INTERMEDIARIES UNDER IT ACT 2008

Jahnavi Singh*

Abstract

The Information Technology Bill, 2008 has been passed by both the houses of Parliament in the month of December, 2008 and was signed by the President of India on February 5, 2009. The Amendment Act aims to make many changes in the existing Indian cyber law framework, which includes incorporation of Electronic Signature i.e. enable authentication of electronic records by any electronic signature technique. There were also insertions of new express provisions to bring more cyber offences within the purview of the Information Technology Act, 2000. There are various provisions in the new amendment which were relating to data protection and privacy as well a provision to curb terrorism using the electronic and digital medium. The original Act is basically the legislation which provide legal status for e-commerce and e-transactions so as to facilitate e-governance and to prevent computer based crimes and ensure security practices and procedures with the context of widest possible use of information technology worldwide. The amendment has defined "intermediary". Now, Intermediaries are required to remove unlawful data or content on receiving information about it. In today's world, technology has its own importance. But it's really a matter of concern that India does not have any legislation to basically deal with the matter related to privacy but some or the other way IT Act provides protection only in the form of damages and nothing else. The other important section in this act is the importance of intermediaries and at what extend they can provide information or can keep any data with them only. The main aim of writing this paper is to give society a basic idea with regard to protection of data and what is the importance of intermediaries under information technology act and what are their liabilities under this act. With regard to internet, the IT Act 2000 says that the intermediaries should protect the data they collect and handle, and should impose conditional liability on intermediaries for their hosted content if such content infringes the privacy of an individual. However, these laws are inadequate to deal with the new concerns that have arisen as a result of the rapid advances in technology and re-shaping of the internet.

Keywords: *Intermediaries, Liability of intermediaries, Protection of data.*

* *Student* @ Amity Law School, Noida; Contact: +919811446735; Email: avipriya66@gmail.com

INTRODUCTION

In today's world, technology is playing a very important role. Now a day's, people are so busy in their social life that they don't get time to spend some time with their loved once. We can say that technology is controlling the whole society or world. Technology is good for the society as well as evil for the society. If we talk about technology in good sense then the first reason why technology is good for the society is that it connects us throughout the world.[1] We basically share our past, enrich our present and secure our future through the use of social media. Skype and Google are the best way to connect with our friends, family. Texting, calling, and e-mailing have made a great chance as by which we keep in touch and these forms of communication only continue to advance.

The second reason why Technology is good for the society is that it conserves energy and produces more goods. HOW? Basically technology allows us to find different alternatives of using non Renewables and costly resources. From hybrid vehicles to energy efficient light bulbs, there are ways to save everywhere. One machine can do today in minutes what in years past would have taken days to accomplish. The third reason why technology is good for the society is that it helps in doing online payments, and for business purpose technology is playing a very important role. For example: there are many social websites which are doing their business in a very good way and is also expanding their business with the help of technology. Some of the best websites are Flipkart, Amazon, Jabong, etc. As we are being saying that technology is good for society but it is also evil for the society. HOW? Basically the first reason is that Cyber bullying and sexual predator activity is reaching new lengths. As technology grows, so does the means by which predators and bullies can target their victim? The second reason is the depravation of privacy and security. We know that world is experiencing many advances in the technology but they are also facing problems with regard to privacy and security. Privacy issues are basically connected with tracking location and spying on information.[2] It is correctly said that it is very easy for the professionals to trace and keep an eye on any of the electronic devices that connects to a network by simple tracking the IP location. Now a days some advertising websites can track location, watch what users do and see what the users like and dislike by s doing a survey of which products are more preferred, while some countries usually focus on another countries to maintain its internal security and check on extremely important information

[1] Apar Gupta on information technology Act, p.9
[2] *Ibid* at 11

which would be necessary for them. The third reason why technology is not good for the society is the social issues. For the benefit purpose enormous websites are being established and games are one of them. Some of the games make it more similarities to the real life. Games are so realistic that they are killing and other disgusting scenes are included in games. These serious effects are basically divided into two main categories which are tempering fluctuating and lack of social skills. The forth reason is that people use to thread the victims by making amigos videos which may lead to suicide of the victims.

Initially technology was made to serve the world but people have use it in a wrong way which have basically caused serious problems that are health problems, privacy problems and social problems. Health problems are considered as critical issues which affects mental and physical health of the user. Moreover, privacy is negatively affected due to spying and stealing of information of users. One of the important points is that the socializing is getting affected by rapid change of temper and lack of social skills. People should spend less time and communicate with each other and use technology in rates that it doesn't hurt people to avoid getting any problems in the future.

So to protect the technology activities from all frauds government has enacted Information Technology Act 3000 and it was amended in the year 2008 and was named as Information Technology Act (Amendment) 2008.

INFORMATON TECHNOLOGY ACT, 2008

Information Technology act 2000 was passed in the month of October 2000 by the Parliament. This act basically dealt with cybercrime and electronic commerce. It also establishes a Cyber Appellate Tribunals and penalties are also imposed under this act. So before doing any crime related to technology people use to think 100 times as now a day's it's not easy to do any types of crime related to technology. After few years in the year 2008 the amendments were taken place where a new section was introduced i.e. Section 66A which penalised sending of offensive messages. Section 69 also came into existence which gave power to the authorities for the interception or monitoring of any information through any computer resource. The original act was developed to promote e-commerce and also to prevent cybercrimes.[3]

Information Technology Act 2008 amendments were done as the original bill has failed to

[3] Section 69 of IT Act, 2008

improve further development of IT sector and related security concerns. Many changes were taken place and some of them were a new definition were given to the word "communication device".[4] This act has focused on implementing the electronic signature by making the owner of the given IP address responsible for content accessed and have also focused on making corporation responsible for implementing effective data security practices and liable for the breaches.

These Amendments have been criticized for decreasing the penalties for cybercrimes and also for the government to monitor, lacking sufficient safeguards to protect the civil rights of the individuals. Section 69 of this act authorizes intercept, and block data at its discretion. Pavan Duggal a law consultant says that 'The act has provided the government with the power of surveillance block data traffic. This new power has given the government a texture and colour of being a surveillance state.

OBJECTIVES OF THE ACT

- To provide legal recognition of electronic records and digital signature.
- To establish a regulatory authority to supervise the activities of cyber crimes.
- To provide civil and criminal liability for contravention of this act as to prevent misuse of e- business transaction.
- To amend Reserve Bank of India Act 1934 to facilitate electronic fund transfer between the financial institutions.
- To provide legal recognition to business contacts and creation of rights and obligations through electronic media.
- To suitability amend existing laws in India to facilitate e- commerce.

Till now we came to know many things about the technology and The Information Technology Act, 2008.

INTERMEDIARIES UNDER INFORMATION TECHNOLOGY ACT, 2008

Intermediaries have been defined under section 2 (1) (w) of Information Technology Act, 2008.

[4] Section 2(1) of IT Act, 2008

Intermediaries are the person who on behalf of any other person stores or transmits that message or provides any services with respect to that message.[5] This act has clarified the definition of Intermediaries including the telecom service provider, web-hosting service provider, online payment sites, internet service provider, and many more. Intermediaries are entitled that provide services enabling the delivery of online content to the end user. Some of the players involved in this are as follows:

- *Internet Service Provider*: ISPs like Airtel basically help users to connect to the internet by means of wired or wireless connections.
- *Web Hosts*: These are service providers like godaddy.com that provide space on server computers to place files for various web sites so that these sites can be accessed by users.
- *Interactive Websites*: These include social sites such as Facebook, Twitter, snapchat etc, which act as a platform to store the blogging platform such as BlogSpot or word press. There are auction sites such as EBay etc.
- *Cyber Cafes*: All information as being given from here and basically are used by the society.

An intermediary may held to be liable for infringing content hosted on its platform only when it has specific or actual knowledge or a reason to believe that such information may be infringing. Insertion of advertisements and modification of content formats by an intermediary via an automated process and without manual intervention does not result in the intermediary being deemed to have actual knowledge of the content hosted.

Once an intermediary has been informed by a complainant of potentially infringing content hosted on its platform, it is not obligated to proactively verify and remove content subsequently hosted on its platform that may infringe the intellectual property rights of the complainant.

Before the Information Technology Amendment Act 2008 came into force, the scenario in India was worse for intermediaries. Intermediaries were liable for their users content. This led to the arrest of Bazee.com chief Avinash Bajaj in connection with the sale of the infamous DPS Noida MMS clip CD on the website. Post the Bazee.com fiasco the Information Technology Laws have been amended The Information Technology (Amendment) Act 2008 makes a genuine

[5] *Ibid*

effort to provide immunity to the intermediaries but needs to plug in some gaps so as to enable the intermediaries to operate without fear and inhibitions.

SECTION 79 OF INFORMATION TECHNOLOGY ACT, 2008

Section 79 of information technology regulates the liability of a wide range of intermediaries in India. So as per section 79 intermediaries are also expected to adhere to several sets of fairly detailed rules that have been issued under this provision.[6]

According to section 79(1) of Information technology act, 2008 the intermediaries are not liable for any third party information, data as made available by him. Section 79(2) of information technology act says that the provision of sub section (1) will apply only:

a) if the function of intermediaries is limited as to providing excess to communication system over which the information has been made available basically by the third parties which is being transmitted or temporarily stored or

b) The second thing is that if the intermediaries does not initiate the transmission or does not select the receiver of the transmission, or does not select or modify the information contained in the transmission

c) The intermediaries observes that as due diligence led to discharging of his duties and also to observe such other guidelines as the central government have applied.

As the second provisions deals with where the sub section (1) of this act will apply same is the sub section (3) of this act says where the first provision will not apply. It says that sub section (1) of this act will not apply:

a) If the intermediaries have agreed together or abetted whether by threads or promise or

b) upon receiving or getting any actual knowledge or has been notified by the appropriate Government or any agency that any information, data or communication link residing in or has been connected to a computer resource which is being controlled by the intermediary and has been used to commit the unlawful act, the intermediary basically fails to expeditionly remove or disconnect the access to that material on that resource without going through the evidence in any manner.

[6] Section 79 of IT Act,2008

HOW DOES INTERMEDIARIES RULE OPERATE?

The new rule is mandatory for the intermediaries as to impose a set of rules and regulations on users. The rules further tell about the terms that would include a broad list of categories of content which should not be posted or used by the users. Some of the list of unlawful content involves information that is greatly harmful, harassing the person,, [7]defamatory, obscene, pornographic, hateful, or racially, ethnically objectionable, , relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever it may contain. These words are too bad and may result in broad interpretation and may content to imprisonment.

Now the second important factor is that if any person aggrieved by any content on the internet can ask the intermediaries to take down such content. Intermediaries are in liability to remove access to such content within a period of 36 hours from the time of receipt of the complaint. The rules do not provide for the creator of the content to respond to this complaint. In fact, the rules do not even provide for the intermediaries to inform the user who posted the content regarding the complaint. The intermediaries that do not comply with take-down notice lose the protection from any legal liability that could arise over user content.

This rule basically also deal with the government's power to access user information from the intermediary and the power of the intermediary to disconnect user access. The Rules mandate that intermediaries have to co-operate with government agencies and provide information to them for the purpose of verification of identity, or for prevention, detection, investigation, prosecution etc. when a request has been made by the agency in writing. The Intermediary also has to inform the user that if in future if there might be a case of violation of any rules and regulations the user agreement or privacy policy and the intermediary shall terminate the access to its service.

CONCLUSION

The Act says that however, under Section 79 no directions are given to intermediary to install any appropriate software so as to prevent transmission of obscene or pornographic material or any infringed material. Therefore, intermediary must be given effective directions for ensuring installation of appropriate software for preventing pornographic or obscene material being transmitted over their networks and protection against viruses.

[7] Available at: www.inflibnet.com