SOCIAL MEDIA – A CRITICAL LEGAL STUDY

***Author**: Nidhi Sharma, Pursuing LL.M. from Manipal university*

Social media: trending influence towards cybercrime

Abstract

Today it's an era of the cyber world and there is a massive expansion in the growth of technology. As Information Technology evolved it gave birth to cyberspace where the internet provides unrestricted access and opportunities to many people to have access to any information, data storage at any time with the help of high technology. This led to the inevitable misuse of technology in the cyber world and as a result giving rise to various "cyber crimes" at the domestic as well as at the international level. It seems that everyone is a member of a social network these days. As popularly known as "social networking" is the new fad in India and very few people could escape from its clutch. Consequently, this has given rise to many legal issues as well. Most of these legal issues pertain to online acts or omissions that are resulting in giving rise to civil and criminal liabilities.

it is noteworthy that Article 19 (1) (a) of the Constitution of India, 1950 guarantees the "Right to freedom of speech and expression". This is a fundamental right guaranteed to all citizens of India. Freedom of expression is not absolute freedom that anybody can claim to enjoy. It is always subject to certain reasonable restrictions which the State may impose in the interest of the citizens of the country. Human beings are social creatures. We need the companionship of others to thrive in life, and the strength of our connections has a huge impact on our mental health and happiness. Being socially connected to others can ease stress, anxiety, and depression, boost self-worth, provide comfort and joy, prevent loneliness, and even add years to your life. On the flip side, lacking strong social connections can pose a serious risk to your mental and emotional health.

Social media – a critical legal study

Social media law in India is regulated by the Information Technology Act which was enacted in the year 2000 to regulate, control and deal with the issues arising out of IT. Social networking media is an "intermediary" within the meaning of the Indian information technology act 2000 (IT Act 2000). Thus social networking sites in India are liable for various acts or omissions that are punishable under the laws of India[1].

Section 66A of the IT Act has been enacted to regulate the social media law in India and assumes importance as it controls and regulates all the legal issues related to social media law in India. This section restricts the transmission, posting of messages, emails, comments which can be offensive or unwarranted. The offending message can be in the form of text, image, audio, video or any other electronic record which is capable of being transmitted. In the current scenarios, such sweeping power under the IT Act provides a tool in the hands of the Government to curb the misuse of the Social Media Law India in any form.

The original Section 66 of the IT Act 2000 was only limited to hacking which proved to be ineffective in tackling the problems of wrongful emails, messages and campaigns on social media like Facebook, Twitter. However, in 2015, in a landmark judgment upholding the right to free speech in recent times, the Supreme Court in Shreya Singhal and Ors. vs Union of India, struck down Section 66A of the Information & Technology Act, 2000. The ruling which is being lauded by the common man and legal luminaries alike, found the Cyberlaw provision to be open-ended, vague and unconstitutional owing to the restriction it caused to the Indian citizens' right to free speech.

The repeal of S.66A does not however result in an unrestricted right to free speech since analogous provisions of the Indian Penal Code (IPC) will continue to apply to social media online viz. Intentionally Insulting Religion Or Religious Beliefs (S. 295A), Promoting Enmity Between Groups On Grounds Of Religion, Race Etc. (S. 153A), Defamation (S. 499), Statements

[1] https://technology.findlaw.com/modern-law-practice/understanding-the-legal-issues-for-social-networking-sites-and.html

conducing to Public Mischief (S. 505), Insulting The Modesty Of A Woman (S 509), Criminal Intimidation (S 506), Sedition (S124-A), etc.

One of the important sections that would be effective against posting offensive messages on social media would be invoking sec 499 and 500 of IPC. Under the IPC, the defamatory statement could be oral or written or in sign language or by visible representation and should be made/ published to harm or with knowledge about its defamatory character (IPC, section 499). Thus, section 499, IPC is wide enough to encompass the publication and dissemination of defamatory content via electronic means. Defamation is punishable under section 500, IPC.

Further, the law against obscenity is a reasonable restriction on the "fundamental right to freedom of speech and expression". Technology has expanded the ambit of the offence of obscenity. Today, obscene material (including pornography) is easily available at the click of a mouse and people can access it in the privacy of their homes. The Internet facilitates the creation as well as rapid transmission of such material across the world. Legal regulation is complicated by the fact that there is no universally acceptable definition of obscenity. What is considered obscene material in one country may not be considered so in another. Technologically also, there is the absence of effective filters to screen out objectionable material on the Internet.

The traditional law dealing with obscenity (including pornography) in India is contained in sections 292-294 of the IPC. Section 292, IPC prohibits the sale, letting on hire, distribution, public exhibition and circulation etc., of obscene material. Section 293 provides enhanced punishment for sale etc. of obscene material to any person under the age of twenty years. Even an offer or attempt to do so is punishable. Publishing as well as circulating obscene photographs of women is also punishable under sections 3 and 4 of the Indecent Representation of Women (Prohibition) Act, 1986. These provisions can also be used for punishing people who circulate obscene material in electronic form.

Given the above, though sec 66A of the IT Act has been held unconstitutional by the apex court still a victim of cyber offence would not be rendered remediless and could invoke the appropriate section and law to get desired relief.

Influence of Cyber Crimes in Social Media

"Cybercrime" is a combination of two terms "crime" with the root "cyber" derived from the word "cybernetic", from the Greek, "kubernân", which means to lead or govern. The "cyber" environment includes all forms of digital activities, irrespective of whether they utilise a single network. Cyberspace is borderless as no Courts across the globe can claim jurisdiction. Any illegal act which involves a computer, computer system or computer network is cybercrime. Further, any offence taking place on the computer can be said to be a cyber-offence[2]. The IT Act distinguishes between cyber contraventions and cyber offences. Former is a violation of law or rule of procedure which may or may not attract a liability to pay a penalty as the offender faces civil prosecution. However, an offence is an act prohibited and made punishable by fine and/ or imprisonment as the offender faces criminal liability[3].

Primarily, cyber-attacks can be found in three forms. First, they attack electronic identity. With the use of sophisticated malware tools, they get hold of sensitive personal information available in social media and other shopping websites; they steal credit information or create fake identity in social media. Second, attack on women and minors. Child Pornography is an industry that thrives on the growth of the cyber space[4]. Women and children are most frequently victimised compared to men by sharing obscene pictures or violent videos in the virtual world harming their reputation. Youngsters are often lured by hoax messages and fake identities in social media and they fall prey to offenders in cyberspace as well as the real world. Third, attack on infrastructures. Infrastructures are often easy targets of cyber terrorism. These attacks on vital services can paralyse a nation by causing an unprecedented impact on the economy, health care, military, power and more[5].

The Oxford Dictionary defines a social network as "A dedicated website or other application which enables users to communicate with each other by posting information, comments,

[2] https://www.business-standard.com/article/opinion/social-media-misuse-and-indian-cyber-law-115100700139_1.html
[3] 4 Section 2(n) of the Code of Criminal Procedure, 1973 and Section 40 of Indian Penal Code, 1860
[4] India ranks second in cyber attacks through social media Yuthika Bhargava April 22, 2015http://www.thehindu.com/news/national/india-ranks-second-in-cyber-attacks-through-social-media/article7130961.ece
[5] A Study on Cyber Crime and Security Scenario in INDIA Yougal Joshi1, Anand Singh International Journal of Engineering and Management Research, Volume-3, Issue-3, June 2013

messages, images, etc." This could be in the form of social media websites, blogs, and chat rooms. Anonymity and fake identity are the hallmarks of cybercrimes. Lack of awareness among netizens, poor security features associated with these websites and overuse of social media has enabled cyber offenders to engulf these innocent people into fraudulent or any other criminal transactions.

Cybercrimes that are commonly prevalent in social media are cyber defamation, cyber obscenity pornography, cyberstalking, hacking, privacy infringement, internet fraud, unauthorized disruption of the computer system through virus and using any person's copyright[6].

Impact of Privacy

Privacy involves the right to control one's personal information and the ability to determine how that information should be obtained and used. "Right to Privacy" is recognised as Fundamental Rights under Article 21 of the Constitution of India which deals with the right to life and liberty. Although the right to privacy does not find explicit mention in the Constitution, this has been recognised in various judicial pronouncements. However, the ramifications of the right to privacy in the virtual world are not a settled issue. The possible privacy infringement in social media can be illustrated through examples of Facebook and Orkut. Orkut, once touted as one of the first popular social networking sites, lost its shine when Facebook came into the picture. Many have not deactivated their account and hence were available in public for exploitation of sensitive personal information. The public search option available on Facebook enables the personal information of users to be exposed to anyone who types the name in the search engine. Opting 'Public' in privacy settings for information as gender, networks, username, email id, phone number, pictures and videos poses a risk to the identity of the person. Further, the use of applications and games available in social media runs a grave risk to the identity of the person. These applications do not work in a secure mode. They further seek access to all personal information.

[6] Legal Implications of Cyber Crimes on Social Networking Websites, Nikita Barman, International Journal of Scientific and Research Publications, Volume 5, Issue 12, December 2015 http://www.ijsrp.org/research-paper-1215/ijsrp-p4850.pdf

Cyber-attack on social media is generally understood as an infringement of the Data Protection laws. An individual's details like name, address, interests, family, etc. are often available on various social media web sites. In India, data protection is governed by Sections 43A, 72A, 69 and 69B of the IT Act.

Section 43A widens the scope of data protection by the inclusion of the definition of "Sensitive Personal Data or Information", and also imposes responsibility for "Reasonable Security Practice" to be followed by the data handlers. In case of infringement, data handlers and cyber offenders can be slapped with an exorbitant penalty which may even exceed Rs. 5 crores. Section 72A specifies liability for intermediary if he discloses "personal information" which he accessed while providing services under a contract and such disclosure was made to cause or knowledge that he is likely to cause wrongful loss or wrongful gain to a person. Sections 69 and 69B empower the State to issue directions for the interception, monitoring and even collection of traffic data or information through any computer resource for cyber security[7].

Cyber Defamation

Cyber defamation refers to the publication of defamatory content in electronic form. To determine cyber defamation, the Court has taken into consideration factors like time of occurrence, mode of publication and jurisdiction. Being borderless, determination of jurisdiction is a difficult job. In *Joseph Gutnick v. Dow Jones & Company Inc.*, the High Court of Australia upheld that the place of publication (or the jurisdiction) is the place where the defamatory statement is made and that place is the one in which that particular information is downloaded and not where the statement is uploaded or where the publisher's server resided[8]. Cyber defamation is punishable under Indian law by reading Section 499 of the Indian Penal Code ("IPC") and Section 4 of the IT Act. Earlier, cyber defamation was also recognised in S.66A which penalises the publication of information that is grossly offensive. However, this is struck by Supreme Court as it violates Article 19 (1) (a) of the Indian Constitution[9].

[7] https://www.soravjain.com/cyber-security-for-women-in-social-media
[8] *Joseph Gutnick v. Dow Jones & Company Inc.* [2001] VSC 305.
[9] *Sreya Singhal v. Union of India* AIR 2015 SC1523.

Cyber Pornography

Cyber pornography or cyber obscenity, which includes pornographic websites, pornographic magazines, provides an online medium for stimulating sexual behaviour. Earlier, the test of obscenity is the Hecklin's test- 'the tendency to deprave and corrupt those whose minds are open to such immoral influences' is considered to be obscene[10]. In *Ranjeet Udeshi v. State of Maharastra*, the Supreme Court interpreted the word 'obscene' as that which is 'offensive to modesty or decency, lewd, filthy and repulsive[11]. Hence obscenity without a social purpose or profit cannot claim protection under the ambit of free speech. Further, in *Ajay Goswami v. Union of India*, the Supreme Court propounded that the test for judging a work should be that of "an ordinary man of common sense and prudence and not an out of ordinary or hypersensitive man[12]". ICANN (Internet Cooperation for Assigned Names and Numbers) has given formal recognition to cyber pornography with the recognition of the 'xxx' domain. However, child pornography is deeply condemned across the world. Inspired by Article 9 of the Convention of Cyber Crime, the IT Act under 67B penalises child pornography. Cyber obscenity is a criminal offence. It imposes liability on the offender based on Sections 66E and 67. Section 66E protects bodily privacy by punishing the person who captures pictures of private parts of a person without consent. Publication and transmission of sexually explicit content in the online medium are prohibited under Section 67A.

Cyber Stalking

This includes the acts to harass or contact another in pursuance of stalking another person by keeping anonymous identity using the electronic medium. The Criminal Law (Amendment) Act, 2013 adds a new section 354D to penalise stalking.

Fraudulent Transactions and Misrepresentations

Impersonation is one of the most widely seen fraudulent transactions in social media. Social Networking websites are replete with fake profiles which are created with the sole purpose of taking out information and other personal details like bank account number, credit card number.

[10] *Regina v.Hicklin* (1868) 3 QB 360
[11] *Ranjeet Udeshi v. State of Maharastra* AIR 1965 SC 881
[12] *Ajay Goswami v. Union of India* (2007) 1 SCC 169

Virus Attack

A virus attack is generally executed by sending messages on social networking websites or asking the person to open the link to the computer. Virus contamination destroys, alters, damages data residing in a computer or cloud. Section 43 (c) of the IT Act imposes liability upon the offender to pay compensation to the person who is affected by the introduction of any computer contaminant or virus into any computer, computer system or computer network.

Hacking

Hacking is usually a premeditated process, where the hacker studies security features of the target and develops programs under it, to gain unauthorized access. In simple terms, hacking means trespass in the virtual world. Section 43 of the IT Act punishes unauthorized access to a computer resource committed "dishonestly or fraudulently". Here, the aggrieved party must prove mens rea.

Cyber Bullying

Posting any kind of humiliating content on social media or sending vulgar messages online, or threatening to commit any act of violence, or stalking using calls, messages or threatening of child pornography is called cyberbullying. Many Indian laws can allow a woman to deal with this and with the help of the Indian police, you can sort this particular issue. One of the best examples here is singer Chinmayi was threatened by a few bunches of people on Twitter and she took police's help to detain them as she was getting rape and murder threats from people for quite some time.

Information Theft

Informational theft occurs when an imposter identifies key pieces of personally identifiable information like social security, driving license number to impersonate someone else. Many people tend to store passwords or bank details on their email. Many people try to have a very private conversation on Facebook or Instagram messengers. Businesswomen are also more likely to be at the risk of information theft especially concerning their organization. Women bloggers these days are faced with plagiarism of various types. When they try to open their business page

on Facebook for the first time, there are chances that their competitors would already have promoted bad things to bring down their reputation.

Photo Morphing

Photo morphing is a special effect that allows a person to morph or change one image or shape into another without any difficulty. As per the 4th quadrant of 2017, there are roughly around 3.2 Billion images shared every day. It is easy for a hacker to use your images, morph them and then use them for porn sites or blackmailing for financial/sexual gains. You can't stop anyone from morphing. If your images are publicly available, people can easily access them and make use of them to morph. Every popular male and female celebrity are probably photo-shopped and used by most porn sites to satisfy sexual fantasies. You never know, when someone takes your photographs and uses them.

Preventive Measures

To improve cybersecurity various precautionary steps can be kept in mind by netizens. These include:

- Always avoid sending any photograph online particularly to unknown friends or strangers to avoid misuse of photographs.
- Always update anti-virus software to guard against virus attacks.
- Backing up files enables data loss due to virus attack.
- Payment made for accessing games and applications in social networking sites must be made in the secure payment system to avoid invasion of credit information.
- Kids must be given awareness classes about social media cybercrimes.
- Security programmes that give control over cookies must be preferred.
- Website owners and intermediaries must monitor traffic and regulate any abnormality on the website.

Conclusion

Cybercrimes have been menacing social media since its inception. This is manifested in form of fraudulent transactions, hacking, virus attack, cyber defamation and cyberstalking. Even though

India has effective laws to deal with these crimes, the conviction rate is negligible. Cyber Forensics is a growing area. It must be promoted to determine methods to detect Cyber Evidence. Further, necessary amendments must be made in Indian law to be read harmoniously with the IT Act to control Cybercrimes.