pen ACCLAIMS

Volume 10, May 2020 ISSN 2581-5504

"Defamation in the Cyber Space"

Avantika Nandy
Fairfield Institute of Management and Technology

CYBER SPACE

The term cyberspace was initially introduced by William Gibson in his 1984 book, "Neuromancer". Gibson criticized the term in later years, calling it "evocative and essentially meaningless.

Cyberspace is a concept describing a widespread, interconnected digital technology. It refers to the virtual computer world, and more specifically, is an electronic medium used to form a global computer network to facilitate online communication. Cyberspace allows users to share information, interact, swap ideas, play games, engage in discussions or social forums, conduct business and create intuitive media, among many other activities.

Cyber space is the hub of vast amount of sensitive data, personally identifiable information, protected health information, personal information, intellectual property, data and governmental and industry information systems because of which there arises an immense necessity for keeping the cyber space secure from any malicious activity such as theft or damage attempted by criminals and adversaries .

With the advent of technology dependent generation, the graph of the cybercrimes seems to rise with the passage of time. now the term of cybercrime is not just limited to that of breaching firewalls etc but now there has been a lot more added to the area of cybercrime. It is ever evolving with the time and technology. Cybercrime is on the increase because of the feasibility and easy approach of the act of crime but more because of the novelty of anonymity related to it. the people are able to hide themselves behind their systems etc to commit an act which they are not able to do in the real world.

TYPES OF CYBER CRIMES

1. **Against Individuals** - This category of cybercrime involves one individual distributing malicious or illegal information online. This can include cyberstalking, distributing pornography and trafficking.
2. **Against Property** - This is similar to a real-life instance of a criminal illegally possessing an individual's bank or credit card details. The hacker steals a person's bank details to gain access to funds, make purchases online or run phishing scams to get people to give away their information. They could also use a malicious software to gain access to a web page with confidential information. cybercrimes against all forms of property include unauthorized computer trespassing through cyberspace, computer vandalism, transmission of harmful programs, and unauthorized possession of computerized information.

Volume 10, May 2020 ISSN 2581-5504

3. **Against Government** - This is the least common cybercrime, but is the most serious offense. A crime against the government is also known as **cyber - terrorism.** Government cybercrime includes hacking government websites, military websites or distributing propaganda. These criminals are usually terrorists or enemy governments of other nations.

CYBER DEFAMATION

The term defamation is used to define the injury that is caused to the reputation of a person in the eyes of a third person. The injury can be done by words oral or written, or by signs or by visible representations. The intention of the person making the defamatory statement must be to lower the reputation of the person against whom the statement has been made in the eyes of the general public.

In the famous case of **Ram Jethmalani vs Subramaniam Swamy** [1]it was held by Justice Pradeep Nandrajog that statement made by defendant was prima facie defamatory. It was a case of exceeding the privilege and that by itself was held to be evidence of malice. The statement was quite on connected with and irrelevant to the situation, actual malice on part of defendant was well established. This harmed the image of plaintiff at large and such allegation destroy the personal and political reputation as LTTE is banned organization and connecting the name with it leads to loss of reputation. However, such loss is not recoverable said by Justice but still compensation of Rs 5 Lacs was awarded in favour of plaintiff and against the defendant considering his professional status and his social status.

Defamation is not only limited to the oral and written statements but it is also applicable to the statements made on the cyber space which hurt the reputation of a person. The defamation over the Cyber space is called as **Cyber Defamation.**

Cyber defamation is a new concept but the traditional definition of the term defamation is application to the cyber defamation as it involves defamation of a person through a new and a virtual medium.

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. 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

[1] Ram Jethmalani vs Subramaniam swamy

Volume 10, May 2020 ISSN 2581-5504

the economy of a country depending upon the information published and the victim against whom the information has been published.

In traditional libel law there are three different types of defamatory statements

1. The first is a statement that is defamatory on its face and which is obviously defamatory.
2. The second is a statement which contains false innuendo. False innuendo is a defamatory statement that has an inferential meaning, therefore only persons with the necessary contextual knowledge appreciate that the statement is defamatory.
3. The third is legal innuendo. while no defamatory on their face these statements are defamatory when viewed together with extrinsic circumstances.

CYBER DEFMATION LAW IN INDIA

The laws for the offence of cyber defamation is constituted in the statute of Indian penal code 1860, information technology act 2000 and the Indian evidence act 1872.

Under the Indian Penal Code, 1860

1. **Section 499 – Defamation**

   Whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said to defame that person.

   - The punishment for defamation is given in Section 500 [2]of the Indian Penal Code, 1860.

2. **Section 469 - Forgery for purpose of harming reputation**

   Whoever commits forgery, shall harm the reputation of any party, or knowing that it is likely to be used for that purpose, shall be punished with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine.

3. **Section 503 – Criminal Intimidation**

   Whoever threatens another with any injury to his person, reputation or property, or to the person or reputation of any one in whom that person is interested, with intent to cause alarm to that person, or to cause that person to do any act which he is not legally bound to do, or to omit to do any act which that person is legally entitled to do, as the means of avoiding the execution of such threat, commits criminal intimidation.

The punishment for criminal intimidation is given in Section 506[3] of the Indian Penal Code, 1860

[2] Whoever defames another shall be punished with simple imprisonment for a term which may extend to two years, or with fine, or with both.

Volume 10, May 2020 ISSN 2581-5504

Under Information Technology Act, 2000.

1. **Section 66A** – Punishment for sending offensive messages through communications service etc.

The Section 66A of the Information Act, 2000 does not specifically deal with the offence of cyber defamation but it makes punishable the act of sending grossly offensive material for causing insult, injury or criminal intimidation.

Section 66A of the IT Act defines the punishment for sending "offensive" messages through a computer or any other communication device like a mobile phone or a tablet. A conviction can fetch a maximum of three years in jail and a fine.

In **Shreya Singhal v. Union of India** [4]judgment upholding freedom of expression, the Supreme Court has struck down Section 66A of the amended Indian Information Technology Act, 2000 of IT Act, a provision in the cyber law which provides power to arrest a person for posting allegedly "offensive" content on websites. The apex court ruled that the section falls outside Article 19(2) of the Constitution, which relates to freedom of speech, and thus has to be struck down in its entirety.

2. **Section 67**[5] - Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or tends to deprave and corrupt persons shall be punished."

- Kerala High Court in Sreekumar v. State of Kerala[6] held that "Abusive words lacking lascivious elements cannot be brought within contours of S. 67 of Information Technology Act".
- Madras High court in I. Linga Bhaskar & Others V. The State[7] held that "Emoji is sent to express one's feelings about something and cannot be treated as an overt act by others".

Under Indian Evidence Act, 1872 (for admissibility of defamatory content)

1. **Section 65A & 65B** – Cases in which secondary evidence relating to documents may be given.

[3] Whoever commits, the offence of criminal intimidation shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both; if threat be to cause death or grievous hurt, etc.—And if the threat be to cause death or grievous hurt, or to cause the destruction of any property by fire, or to cause an offence punishable with death or 1[imprisonment for life], or with imprisonment for a term which may extend to seven years, or to impute, unchastity to a woman, shall be punished with imprisonment of either description for a term which may extend to seven years, or with fine, or with both.

[4] Singhal v. Union of India, (2013) 12 S.C.C. 73

[5] State of Tamil Nadu vs Suhas Katti

[6] Sreekumar v. State of Kerala, 2019 SCC Online Ker 1305.

[7] I. Linga Bhaskar & Others V. The State, through the Inspector of Police, Thoothukudi South Police Station & Another.

Volume 10, May 2020 ISSN 2581-5504

- **What is admissible in court as evidence?**
    a) Any electronic record printed on a paper or recorded or copied in optical or magnetic media shall be considered as a document and shall be admissible by court.
    b) Online chats are also admissible.
    c) Electronic mails are also admissible.

The bench said that section 65 B of Evidence Act is a procedural provision and if the electronic evidence is "authentic and relevant" the same can certainly be admitted, subject to the satisfaction of the court and it may depend on situation such as "whether the person producing such evidence is in a position to furnish certificate under Section 65B(4) .

- According to section 65A and 65B of the Indian evidence act the electronic records are admissible in the court. **In State of Tamil Nadu vs Suhas Katti** and **SMC vs Jogesh Kwatra** it was held that online chats and emails are admissible in evidence under 65B of Indian evidence act.
- In the first case of cyber defamation in India :

SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra, [8]the reputation of a corporate was being defamed by an employee of the plaintiff company by sending derogatory, defamatory, obscene, emails obscene, vulgar, filthy and abusive emails to its employers and also to different subsidiaries of the said company all over the world with the aim to defame the company and its Managing Director. The Hon'ble Judge of the Delhi High Court passed an ex-prate ad interim injunction observing that a prima facie case had been made out by the plaintiff.

Consequently, the Delhi High Court restrained the defendant from sending derogatory, defamatory, obscene, vulgar, humiliating and abusive emails either to the plaintiffs or to its sister subsidiaries all over the world including their Managing Directors and their Sales and Marketing departments. Further, Hon'ble Judge also restrained the defendant from publishing, transmitting or causing to be published any information in the actual world as also in cyberspace which is derogatory or defamatory or abusive of the plaintiffs.

- In the case of **Kalandi Charan Lenka Vs. State of Odisha** [9] the petitioner was continuously being stalked, and a fake account of her was later created and obscene messages were sent to the friends by the culprit. A morphed naked picture was also posted on the walls of the hostel where the victim stayed. The court held the culprit liable for his offence.
- **In the case of Rajiv Dinesh Gadkari through P.A. Depamala Gadkari vs Smt. Nilangi Rajiv Gadkari** [10]– In this case, after receiving a divorce letter from her husband, the respondent filed a suit against the husband for continuously harassing

[8] SMC Pneumatics India Pvt. Ltd. v. Jogesh Kwatra, CS(OS) No. 1279/2001 (Delhi High Court, 2001)
[9] Kalandi Charan Lenka vs State of Odisha (Odisha high court, 2017)
[10] Rajiv Dinesh Gadkari through P.A. Depamala Gadkari vs Smt. Nilangi Rajiv Gadkari

Volume 10, May 2020 ISSN 2581-5504

her by uploading vulgar photographs and defaming her. The offence has already been registered and maintenance of Rs. 75,000 per month has been claimed by the wife(respondent).

Liability of Internet Service Provider (ISP) and Intermediary in India

Section 79 of the IT Act, 2000 exempts the liability of intermediaries except in cases where the: -

a) Where the ISP has conspired, abetted or induced the unlawful act.
b) If the ISP fail to remove or disable the information, data or communication link in question.

Laws Governing Cyber Defamation in Abroad

UNITED KINGDOM

Under English law, there is a distinction between libel and slander. Libel not slander is punishable under Criminal law. In fact, slander is no offence in criminal law and is offence only in civil law.

- Defamation actions in relation to the Internet have so far involved libel. Libel must be widely 'published'. You could libel someone using electronic networks by:

a) Sending an email, or an email attachment, where that email is widely posted or forwarded;
b) Making material available via a web page;
c) Posting to an email list or newsgroup; or
d) Streaming audio or video via the Net.

- In **England**, the Defamation Acts of 1952 and 1996 are the important statutes. Under article 4 and 6 of the Defamation Act no such action for defamation shall be brough after the expiration of one year from the date on which the cause of action accrued.
- Forms of UK defamation include:
  a) Print;
  b) Broadcast (Broadcasting Act of 1990);
  c) Film or Videos;
  d) Internet; and
  e) Statements made during public performances of a play (Theatres Act of 1968).
- Under UK law it is possible to defame corporations as well as individuals.
- The important issue to consider is not how the defamatory statement makes the victim feel, but the impression it's likely to make on people reading it. In **Loutchansky vs Times newspapers Ltd**[11] it was held that publication over the internet occurs when a reader accesses the text, this means that a fresh publication takes place every time someone reads the material.

[11] Loutchansky vs Times newspapers Ltd, (No 2) (2001).

Volume 10, May 2020 ISSN 2581-5504

- In the case of **Jameel v. Wall Street Journal** [12]the Wall Street Journal was able to prove that a defamatory article had only been downloaded by five people in the U.K., which included the claimant's lawyer. The courts ruled that there had been "no substantial publication" in the U.K.

UNITED STATES

In United States**,** defamation law is much less plaintiff friendly as compared to its European counterpart due to the enforcement of the First Amendment. (Freedom of religion, press, expression. Ratified 12/15/1791). In America, not every publication of a defamation gives rise to a separate claim but it only allows one claim of primary publication.

- To win a U.S. defamation lawsuit, the plaintiff, at the very least, must prove that the defendant:

a) Published or otherwise broadcast an unprivileged, false statement of fact about the plaintiff;
b) Caused material harm to the plaintiff by publishing or broadcasting said false statement of fact;
c) Acted either negligently or with actual malice;

Liability of ISP and Intermediary in the USA

Section 230 of **the Communication and Decency Act, 1996** precludes court from entertaining claims that would place ISPs in a publisher's role in matters concerning Cyber Defamation. It also absolves ISPs (hosting companies, websites, developers etc) of defamation liability over user comments and content.

The advent of the Communications Decency Act of 1996 **,** especially Section 230, provided new legislation targeted at the Internet and issued immunity from liability for "interactive computer services" and their users . If the plaintiff is deemed a public figure the standard of actual malice [13]must be met:

- To be considered immune in a case involving the CDA, courts use a three-part test:

a) The defendant must be a "provider or user" of an "interactive computer service."
b) The cause of action asserted by the plaintiff must "treat" the defendant "as the publisher or speaker" of the harmful information at issue.
c) The information must be "provided by another information content provider," i.e., the defendant must not be the "information content provider" of the harmful information at issue. (CDA)

[12] Jameel v. Wall Street Journal (2006)
[13] New York Times Co. v. Sullivan, 376 U.S. 254 (1964)

Volume 10, May 2020 ISSN 2581-5504

The cyber The **Computer Fraud and Abuse Act** (**CFAA**) [14]is a United States cybersecurity bill that was enacted in 1986 . It was enacted in response to concern that computer-related crimes might go unpunished.

The three major court cases in "cyberlibel" liability are keys to understand the current climate of the courts - **Cubby v. CompuServe (1991), Stratton Oakmont v. Prodigy (1995)**, and **Zeran v. America Online (1996)**. These three cases, along with several other attempts at litigation, have driven the courts' opinions on internet libel cases.

- **Cubby, Inc. vs. CompuServe Inc.[15]**

In this very first major published case on Internet libel, the plaintiff, Cubby, Inc. claimed damages due to one of CompuServe's hundreds of independent, self-operated forums. The journalistic forum called, "Rumorville" had an electronic gossip magazine called "Skuttlebut" on which a defamatory comment about Cubby, Inc was posted. Because CompuServe does not review the contents of publications prior to postings, the court found that CompuServe held a position analogous to a distributor, thereby relieving CompuServe from the liability that a publisher would face. This finding is based on the court case **Smith v. California**, in which the United States Supreme Court held that a distributor must have demonstrable knowledge of the erroneous (and defamatory) content of a publication prior to dissemination in order to be held liable for releasing that content. Prior landmark cases involving plaintiffs pressing libel charges against a carrier, including **N.Y. Times v. Sullivan** and **Western Union Telegraph v. Lesesne**, have found that carriers, or distributors of published works, do not hold responsibility for libel unless they had reasonable knowledge beforehand of the libellous material they had distributed.

- **Stratton Oakmont vs. Prodigy (1995)[16]**

This case is an instance of libellous remarks over a public on-line forum triggered a company to sue a network service provider. On a widely read financial matters forum called "Money Talk," a Prodigy user had posted about Daniel Porush, the president of Stratton Oakmont, an investment securities firm, and his employees. Porush, the poster claimed, was "soon to proven criminal," and further, Stratton Oakmont, Inc., was a "cult of brokers who either lie for a living or get fired." After reading this posting on Prodigy, Porush filed suit against the network service claiming Prodigy liable for this poster's libellous claims. Prodigy, on its legal behalf, claimed the status of a distributor (as in the case of Cubby vs. CompuServe). However, Stratton Oakmont argued that due to Prodigy's editorial control over content, Prodigy should be more correctly classified as a publisher. In essence, this is because Prodigy made clear to all users that it retained the right to edit, remove, and filter messages in its

[14] United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009)

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

[16] Stratton Oakmont vs. Prodigy (1995)

Volume 10, May 2020 ISSN 2581-5504

system in order to ensure a "family" atmosphere on-line. Because of these claims, the court classified Prodigy as a publisher and awarded damages to Stratton Oakmont.

- **Zeran vs. America Online (1996)**[17]

In the case of Zeran vs. America Online, in which a user was victim of a malicious hoax. The plaintiff, Kenneth Zeran, had his address and phone number posted in connection with advertisements for souvenirs (T-shirts, mugs, etc.) glorifying the Oklahoma City Bombing. An unknown AOL (America Online) user had obtain Zeran's personal information and posted these ads throughout AOL. Zeran received many disturbing threats due to this hoax, and was continually harassed via telephone and post. He sued AOL claiming negligence on AOL's behalf in allowing such notices to be posted, despite the complaints and postings he had registered with AOL upon first learning of the impersonation. Using the CDA (Communications Decency Act of 1996) as its defense, AOL claimed immunity through the protection that the CDA provides Internet providers. The courts ruled in favour of America Online, upholding that interactive computer service providers may not be held liable for posting defamatory statements posted by 3rd parties via the ISP. Effectively, this decision reversed the findings of Stratton Oakmont, Inc. vs. Prodigy.

CONCLUSION

"With great power comes great responsibility"

With the advent of the internet age the use of technology and its potential misuse both have become a non-exhaustive subject. The convenience in communication has increased tremendously. However, such convenience comes with a catch. The effortless transfer of data and information over the internet has made it a critical hotspot for for many cyber-crimes and one of the most them is defamation. Although, there are laws in place which prohibit people from posting such defamatory content online, but most people are not aware of the same or are too negligent to realize the boundaries separating a defamatory content and a non-defamatory content. At times, when free speech runs contradictory to a person's reputation it becomes pertinent for the State to establish a boundary, lest that free speech becomes a weapon in the hands of certain people. There is a dire need of a system to educate and make people aware about the cyber space and the cyber ethics. Further, the intermediaries which provide such an open platform should monitor the content posted on it and take appropriate actions against such users who post such defamatory content in order to avoid repetition in the future.

[17] Zeran vs. America Online (1996)