

## LEGAL CONTROL ON SOCIAL NETWORKING SITES IN INDIA

| Authored By : Manoj Singh |

In present days social networking sites are very much popular. We are spending our time on social networking sites. Facebook, YouTube, LinkedIn, Twitter are some popular social networking sites. Social networking websites are those websites which provide us a platform on which we can share our ideas, interests, formations, photos, videos etc but on the name of freedom of speech and expression people are creating nuisance on social networking sites by posting offensive materials to promote religious hatred and incendiary materials. A number of provisions are applicable on regulating it but important RTI Act, I.T. Act, 2000 and I.T. Amendment Act, 2008 main statutes. Although a number of laws are applicable on social networking sites still there is some lacuna as they are not sufficient to tackle problems originated from social networking sites. A separate and strict law is required to tackle this problem efficiently.

Key words- social networking sites, RTI Act, I.T. Act, 2000 and I.T. Amendment Act, 2008.

In present days we social networking sites are very much popular. We are spending our time on social networking sites. Facebook, YouTube, LinkedIn, Twitter are some popular social networking sites. Social networking websites are those websites which provide us a platform on which we can share our ideas, interests, formations, photos, videos etc. Such websites allows chat between friends. In 1994 first networking site was developed and the AOL messenger service was the first popular instant messaging services evolved in 1997. THEGLOBE.COM, Myspace.Com, facebook, twitter came into existence in 1995, 2003, 2004 and 2006 respectively.

Facebook was basically designed for Harvard students but later on it was opened to the public in 2006. It was founded by Mark Zuckerberg myspace a highly customize social network started in 2003, continues to reposition itself in industry. Twitter is phenomenon that transcends social networking to provide an outlet for news, trends etc and LinkedIn has over 50m member worldwide<sup>18</sup>. As of September 2014:

71% of online adults use Facebook

23% of online adults use Twitter

26% use Instagram

28% use Pinterest

28% use LinkedIn.<sup>19</sup>

On the name of freedom of speech and expression people are creating nuisance on social networking sites by posting offensive materials to promote religious hatred and incendiary materials. According to Justice Markandey Katju “The pictures and other content show

<sup>18</sup> Fabio Giacomini and Mohd. Hasan Zaidi, Electronic Evidence, 896, (Ed.1<sup>st</sup>, 2012).

<sup>19</sup> <http://www.pewinternet.org> accessed on 01march, 2018.

religious figures of certain communities in a highly offensive and even pornographic manner. Such material is bound to create religious hatred and lead to most undesirable consequences,” the former Supreme Court judge said in a statement.

His comments come in the wake of the controversy triggered by Mr. Sibal's comments about objectionable material on the Internet.

Justice Katju said that following the controversy he had carefully examined the content, pictorial and the rest on the Internet and had come across highly offensive material.

“The pictures I have seen not only hurt the religious sentiments of members of certain religious communities, but are also outrageous, inflammatory and egregious, and are bound to disturb peace and result in serious law and order problems.”

He said that as per section 153A of the IPC, it is a criminal offence to promote, or attempt to promote disharmony, feelings of enmity or hatred or ill-will among different religious communities or groups, or do an act which is prejudicial to the maintenance of harmony among different religious groups or communities, and which is likely to disturb public tranquility.

“I have carefully perused the material in question and am of the opinion that there can be no manner of doubt that they attract Section 153A of the Indian Penal Code. Hence I am of the view that such offensive material should be removed or filtered out from the social network sites on the Internet immediately.

“Article 19(1)(a) of the Constitution which provides for freedom of the media, is subject to Article 19 (2) which states that restrictions can be placed on this freedom in the interest of public order, decency and morality.

“I strongly support freedom of the media; no freedom is absolute, and all freedoms are subject to reasonable restrictions in the public interest<sup>20</sup>.”

As for as legal control on social networking websites three statutes are important RTI Act, I.T. Act, 2000 and I.T. Amendment Act, 2008.

Under the Information Technology Act, 2000, the Central Government has enacted various rules and regulations regarding social media. Information Technology (Reasonable Security Practices And Procedures And Sensitive Personal Information) Rules 2011. First statute of India which defined sensitive personal data Sensitive personal data or information of a person means such personal information which consists of information relating to;—

- (i) password;
- (ii) financial information such as Bank account or credit card or debit card or other payment instrument details;
- (iii) physical, physiological and mental health condition;
- (iv) sexual orientation;
- (v) medical records and history;

<sup>20</sup> <http://www.thehindu.com/news/national/katju-favours-filtering-of-offensive-internet-content/article2710182.ece> accessed on 03 March, 2018.

(vi) biometric information;

(vii) any detail relating to the above clauses as provided to body corporate for providing service; and

(viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise: provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.

For the purpose of protecting such sensitive personal data, the Government has mandate that any legal entity who is processing, dealing or handling sensitive data must implement reasonable security practices and procedures<sup>21</sup>

Social networking sites come under the definition 2(1) (w) of I.T.Act, 2000 so Information Technology (Intermediaries Guidelines) Rules 2011 are applicable on them.

The intermediary shall observe following due diligence while discharging his duties, namely:

(1) The intermediary shall publish the rules and regulations, privacy policy and user agreement for access-or usage of the intermediary's computer resource by any person.

(2) Such rules and regulations, terms and conditions or user agreement shall inform the users of computer resource not to host, display, upload, modify, publish, transmit, update or share any information that —

(a) belongs to another person and to which the user does not have any right to;

(b) is grossly harmful, harassing, blasphemous defamatory, obscene, pornographic, paedophilic, libelous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever;

(c) harm minors in any way;

(d) infringes any patent, trademark, copyright or other proprietary rights;

(e) violates any law for the time being in force;

(f) deceives or misleads the addressee about the origin of such messages or communicates any information which is grossly offensive or menacing in nature;

(g) impersonate another person;

(h) contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer resource;

<sup>21</sup> S.8 of Information Technology (Reasonable Security Practices and Procedures and Sensitive, 2018.Information Personal) Rules 2011 accessed on 08 March, 2018.

(i) threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign states, or public order or causes incitement to the commission of any cognizable offence or prevents investigation of any offence or is insulting any other nation

(3) The intermediary shall not knowingly host or publish any information or shall not initiate the transmission, select the receiver of transmission, and select or modify the information contained in the transmission as specified in sub-rule (2): provided that the following actions by an intermediary shall not amount to hosing, publishing, editing or storing of any such information as specified in

Sub-rule: (2) —

(a) temporary or transient or intermediate storage of information automatically within the computer resource as an intrinsic feature of such computer resource, involving no exercise of any human editorial control, for onward transmission or communication to another computer resource;

(b) removal of access to any information, data or communication link by an intermediary after such information, data or communication link comes to the actual knowledge of a person authorized by the intermediary pursuant to any order or direction as per the provisions of the Act;

(4) The intermediary, on whose computer system the information is stored or hosted or published, upon obtaining knowledge by itself or been brought to actual knowledge by an affected person in writing or through email signed with electronic signature about any such information as mentioned in sub-rule (2) above, shall act within thirty six hours and where applicable, work with user or owner of such information to disable such information that is in contravention of sub-rule (2). Further the intermediary shall preserve such information and associated records for at least ninety days for investigation purposes,

(5) The Intermediary shall inform its users that in case of non-compliance with rules and regulations, user agreement and privacy policy for access or usage of intermediary computer resource, the Intermediary has the right to immediately terminate the access or usage rights of the users to the computer resource of Intermediary and remove non-compliant information..

(6) The intermediary shall strictly follow the provisions of the Act or any other laws for the time being in force.

(7) When required by lawful order, the intermediary shall provide information or any such assistance to Government Agencies who are lawfully authorized for

Investigative, protective, cyber security activity. The information or any such assistance shall be provided for the purpose of verification of identity, or for prevention, detection, investigation, prosecution, cyber security incidents and punishment of offences under any law for the time being in force, on a request in writing stating clearly the purpose of seeking such information or any such assistance.

(8) The intermediary shall take all reasonable measures to secure its computer resource and information contained therein following the reasonable security practices and procedures as prescribed in the Information Technology (Reasonable security practices and procedures and sensitive personal Information) Rules, 2011.

(9) The intermediary shall report cyber security incidents and also share cyber security incidents related information with the Indian Computer Emergency Response Team.

(10) The intermediary shall not knowingly deploy or install or modify the technical configuration of computer resource or become party to any such act which may change or has the potential to change the normal course of operation of the computer resource than what it is supposed to "perform thereby circumventing any law for the time being in force:

Provided that the intermediary may develop, produce, distribute or employ technological means for the sole purpose of performing the acts of securing the computer resource and information contained therein.

(11) The intermediary shall publish on its website the name of the Grievance Officer and his contact details as well as mechanism by which users or any victim who suffers as a result of access or usage of computer resource by any person in violation of rule 3 can notify their complaints against such access or usage of computer resource of the intermediary or other matters pertaining to the computer resources made available by it. The Grievance Officer shall redress the complaints within one month from the date of receipt of complaint.

Expressing concern over misuse of social media and internet, particularly after the controversial section 66A of the Information Technology Act was scrapped by the Supreme Court, a bench of Justices Dipak Misra and Prafulla C Pant said Parliament should bring a new law to regulate the social media<sup>22</sup>.

Social networkings sites are easily accesible.They have direct impact on mind which is misused now days. Most of the People think that materials on social networking sites are true but it not always correct. Although a number of laws are applicable on social networking sites still there is some lacuna as they are not sufficient to tackle problems originated from social networking sites. A separate law is required to tackle this problem efficiently.

*an imprint of cybertalkindia*  
www.cybertalkindia.com

<sup>22</sup> <http://timesofindia.indiatimes.com/tech/social/SC-calls-for-new-law-to-regulate-social-media/articleshow/48384370.cms> accessed on 09<sup>th</sup>, March, 2018.