

## **ONLINE DEFAMATION OF WOMEN IN INDIA: AN INTRUDER OF THEIR RIGHT TO PRIVACY-A CRITICAL ANALYSIS**

**Dr. Amandeep Kaur<sup>1</sup>**

**Navreet Kaur<sup>2</sup>**

### **Abstract**

The growth and development of the technology have brought enormous changes in day to day life. The internet has made communication and access to information easier. Defamation is a legal wrong emerging from an act of injuring a person's reputation and sully their character without lawful justification and excuse. Cyber defamation is considered to be the act of defaming, insulting, offending or otherwise causing harm through false statements pertaining to an individual in cyber space. In India, civil as well as criminal defamation incidents have geared up to a considerable extent both online and offline irrespective of the presence of stringent laws to that effect. The overuse of data by young people is also indirectly resulting in the rise of internet crimes against women. The law of defamation is of great importance and value because it deals with the subject which is directly associated with the integrity and honour of mankind in India and more importantly it is associated with our Fundamental Right to Privacy engraved from Article 21. The present paper is an analysis of various kinds of online crimes against the women and their impact. An attempt has been made to suggest possible socio-legal measures to combat the problem of online defamation against women.

### **1. INTRODUCTION**

Next to life, what one cares most is his reputation. Sometimes, we find an individual giving it the foremost place, preferring death rather than living a life of ignominy and disgrace. We have heard of stories and even historical narratives of our ancient warriors and Rajput ladies having committed suicide, rather than falling into the hands of their enemies and being compelled to live in shame and disgrace at the cost of their reputation. Reputation is in fact a great internal force in the mind of every man, impelling him to do things. Love of reputation inspires individuals to do great things and even face risks. On a careful analysis of human mind, one will find this element of longing for name and reputation as the basic motive of most actions. Authors, scientists, poets, and all others, who are engaged in certain activities, have in the innermost recess of their hearts a longing

---

<sup>1</sup> Assistant Professor, Department of Laws, Guru Nanak Dev University Regional Campus, Gurdaspur(Punjab)

<sup>2</sup> Research Scholar, Department of Laws, Guru Nanak Dev University Regional Campus, Gurdaspur(Punjab)

to earn a name in their respective fields of activities. If you remove this instinct in man, he is deprived of his mainspring in life.<sup>3</sup>

## **2. MEANING OF DEFAMATION**

Reputation means "the estimation in which a person or thing is generally held" i.e. the good name one has. In other words, it is a favorable and publicly recognized name or standing: "Reputation is what other people tell about a man and it is different from character which one has in himself or possessed by himself."<sup>4</sup>

The essence of offence of defamation is the harm caused to the reputation of a person. Defamation is nothing but causing damage to reputation of another. The word defamation is derived from Latin word Diffamare. Semantics or etymology of Latin word Diffamare provides that it means "spreading evil report about someone".

**Salmond** defines the wrong of defamation as the publication of a false and defamatory statement about another person without lawful jurisdiction.<sup>5</sup>

**Blackburn and George**<sup>6</sup> define defamation "the tort of publishing a statement which tends to bring a person into hatred, contempt or ridicule, or to lower his reputation in eyes of right thinking members of society generally."

Defamation is a statement which harms the reputation of a person or which lowers the good being of a person in society and such statement has been made without any lawful justification. It is a libel if the statement is in a permanent form and it is a slander, if it consists insignificant words or gestures. Generally the statements in written form are considered to be in permanent form.

Defamation and reputation both are correlated. The harm to reputation is called defamation. In that way, one cannot speak or publish anything about anyone. But this is not the case. Our freedom to speech and expression has been secured by our constitution where it has been declared to be our fundamental right under Article 19(1)(a). Moreover section 500 Of Indian Penal Code consists of some exceptions where publication of derogatory statements cannot be termed as criminal defamation

The law of defamation, thus, is of great importance and value because it deals with the subject which is directly associated with the integrity and honour of mankind. It becomes even more important when any private information is published in defamatory form resulting in the violation of right to privacy- an expression of Right to life and expression under Article 21 of the constitution of India. In India, civil as well as criminal defamation incidents have geared up to a considerable extent both online and offline irrespective of the presence of stringent laws to that effect. Cyber space has become an instrument for offenders to victimize or infringe women, the most vulnerable targets on internet after children. Internet has opened flood gates for various crimes against women in the cyber space. Even though, draftsmen and other world leaders who participate in EC conventions

---

<sup>3</sup> P.S.Pillai, Criminal Law ,1207(LexisNexis Butterworths, India,2008)

<sup>4</sup>Vadackumchery James; U.N. Universal Declaration of The man Rights and Criminal Justice,92( Concept Publishing Co. Pvt. Ltd., New Delhi, 2012)

<sup>5</sup> Salmond on Torts, 361(13<sup>th</sup> Ed., 1961)

<sup>6</sup> Blackstone and George, Elements on the law of Torts ,167( 2<sup>nd</sup> Ed., 1949)

for establishing strict rules to control cyber crime against children ,never considered victimization of women in the cyber space as a big issue like child pornography or hacking which require attention. Modern innovations have made life easier for women across the world, but side by side, these have led to rise in the crimes of electronic Violence against women.<sup>7</sup> According to the National Crime Records Bureau, nearly 3.78 lakh cases of crime against women were reported in 2018 alone. Add to this, online rape threats, harassment, cyber stalking, blackmail — which are rampant in the virtual world — and the number could be lot larger. With women using traditional and innovative media to grab growth opportunities, creating a safer offline and online space is the need of the hour.<sup>8</sup>

### **3. RIGHT TO PRIVACY**

Defamation has direct impact on the privacy of an individual. Thus it becomes very much important to discuss it in Indian scenario as well as its international importance.

#### **3.1 :Indian Constitution**

Indian constitution provides certain fundamental rights to its citizen irrespective to their gender. Both women and men are the subjects of fundamental rights. In India, the right to privacy is not specifically mentioned as Fundamental Right. The right to privacy in India has developed through a series of decisions over the past 60 years. Over the years, inconsistency from two early judgments created a deviation of opinion on whether the right to privacy is a fundamental right.

The issue of privacy was dealt with both as a fundamental right under the Constitution and as a common law right since the 1960's. Privacy was not considered as a fundamental right was first held by the supreme court in the year 1954 by an eight-judge bench in *M.P. Sharma v. Satish Chandra case*<sup>9</sup>, while dealing with the power to search and seize documents from the Dalmia Group, dismissed the existence of right to privacy on the basis that the makers of constitution.

In *Kharak Singh v. State of U.P.*<sup>10</sup>, the meanings of the expressions “life” and “personal liberty” in Article 21 were considered by the Apex Court. Although the majority found that the constitution contained no explicit guarantee of a “right to privacy”, it reads the right to personal liberty expansively to include a right to dignity. The court in its decision invalidated a Police Regulation that provided for nightly domiciliary visits, calling them an “unauthorized intrusion into a person’s home and a violation of ordered liberty.” However,

---

<sup>7</sup> Jaspreet Singh, Violence against women in cyber world: A special Reference to India, IJARMSS, 60 (2015)

<sup>8</sup> Rekha Sharma, Assuring women’s safety in virtual world, the hindubusinessline, (July 17, 2020, 8:40AM), <https://www.thehindubusinessline.com/opinion/assuring-womens-safety-in-the-virtual-world/article30956278.ece>

<sup>9</sup> A.I.R. 1077 (India 1954).

<sup>10</sup> A.I.R. 1295 (India 1963).

it also upheld that as the right of privacy was not guaranteed under the Constitution, and hence Article 21 of the Indian Constitution (the right to life and personal liberty) had no application. Justice Subbarao's dissenting opinion clarified that, although the right to privacy was not expressly recognized as a fundamental right, it was an essential ingredient of personal liberty under Article 21.

Recently, in *K.S. Puttaswamy (Retd.) v Union of India*<sup>11</sup>, the Supreme Court endorsed right to privacy as a fundamental right. The one page order signed by all nine judges declared: The right to privacy is protected as an intrinsic part of the right to life and personal liberty under article 21 and as a part of the freedoms guaranteed by part 3 of the constitution.

### **3.2 :International Scenario**

Privacy is a fundamental human right, enshrined in numerous international human rights instruments. It is central to the protection of human dignity and forms the basis of any democratic society. It also supports and reinforces other rights, such as freedom of expression, information and association.

A definite legal definition of 'privacy' is not available. Some legal experts tend to define privacy as a human right enjoyed by every human being by virtue of his or her existence. It depends on no instrument or charter. Privacy can also extend to other aspects, including bodily integrity, personal autonomy, informational self-determination, protection from state surveillance, dignity, confidentiality, compelled speech and freedom to dissent or move or think. In short, the right to privacy has to be determined on a case-by-case basis. Privacy enjoys a robust legal framework internationally. Article 12 of the Universal Declaration of Human Rights, 1948 and Article 17 of the International Covenant on Civil and Political Rights (ICCPR), 1966, legally protect persons against "arbitrary interference" with one's privacy, family, home, correspondence, honour and reputation. India signed and ratified the ICCPR on April 10, 1979, without reservation. Article 7 and 8 of the Charter of Fundamental Rights of the European Union, 2012, recognizes the respect for private and family life, home and communications. Article 8 mandates protection of personal data and its collection for a specified legitimate purpose.

## **4. KINDS OF CYBER CRIMES AGAINST WOMEN**

The expanding reach of computers and the internet has made it easier for people to keep in touch across long distances. However, the means that enable the free flow of information and ideas over long distances also give rise to a worryingly high incidence of irresponsible behavior. The vulnerability and safety of women is one of the biggest concerns of any criminal and penal law, but unfortunately women are still defenseless in cyber space. Cybercrime against women is on at alarming stage and it may pose as a major threat to the security of a person as a whole. The World Wide Web allows users to circulate content in

---

<sup>11</sup>Decided on Aug. 24, 2017

the form of text, images, videos and sounds. The widespread circulation of such content is particularly harmful for women. In recent years, there have been numerous reports of women receiving unsolicited emails which often contain obscene and obnoxious language. India is considered as one of the very few countries to enact Information Technology Act, 2000 to combat cyber-crimes. This Act widely covers the commercial and economic crimes. Despite this the issues regarding women still remain untouched under this Act. Social networking, Internet and electronic network has exposed women to various cyber crimes, of which some have sensitive effects on the image, security and privacy of women. Some of them are as follows:

#### **4.1: Cyber defamation:**

Cyber defamation occurs when with the help of computers and internet someone published derogatory or defamatory information to all of that person's friends or the perpetrator post defaming stories about the victim. Although this can happen to both genders, but women are more vulnerable. Unfortunately cyber defamation is not defined by the IT Act 2000 and it is treated by the criminal justice system under the same provisions of cyber pornography or publication of obscene materials in the internet.

#### **4.2: Cyber Harassment via E-mail:**

Harassment via email is a form of harassment, which includes blackmailing, threatening, and constant sending of love letters in anonymous names or regular sending of embarrassing mails to one's mail box. Eight out of ten people in India have experienced some form of online harassment, with 41% of women having faced sexual harassment on the web, according to a new survey commissioned by Cyber-security Solutions Firm, Norton by Symantec<sup>12</sup>. With the advancement of technology that obscene is no longer a local phenomenon. It is now global and dynamic in nature and thus needs strict interpretation of statutes.<sup>13</sup>

#### **4.3: Hacking**

Hacking means unauthorized access to computer system or network, and it is the most predominant form of cyber crime. It is an invasion into the privacy of data, it mostly happens in a social online community to demean a woman by changing her whole profile into an obscene, derogatory one. The reasons vary from personal hatred, revengeful mind to even just for fun. Even though some social networking communities like Facebook have the option of reporting profiles as bogus, photo Video lock, special tools for reporting, still, many women are kept in dark, when their email-ids or even websites are hacked.

Morphing, hacking, and email spoofing are interrelated and attract Sections 43 (penalty for damage to computer, computer system etc.) and 66 (hacking of the computer system; first proviso to the said section states that whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value, its utility or

---

<sup>12</sup> Yuthika Bhargava, "8 out of 10 Indians have faced online harassment", The Hindu, Oct.5, 2017

<sup>13</sup> Shobnajeet, Cyber crimes against women in India: Information technology Act, 2000, 47 Elr Cri L 8892, 8891-8895 (2012)



affects injuriously by any means, commits hacking) of the IT Act 2000. The perpetrator can also be booked under the IPC for criminal trespass under Section 441, Section 290 for committing public nuisance, Section 292A for printing or publishing grossly indecent or scurrilous matter or matter intended to blackmail and under Section 501 for defamation.<sup>14</sup>

#### **4.4: Cyber stalking**

Cyber stalking is one of the most talked about net crimes in the modern world. The Oxford dictionary defines stalking as "pursuing stealthily". Cyber stalking involves following a person's movements across the Internet by posting messages (sometimes threatening) on the bulletin boards frequented by the victim, entering the chat-rooms frequented by the victim, constantly bombarding the victim with emails etc. Cyber Stalking usually occurs with women, who are stalked by men, or children who are stalked by adult predators or paedophiles. Typically, the cyber stalker's victim is new on the web, and inexperienced with the rules of netiquette & Internet safety. Their main targets are the mostly females, children, emotionally weak or unstable, etc. It is believed that Over 75% of the victims are female. The motives behind cyber stalking have been divided in to four reasons, namely, for sexual harassment, for obsession for love, for revenge and hate and for ego and power trips. Cyber stalkers target and harass their victims via websites, chat rooms, discussion forums, open publishing websites (e.g. blogs and Indy media) and email. The availability of free email and website space, as well as the anonymity provided by these chat rooms and forums, has contributed to the increase of cyber stalking as a form of harassment.

In 2013, Indian Parliament had made amendments to the Indian Penal Code, wherein it introduced cyber stalking as a criminal offence. As per Section 354(d) of the Criminal Law (Amendment) Act, 2013, Stalking has been defined as any man who contacts a woman, despite clear indication of disinterest to such contact by the women, or monitoring of use of interest or electronic communication of a woman. Section 354(d)(2) states the punishment for the offence as a man committing the offence of stalking would be liable for imprisonment up to three years for the first offence, and shall also be liable to fine and for subsequent conviction would be liable for imprisonment up to five years and with fine.

#### **4.5: Cyber Obscenity:**

Conventional law of obscenity is contained under sections 292 and 293 of Indian Penal Code. Section 292 deals with the sale of obscene books, drawing or any other object and section 293 provides punishment to person dealing in cyber pornography that is accessible to person under twenty years of age. S.292 of the Indian Penal Code defines obscenity as that which is 'lascivious or appeals to the prurient interest or tends to deprave or corrupt persons'. A major breakthrough was witnessed when the Indian Supreme Court held (Aveek Sarkar & Anr. Vs. State Of West Bengal, 2014) that a nude picture of a woman is not obscene if the picture has no tendency to deprave or corrupt the minds of people in who view it.

S.354A of the Indian Penal Code forcibly showing pornography to a woman is included under sexual harassment. S.354C of the Indian Penal Code deals with voyeurism. The offences included are capturing image of a woman in a private or sexual act with a hidden device, without her consent. If consent is taken to the capture of the images but not to its distribution, then also it is an offence.

S.67 of IT Act provides punishment for publishing or transmitting obscene material in electronic form. S.67-A of IT Act deals with mainstream pornography and provides

---

<sup>14</sup> Dr. Shalini Kashmira, Mapping Cyber Crimes Against Women in India, 1 IRJCL 29,22-38 (2014)

punishment for publishing or transmitting material containing sexually explicit act in electronic form. With sections 66-E (violation of privacy), 67, 67-A and 67-B obscenity has been brought under legal dominion. Further by implications of the law, mainstream pornography has been differentiated from child pornography.

### **5. INDIAN LEGAL SCENARIO ON DEFAMATION**

The fundamental object and purpose of criminal law is not only to protect and to conserve the safety and security of primary personal rights of individuals, such as right to life, right to body, right to property, right to habitation., etc., but also to protect and guard public morals and public decency and to conserve the moral welfare of the State. Thus, it is the duty of the State to guard the citizens against attacks which may be insidious and punish an individual for obscene publications which tend to corrupt morals.<sup>15</sup> The importance of the protection of such rights can be visualized from the resolution passed by the International Convention for the Suppression and Circulation of, and Traffic in, obscene publications at Geneva as long as 1923.<sup>16</sup>

The offence is well explained in the IPC under Section 499<sup>17</sup>. The section mentions that defamation may be made by words which may be either spoken or written. It may be made even by signs or visual representation. If the imputation made in any of such ways is published and it results in the harm to the reputation of concerned person, it will be defamation. Ten exceptions have also been attached to the section. If the imputation is covered by any of them, the person will be exempted from the liability. It is significant to mention here that the law has been extended to electronic documents by the amendment in IT Act, 2000. Section 500<sup>18</sup> where punishment with simple imprisonment which may extend to two years or with fine or with both has been mentioned.

Cyber Defamation is a new concept but the traditional definition of the term defamation is applicable to the cyber defamation as it involves defamation of a person through a new and a virtual medium. If any such act takes place by using internet or on cyber space, it will be called online defamation or cyber defamation. E.g. if any defamatory statement is made on social media as on Twitter or Facebook etc.

Section 469 deals with forgery but it have been stated that if by creating a false document, harm to the reputation of a person is caused, the person will be held liable.

Section 503 deals with the offence of criminal intimidation by use of electronic means to damage one's reputation in society.

Indian Penal Code, Criminal Procedure Code and selected sections of Information Technology Act, 2000 deal with the protection from cyber crime .Section 66A of the IT Act was quashed by the Supreme Court in *Shreya Singhal v. Union of India*<sup>19</sup> . the section was held unconstitutional as it violated the right to freedom of expression guaranteed under

---

<sup>15</sup> Soma Sarkar, Legal article on Obscenity, Law Times Journal, (July 17,2020,7:30PM)

<https://lawtimesjournal.in/obscenity-under-ipc/>

<sup>16</sup> H.S. Gour, Penal Law of India, 11th Edn, (2000), Vol. III, pp. 2263 to 2299 India signed the Convention on 12th September 1923

<sup>17</sup> Section 499: Defamation- "whoever by words either spoken or intended to be read or by signs and visual representation 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, except in the cases hereinafter excepted to defame that person.

<sup>18</sup> Section 500: Punishment for defamation.—whoever, defames another shall be punished with simple imprisonment for a term which may extend to two years, or with fine, or with both.

<sup>19</sup> (2013) 12 SCC 73

Article 19(1) (a) of the Indian Constitution. After the amendment in 2008, new Sections have been inserted as Section 67 A to 67 C. Section 67 A and 67 B insert penal provisions in respect of offences of publishing or transmitting of material containing sexually explicit act and child pornography in electronic form. Section 67C<sup>20</sup> deals with the obligation of an intermediary to preserve and retain such information as may be specified for such duration and in such manner and format as the central government may prescribe. These provisions do not mention anything about e-mail harassment of different type but in general they are used to book the perpetrators along with Section 292 of the IPC for printing or publishing grossly indecent or scurrilous matter or matter intended to blackmail, and under Section 509 of the IPC for uttering any word or making any gesture intended to insult the modesty of a woman. In such cases the victim goes to the police station to report the crime of harassment and thereby it is regulated as per the general laws and not by the provisions of cyber laws. The issues related to publication or transmission of obscene information in electronic form under Section 67 of IT Act 2000 may be looked from the perspective of 'extraterritorial' jurisdiction.

## **6. CRITICAL ANALYSIS OF LEGAL PROVISIONS ON DEFAMATION**

### **6.1: No existing definition of Cyber Defamation is there**

Information Technology Act, 2000 is the legislation which exclusively deals with the cyber crimes in India. With the enactment of this legislation, relevant amendments were made to the Indian penal code, Indian Evidence Act as well as in the Code of Criminal Procedure. But the major lacuna in this Act is that it nowhere specifically define cyber defamation. At least the offence as such must have been defined under the Act of 2000. Otherwise the task of combating cyber crimes would get defeated.

### **6.2: No strict implementation of laws**

In India even though we have IT Act in the shape of cyber law but it lacks implementation. First of all, all matters are not reported and which are reported are not properly investigated which leads to improper adjudication too. Most of the time victims out of shame and embarrassment never report these crimes so that their identity might be revealed by doing this and hence the social stigma in the society would worsen their life further. As a result most of these crimes go unreported which is a sad state of affair. It leads to encouragement to the bad elements sitting on internet and increase in these crimes too.

### **6.3: Jurisdictional problem**

Cyberspace has a worldwide approach. Thus, while dealing with cyber defamation the biggest problem which comes on the way is jurisdictional problem. It is very difficult to ascertain where a complaint should be launched. It may be possible that victim belongs to one country and the accused belongs to another. The laws relating to cyber defamation may vary in both these countries. It could be difficult to ascertain which law is to be applied to that crime. It is a matter of extra-territorial jurisdiction so it is very difficult to book the criminal who is already sitting outside the jurisdiction of those courts within which the victim is residing at the time of commission of crime. In short, these jurisdictional issues let go many criminals unpunished.

---

<sup>20</sup> Section 67C: Preservation and retention of information by intermediaries. -

(1) Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe.

(2) Any intermediary who intentionally or knowingly contravenes the provisions of sub-section (1) shall be punished with an imprisonment for a term which may extend to three years and also be liable to fine



#### **6.4: Loss of evidence**

Cyber world is full of technicalities. Only a person with special knowledge and experience can deal with it. In India, we don't have trained police personnel to investigate into. Even though cyber cells have been established but those are only a number of across India which is not sufficient. Without trained officers, no effective investigation can be conducted as evidence may not be properly collected.

#### **6.5: Liability of Internet service providers is not fixed**

Section 79 of IT Act, 2000 puts liability upon internet service provider in case they conspire, abet, aid or induce in publication of defamatory material. However, they won't be liable if he is merely providing access to the communication forum. Due to this proviso, they escape from their liability and show their inability to keep check due to wide usage of internet.

### **7. CONCLUSION AND SUGGESTIONS**

From the above discussion it can be concluded that internet somehow is posing a great threat to the security and safety of women in India. The younger women i.e. age group falling in 15 to 30 are the most vulnerable group which becomes an easy target of evil minded people. It is suggested that internet must be used with proper care and caution. Overuse or misuse of internet both can lead to crimes and chaos in the society. It is equally the duty of women to be vigilant and cautious while using internet. Posting almost everything about one's personal daily routines is not a wise approach which is very commonly done by the younger generation these days. One should not use the internet blindly without securing one's account. Proper passwords should be placed which could be changed frequently. Furthermore, here are some suggestions which can be considered:-

#### **7.1: Proper definitions to cyber crimes must be assigned**

The definition of cyber defamation depends on the traditional definition assigned to general defamation for proper understanding of the offence. Even under the Information Technology Act, 2000 there is no specific provision which is explaining the meaning of cyber defamation. Though cyber defamation is an aggravated form of slander in the matter of publication but content wise there is much more difference between the two.

#### **7.2: Awareness among women**

Defamation is the intentional infringement of the reputation of a person and in India reputation becomes important when it concerns a woman. So many matters are not reported because they are related to the reputation of women. We need to make women more aware of their rights. They should be educated about cyber crimes and how they can maintain their privacy and most importantly if their privacy is interfered with what are the options available to them. The problem would be solved only when the victimized woman then and there report back or even warn the abuser about taking strong actions.

#### **7.3: Development of cyber forensics**

This is the most important step which needs to be taken. Cyberspace needs the special technical knowledge with special training. So many technicalities comes the way while dealing with cyber crimes e.g. from which computer the information was generated or IP address of computer may be changed, hacking etc. if there are cyber forensics, these technicalities may be minimized. It may be helpful in ascertaining the issue of jurisdiction too.

#### **7.4: Need to give a universal approach to cyber laws**

As the cyber crimes are of universal phenomenon, the law regarding to it may also be so. If the states in connivance with each other make the cyber law of universal application there are so many issues of cyber crimes which may be resolved e.g. jurisdictional issue, collection of evidence, proper investigation, ascertainment of true culprit etc.

#### **7.5: Trained investigating agencies**

The loss of evidence is the biggest disadvantage which is attached to cyber defamation because for cops it becomes difficult to ascertain from which computer the remarks were posted or IP address of computer etc. with the help of trained investigating agencies procurement and preservation of evidence may become easier. The personnel must have knowledge of related laws as well as technical knowledge.

With the help of above suggested measures we can curb cyber crimes against women effectively and efficiently.