VOLUME 1 | ISSUE 4

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

DEFAMATION IN CYBER SPACE

- Sagrika Garg[1]

"LIFE IS AN AFFIRMATION, NOT A DEFAMATION"[2]

ABSTRACT

Accessibility, anonymity, privacy, solitude of one's own area, and the interactive, responsive character of online communications have made users significantly less inhibited than in the past, particularly when it comes to the contents of their messages. There's no shortage of Soniya Gandhi-Manmohan Singh jokes and cartoons flooding your Facebook feed.The internet has made it far easier than ever before to anonymously transmit defamatory words to a global audience. Everyone can now be a publisher as well as a victim of libelous publication on the internet. For a defamatory charge to be proven, it only needs to be disclosed to one person.Every time an email is forwarded to another person or defamatory text is shared on Facebook, it is published again and again, providing further cause for action. As a result, online has become an extremely vulnerable environment for defamation. There's no question that a John Doe lurks somewhere in internet. The difficulty in identifying the culprit, as well as the extent to which Internet Service Providers (ISPs) should be held liable for supporting the defamatory activity, exacerbates the problem.

In view of some of the most historic rulings on this topic in India and the United Kingdom, the current paper aims to highlight key legal provisions on cyber defamation and the liability of internet service providers or intermediaries. The author also attempts to emphasise some of the practical challenges that come with prosecuting such cases, particularly in terms of jurisdiction and forum shopping.Because India is a new battleground for cyber disputes and crimes, the cases are few, but

[1] Student at JEMTEC Scool of Law
[2] Rick Tumlinson

they show how India lags behind in terms of the legislative framework that governs information technology law and the gaps that exist in present legislation.

KEY WORDS: *CYBERCRIME, CYBER PHISHING, DEFAMATION, INFORMATION TECHNOLOGY, PUBLISHERS.*

INTRODUCTION

The internet is a specialized term utilized for the electronic vehicle of PC organizations, wherein online correspondence happens. It wakes up just when at least two PCs are arranged together. The term has a wide significance and isn't simply limited to the web yet additionally incorporates PCs, PC organizations, the web, information, programming and so on the violations that are perpetrated by utilizing the PC as an instrument, or an objective or a mean for propagating further wrongdoings falls inside the meaning of cybercrime. Digital law is the law that oversees the wrongdoings carried out inside the internet. Digital Slanderis additionally a cybercrime.

Digital slander is distributing of abusive material against someone else with the assistance of PCs or web. In the event that somebody distributes some abusive assertion about some other individual on a site or send messages containing disparaging material to different people with the aim to criticize the other individual about whom the assertion has been made would add up to digital slander. The mischief caused to an individual by distributing a slanderous assertion about him on a site is boundless and hopeless as the data is accessible to the whole world. Digital maligning influences the government assistance of the local area all in all and not simply of the individual casualty. It likewise affects the economy of a nation relying on the data distributed and the casualty against whom the data has been distributed.

CYBER DEFAMATION IN INDIA

The average person's life has changed dramatically since the internet was invented. The internet has made it possible to communicate with people all around the world. It has brought the rest of the globe closer to every man who has internet connection. It has proven to be a repository of vast amounts of data that the average person could not easily access. It has also given business and trade

new dimensions. Anything is possible with the internet, including social networking, entertainment, shopping, job hunting, and recruitment.

The growing usage of the internet has given crime a new face and provided a new medium for criminals to perpetrate crimes.

The electronic medium of computer networks, in which online communication takes happen, is referred to as cyberspace. It only comes to life when two or more computers are connected via a network. The phrase has a broad definition that encompasses not just the internet but also computers, computer networks, the internet, data, and software. Cybercrime refers to crimes done with the use of a computer as an instrument, a target, or a means of committing more crimes. The legislation that governs crimes committed in cyberspace is known as cyber law. Cyber libel is also a form of cybercrime.

The Internet is a key source of defamation[3] because of the vast amount of information available and the ease with which it may be transferred. After conducting research on the subject, it can be concluded that India's current legal situation does not provide an effective response to situations of cyber defamation. Defamation laws should also be sufficiently flexible to apply to all forms of media. As defamation laws evolve in the Internet age, applying the principles of 18th and 19th-century cases to issues that arise on the Internet in the twenty-first century becomes nearly impossible.

PRE-REQUISITE OF DEFAMATION

To comprise the maligning, it is fundamental that there should be a slanderous explanation which should be perceived by the correct reasoning or sensible disapproved of individual as alluding to the individual criticized. One of the obligatory prerequisites is that the abusive assertion should be distributed and imparted to certain people other than the individual stigmatized[4].

In this way, if the correspondence of the slanderous assertion is between the individual stigmatizing and criticized for example direct SMS, Email, Whatsapp message and so forth, it would not add up to criticism inside the importance of section 499 of the IPC. It will cover the circumstances where

[3]The action of damaging the good reputation of someone; slander or libel.
[4] Describe or regard as worthy of disgrace or great disapproval.

the correspondence of the slanderous assertions has been made to the third individual for example WhatsApp Gathering, Open web, Long range informal communication Sites/Websites and so on where it very well may be seen by the people other than the individual stigmatized.

TYPES OF CYBER CRIMES

1.Against individuals:

This type of cybercrime includes a single person disseminating malicious or unlawful information through the internet. This can include cyber stalking, pornographic distribution, and human trafficking.

2. **Against Property:**

This is analogous to a real-life situation in which a criminal gains illegal access to a person's bank or credit card information. The hacker takes a person's bank accountinformation in order to obtain access to funds, make online transactions, or launch phishing schemes to trick individuals into giving over their personal information. They could even employ malicious software to get access to a website containing sensitive data. Unlawful computer trespassing across cyberspace, computer vandalism, delivery of destructive programs, and unauthorized ownership of computerized information are all examples of cybercrimes against all types of property.

3. **Against Government:**

This is the least prevalent type of cybercrime, yet it is also the most serious. Cyber-terrorism is a crime committed against the government. Hacking government and military websites, as well as delivering propaganda, are examples of government cybercrime. Terrorists or foreign countries' enemies are frequently the perpetrators of these crimes.

PROBLEMS AND ISSUES IN CYBER DEFAMATION

Our ever-increasing reliance on the Internet for social networking sites has resulted in a slew of legal difficulties in the country. When it comes to online pages like blogs or other media sites like newspapers or magazines, the most difficult component of defamation can be identifying the individual who has intended to hurt our reputation or the third party who has seen the

defamatory comment. This is due to the fact that bloggers can be open or choose to remain anonymous in order to protect themselves.

As a result, if the statement appears on someone's blog, it may be difficult to determine who made it. It's much more difficult to identify the readers who write comments on blogs or online news items because most sites don't require users to use their real names or disclose any personal information, such as their name, address, or e-mail address. Even if they do, it's possible that they'll supply misleading information. As a result,locating these individuals becomes tough. When a defamatory statement is posted on social media platforms like Facebook, it quickly spreads and is read by a huge number of people, inflicting harm to the individual who made the statement.

REMEDY FOR DEFAMATION: CHALLENGES

The greatest test for Slander in the Advanced Space is against whom the activity ought to be started for criticism. The Mocking of Personality, Pantomime and Secrecy is simple and as such knowing the character of the individual who has caused the slander may not be practical at the principal occasion and thusly it could be hard to start the procedure for criminal criticism of recording the suit for harms for Maligning. The suitable advance in such a case is two-crease, first, to start the procedure for following the character and second, to start the procedure for criminal or common criticism however these done then again or at the same time which thusly suggests to initially finding the personality and afterward to start the lawbreaker or common continuing. To follow the Character, the Criminal Continuing can be started for Maligning by documenting an objection under Section 200 Cr. P.C., joined by an application under Section 202 Cr.P.C. with a solicitation to court to guide the police to direct request to follow the personality of an individual by finding IP address or gathering the other pertinent confirmations from Web. The other choice which additionally can be investigated especially in the situations where any cognizable offense is made out separated from the criticism, at that point to document criminal grumbling for enlistment of the FIR which may empower following of the Personality of the guilty party just as assortment of different confirmations to demonstrate the offense of maligning.

The primary goal for the abused party in such instances of Criticism is to get eliminate the substance from the Web which can be conceivable just through the court besides in cases including Profanity. If there should arise an occurrence of a vulgar profile, the interpersonal interaction sites may eliminate the substance as it might abuse their own protection strategies. The cure of obstructing/evacuation of the substance can be benefited in the common just as criminal continuing. The expulsion of the substance can be plausible just in situations where the culpable site is situated in India and if there should arise an occurrence of unfamiliar site; the lone choice is for obstructing of the substance.

In any case, in the latest instance of Master Ramdev and Anr. v. Facebook Inc. &Ors., Equity Pratibha Singh had passed a request to eliminate all slanderous substance posted online against yoga master Baba Ramdev dependent on a book named "Godman to Investor the untold story of Baba Ramdev", with no regional breaking point, referencing that if the substance is transferred or assuming is situated in India on a PC Asset, the Courts in India ought to have Global Purview to pass Overall Directives.

CASE LAWS

- **Cubby, Inc. vs. CompuServe Inc.[5]. -** In this absolute first major distributed case on Web criticism, the offended party, Cubby, Inc. guaranteed harms because of one of CompuServe's many autonomous, self-worked discussions. At that point editorial gathering called, "Rumorville" had an electronic tattle magazine called "Skuttlebut "on which a disparaging remark about Cubby, Inc. was posted. Since CompuServe doesn't audit the substance of distributions preceding postings, the court found that CompuServe stood firm on a footing practically equivalent to a merchant, accordingly soothing CompuServe from the responsibility that a distributer would confront. This finding depends on the legal dispute Smith v. California, in which the US High Court held that a wholesaler should have obvious information on the mistaken (and abusive) substance of a distribution before scattering to be expected to take responsibility for delivering that content. Earlier milestone cases including offended parties squeezing criticism charges against a transporter, including N.Y. Times v. Sullivan and Western Association Broadcast v. Lesesne, have discovered that transporters, or

[5] Cubby, Inc. vs. CompuServe Inc., 776 F.Supp. 135(S.D.N.Y. 1991)

merchants of distributed works, don't hold duty regarding slander except if they had sensible information in advance of the offensive material they had circulated.

- **Stratton Oakmont vs. Prodigy (1995)[6] -** This case is an occurrence of offensive comments over a public on-line gathering set off an organization to sue an organization specialist co-op. On a generally perused monetary issue gathering called "Cash Talk," a Wonder client had posted about Daniel Porush, the leader of Stratton Oakmont, a venture protections firm, and his representatives. Porush, the banner guaranteed, was "soon to demonstrated crook," and further, Stratton Oakmont, Inc., was a "clique of representatives who either lie professionally or get terminated." Subsequent to perusing this posting on Wonder, Porush recorded suit against the organization administration asserting Wonder obligated for this present banner's hostile cases. Wonder, for its lawful benefit, guaranteed the situation with a merchant (as on account of Cubby versus CompuServe). Notwithstanding, Stratton Oakmont contended that because of Wonder's publication command over content, Wonder ought to be all the more accurately delegated a distributer. Fundamentally, this is on the grounds that Wonder clarified to all clients that it held the option to alter, eliminate, and channel messages in its framework to guarantee a "family" environment on-line. On account of these cases, the court arranged Wonder as a distributer and granted harms to Stratton Oakmont.
- **Zeran vs. Americaonline (1996)[7] -** On account of Zeran versus America On the web, in which a client was survivor of a pernicious deception. The offended party, Kenneth Zeran, had his location and telephone number posted regarding ads for gifts (Shirts, mugs, and so forth) celebrating the Oklahoma City Bombarding. An obscure AOL (America On the web) client had get Zeran's own data and posted these promotions all through AOL. Zeran got many upsetting dangers because of this trick, and was ceaselessly pestered by means of phone and post. He sued AOL guaranteeing carelessness for AOL's benefit in permitting such notification to be posted, regardless of the protests and postings he had enlisted with AOL upon first learning of the pantomime. Utilizing the CDA (Correspondences Tolerability Demonstration of 1996) as its guard, AOL guaranteed resistance through the security that the CDA gives Internet services. The courts decided for America Web based, maintaining that intelligent PC specialist organizations may not be expected to take responsibility for posting

[6] Stratton Oakmont vs. Prodigy (1995)
[7] Zeran vs. America Online (1996)

disparaging articulations posted by outsiders through the ISP. Viably, this choice switched the discoveries of Stratton Oakmont, Inc. versus Wonder.

- **Kalandi Charan Lenka vs. State of Odisha**[8] — In this case, the petitioner was hounded on a regular basis, and the offender created a bogus account for her and sent obscene messages to her friends. On the walls of the hostel where the victim slept, a modified naked photograph was also put. The perpetrator was found guilty of his crime by the court.
- **Rajiv Dinesh Gadkari through P.A. Depamala Gadkari vs. Smt. Nilangi Rajiv Gadkari**[9]– In this case, after obtaining a divorce letter from her spouse, the respondent filed a lawsuit against him for harassing her and defaming her by posting lewd images on social media. The offence has already been reported, and the wife has requested support of Rs. 75,000 per month (respondent).

LIABILITY IN CYBER DEFAMATION

In India, a person can be held accountable for defamation in India under both civil and criminal law.

1. INDIAN PENAL CODE

Laws applicable for cyber defamation

According to *Section 499 of the Indian Penal Code*, "Whoever makes or publishes any imputation of any person by words either said or meant to be read, or by signs and visual representations, intending to hurt or knowing or having reason to suspect that such imputation will affect the reputation of such person is said, except in the instances hereby excepted to defame such person,".

According to *Section 500 of the IPC*. "Any person found responsible under section 499 would be punished with imprisonment for two years or a fine or both,"

Forgery is dealt with in Section 469. If someone fabricates a document or account in order to undermine a person's reputation. This offence is punishable by up to three years in prison and a fine.The offence of criminal intimidation by use of electronic means to harm one's reputation in society is covered by *Section 503 of the IPC*.

[8]Held on 16th January 2017
[9] Held on 16th October 2009

2. INFORMATION TECHNOLOGY ACT, 2000

Information Technology Act of 2000, *Section 66A* – In the year 2015, the Supreme Court overturned this law. The section outlined the consequences of transmitting "offensive" texts by computer, mobile phone, or tablet. Because the government did not define the term "offensive," The government began to use it as a tool to stifle free speech. The Supreme Court of the United States struck down the entire section in 2015.

A person can file a complaint with the cybercrime investigation cell if he or she has been defamed in cyberspace. It is a division of the Department of Criminal Investigation.

"You must be the change you wish to see in the world"[10]

COMPARATIVE ANALYSIS OF LAWS BETWEEN INDIA AND UK

A comparison of cyber security techniques in India and the United Kingdom reveals a few common themes in certain areas and significant differences in others. The differences in approaches can be attributed to different conditions in the two countries to a large extent. Regardless, despite a big gap in verifiable access to innovation and assets to contribute to securing cyber space, India has progressively emphasized cyber security as a vital strategy issue over the last two decades. The United Kingdom has developed protocols and regulations, and cyber security has been a strategic concern for far longer than it has in India. In general, the UK's cyber security system is more comprehensive and robust than India's. However, based on the indicators in the Global Cyber security Index, India isn't far behind the United Kingdom in terms of cyber security responsibility and advancement. This could also be one of the reasons why

the two countries are unable to apply existing rules to new circumstances in cyberspace. From a power standpoint, the two countries' strategies are becoming closer, as seen by the casing of national security programs. In both locations, knowledge and resistanceestablishments are also strongly linked to cyber security. However, the differentiating proof of entertaining, hazards, and points and aims of the cyber security plan differs significantly. The UK is notably more open to multi-partner contributions to reduce its tactics, but India's cyber security remains divided between private and government efforts, focusing on national security concerns in general. The UK's

[10] Mahatma Gandhi

command of multi-partner standards should be welcomed by India, which has only just realised the importance of multi-stakeholderism in the global context. In terms of disseminating cyber security awareness and developing indigenous cyber security research, the Indian government can do a lot more. India could also benefit from the UK's delicate approaches, such as the implementation of the cyber fundamentals scheme, to encourage firms to adopt security best practices without imposing strict guidelines. Central elements of the cyber security architecture, such as the formation of crisis response organizations and fundamental data insurance, remain unchanged between the two wards. Aside from them, there are a few different establishments that handle different cyber security orders. As a result, it's critical that the planned National Cyber Coordination Center, modelled after the UK's National Cyber Security Center, serve as a one-stop shop for cyber security issues. Furthermore, each organization's jobs must be clearly divided in order to keep a strategic distance from cover and ensure accountability. India's general approach to dealing with cybercrime looks to have been stalled for political reasons. The Budapest Treaty, which establishes global participation in cyber security and cyber misbehavior and to which the UK is also (though belatedly) a signatory, is an important aspect of universal coordination on cyber security issues, which would be much more difficult to haggle on a specific basis. Given the large degree of engagement required to investigate cyber threats, it is urged that India return to the possibility of taking on global responsibilities. Indian cyber security is also lacking in major norms on which such legislation should be based. The fundamental requirements The UK plan ensures that the fundamental technique for cyber security considers aspects of common freedoms and individual interests on the internet as a shared asset. While this may place pressure on the administration's control over cyber security, security policy should be tailored to protect common freedoms rather than the other way around. In any event, the UK's operations must balance national security concerns with concerns about protection and reconnaissance raised by common liberties.

CONCLUSION

The current tendency in legislation, as well as the judicial attitude to such offences, appears to be that they are treated lightly, and the penalties are insufficient in view of the gravity of the offences. Though the Government of India requested the Law Commission to issue a well-considered judgment on the desirability of dealing with certain anti-social and economic offences appropriately

and quickly, such as those intended to block or prohibit the country's economic development and harm its economic health, tax evasion, hoarding, and black-marketing, among others; However, it does not specifically mention cybercrime, such as slander in cyberspace.

Defamation laws should be broad enough to cover all forms of media. It will always be necessary to strike a balance between freedom of expression and reputation. The problem is that most defamation laws throughout the world were enacted at a time when most defamatory writings were either spoken or the result of crude printing. As a result, applying ideas derived from 18th and 19th century cases to concerns that may occur on the internet in the twenty-first century is impractical. The ultimate goal of global legislation should be to lower the costs of international trade by removing inconsistencies and uncertainty caused by differences in national laws.

"Defamation is becoming a necessity of life: in as much as a dish of tea in the morning or evening cannot be digested without this stimulant."[11]***

[11] Thomas Jefferson