International Journal of Pure and Applied Mathematics
Volume 119 No. 17 2018, 1717-1727
ISSN: 1314-3395 (on-line version)
url: http://www.acadpubl.eu/hub/
Special Issue

http://www.acadpubl.eu/hub/

A Critical Study on Cyber Defamation and Liability of ISPS

[1]T. Pradeep and [2]Aswathy Rajan

[1]Saveetha School of Law, Saveetha Institute of Medical and Technical Sciences, Saveetha University, Chennai. haipradeep@live.com

[2]Saveetha School of Law, Saveetha Institute of Medical and Technical Sciences, Saveetha University, Chennai. aswathyrajan.ssl@saveetha.com

Abstract

Accessibility, anonymity, privacy, seclusion of one's own space, and the interactive, responsive nature of communications on the internet, has made the users far less inhibited than before especially about the contents of their messages. There is no dearth of Soniya Gandhi-Manmohan Singh jokes and cartoons coming as your regular Facebook updates. The internet has made it far easier than ever before to disseminate defamatory statements to a worldwide audience with impunity. Now, on the internet everyone can be a publisher as well as a victim of defamatory publication. A defamatory allegation need only be disclosed to one person for publication to be proved. Since a publication on internet can be circulated to literally countless number of people, every time an email is forwarded to another person or defamatory content is shared on Facebook, it is published again and again creating further cause of action. This has led to cyberspace becoming a highly prone area for defamation. No doubt a John Doe always lurks around in the cyberspace. The issue is further aggravated by the difficulty in identifying the perpetrator, and the degree to which Internet Service Providers (ISP's) should be held accountable for facilitating the defamatory activities.[i]

The present paper tries to point out relevant legal provisions on cyber defamation and liabilities of internet service providers or intermediaries in the light of some of the most landmark judgments on this issue in India and UK. The author further tries to highlight some of the practical difficulties with prosecution in such cases especially with regard to jurisdiction and forum shopping. Since India has just emerged as a new battleground for cyber disputes and crimes, the cases are not many but nonetheless they indicate how India is lagging behind as regards legislative framework covering information technology law and prevailing lacunae in the current legislations.

Key Words: Cybercrime, cyber phishing, defamation, information technology, publishers.

1. Introduction

Cyberspace is a technical term used for the electronic medium of computer networks, in which online communication takes place. It comes alive only when two or more computers are networked together. The term has a very wide meaning and is not only restricted to the internet but also includes computers, computer networks, the internet, data, software etc. The crimes that are committed by using the computer as an instrument, or a target or a mean for perpetuating further crimes falls within the definition of cyber crime. Cyber law is the law that governs the crimes committed within the cyberspace. Cyber Defamation is also a cyber crime.[ii]

Cyber defamation is publishing of defamatory material against another person with the help of computers or internet. If someone publishes some defamatory statement about some other person on a website or send emails containing defamatory material to other persons with the intention to defame the other person about whom the statement has been made would amount to cyber defamation.[iii] The harm caused to a person by publishing a defamatory statement about him on a website is widespread and irreparable as the information is available to the entire world. Cyber defamation affects the welfare of the community as a whole and not merely of the individual victim. It also has its impact on the economy of a country depending upon the information published and the victim against whom the information has been published. [iv]

2. Aim of the Study

- To understand about the cybercrime.
- To analyses and use the preventive measures available to control cyber defamation.
- To know the reason for cyber hacking.
- To study about the cyber defamation in publisher's liability.

3. Statement of the Problem

Whether the Indian Penal Code and Information Technology Act provides adequate punishment regarding cyber defamation in publisher's liability in comparison with other cyber-crimes.

Hypothesis

HO: There is no effective legislation regarding the cyber defamation in publisher's liability.

HA: There is effective legislation regarding the cyber defamation in publisher's liability.

4. Materials and Methods

The researcher more on relied on the secondary source of data such as books, journals, e-sources, articles and newspaper. Due to the shortage of the time, the researcher in which primary source of the data such as interview and field research is not more adequacy in result of data collection and interpretation in which parameters so described Under this counteractive action and early intercession structure, immense research is being directed to figure out which of the numerous current projects are genuinely powerful.

5. Research Methodology

The present research is conclusive, descriptive and based on non- empirical design. Qualitative data was generated to test the research hypothesis. In order to collect data on the dimensions of the study, a research instrument was designed. The study was conducted on secondary source of data books, articles, journals, e-sources, theories and the relevant provision with decided case laws. Focusing on these three areas put forward specific research problems.

Sample Size Calculation Sources of Study

Only secondary sources are available. The secondary sources include books which is available in English, E-sources. Primary source of interview can't be conducted which researcher unable to refer due to shortage of time.

6. Limitation of the Study

Primary sources, compared to the secondary sources, are limited. Researcher had to rely more on secondary sources available in books, e-sources gather information about the study. The researcher was unable to visit and interview the personnel like construction workers and their employers.

Cyber Defamation in India

In India, a person can be liable for defamation both under civil and criminal law. Section 499 of the Indian Penal Code which deals with defamation when expanded also covers the cases of cyber defamation. However, with the new amendment in the Information Technology Act, 2000, India now has express provision on Cyber Defamation.[v]

Section 66A of Information Technology Act, 2000 "Any person who sends, by means of a computer resource or a communication device,-

- any information that is grossly offensive or has menacing character; or
- 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 makes by making use of such computer resource or a communication device,

- 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."

Liability of ISPS & Intermediary in India

Section 79 of Information Technology Act, 2000 As per Section 79 of the IT Act, ISPs are not liable for any third party information, data, or communication link made available or hosted by them so long as

- their function is limited to only providing access to communication system;
- they do not- (a) initiate transmission; (b) select the receiver of the transmission, and (c) select or modify the information contained in the transmission
- they exercise due diligence in their duties and adhere to any guidelines which may be prescribed.

However, ISPs can be held liable in the following situations

If they have conspired, abetted or induced in the unlawful act,

If, they fail to expeditiously remove or disable access to any information, data or communication link upon receiving the knowledge or on being notified by appropriate Government agency that such information, data or communication link is being used to commit unlawful act without interfering with the evidence;[vi]

As a curious deviation from the position of law in commonwealth countries, the IT Act, 2000 bears a certain degree of similarity with the laws in the United States in cases of cyber defamation. Though the new amendment does not shift the burden of proof from defendant to plaintiff, it definitely makes it easier for the defendants to prove their innocence in the event they have acted bona fide and complied with the obligations under Section 79 of the Act and Rule 3 of the IT Rules, 2011. However, although ISP's are theoretically not liable for posting and transmitting defamatory information, they are nevertheless frequently joined as defendants in defamation lawsuits because of their deeper pocket.[vii]

The question that next comes up is the extent of involvement of ISPs in publication of defamatory content. In this context, it is important to understand and appreciate the difference between primary publisher and secondary publisher. The U. K. Defamation Act 1996 defines a primary publisher as – "a person whose business is issuing material to the public and who issues the material in the course of that business and those who are only involved in processing, making copies, distributing or selling any electronic medium in which the statement is recorded are defined as secondary publishers." A secondary publisher can thus escape liability for handling third party

defamatory material if it is able to prove that (a) it was merely acting as a conduit; (b) it exercised due diligence and, (c) it was not aware of the defamatory nature of such material and immediately removed the content once informed or notified by appropriate Government agency. Therefore, ISPs in certain cases may act as primary as well as secondary publishers. If the ISPs exercise editorial control over messages posted on bulletin boards, use Board Leaders to enforce the content guidelines or provide them with an emergency delete function to control content there is great likelihood that they may end up being treated as a primary publisher.

Comparison of India with Other Countries on the Basis of Cyber Law, Crime and IT Services

This blog is about a small comparison between developing countries like India and developed countries like USA and China . India is developing day by day in every sector but in IT and cyber sectors it is far back than other developed countries like USA and China .In developed countries awareness and knowledge among the people regarding cyber and IT law is much better than the developing countries. People are more aware regarding their rights and privacy in developed countries .[viii] Most of the countries have the separate rules , regulations and laws which maintain n deals with the cyber sectors of the country which provides a security to the citizens of that country . India also has a separate act called IT Act which was amended in 2008 last time which was come into force in the year 2000 first time. But this act not that sufficient that it can manage the IT and cyber sectors of India properly . It is like a coin which has two faces; good as well as bad.[ix]

IT act (amended)2008 provides many reliefs regarding cyber crimes to the common people of India because of which common people are now safe from different types of crimes like voyeurism which is mentioned under section 66 E of IT act and section 345C of the IPC 1860 also provides same ; one of these crimes is hacking mentioned under section 43 of IT act and some others are cyber terrorism , identity theft etc. But in developed countries there are so many advanced laws and acts are imposed for the security of cyber users like in China and USA there are some special acts for the individuals.[x]

In developed countries like China and USA the new Cybersecurity law is too tight and brings restrictions to foreign companies doing business in the countries which protects the countries and controls the cybercrime rates. On the other hand India also making many efforts to make the country efficient to provide better services and protection in cyber sector. In 2013 , government of India introduced a National Cyber Security Policy with the aim of protecting information infrastructure, reducing vulnerability , increasing capabilities and safeguarding it from cyber-attacks . India is now on the way to make the IT act more efficient which needs some more amendments which can be possibly done in near future and our country will also compete the foreign developed countries in cyber and IT protection sector.[xi]

Case Laws in India

Asia's first case of cyber defamation was filed in India in 2001. The case was SMC Pneumatics India Pvt. Ltd. v. Jogesh Kwatra1. In this case, the defendant Jogesh Kwatra, an employee of the plaintiff's company started sending defamatory emails to his employers and different subsidiaries of the company all over the world. The plaintiff thereafter filed a suit for permanent injunction restraining the defendant from posting such defamatory remarks. The Hon'ble Delhi High Court in this case allowed an ex-parte ad interim injunction observing that a prima facie case was made out by the plaintiff and restrained the defendant from posting such remarks.[xii]

Avnish Bajaj vs. State[xiii]

Facts of the Case

Another significant case was Avnish Bajaj vs. State2 more popularly known as DPS MMS Scandal case. The case involved an IIT, Kharagpur student Ravi Raj, who placed on the baazee.com a listing offering an obscene MMS video clip for sale with the username 'aliceelec'. Despite the fact that baazee.com have a filter for posting of objectionable content, the listing nevertheless took place with the description, "Item 27877408 – DPS Girls having fun!!! full video + Baazee points." The item was listed online around 8.30 pm in the evening of November 27th 2004 and was deactivated, around 10 am on 29th November 2004. The Crime Branch of Delhi police took cognizance of the matter and registered an FIR. Upon investigation, a charge sheet was filed showing Ravi Raj, Avnish Bajaj, the owner of the website and Sharat Digumarti, the person responsible for handling the content, as accused. Since, Ravi Raj absconded; the petition was filed by Avnish Bajaj, seeking the quashing of the criminal proceedings.

Arguments

The court in this case observed that a prima facie case for the offence under Section 292 (2) (a) and 292 (2) (d) of Indian Penal Code (IPC) is made out against the website both in respect of the listing and the video clip respectively. The court noted that "[b]y not having appropriate filters that could have detected the words in the listing or the pornographic content of what was being offered for sale, the website ran a risk of having imputed to it the knowledge that such an object was in fact obscene", and thus it held that as per the strict liability imposed by Section 292, knowledge of the listing can be imputed to the company.

As regards Avnish Bajaj, the court surprisingly held that since the Indian Penal Code does not recognize the concept of an automatic criminal liability attaching to the director where the company is an accused, the petitioner can be discharged under Sections 292 and 294 of IPC. Eventually, Avnish Bajaj in this case was not declared guilty

The author respectfully submits that there was no sound reason to absolve the director, Avnish Bajaj in this case. The concept of corporate criminal liability could have been applied to impose appropriate penalty on the director. The argument also derives support from Article 12 of the European Convention on Cyber Crime which provides for imposition of criminal liability on the legal person having a power of representation, authority to take decisions and exercise control. Clause 2 of Article 12 of the Convention provides that a legal person can be held liable where the lack of supervision or control by a natural person acting under his authority has made possible the commission of a criminal offence.

Although India has not ratified this Convention as yet, the said provision could have been taken as a guiding principle to impose liability on Avnish Bajaj. Furthermore, the stance taken by the Court in this case does not even contribute to the determination of the extent of liability of ISPs and their directors, as the Court did not specifically delve into these issues and settle the law on this subject.[xiv]

Vyakti Vikas Kendra, India Public Charitable Trust Thr Trustee Mahesh Gupta & Ors vs. Jitender Bagga & Anr.[xv]

Facts of the Case

Delhi High Court in this case first held Google to be an "intermediary" within the definition of Section 2(1)(w) and Section 79 of the Information Technology Act, 2000. The Court accordingly pointed out that under Section 79(3)(b) of the IT Act, 2000, Google is under an obligation to remove unlawful content if it receives actual notice from the affected party of any illegal content being circulated/published through its service. Google is also bound to comply with Information Technology (Intermediaries Guidelines) Rules 2011. The Court observed that Rule 3(3) of the IT Rules read with Rule 3(2) requires an intermediary to observe due diligence or publish any information that is grossly harmful, defamatory, libelous, disparaging or otherwise unlawful. Rule 3(4) of the Rules creates obligation on an intermediary to remove such defamatory content within 36 hours from receipt of actual knowledge.

Decision

Thus, in the present case, Google was directed to remove all defamatory contents about the plaintiffs posted by the defendant No.1 from its website www.blogger.com as well as all the links containing defamatory content within 36 hours from the date of knowledge of the order passed by this Court. Defendant No.1 was restrained from sending any such e-mails or posting any material over the internet having a direct or indirect reference to the plaintiffs or the Art of Living Foundation or any member of the Art of Living Foundation, or His Holiness Sri Sri Ravi Shankar.

Liabilities of ISPS and Intermediary in United States and United Kingdom

In United States, Section 230 of the Communication and Decency Act, 1996 prvides that- "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." 4 In other words, it precludes courts from entertaining claim that would place ISPs in a publisher's role.[xvi]

On the contrary, the law on cyber defamation is quite stringent in United Kingdom (UK) and European Union (EU) countries. A very recent decision of Court of Appeal (Civil Division) in Payam Tamiz v Google Inc. makes the stand very clear that if online service providers do not immediately take down the content that is alleged to be defamatory, they can be held liable. The present case was filed by Payam Tamiz, an English Conservative politician against Google Inc. and Google UK for anonymous defamatory comments on a blog created on Google's blogger platform called, "London Muslim". In Court in this case held that once Google was notified of allegedly defamatory content, it became a "publisher by acquiescence" and therefore may be held liable for failing to remove the content. The role of Google in operating 'Blogger' is not purely passive as they provide design tools, a URL (Uniform Resource Locator) 6, advertisements, service on terms of their choice and can remove or block access to any blog.

The finding of Richards LJ in this case was based on interpretation of Section 1(1)(c) of the UK Defamation Act of 1996, which when applied to cyber defamation cases waives liability for an intermediary only when it "did not know, and had no reason to believe, that what [it] did caused or contributed to the publication of a defamatory statement." It is to be noted that such an approach is different from the construction and import of Section 230 of the Communications Act in US, which provides wider protection for intermediaries.[xvii] Although, the Court in this case eventually ruled in Google's favor due to uncertainty regarding evidence, the case still raises serious concerns in particular the gate-keeping obligations creating a massive burden for intermediaries and ISPs.

Choice of Jurisdiction

Choice of jurisdiction poses the biggest challenge to cases of cyber defamation. The new information age has raised a question mark on the adequacy of traditional jurisdictional regimes where interstate disputes arise in cyberspace. It has also been argued by many scholars that traditional choice-of-law doctrines are inadequate to determine which state law to apply in interstate cyber-disputes. The overwhelming criticism is that "old choice of-law doctrines fail to provide any meaningful guidance in the virtual world because these doctrines depend on notions of physical location. Many of these criticisms focus on the law of defamation in cyberspace, or "cyber defamation" in particular. Cyber defamation thus provides the perfect lens to examine the adequacy of traditional

choice-of-law regimes in cyberspace.[xviii]

7. Conclusion

The problem of determining the jurisdiction in cyberspace is further aggravated by the fact that plaintiffs have the luxury of "forum shopping" or choosing the jurisdiction with the laws most favorable to them. Such problem of jurisdiction can be of two types, one where alleged defamatory material is published in only one state and second when it is multistate. In first case, the presumption is that the law to be applied is "the . . law of the state where the publication occur." However, in multistate defamation actions the presumption is that the state with the most significant relationship will be "the state where the person was domiciled at the time." In cases involving corporations or other legal persons, "the state of most significant relationship will usually be the state where the corporation, or other legal person, had its principal place of business at the time." The judicial trend in this regard is that instead of creating new regimes for cyber-defamation disputes, most courts apply traditional choice-of-law doctrines-usually sub silentio-and utilize old analogies to deal with the substance of cyberspace.[xix]

It is evident, however, that whether someone defames a party over a broadcast, by fax, in print, or in cyberspace, the defamed party's reputation is still injured in a sovereign state where that state has a real-space interest in protecting its citizens' reputation from injury. Therefore, any criticism of choice-of-law doctrine for cyber defamation falls flat because cyberspace is neither unique nor special for choice-of-law purposes, and there exists no reason to single out cyber defamation as something in need of reformulated choice-of-law rules.[xx]

References

[1] https://www.quora.com/What-is-the-conviction-for-cyber-defamation-in-India

[2] Hannan.M & Blunde;;. B (2004). "electronic crime- it not only the big end of town that should be worried"' we-B centre & edith cowan university, PP 1-9.

[3] Article on one in the three cyber attacks in banks are successful by Riju Mehta April 27, 2017, economic times.

[4] Kumar. A (2002) "cyber crime- crime without punishment", available at unpanl.un.org.

[5] Perumal, subramoniam Arumuga, Impact of cyber crime on virtual banking (ovt 24,2008) available at www.ssrn.com

[6] Amar Singh and his wife Neha Panjani [2012 case in US]

[7] cyber extortion risk report 2015, NYA International, oct 2015

[8] https://wikispaces.psu.edu/display/IST432TEAM4/Cyber+and+Online+Defamation

[9] John La Cour (April 29, 2014) vishing campaign steals card from customers of dozens of banks [online] available at www.blog.phishlabs.com

[10] http://www.jusimperator.org/2017/11/27/comparison-of-india-with-other-countries-on-the-basis-of-cyber-law-crime-and-it-services/

[11] Umashankar sivasubramannian vs ICICI bank 2008, Tamil Nadu

[12] www.cyberlawsindia.com

[13] https://indiancaselaws.wordpress.com/2013/10/20/avnish-bajaj-vs-state-dps-mms-scandal-case/

[14] Muthukumaran.B (2008), “cyber crime scenario in India”, criminal investigation department Review, January, pp. 17-23.

[15] https://indiankanoon.org/doc/121103864/

[16] https://cyberdefamation.in/popular-cyber-defamation-cases-india/

[17] https://www.myadvo.in/blog/defamation-in-the-age-of-internet-the-indian-scenario/

[18] Kumar vinod- winning the battle against cyber crime by Parthasarthi Pati

[19] https://www.lawfarm.in/blogs/cyber-defamation-in-india

[20] http://www.legalservicesindia.com/articles/defcy.htm