assent on 5th February 2009 and came into force on 27th, 2009.
28. This writ petition has been filed by Shreya Singhal of Delhi. The writ petition can be accessed online, URL: http://www.scribd.com/doc/115031416/Shreya-Singhal-v-Union-of-India.
29. See Ministry of Communications and Information Technology, Government of India, Advisory on Implementation of Section 66A of the Information Technology Act, 2000 (9th January 2013), available on the Web, URL: http://deity.gov.in/sites/upload_files/dit/files/Advisoryonsection.pdf.