



Cyber Defamation – A Scratch in Privacy

R. Deepika

4th Year, B. Com, LLB(Hons), School of Excellence in Law, Dr. Ambedkar Law University, Tamilnadu

ABSTRACT

With the rise of social media and online communication, cyber defamation has become a serious problem in India. Cyber defamation is the act of defaming someone through online communication. It is a criminal offense in India, and those found guilty can face legal consequences. Cyber defamation can take many forms, including posting defamatory comments on social media, publishing defamatory articles on websites, and sending defamatory emails or messages. The impact of cyber defamation can be devastating, as it can affect a person's personal and professional reputation, as well as their emotional well-being. Cyber defamation is a serious offense that can have significant consequences for both the victim and the perpetrator. In India, cyber defamation is a growing problem that requires urgent attention. This article will discuss cyber defamation in India, its laws, and legal consequences.

Key Words : media, communication, cyber defamation, guilty, reputation, consequences

WHAT IS CYBER DEFAMATION?

Cyber defamation is a type of defamation that occurs through online communication. It is the act of defaming someone through the use of the internet, social media platforms, emails, or any other form of online communication. Cyber defamation can be done in many ways, such as posting false and defamatory content, sharing someone else's personal information without their consent, or spreading rumors about them.

Cyber defamation can have serious consequences on a person's reputation and career. Once something is posted online, it can be shared and spread quickly, making it difficult to erase the damage done.

DEFINITION OF CYBER DEFAMATION

Cyber defamation refers to the act of publishing false, malicious, or defamatory statements about a person online. These statements can take many forms, including written posts on social media, blogs, or websites, as well as spoken statements on podcasts or videos. Cyber defamation can be intentional or unintentional, and can be committed by individuals or groups.

Cyber defamation can be a violation of both civil and criminal law, depending on the nature and severity of the statements made. In some cases, cyber defamation can also be a violation of a website's terms of service, which can result in the removal of the offending content and the suspension or termination of the user's account.

CYBER DEFAMATION LAWS IN INDIA:

Cyber defamation is a criminal offense under Section 499 of the Indian Penal Code (IPC). Under this section, anyone who intentionally defames another person through online communication can be punished with imprisonment for up to two years, a fine, or both.

In 2018, the Ministry of Electronics and Information Technology (MEITY) released a draft of the Information Technology [Intermediaries Guidelines (Amendment) Rules], which aimed to hold intermediaries like social media platforms accountable for the content posted on their platforms. The draft rule requires intermediaries to remove content within 24 hours of receiving a complaint and provide assistance to law enforcement agencies in investigating cyber defamation cases.

- Section 66D of the Information Technology Act deals with identity theft and punishes any person who impersonates someone else by using a computer resource or communication device. This section also covers the use of false digital signatures and is punishable with imprisonment for up to three years and a fine.
- Section 67 of the Information Technology Act deals with the publishing or transmitting of obscene material in electronic form. The section states that any person who publishes or transmits any material that is lascivious or appeals to prurient interests can be punished with imprisonment for up to three years and a fine.

- Section 67A of the Information Technology Act deals with the publishing or transmitting of sexually explicit material in electronic form. The section states that any person who publishes or transmits any material that contains sexually explicit acts can be punished with imprisonment for up to five years and a fine.
- In addition to these provisions, there are several other sections of the Information Technology Act that can be used to address cyber defamation, including Sections 43, 66E, and 72. These provisions deal with unauthorized access, violation of privacy, and breach of confidentiality, respectively.
- Section 500 of the IPC provides for the punishment for defamation and states that any person who commits defamation can be punished with imprisonment for up to two years, a fine, or both. These provisions can be used to address cyber defamation as well, as they cover any form of communication, whether it is spoken or written.

THE PROCEDURE OF A CYBER DEFAMATION CASE IN INDIA :

FILING A COMPLAINT:

The first step in a cyber defamation case is to file a complaint with the police. The complainant must provide all the necessary details, including the nature of the offense, the identity of the accused, and any evidence they have to support their claim. The police will then register the complaint and begin an investigation into the matter.

HOW TO FILE A COMPLAINT FOR CYBER DEFAMATION:

If someone has been a victim of cyber defamation, they can file a complaint with the police. The complaint can be filed at any police station or cyber cell. The complaint which is going to be filed must have the following information in that complaint:

- Details of the defamatory content
- Name of the person
- Date and time of the post
- Any other relevant information, such as screenshots or links to the content
- Once the complaint is filed, the police will investigate the matter and take appropriate legal action against the person responsible.

INVESTIGATION:

After registering the complaint, the police will begin an investigation into the matter. They will collect evidence, including digital evidence, and question witnesses. The police may also seek assistance from cybercrime experts to help with the investigation.

ARREST:

If the police find evidence that supports the allegations of cyber defamation, they may arrest the accused. The arrest can only be made after obtaining a warrant from a magistrate. The accused will be produced before the magistrate, who will decide whether to grant bail or remand them in custody.

CHARGE SHEET:

After the completion of investigation the charge sheet will be prepared by police. The charge sheet contains all the evidence collected during the investigation, along with the charges against the accused. The charge sheet is then presented to the court.

TRIAL:

The trial in a cyber defamation case is conducted in the court of law. The accused is given an opportunity to defend themselves and present evidence in their favor. The prosecution must prove beyond a reasonable doubt that the accused is guilty of cyber defamation.

VERDICT:

After hearing the arguments from both sides and examining the evidence, the court will deliver its verdict. If the accused is found guilty, they will be sentenced accordingly. If they are found not guilty, they will be acquitted of all charges.

APPEAL:

If either party is dissatisfied with the verdict, they can appeal to a higher court. The appeal must be filed within the prescribed time limit and must contain all the necessary details, including the grounds for the appeal.

TYPES OF DEFAMATION

LIBEL DEFAMATION:

Libel is a form of defamation that involves a false statement that is made in a permanent form, such as in writing or through broadcasting. Libel can include any published material that is false and harms the reputation of a person or organization. Examples of libel can include newspapers, magazines, television shows, websites, and social media posts.

In order for a statement to be considered libel, it must meet the following criteria:

- The statement must be false.
- The statement must be published, meaning it is communicated to a third party.
- The statement must be defamatory, meaning it harms the reputation of the person or organization.
- The statement must identify the person or organization being defamed.
- If a statement meets these criteria, the person or organization who made the statement can be sued for libel.

SLANDER DEFAMATION:

Slander is a form of defamation that involves a false statement that is spoken or otherwise communicated in a transient form. Slander can include any spoken words or gestures that are false and harms the reputation of a person or organization. Examples of slander can include rumors, gossip, and spoken statements made in public.

In order for a statement to be considered slander, it must meet the following criteria:

- The statement must be false.
- The statement must be spoken or otherwise communicated in a transient form.
- The statement must be defamatory, meaning it harms the reputation of the person or organization.
- The statement must identify the person or organization being defamed.
- If a statement meets these criteria, the person or organization who made the statement can be sued for slander.

DIFFERENCES BETWEEN LIBEL AND SLANDER DEFAMATION

The main difference between libel and slander defamation is the form in which the false statement is communicated. Libel involves a false statement that is published in a permanent form, while slander involves a false statement that is spoken or otherwise communicated in a transient form.

Another difference between libel and slander defamation is the burden of proof required to win a lawsuit. In a libel lawsuit, the plaintiff must prove that the defendant made a false statement that was published, defamatory, and identified the plaintiff. In a slander lawsuit, the plaintiff must prove the same elements, as well as that the statement caused actual harm to the plaintiff.

CYBER DEFAMATION CAN BE DONE THROUGH:

The most common types of cyber defamation include,

ONLINE REVIEWS AND RATINGS:

Online reviews and ratings are a common way for people to share their opinions about products, services, and businesses. However, these reviews can also be used to defame individuals or companies. False or negative reviews can harm a business's reputation, and can result in a loss of revenue and customers.

SOCIAL MEDIA POSTS:

Social media platforms like Face book, Twitter, and Instagram provide users with a way to share their thoughts and opinions with others. However, these platforms can also be used to spread false or defamatory statements about individuals or groups. Social media posts can be shared quickly and widely, making it difficult to control the spread of false information.

BLOG POSTS AND ARTICLES:

Blogs and websites provide individuals with a platform to share their opinions and ideas with others. However, these platforms can also be used to publish false or defamatory statements about individuals or companies. Blog posts and articles can be shared on social media and other websites, increasing the reach of the defamatory statements.

EMAIL AND MESSAGING:

Email and messaging platforms like Gmail, Yahoo, and WhatsApp can also be used to defame individuals or companies. False or defamatory statements can be sent directly to a person or group, making it difficult to track down the source of the statements.

LEGAL REMEDIES FOR CYBER DEFAMATION IN INDIA

There are several legal remedies available to victims of cyber defamation in India. These include civil and criminal remedies.

CIVIL REMEDIES:

Civil remedies for cyber defamation include filing a civil suit for damages. The victim can seek compensation for any harm caused to their reputation as a result of the defamatory content posted online. In addition to damages, the court can also issue an injunction restraining the defendant from posting any further defamatory content.

CRIMINAL REMEDIES:

Criminal remedies for cyber defamation include filing a criminal complaint under Section 499 and 500 of the Indian Penal Code. The victim can file a complaint with the police, who will investigate the matter and file a charge sheet in court. If the court finds the accused guilty of cyber defamation, they can be punished with imprisonment for up to two years, a fine, or both.

The Information Technology Act, 2000 also provides for criminal remedies for cyber defamation. Section 66A of the Act makes it an offense to send offensive messages through communication services. The section was struck down by the Supreme Court of India in 2015, but other provisions of the Act, such as Section 66D, which provides for punishment for cheating by person can be used to address cases of cyber defamation

CONSEQUENCES OF CYBER DEFAMATION

The consequences of cyber defamation can be severe, both for the individual who is defamed and for the person who commits the defamation. Some of the consequences of cyber defamation include:

DAMAGE TO REPUTATION:

Cyber defamation can harm an individual's personal and professional reputation. False or defamatory statements can be spread quickly and widely online, making it difficult for the individual to control the damage to their reputation.

LOSS OF INCOME:

Cyber defamation can also result in a loss of income for individuals or businesses. False or negative statements can harm a business's reputation, leading to a loss of customers and revenue.

EMOTIONAL DISTRESS:

Cyber defamation can also cause emotional distress for the individual who is defamed. The stress and anxiety of dealing

HOW TO FILE A COMPLAINT FOR CYBER DEFAMATION:

If someone has been a victim of cyber defamation, they can file a complaint with the police. The complaint can be filed at any police station or cyber cell. The complaint which is going to be filed must have the following information in that complaint:

- Details of the defamatory content
- Name of the person
- Date and time of the post
- Any other relevant information, such as screenshots or links to the content
- Once the complaint is filed, the police will investigate the matter and take appropriate legal action against the person responsible.

ESSENTIAL ELEMENTS FOR CYBER DEFAMATION:

FALSE STATEMENTS:

The first essential element of cyber defamation is that the statements made must be false. It cannot be considered as defamation when the given statement is true. The statements must be factual, and they must be proven to be false to constitute defamation. The burden of proof lies with the person making the claim of defamation.

PUBLICATION:

The second essential element of cyber defamation is publication. The false statements must be published or communicated to a third party. This means that the statements must be made public and accessible to others. The publication can occur on various digital platforms, such as social media, blogs, forums, or online news websites.

IDENTIFICATION:

The third essential element of cyber defamation is identification. The false statements must be specifically directed towards an individual or entity, and they must be identifiable. This means that the statements must be about a specific person or business, and they must be clearly identifiable as such. If the statements are general in nature and cannot be attributed to a specific person or business, then they cannot be considered defamatory.

DAMAGES:

The fourth essential element of cyber defamation is damages. The false statements must have caused actual harm or damages to the person or entity. This harm can be in the form of loss of reputation, loss of business, emotional distress, or any other form of damages. The damages must be proven to be a direct result of the false statements made.

FAULT:

The fifth essential element of cyber defamation is fault. The person making the false statements must have acted with negligence or malice. Negligence refers to the failure to exercise reasonable care when making the statements. Malice refers to the intent to cause harm or damage to the person or entity. If the person making the false statements did not act with negligence or malice, then they cannot be considered liable for defamation.

DEFENSES:

The sixth essential element of cyber defamation is defenses. There are several defenses that can be used to protect against claims of cyber defamation. These defenses include truth, fair comment, and privilege. Truth refers to the fact that if the statements made are true, then they cannot be considered defamatory. Fair comment refers to the right to express an opinion on a matter of public interest. Privilege refers to the right to make statements in certain circumstances, such as in court proceedings or during legislative debates.

PREVENTIVE MEASURES FOR CYBER DEFAMATION:

Prevention is better than cure. Here are some preventive measures that individuals can take to protect themselves from cyber defamation:

- Always be cautious what you do online
- Make sure you do not share personal things with unknown person
- Set a strong password for all online handlings
- Make sure that your privacy was set on in social media
- Do not indulge in online arguments and do not believe the rumors and share the same
- Always report the content which you feel defamatory

IMPACT OF CYBER DEFAMATION

IMPACT ON INDIVIDUALS:

The impact of cyber defamation on individuals can be severe, as it can cause harm to their reputation and standing in the community. Individuals who are victims of cyber defamation can face ridicule, harassment, and even loss of employment. The spread of false information through social media can be swift, and it can be difficult to control or contain the damage caused by such information.

In India, there have been several cases of cyber defamation where individuals have been subjected to abusive and derogatory messages on social media platforms. For instance, in 2016, the famous actor and comedian was subjected to cyber defamation on Twitter, where he was accused of tax evasion and corruption. The false allegations caused significant damage to his reputation and career, leading to a decline in his popularity and a loss of endorsement deals.

IMPACT ON BUSINESS:

Impact on Businesses Cyber defamation can also impact businesses, particularly small and medium enterprises (SMEs) that rely on their reputation to attract customers. In India, SMEs contribute significantly to the economy, and any damage to their reputation can have a significant impact on their survival and growth.

Businesses that are victims of cyber defamation can face a decline in sales, loss of customers, and damage to their brand image. For instance, in 2019, a hotel in Jaipur was subjected to cyber defamation on

Trip Advisor, where it was falsely accused of discrimination against foreign tourists. The false allegations caused significant damage to the hotel's reputation, leading to a decline in bookings and a loss of revenue.

IMPACT ON GOVERNMENTS:

Cyber defamation can also impact governments, as false information and propaganda can be spread rapidly through social media, leading to unrest and social tension. In India, social media platforms have been used to spread rumors and fake news, leading to violence and communal unrest in several parts of the country.

The impact of cyber defamation on governments can also be political, as false information can be used to manipulate public opinion and influence elections. For instance, in the run-up to the 2019 general elections in India, several political parties were accused of spreading false information on social media to influence voters.

IMPACT ON SOCIETY:

Cyber defamation can have a broader impact on society, as it can lead to a decline in trust and confidence in institutions and individuals. The spread of false information through social media can create an environment of fear and mistrust, leading to social polarization and a breakdown of social cohesion.

In India, the impact of cyber defamation on society can be seen in the rise of hate speech and communalism. Social media platforms have been used to spread hate speech and incite violence against religious and ethnic minorities, leading to a rise in communal tensions and violence.

CASELAWS RELATED TO CYBER DEFAMATION➤ ***Shreya Singhal v. Union of India***¹

This landmark case struck down Section 66A of the Information Technology Act, 2000, which criminalized online communication that was deemed "offensive" or "menacing" in nature.

➤ ***Subramanian Swamy v. Union of India***:

In this case, the Supreme Court² held that a person cannot be sued for defamation for statements made in the course of an official proceeding, such as a parliamentary debate.

➤ ***Google India Pvt. Ltd. v. Visaka Industries***:

This case dealt with the issue of intermediary liability in cases of online defamation. The court held that online platforms such as Google³ cannot be held liable for third-party content posted on their platforms.

➤ ***LIC of India v. Manohar Lal Sharma***:

In this case, the Delhi High Court⁴ held that a person cannot be sued for defamation for statements made in the course of judicial proceedings.

➤ ***Ram Jethmalani v. Subramanian Swamy***:

This case dealt with the issue of whether statements made on social media platforms such as Twitter can be considered defamatory. The court⁵ held that such statements can indeed be considered defamatory.

➤ ***Super Cassettes Industries Ltd. v. MySpace Inc.***:

This case dealt with the issue of jurisdiction in cases of online defamation.⁶ The court held that Indian courts have jurisdiction over cases of online defamation even if the defamatory content is hosted on servers outside India.

¹ (2013) 12 s.c.c.73

² 2016 SCC vol.7

³ 2019 SCC online SC 1587, decided on 10.12.2019

⁴ AIR 1981 DELHI 171

⁵ AIR 1988(4) SCC 419

⁶ Decided on : 29.07.2011

➤ ***Sahara India Real Estate Corporation Ltd. v. SEBI:***

In this case, the Supreme Court held that statements made in the course of a public debate on a matter of public interest cannot be considered⁷ defamatory.

➤ ***Pawan Kumar v. State of Haryana:***

This case dealt with the issue of whether a person can be held liable for sharing defamatory content on social media. The court⁸ held that such a person can indeed be held liable for defamation.

➤ ***Dharambir v. CBI:***

In this case, the Delhi High Court held that a person cannot be held liable for defamation for statements made in the course of an investigation.⁹

➤ ***Indian Oil Corporation Ltd. v. NEPC India Ltd.:***

This case dealt with the issue of whether a company can be sued for defamation. The court held that a company can indeed be sued for defamation¹⁰ if it has made a defamatory statement about another company or individual.

SUGGESTIONS :

Suggestion 1: Awareness campaigns

The first step to addressing the problem of cyber defamation is to raise awareness about its impact and the legal consequences. The government and civil society organizations can run awareness campaigns to educate people about the dangers of cyber defamation and the legal framework surrounding it. These campaigns can also highlight the importance of responsible online behavior and the need to respect the privacy and dignity of others.

Suggestion 2: Strengthening the legal framework

India has laws that protect individuals against defamation, including the Indian Penal Code, the Information Technology Act, and the Right to Information Act. However, these laws need to be strengthened to address the unique challenges posed by cyber defamation. The government can consider introducing specific provisions that address cyber defamation, including the regulation of online platforms and the imposition of stricter penalties for those who engage in cyber defamation.

Suggestion 3: Improving the capacity of law enforcement agencies

Law enforcement agencies play a crucial role in combating cyber defamation. However, many of these agencies lack the necessary resources and capacity to investigate and prosecute cyber defamation cases effectively. The government can address this by providing specialized training to law enforcement officials and equipping them with the necessary tools and technologies to investigate cyber defamation cases.

Suggestion 4: Collaboration between online platforms and law enforcement agencies

Online platforms such as social media sites, search engines, and online marketplaces can also play a vital role in combating cyber defamation. These platforms can collaborate with law enforcement agencies to identify and remove defamatory content and take action against those who engage in cyber defamation. The government can encourage such collaboration by introducing incentives for online platforms that take proactive measures to combat cyber defamation.

Suggestion 5: Strengthening the role of the judiciary

The judiciary plays a crucial role in adjudicating cyber defamation cases and upholding the rule of law. However, there is a need to strengthen the capacity of the judiciary to deal with cyber defamation cases effectively. This can be achieved by providing specialized training to judges and magistrates and by introducing specialized cyber defamation courts to handle such cases.

CONCLUSION:

Cyber defamation is a serious problem in India. It can have serious legal, social, and economic consequences on a person's life. The Indian government has enacted laws to protect individuals from cyber defamation, and those found guilty can face legal consequences. Cyber defamation is a growing concern in India, and it can have significant consequences for individuals and society as a whole. While the legal framework is in place to address this issue, more needs to be done to educate individuals about the impact of cyber defamation and to prevent such behavior from occurring in the first place. As India continues to embrace the digital age, it is essential to ensure that individuals and organizations alike are held accountable for their actions online, and that the internet remains a safe and secure space for all.

⁷ (2013) 1 SCC 1. Decided on 31.08.2012

⁸ (1995) 109 PLR 534

⁹ 148 (2008) DLT 289

¹⁰ (2006) 6 SCC 736