ISSN: 0975-833X

Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 14, Issue, 11, pp.22842-22845, November, 2022
DOI: https://doi.org/10.24941/ijcr.44205.11.2022

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

RESEARCH ARTICLE

LAW RELATING TO DEFAMATION IN CYBERSPACE IN INDIA

***Ramesh, A.**

Assistant Professor, VS Law College, Ballari, Karnataka

ARTICLE INFO

Article History:
Received 18th August, 2022
Received in revised form
24th September, 2022
Accepted 15th October, 2022
Published online 30th November, 2022

Key words:

Defamation, Cyberspace, Cyber Jurisdiction, ISP's, Intermediaries.

Corresponding Author: Ramesh, A.

ABSTRACT

The term "defamation in Cyberspace" is nowhere defined in India. The traditional definition of defamation is applicable to defamation in Cyberspace in India. Even there is no particular legislation to govern defamation in cyberspace in India. Section 499 & 500 of Indian Penal Code and the provisions of Information Technology Act 2000 is often applied by the courts for defamation cases in cyberspace. Internet Service Providers and Intermediaries are exempted from liability under Information Technology Act 2000. Therefore there is a need to enact separate law to govern online defamation.

Citation: ***Ramesh, A.*** **2022.** "Law Relating to Cyber Defamation in India*". International Journal of Current Research*, 14, (11), 22842-22845.

INTRODUCTION

For the right thinking people in society, defamation is an intentional act to harm a person's reputation. Defamation[1] is a term used to describe a wide range of actions in which it is alleged that statements made about an individual that are untrue or unjustified have had the effect of lowering that individual's standing in the eyes of the public at large.[2] Depending on the culture, the type of comments that would have this effect varies. defamation is committed either by written words or spoken words, generally termed as a libel and slander respectively, and constitutes both, civil and criminal wrong in India.
Any form of defamation action chills free speech, but criminal defamation has a particularly troublesome effect. Defendants in criminal cases are confronted with a formidable adversary: the state. Criminal defamation is punishable for crime if found guilty.

To make matters worse, powerful public figures frequently use their positions to bring criminal cases. This only serves to increase the tension. Civil law provides protection for defamation claims because they are private matters between two individuals. Under the law of torts, an action for defamation will lie only on the proof that the statement made is falsely addressed to the complainant and published before a third person. Even if such statement is made to a single person, other than the complainant, is sufficient to be considered as defamation.[3] Defamation is defined in the Indian Penal Code, 1860, as anyone who intentionally harms the reputation of another person by implying that they are dishonest, or who has reasonable cause to believe that they are dishonest, is established the defamation. Sections 501 and 502, defamation is punishable by up to two years in prison, a fine, or both, for the publication, replication, or sale of defamatory materials. Aside from criminal intimidation, defamation is also covered by this Code, which holds the perpetrator of such acts criminally responsible and punishes them. Further the law of defamation in India also seemed to have its strong roots on the adoption of the Indian Constitution, but not absolute. The defamation has been included as one of the grounds on which reasonable restriction could be imposed. However the doubts regarding the constitutionality of section 499 and 500 of the IPC, 1860 has been raised, on the ground that they affect the constitutional freedom enshrined in Article 19(1)(a). Defamation law can have a devastating effect on speech if it is not carefully applied, limiting both the right to express oneself and the right to receive information, opinion, and

[1] More than any other media, anyone who receive Internet-published material can redistribute it to as many recipients as they want with no effort. By its very nature, some information and content is ripe for repurposing. Relevant e-mails and comments, for example, can swiftly spread among a big number of individuals in numerous nations, as most internet users are aware.

[2] The defenses against defamation law may also be affected by the worldwide character of the media. There are many factors that might be considered when deciding whether a piece of defamatory material is pertinent to a public issue, such as where it was published. In several Australian jurisdictions, legislative defenses of justification may not be available if a publication is made outside of the jurisdiction. When defamatory content is published in numerous jurisdictions over the Internet, defendants may lose the right to use a defense of privilege.

[3] Dr. C. Rajashekhar and Ms. Nikhila S. Tigadi, KLE Law Journal, titled: Dynamics of Cyber Defamation in India: An overview, 2015 Issue, pp-1-21

ideas. Defining and enforcing a defamation law without infringing on the right to free speech is difficult, but necessary. Threats of defamation suits can silence debate on contentious issues, even if the standards set by the law are reasonable. It is not uncommon for those in positions of power to file defamation suits in order to protect their reputations and to keep dissenting viewpoints at bay.

Legislative Framework: Position in India: Although, the mode of committing the defamation has taken new dimension in the technological era but yet the traditional definition of defamation, as defined under the IPC is applicable to the new one with wider interpretation. Until 2000, it was only the IPC which regulated the cyber defamation in India. In 2000, to regulate the wide spread use of internet for cyber-crime, amongst others, IT Act 2000[4] was enacted, followed by the amendment in 2008. However, even after the enactment of IT Act 2000, the court applied the provisions of IPC to decide the suits on cyber defamation cases. This implies that presently it is the IPC and IT Act 2000, along with its amendment and the rules made there under, govern the cyber defamation in India. Cyber Jurisdiction is also a biggest challenge for the courts to apply the national law and decide the cases.

Cyber Jurisdiction: Indian Perspective: The Model Law on E-commerce[5] 1996, and the Information Technology Act, 2000, leave out any reference to the jurisdiction of courts in the virtual world. This is a major flaw. To what extent, if any, does today's law of jurisdiction apply to cyberspace as well as to the physical world?

There are two schools of thought on this:

- A distinct law of jurisdiction must be established for each of the two realms if they are unrelated.
- As long as the two are linked in some way, the physical world's laws of jurisdiction can be applied to both with appropriate changes.
- As a result of the absence of physical boundaries in cyberspace, it is argued that a new system of law and jurisdiction is required for the cyberspace realm. It appears that this notion is illogical, given that despite the absence of geographic limits in the cyber world, physical boundaries still exist. Because of a variety of factors, including the enormous disparity between rich and developing countries, it is impossible to create distinct laws of jurisdiction for the cyber space.[6] Although there are no physical boundaries in the cyber space, there is an argument that the law will be applied to netizens because they are citizens of that country. As a result, current law governing the physical world can be applied to the cyber realm with only modest alterations. Logic would seem to support this position. As a result, the current law of the physical world, with slight alterations, is applicable to the cyber world as well.

Liabilities of Intermediaries-IT Act 2000: In today's paperless world, various individuals or authorities serve as intermediaries, with the primary responsibility of managing computer systems, networks, and the internet. They also offer a variety of services such as server hosting, client webpage hosting, and so on. The role of the intermediary, on the other hand, is risky.

For example, the client's webpage hosted on the intermediary server may contain obscene material that infringes on the rights of others. In such a case, the role of the intermediary is simply to relay third-party[7] information to the public, and he should not be held liable if he makes reasonable efforts to prevent access.

In some cases, the intermediary is exempt from liability[8]: **Section 79-** It is vital to highlight that an intermediary is not liable under the IT Act. He may establish rules or regulations for users. The following requirements, however, must be met:

- Third-party data may be sent, stored, or hosted by the intermediary, but the intermediary's function is limited to facilitating access to that communication. Or
- The intermediate does not initiate or receive the transmission or select or modify the data contained in the communication.
- The intermediary performs his duties under this Act, as well as rules of the Central Government on his behalf, with due diligence.
- Rule 3 of the IT (Intermediaries Guidelines) Rules, 2011 states that an intermediary shall undertake due diligence:[9] The intermediary must perform the following due diligence when carrying out his responsibilities:

- The intermediary must post the intermediary's rules, privacy policy, and user agreement before anybody can access or utilize the intermediary's computer resources.[10]
- Computer users must be made aware that they are not permitted to host, display or otherwise distribute any material that is blasphemous, defamatory, obscene, pornographic, libelous, invading someone else's privacy, hateful, disparaging, in any way and
  - do not harm the youth;
  - Patent, trademark, copyright, and other intellectual rights may be infringed;
  - Is in contravention of any current law;
  - Any information that is extremely insulting or menacing is communicated in violation of this rule,
  - Assume the identity of someone else;
  - The ability to damage, destroy, or limit the usefulness of any computer resource is one of the primary goals of malicious software code, data, or programmes.
  - Is a danger to India's national cohesion and sovereignty, cordial ties with other countries, or public order; incites criminal activity; obstructs the investigation of criminal activity; belittles the other country's government.[11]
  - Neither the intermediary nor the recipient of the transmission may knowingly host or publish any material; nor may the intermediary initiate, choose, or edit the information contained in the transmission.
  - Computer resources can store the information in a short or intermediate state without the requirement for any human involvement to transmit or communicate it to another computer resource.
  - Any information or communication link that the intermediary has access to must be immediately removed from the intermediary in line with any instruction or

[4] Information and technology are the two words that make up the acronym IT. For making decisions, communicating, gaining knowledge, and being more productive, information is crucial. In order to arrive at a conclusion, a collection of data is referred to as information. Textual, numerical, graphical, audio/video, or other media can all be used to portray information like facts, figures, and ideas. But in order for info to be valuable, it must be accurate; timely; complete; exact; accurate, and relevant. Technical information and knowledge are needed to carry out everyday tasks like research and development in a wide range of industries.

[5] When we talk about e-commerce, we're referring to the practice of conducting business on the internet, whether it's through the sale of goods and services that are traditionally delivered in the physical world or digital things like software.

[6] V Mitter, Law of Defamation & Malicious Prosecution, (Universal Law Publishing Co. Pvt.Ltd, New Delhi, (2015), pp-237-323

[7] Third-party information refers to information that the intermediary receives, stores, or transmits from an independent individuals or groups.

[8] According to the 2011 Rules, an intermediary can claim safe harbor protection if they can demonstrate that they took action within 36 hours after being notified of infringing material on their site.

[9] It is the intermediary's legal obligation to exercise due diligence to ensure that the illegal content is not transmitted or published, and this obligation is enshrined in law. The term "due diligence" refers to taking reasonable steps to avoid committing an offence or contravening the law, i.e., determining whether the information it transmits is illegal. A duty to take reasonable precautions is what we mean by this.

[10] Ibid

[11] Ibid

directive issued by the Act, if the intermediary is brought to the attention of it.

- In order to comply with the sub-rule (2) any information that is contrary of the intermediary's computer system, the intermediary's computer system shall act within 36 hours after receiving written or through mail concerning any such info (2). A minimum of ninety days' worth of further records and information must be kept by the intermediary for the purpose of inquiries.

Indian intermediaries have put these rules into action. It's not clear what the phrase ".... Shall act within thirty-six hours...."[12] means, Sub-rule (4) of Rule 3 says as much.[13] A notification from the Ministry of Communications and Information Technology said that the intended meaning of Rule 3(4) is that the intermediary must respond to or acknowledge complaints received by it within 36 hours of receiving them and take appropriate action in accordance with Rule 3(2), which was clarified by MCIT. In addition, the intermediary's Grievance Officer must resolve such complaints immediately, but no later than one month after receiving them in accordance with Rule 3(11). Grievance redress procedures should be made available to the general public by the intermediary.

- All applicable laws, laws and guidelines, user agreement, and security policy must be communicated to the user in the case of non-compliance; Intermediary may immediately terminate and remove non-compliant material from Intermediary's computer resources.
- As long as any applicable laws are in effect, intermediaries must adhere to them.
- Any information or support the intermediary provides to Government Agencies that are legitimately allowed for investigation, protection, or cyber security activities must be done so in accordance with the law. There must be an official written request outlining the specific purpose for which such information and help is requested.
- In accordance with the IT (Reasonable Security Practices and Procedures and Sensitive Personal Information) Rules, 2011, the intermediary must take all reasonable measures to secure its computer resource and the information contained within.[14]
- It is the intermediary's responsibility to notify and give information to the Indian Computer Emergency Response Team (ICERT) in the event of a cyber security incident.
- A computer resource's "technical configuration" can't be altered in any way by an intermediary in order to avoid infringing any current regulations, therefore the intermediary can't knowingly deploy, install, or modify the technical configuration of a computer resource. To safeguard it, the Intermediary could potentially develop, produce, distribute, or apply technological tools.
- Breach or use of computer resources by any individual in violation of rule 3 must be reported to the intermediary via the intermediary's website, which must also provide the name and contact information of a Grievance Officer. The Grievance Officer must respond to complaints within a month of receiving them.

Exceptions: For example, the intermediary may be held responsible in the following scenarios:

- The intermediary has conspired; the intermediary has facilitated; the intermediary has helped; the intermediary has authorized.
- A computer resource under the intermediary's supervision that is being used to commit the criminal act is not removed or disabled without tainting the evidence in any manner after the intermediary has received notice from the appropriate government agency.
- When he violates the directions of the competent authorities given under the provisions of this Act, i.e. Sections 67C, 69, 69A, 69B and 70B.

CONCLUSION

Freedom of speech and expression is a human right permitted under various international instruments. Two such examples are Article 19 of Universal Declaration of Human Rights, 1948 ad article 19 of ICCPR, 1966 which permit freedom of speech and expression i.e., Article 19 of UDHR, 1948 says “Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference ad to seek, receive and impart information and ideas through any media and regardless of frontiers. Further, Article 19(2) of the ICCPR, 1966 also permit freedom of speech and expression i.e., Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or print, in the form of art, or through any other media of his choice. Human Rights Council in 2014 adopted a resolution that human rights offline also apply online. Various countries have enacted laws for online free speech. However, in India freedom of speech and expression through online communication was hanging in the air and netizens in India are not enjoying this right as permitted under various instruments and Article 19(1)(a) of the Indian Constitution as Section 66A of the IT Act, 2000 imposes unreasonable restrictions on online free speech which are not mentioned under article 19(2) of the Constitution. However, now Section 66A has been abolished by the Apex Court of India in Feb. 2015 in *Shreyas Singhal v Union of India* and citizens have online freedom of speech and expression as is accepted by the Human Rights Council.

There are three main models of liability of intermediaries; *The strict liability model: The safe harbor liability model (The Vertical approach and The horizontal approach); and The broad immunity model*. Different models are followed by different countries. Consequently, under cyber law of almost every country, intermediaries are made liable where they fail to perform their duties i.e. the USA, France, China, Japan, etc. Further, the Special Rapporteur on the promotion and protection of the right to freedom had also criticized the liability of the intermediaries in restricting the freedom of speech and expression of the netizens and had made various recommendations.

In India, *the safe harbor liability model (horizontal approach)* is followed, and under Section 79 of the Information Technology Act 2000, the intermediary is not liable for online communication of a third party. The need of the hour is to implement various recommendations by the Special Rapporteur on the promotion and protection of the right to freedom.

REFERENCES

Collins Matthew, *The Law of Defamation and the Internet*, Second Edition, Oxford University Press, New York.

Dr. Agarawal & Gupta, *Cyber Laws*, 2009 Edition, Premier Publishing Company, Allahabad.

Dr. Nagaraja M.K, *Cyber Law and Cyber Crime: Analytical approach*, 2014 edition (Bangalore: Sun Publishing House)

Dr. Verma Amita, *Cyber Crimes and Law*, 2012 edition, (Allahabad: Central Law Publications)

[12] A notice and takedown regulatory environment for restricting intermediary liability was established by the IT Act Amendments of 2008 in India (in sync with the US law). This means that if he is made aware of any illegal content on the site, he must take action to remove it. The intermediary can protect himself from liability by using a procedure known as notice and takedown. Intermediaries are now protected from user-generated content in countries like the United States, the European Union, and India. The term "safe harbor" is used to describe this type of protection.

[13] To be eligible for immunity under the IT Act, an intermediary must adhere to Central Government-issued Intermediary Guidelines. Due diligence is mandated for intermediaries under Rule 3 of the IT (Intermediaries Guidelines) Rules, 2011. Rule 3 has eleven sub-rules, namely: Rule 3(1), Rule 3(2), Rule 3(4), and Rule 3(5). (11).

[14] Ibid

Duggal Pavan, *Cyber Law*, First Edition, Universal Law Publications, New Delhi.

Fatima Talat, *Cyber Crimes*, First edition, (Lucknow: Eastern Book Company)

Kubota Takashi, *Cyber Law for Global E-Business*, 2008 Edition, Information Science Reference Publications, New York.

Matthan Rahul, *The Law relating to Computers & the Internet*, 2000 Edition, Butterworths India, New Delhi.

Mali Prashanth, *Cyber Law and Cyber Crimes Simplified*, Fourth Edition, Cyber Infomedia Publishing, New Delhi.

Ryder D Rodney, *Guide to Cyber Laws*, 3rd Edition, Wadhwa & Company, Nagpur.

Sharma Vakul, *Information Technology*, 4th Edition, Universal Law Publications, New Delhi.

Tiwari Garima, *Understanding Laws-Cyber Laws and Cyber Crimes*, First Edition, Lexis Nexis, Nagpur.

Vishwanathan Aparna, *Cyber Law-Indian and International Perspectives on Key Topics*, First Edition, Butterworths, Wadhwa, Nagpur.

Journals

Prof. Rajshekar, titled: *Cyber Defamation*, KLE'S Law Journal, 2016 edition, KLE Society Publications.

****