

## 9 RMLNLUJ (2017) 175

### Cyber Stalking and The Plight of Women in India — A Legal Perspective

by  
Archana Sarma<sup>\*</sup>

#### I. INTRODUCTION

In June 2016, in Salem district of Tamil Nadu, a 21-year-old woman saw a picture of her face, digitally superimposed on the body of another woman, posted on a social networking site. She informed her parents, and also identified the man responsible for it. It was alleged that she had rejected his proposal of marriage, and to get back at her, he morphed her picture using a mobile phone app, uploaded it on the site and tagged her on the post. The woman's father lodged a complaint with the Cyber Crime Cell. A few days later, she found another distorted image tagged to her social networking account with her name and her father's phone number on it. On the same day, the woman committed suicide. In her suicide note, she expressed her complete ignorance about the distorted images and her failure to convince anybody.<sup>1</sup>


With a significant increase in the usage of computer in our daily life and advancement of information technology, the vulnerability for users of computer and internet has remarkably gone up in the cyberspace today. As the technology advances, this tremendously high technical capacity of modern computers/computing devices provides avenues for misuse as well as opportunities for committing crime. Unfortunately, on many occasions, the users fail to recognize the vulnerabilities they are exposed to while browsing internet, uploading posts on social networking sites or storing information in the computer. At the same time, perpetrators use the cyberspace as



a platform for indulging in various criminal activities against the users. In fact, traditional offences such as rape, molestation and different forms of sexual abuse have gained new significance due to the development of information and communication technology. There are incidences of rape scenes in the mobile phone devices, extraction of money by threatening to publish images/videos relating to the same.<sup>2</sup> The Information Technology Act, 2000 (hereinafter known as IT Act, 2000) has recognized various offences relating to cyberspace. Among many offensive acts on cyberspace, online abuse is a common phenomenon all over the world, which has directly or indirectly affected online users of different age groups leading to different forms of harassment such as gender bullying, trolling, stalking etc.<sup>3</sup> Cyber harassment may be defined as a repeated, unsolicited, hostile behaviour by a person through cyberspace with the intent to terrify, intimidate, humiliate, threaten, harass or stalk someone else.<sup>4</sup> Apart from the physical act of harassment being considered as an offence under the Indian laws, any harassment caused through electronic media such as social networking sites, chat rooms, e-mail etc. is also considered to have similar impact as far as traditional offences of harassment are concerned. According to popular perceptions, women in India make most vulnerable targets on the internet and digital communication technology due to their gender and consumability of images of Indian women as subject matter of pornography.<sup>5</sup> On many occasions, women become the target of such abnormal activities to destroy the image of the immediate family members. However, it is unfortunate that multiple cases do

unreported either due to lack of awareness or absence of stringent laws to deal with them. It is also interesting to note that there are a very few cases of this nature which are actually registered and prosecuted. Besides, with the striking down of Section 66A of the Information Technology Act, 2000 in the decision of the Supreme Court in *Shreya Singhal v. Union of India*<sup>6</sup>, there has been a void in law to respond to such offences. Highlighting on the fundamental right to freedom of speech and expression, the judgment held that liberty of thought and expression is not merely an inspirational ideal. It is also "a cardinal value that is of paramount significance under our constitutional scheme." Under such a paradoxical situation, where the legal fraternity insists on upholding right to freedom of speech and expression on the one hand and use of cyberspace for publishing offensive messages/images about women (which also includes stalking) on the other hand, it becomes pertinent to understand the

---

 Page: 177

phenomenon of cyber stalking, its impact on women and the various challenges involved in effectively addressing this menace.

## **II. UNDERSTANDING CYBER STALKING & ITS IMPACT**

### **A. Concept of Cyber Stalking**

Stalking has emerged as a socio-legal problem of the recent time, which has resulted in its incorporation as criminal offence in the Indian laws. According to the Oxford Dictionary, stalking means "pursuing stealthily". In other words, the term stalking refers to following a person with intent to harass or cause inconvenience to him/her. The phenomenon of stalking is also defined as repeated and unwanted harassing behaviour which is threatening and purposefully directed at a specific person (the victim), and would cause a reasonable person to fear bodily injury or death for themselves or members of the family.<sup>7</sup>

Stalking may be characterized by the following:

- A repeated and unwanted harassing behaviour by a person against another.
- Such behaviour may be reflected by a physical act or may be done through electronic means usually the internet and other communication devices.
- The act may cause mental trauma and fear to the victim, sometimes leading to more serious offences.
- The act is a direct intrusion into the privacy of an individual, where the stalker attempts to establish relationship with the victim without his/her consent.

Cyber Stalking is a serious form of harassment posing threat to life of an individual if it is not addressed appropriately. It constitutes harassment of individuals on cyber space through use of information and communications technology (especially the Internet). Such harassment may include actions such as the transmission of offensive and derogatory e-mail messages, identity theft and damage to data or equipment. Cyber Stalking, therefore, constitutes a group of behaviours in which an individual, group of individuals or organisation, uses information and communication technology to harass one or more individuals. Such behaviours may include, but are not limited

---

 Page: 178

to, the transmission of threats and false accusations, identity theft, data theft, damage to data or equipment, computer monitoring, the solicitation of minors for sexual

purposes and confrontation.<sup>8</sup>

## **B. Cyber Stalking and Victimization of Women**

It has often come to be seen that women and young children become victims of such acts leading to threat, harassment, assault and trauma. Privacy in virtual world as well as real life is gradually shrinking and women are the most affected community in this regard. Cyber Stalking is a serious example of infringement of privacy of women in cyberspace.<sup>9</sup> In addition to this, because of the nature of the offence and the target aimed, such abnormal activities leave a serious impression on every aspect of their life. Cyber victimisation of women can be categorised into two main groups: textual victimisation and graphical victimisation. Graphical victimisation may include producing, creating or publishing obscene, derogatory, and pornographic, including revenge pornographic materials on the web to put the victim in shame.<sup>10</sup>

There is no doubt about the fact that traditionally women are considered to be marginalized and disadvantaged section of the society. Even though the Constitution of India guarantees equal rights to men and women, women have been made second grade citizens due to dominantly patriarchal set up of the society. On many occasions, stalking becomes a vindictive instrument for man as an immediate reaction to refusal by the woman to get into any relationship with him. Today, the scenario is far more alarming where internet trolls take to social media website and instant messaging services like WhatsApp to target women activists, journalists, celebrities, academicians and so on to create hatred among the larger community against such women just to gain a sadist pleasure out of it.<sup>11</sup>

According to a comparative data of Working to Halt Online Abuse (WHOA) for the period 2000-2013, it was revealed that women victims generally outnumber male victims when it comes to cyber stalking victimisation and that out of 4043 victims who contacted WHOA in the said



period, 70% were women.<sup>12</sup> Women are targeted by trolls, bullies, stalkers with insulting, defamatory, derogatory statements/pictorial depiction on the internet. Even when women are not connected to the worldwide web, they may be harassed and stalked by unnecessary phone calls and SMSs. This may sometimes result in barring women completely from using any such medium of communication. This shows a blatant violation of rights of women through improper exercise of right to speech and expression on the internet. They are violation of basic human rights including right to equality as guaranteed under Article 14 of the Constitution of India as the right to live with dignity as enumerated in Article 21 of the Constitution. Unfortunately, while deciding in the landmark case of *Shreya Singhal v. Union of India*,<sup>13</sup> constitutionality of Section 66A of the IT Act, 2000, the Supreme Court emphasized on right to freedom of speech and expression, but overlooked the victimization of women in cyber space by misuse of this right. Such victimization would be dangerous for women because of the nature of electronic media which is different from print media.

## **III. CYBER STALKING: LEGAL REMEDIES**

Cyber stalking is a common phenomenon in cyberspace, which go unaddressed many a time due to lack of specific laws and enforcement mechanism. This is a glaring example of serious consequences of stalking in cyberspace. There could be end number of cases of similar nature which go unreported. Social norms and orthodox values play a major role here. Women victims and their family members feel reluctant to report such crime, especially due to fear of damage to their social reputation. Apart



from this, there are various factual reasons for less number of prosecutions of cases of cyberstalking. This may include lack of focused laws, challenges in establishing identity of the perpetrator, lack of proper infrastructure in the criminal justice machinery in India and above all, the absence of servers within the jurisdiction of India, and conflict of laws between Indian laws and laws of countries which host the internet companies/service providers.<sup>14</sup>

The first initiative to formulate a legal framework for the cyber space was perceived in India in the form of E-Commerce Act, 1998. Afterwards, the basic law for the cyberspace transactions in India emerged in the form of the Information Technology Act, 2000 which was significantly amended in the year 2008. The IT Act also amended some of the provisions of the Indian Penal Code, 1860, the Indian Evidence Act, 1872, the Bankers Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934. Though since 2000 the IT Act is in place in India for curbing offences like cyber stalking,



Page: 180

the problem still remains unaddressed as the law is more on papers than on execution because lawyers, police officers, prosecutors and Judges are in a helpless state in apprehending its highly technical terminology.

The offence of cyber stalking was not incorporated in the IT Act when it came into force in 2000 unless the act involved publication or transmission of obscene material within the meaning of Section 67 of the IT Act.<sup>15</sup> Besides, Section 509 of the Indian Penal Code (IPC) partially deals with the offence<sup>16</sup> according to which uttering of any word, making of any sound or gesture or object to be heard or seen by a woman, or intrusion upon the privacy of such woman shall be punishable with imprisonment up to three years and fine. Since Section 509 of IPC defines this act as one of privacy, Section 72 of IT Act was used to deal with cases of cyber stalking to an extent. With the amendment of IT Act in 2008, Section 66A was inserted in the IT Act under which all the cases of cyber stalking were dealt with.

Section 66A. Punishment for sending offensive messages through communication service, etc.

*Any person who sends, by means of a computer resource or a communication device,—*

- a) Any information that is grossly offensive or has menacing character; or*
- b) Any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently makes by making use of such computer resource or a communication device;*
- c) Any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages,*

*shall be punishable with imprisonment for a term which may extend to three years and with fine.*



Page: 181

Besides, e-mail communications amounting to extortion may be dealt with under sections 43, 66, 66C of the IT Act 2000. However, in a significant development and amidst controversies, Section 66A was struck down by a recent judgment, *Shreya Singhal v. Union of India*<sup>17</sup> (decided on March 24, 2015) of the Supreme Court of India declaring it to be in violation of the fundamental right to freedom of speech and expression enshrined in Article 19(1)(a) of the Constitution of India.

In the case, the Supreme Court held:

‘...the wider range of circulation over the internet cannot restrict the content of the right Under Article 19(1)(a) nor can it justify its denial. However, when we come to discrimination Under Article 14, we are unable to agree with counsel for the Petitioners that there is no intelligible differentia between the medium of print, broadcast and real live speech as opposed to speech on the internet. The intelligible differentia is clear — the internet gives any individual a platform which requires very little or no payment through which to air his views. The learned Additional Solicitor General has correctly said that something posted on a site or website travels like lightning and can reach millions of persons all over the world. If the Petitioners were right, this Article 14 argument would apply equally to all other offences created by the Information Technology Act which are not the subject matter of challenge in these petitions. We make it clear that there is an intelligible differentia between speech on the internet and other mediums of communication for which separate offences can certainly be created by legislation. We find, therefore, that the challenge on the ground of Article 14 must fail.’

Even though Section 66A of IT Act has been struck down from the statute book, stalking has finally come to be recognised as an offence under the IPC. Consequently, the offence of cyber stalking is now a part of Section 354D (Stalking) of IPC, if not a complete protection to the offence. This provision was inserted by the Criminal Law (Amendment) Act, 2013. According to this provision, “Any man who—

(i) follows a woman and contacts, or attempts to contact such woman to foster personal interaction repeatedly despite a clear indication of disinterest by such woman; or



(ii) monitors the use by a woman of the internet, email or any other form of electronic communication, commits the offence of stalking:”

Besides, it is worth mentioning that the purpose of Section 354D is to prosecute a man for stalking a woman under circumstances described in the provision. Under such circumstances, for other cases of cyber stalking, Section 506 (Criminal Intimidation) of IPC may also be invoked when such communications involve threat to life, injury etc. Therefore, in the absence of Section 66A, the IT Act needs to be amended to take into account cyber stalking as a substantive offence, which is one of the most under-reported offences in the present scenario.

In India, the concept of regulating cyber stalking continued to generate various opinions; for example, some are of the opinion that cyber stalking can be punishable only when the result is shown through publication or transmission of obscene material within the meaning of S.67 of the Information Technology Act, 2000 (amended in 2008) (which penalises creation, publication, transmission of obscene materials); it can also attract legal provisions meant for defamation (Section 499, IPC) criminal intimidation (Section 503, IPC), eve teasing by way of word or gesture, or act

intended to insult the modesty of a woman (Section, 509). Some opined that erstwhile S.66A of the Information Technology Act, 2000 (amended in 2008) (which prescribed punishment for sending annoying, misleading, etc.), can be used as an effective regulatory provision for cyber stalking. Section 354D of the Indian Penal Code sets these confusions at rest by criminalising cyber stalking as a behavioural pattern. The main aim of this law is to prevent the perpetrator from taking up behaviours which construct cyber stalking. While this is appreciated, it must be remembered that this law was created in the shadow of physical stalking laws and therefore suffers from numerous drawbacks which are further analysed.<sup>18</sup>

The Internet Service Providers may also play a crucial role in regulating publication of controversial materials in cyber space so that such menace can be avoided before it offends the privacy of a woman.

#### **IV. CASES ON CYBER STALKING IN INDIA**

According to the data provided by the National Crimes Record Bureau (NCRB) of India, under the category of “assault on women with intent to outrage her modesty”, 2015 saw 84,222 cases being registered across the country as against 82,235 in 2014. The category includes offences such as



Page: 183

sexual harassment, assault or use of criminal force to women with intent to disrobe, voyeurism, and stalking.<sup>19</sup>

#### **A. Case of Manish Kathuria<sup>20</sup>**

The first reported case of cyber stalking in India was registered in 2003 by Delhi Police and the reason for 2008 amendment to the IT Act, the Manish Kataria case involved the stalking of woman named Ritu Kohli. Ms. Kohli, in her complaint, alleged that a person was using her identity to chat on internet at a particular website in obscene language. The man was alleged to have given her telephone numbers to people in the chat room which ended up the victim receiving phone calls from different places. This adversely affected her personal life with serious inconvenience, trauma and harassment. Finally, during investigation by police, the IP addresses used by the perpetrator helped police reaching out to one Manish Kathuria, who pleaded his guilt and was arrested. A case was registered under Section 509, of the Indian Penal Code (IPC) for “outraging the modesty” of his victim. The IT Act was not invoked in the case, since it had not come into force at the time when the complaint was filed. This case made Indian legislators wake up to the need for a specific legislation to address cyber stalking. However, it was only in 2008 that Section 66A was introduced. Consequently, cases used to be reported under this provision until the same was struck down by the Supreme Court of India as unconstitutional.

It is worth mentioning that an analysis of Section 509 does not explicitly refer to cyber stalking. Under such circumstances, proving cases of cyber stalking still remains a challenge under the existing laws.

#### **B. Karan Girotra v. State<sup>21</sup>**

Shivani Saxena lodged a complaint with the Police that she had married one Ishan on, however, the marriage between them failed within a few days as her husband, Ishan could not consummate the marriage. Both of them started living separately and it was amicably settled between them that after the expiry of one year of their marriage, both of them would file a joint petition, on mutual consent, for the grant of divorce, after which both the parties will be free to marry afresh. In the meantime Shivani came in contact with Karan Girotra in the course of chatting on internet, who



proposed her to marry. The same was declined by Shivani as she was still married

---

 Page: 184


at that point of time. Karan insisted to marry her after her divorce. On the pretext of getting her to his family members, Karan once took her to a house, made her unconscious by offering her drinks and sexually abused her. Obscene photographs of her were also clicked by Karan, who started seeking sexual favour from her under the threat of publishing the nude photographs. As a part of the Roka ceremony, a lot of valuables including a Santro Car were given to Karan from the family of the complainant. Finally, he informed the complainant's mother about breaking off the engagement. Shivani filed a complaint and a case was registered under Sections 328/376 IPC read with Section 66-A of the IT Act.

Though the Court rejected the plea of anticipatory bail of Karan on the ground that nude and obscene pictures of the complainant were circulated by the accused, it had concluded that Shivani had failed to disclose her previous marriage to Karan merely because she agreed to perform the engagement ceremony, even though this was mentioned earlier. The Court also took into account that there was a delay in lodging the FIR by the complainant. The most crucial part is that the complainant had consented to the sexual intercourse and had decided to file the complaint only when Karan refused to marry her. This case highlights the conservative attitude of the Judiciary towards cases of cyber stalking.

### **C. Case of Yogesh Prabhu (First case of Cyber Stalking in Mumbai)**

Even though the conviction rate of cyber stalking had been low since the coming into effect of the amendments to IT Act in 2008, the Mumbai cyber cell secured the first ever conviction in Maharashtra under the IT Act in July 2015. The case was investigated by the cell for online stalking in 2009. A metropolitan magistrate court convicted Yogesh Prabhu for stalking and sending obscene images to his colleague. The court sentenced him to three-years imprisonment and a fine of Rs. 10,000 and Rs. 5,000 under section 66-E (punishment for violation of privacy) of the Information Technology Act, 2008 and section 509 (word, gesture or act intended to insult the modesty of a woman) of the IPC respectively. The conviction was procured on evidence including crucial witness statement stating that the crime was committed using a laptop sponsored by office.<sup>22</sup>

---

 Page: 185

## **V. RULES OF EVIDENCE IN COMBATING CRIMES ON CYBER SPACE**

Addressing cyber stalking does not only have substantive issues specific to women, it also has various other technical obstacles. In a crime involving the use of technology, the evidence furnished is also in electronic or digital form. The collection and preservation of evidence during investigation has really been a challenging factor as far as electronic evidence is concerned. The most challenging aspect is that electronic or digital evidence, by its very nature is invisible to the eye. Therefore, the evidence must be interpreted using tools and techniques other than the human eye.<sup>23</sup> At times, it becomes difficult to test the veracity of such evidence in the absence of an expert.<sup>24</sup> Increasing reliance on evidence extracted from computer systems to bring

about convictions has led to emergence of a new means of scientific investigation i.e. computer forensics.

In a criminal investigation, evidence obtained must survive an admissibility test in convicting the accused. In a civil case, evidence must be properly authenticated and subject to privacy rights. Failure to do so may result in liability for wrongful discharge or invasion of privacy. It is, therefore, important for the computer forensic investigators to understand and respect the legal environment in which they work. It is a widely accepted fact that since technology changes at a much faster rate than the law and is arguably constrained only by the imaginations of its creators, it is crucial to strike a balance between exploiting technology to enhance capabilities and staying within the bounds of legal, acceptable uses. Forensic practitioners must remember that ability to leverage technology is bound by the legal standards and policies governing evidence reliability.<sup>25</sup>

Collecting, handling and presenting evidence has been codified by law, courts and best practices out of law enforcement agencies in many countries. Under the US Federal Rules of Evidence, in order for the 'electronic evidence' to be admissible, it must comply with the 'best evidence rule' and 'chain of custody' must be so that rules out any tampering. In fact, unauthorized modification of computer material is recognized as an offence



under the Computer Misuse Act, 1990 in the UK.<sup>26</sup> Apart from the most important federal statutes affecting computer forensics, the Judiciary had also come up with various models suggesting admissibility of electronic evidence. In India, with the introduction of the IT Act, 2000 and subsequent amendments in the Indian Evidence Act, 1872 and the Indian Penal Code, 1860, the body of law applicable to admissibility of electronic evidence was constituted. However, cyber forensics is an upcoming field and Indian legal and judicial system has to adapt itself according to the same. Till now cyber forensics is not widely and appropriately used by the law enforcement agencies, lawyers, judges, etc. in India. As a result, most of the cyber criminals are either not prosecuted at all or they are acquitted in the absence of adequate evidence.<sup>27</sup>

Admissibility of evidence in a criminal investigation has always been a crucial and frequently debated issue as far as the rules of evidence in any legal system are concerned. However, with the rapid changes involving the computer and its associated devices and features, the nature of crime has undergone radical change, and so is the nature of evidence to be produced before courts. Every legal system has started recognizing crimes involving technology and has adapted itself according to the changing scenario. 'Electronic evidence' is a term incorporated into the Indian Evidence Act, 1872 after the coming into force of the IT Act, 2000, and since then admissibility of electronic evidence has been an issue before courts. Legal community believes that 'electronic evidence' is a new breed of evidence. They also, at times, have an apprehension that the law of evidence as per Indian Evidence Act, 1872 may not hold good for electronic evidence. Some lawyers express doubts and apprehensions about the process of leading electronic evidence in courts. However, this is not true; the traditional principles of leading evidence, along with certain newly added provisions in the Indian Evidence Act through the IT Act, 2000, constitute the body of law applicable to electronic evidence. The challenges, however, need to be understood from the 'rules of evidence' perspective.<sup>28</sup>

The investigation of computer crimes and the gathering of appropriate evidence for a criminal prosecution can be an extremely difficult and complex issue. due primarily



to the intangible and often transient nature of data, especially in a networked environment. The technology renders the process of investigation and recording of evidence extremely vulnerable to defence claims of errors, technical malfunction, prejudicial interference or fabrication. Such claims may lead to a ruling from the court against the

---

 Page: 187

admissibility of such evidence. This has been in conformity with Section 87 of the Police and Criminal Evidence Act, 1984.<sup>29</sup> On the other hand, this may also be mentioned that technology has been used for taking evidence remotely by courts.<sup>30</sup>

## **VI. ELECTRONIC EVIDENCE: CHALLENGES BEFORE THE JUDICIARY**

In a significant ruling in November 2015 in *Shamsher Singh Verma v. State of Haryana*<sup>31</sup>, the Supreme Court allowed compact discs (CDs) to be treated as a document under the law and said that litigants should be allowed to prove or disprove such electronic evidence in judicial proceedings. The apex court, without deciding on the authenticity of a CD in a case, permitted the accused to bring on record the taped telephonic conversations to prove his innocence in a child sexual abuse case. The Supreme Court held that a compact disc (CD) is to be treated as a document under the law and litigants should be allowed to prove the authenticity of such electronic evidence in legal proceedings. The court was passing a judgment in a case of child sexual abuse in which the accused wanted to place on record a CD of taped telephone conversations to prove his "innocence". The Court set aside a Punjab and Haryana High Court order agreeing with the trial court's decision to deny the accused's plea to produce recorded telephonic conversation between his wife and son and the girl's father to prove his point that there was a property dispute between the two families. The apex court did not go into the authenticity of the taped conversations or the CD, but asked the trial court to allow the accused to place it on record.<sup>32</sup>

This is, undoubtedly, a positive approach towards reliance on electronic evidence by the Judiciary.

It is important to see how the judiciary approaches the question of tampering and alteration. In the controversial Aarushi Talwar's murder case (2008), the defense counsel challenged the prosecution version of CBI that Rajesh Talwar (father and prime accused) was awake on the night of the crime and had used Internet connection at regular intervals. The defense counsel alleged that CBI did not provide technical details to the expert who was inconclusive about the use of router, which could not be substantiated before the court. However, the judiciary has started recognizing and

---

 Page: 188

appreciating electronic evidence through various judicial pronouncements,<sup>33</sup> e.g. in *State of Punjab v. Amritsar Beverages Ltd.*<sup>34</sup> (interpreting hard disk within the definition of 'document'), *Jagjit Singh v. State of Haryana*<sup>35</sup> (admissibility of CD containing interviews conducted by a TV channel), *State (NCT of Delhi) v. Navjot Sandhu*<sup>36</sup> (admissibility of intercepted telephone calls), *State of Maharashtra v. Dr Praful B. Desai*<sup>37</sup> (examination of a witness by video conference) etc. including the recent deposition relating to 26/11 Mumbai Terror attack given by David Headley through video conference before a Mumbai Court.<sup>38</sup>

On the other hand, earlier in another recent development, in *Anvar P.V. v. P.K. Basheer*<sup>39</sup>, the Supreme Court settled the controversies arising from the various conflicting judgments as well as the practices being followed in the various High Courts and the Trial Courts as to the admissibility of the Electronic Evidence. The Court interpreted the Sections 22A, 45A, 59, 65A & 65B of the Evidence Act and held that secondary data in CD/DVD/Pen Drive are not admissible without a certificate under Section 65 B(4) of the Indian Evidence Act. It has been elucidated that electronic evidence without certificate U/s 65B cannot be proved by oral evidence and also the opinion of the expert under Section 45A of the Indian Evidence Act cannot be resorted to make such electronic evidence admissible.

Referring to *Navjot Sandhu* case, the Court held:

"The evidence relating to electronic record, as noted herein before, being a special provision, the general law on secondary evidence Under Section 63 read with Section 65 of the Evidence Act shall yield to the same. *Generalia specialibus non derogant*, special law will always prevail over the general law. It appears, the court omitted to take note of Sections 59 and 65A dealing with the admissibility of electronic record. Sections 63 and 65 have no application in the case of secondary evidence by way of electronic record; the same is wholly governed by Sections 65A and 65B. To that extent, the statement of law on admissibility



of secondary evidence pertaining to electronic record, as stated by this Court in *Navjot Sandhu case* (supra), does not lay down the correct legal position. It requires to be overruled and we do so." (Para 22)

The judgment is going to have serious implications in all the cases where the prosecution relies on the electronic data and particularly in the cases of anti-corruption where the reliance is being placed on the audio-video recordings which are being forwarded in the form of CD/DVD to the Court. In all such cases, where the CD/DVD are being forwarded without a certificate under Section 65B of the Indian Evidence Act, such CD/DVD are not admissible in evidence and further expert opinion as to their genuineness cannot be looked into by the Court as evident from the Supreme Court Judgment. It was further observed that all these safeguards are taken to ensure the source and authenticity, which are the two hallmarks pertaining to electronic records sought to be used as evidence. Electronic records being more susceptible to tampering, alteration, transposition, excision, etc. without such safeguards, the whole trial based on proof of electronic records can lead to travesty of justice. Besides, the way the Court has interpreted Sections 63 and 65 in the light of the special provision Section 65B of the Indian Evidence Act; it would be all the more challenging for law enforcement agencies to establish electronic evidence before the court of law. As the courts gain more experiences regarding the definition of computer records and their submission as 'evidence', there are more responsibilities on computer forensic investigators in extracting and consolidating the data which shall be crucial for lawyers and other individuals involved. At the same time, it would be a challenging task for Judiciary to draw conclusion on issues which are highly technical in nature.

## **VII. ADDRESSING CYBER STALKING IN INDIA: CHALLENGES**

There is no doubt about the fact that addressing cyber-crimes involves sound knowledge of information and technology right from the collection of evidence till the same is appreciated by the judiciary.<sup>40</sup> However, it is unfortunate that the country is yet to have cyber-crime investigation best practices. Following are some of the

challenges involving cyber stalking:

- 1. Global Crime & lack of jurisdiction:** The nature of the offence of cyber stalking is global in nature due to which the jurisdiction to investigate becomes a major issue. Whenever a cyber-crime is committed, the server of



Page: 190

the electronic device used for the crime might be located beyond the territorial jurisdiction of India.

- 2. Anonymity of Wrong-doer:** One of the principal features of the internet is its ability to keep the user anonymous, which is considered to be advantageous for the perpetrators as they may keep their identity apparently undisclosed.
- 3. Poor state of Investigation capabilities:** Cyber-crimes investigation capabilities in India are also in a poor state. There is no adequate infrastructure for dealing with crimes involving technology. This results in failure in collecting appropriate evidence to strengthen the prosecution case.
- 4. Tampering of evidence:** Since the cyber space is highly inter-connected, it is easy to tamper with electronic evidence. The law enforcement agencies are not well equipped to avoid such tampering at the stage of collection and preservation of evidence.<sup>41</sup>
- 5. Enhanced Vulnerabilities on Electronic Media:** Since internet is without boundaries, it has a greater audience and the harassment, abuses etc., can be viewed by people sitting in different geographical locations. Besides, internet has the potentiality to morph images, manipulate voice etc. by way of advanced technology which may create serious social disorder. Internet provides wider opportunity to invade privacy of individuals and violate basic right to life, liberty and dignity under Article 21.
- 6. Hindrances from the Society:** Apart from the technical challenges, women encounter other forms of discrimination due to the dominant patriarchal nature of the society. The term 'modesty of woman' is a relative term and it varies from society to society. There have been several cases where victims have been held accountable by the society for sharing photographs on the social networking sites, which are 'objectionable' as set by the society itself. This aggravates the problem.

#### **VIII. CONCLUSION: TOWARDS A BETTER REDRESSAL SYSTEM**

Cyber Stalking is a serious form of harassment on the internet. Besides, deciding on the jurisdiction for dealing with such offence is a challenge before the courts. Hence, there is a need for revisiting the IT Act for prosecution of cases of cyber stalking as well as law enforcement mechanism needs to be better equipped to address such problems in an effective



Page: 191

manner. At the same time, the challenges involving law and technology in dealing with such offences must be addressed effectively to reduce the vulnerability of the users of cyberspace. The article puts forward the following suggestions and observations for a better redressal system for Cyber Stalking:

- 1. Global Crime: Need for International Cooperation** The nature of most of the




cyber-crimes is global in nature due to which the jurisdiction to investigate becomes a major issue. Whenever a stalking takes place in cyber space, the server of the electronic device used for such acts might be located beyond the territorial jurisdiction of India. Hence, it may be feasible to conduct investigation of such cases if it is made mandatory for the service providers such as Facebook, twitter or WhatsApp to install a local server in India. Such arrangement may, to some extent, be able to address the problem of jurisdiction in such cases.

- 2. Stringent laws at National Level** In the absence of a specific provision to address cases of Cyber Stalking, it is highly essential to make necessary amendments in the existing laws or to bring Section 66A of the IT Act back with necessary regulations.
- 3. Need for Inter-State cooperation** Due to serious lack of cooperation and coordination from another state involved in a crime, the investigating agency fails to complete investigation. In this regard, a Cyber-Crime Inter-State Cooperation Cell may be set up and attached with every cyber cell so that it provides exclusive information relating to such crimes.
- 4. Initiative at the Individual Level:** As a measure for protection from such exploitation in cyber space, it is necessary to take precautionary steps such as adequate security measures to ensure not to disclose personal information on the internet in inappropriate fora. Passwords should not be made too easy to be cracked by perpetrators. The privacy settings in social media facilitate blocking of accounts causing annoyance. The same must be taken recourse to avoid unnecessary harassment.<sup>42</sup>
- 5. Revisiting the Right to Freedom of Speech and Expression:** It is ironic that even though cyber victimization includes abuse of fundamental rights and also gender harassments, hardly any solid step has been taken to curb this. There is a need for striking a balance between freedom of speech and expression on the one hand, and right to privacy on the other.

Cyberstalking has become a recent threat for the cyber community in India, especially women irrespective of age or any other social strata

---

 Page: 192

they belong to. It has even gone to the extent of ruining the lives of many young women. Therefore, it is the need of the hour to formulate a technically sound legal framework as well as an impartial mechanism for better redressal of cases of Cyber Stalking in India.

---

\* LL.M, M.Phil (NLSIU, Bangalore), Assistant Professor (Law), The NorthCap University, Gurugram. She is presently pursuing her PhD from National Law University Delhi. <archana.sarma@gmail.com>.

<sup>1</sup> See *Salem woman, 21, kills herself after obscene pictures morphed to look like her were posted on Facebook*, Daily Mail, Jun. 29, 2016, available at <http://www.dailymail.co.uk/indiahome/article-3664841/Salem-woman-21-kills-obscene-pictures-morphed-look-like-posted-Facebook.html> (last visited Feb. 22, 2017).

<sup>2</sup> See DEBARATI HALDER & H. JAISHANKAR, *Cyber Crimes Against Women in India* 8 (2017).

<sup>3</sup> ASHWAQ MASOODI, *For victims of cyber stalking, justice is elusive*, Live Mint, available at <http://www.livemint.com/Politics/St93190XdGvpiclGWwnX0I/For-victims-of-cyber-stalking-justice-is-elusive.html> (last visited Mar. 1, 2017).

<sup>4</sup> See Internet harassment — Cyber stalking, Cyber harassment and Cyber Bullying, Astrealegal, available at <https://www.astrealegal.com/internet-harassment-cyber-stalking-cyber-harassment-and-cyber/> (last visited May, 12, 2017).

<sup>5</sup> See DEBARATI HALDER & H. JAISHANKAR, *Supra* note 2 at 9.

<sup>6</sup> See generally (2015) 5 SCC 1 : AIR 2015 SC 1523.

<sup>7</sup> See generally Ursula Smartt, *The Stalking Phenomenon: Trends in European and International Stalking and Harassment Legislation*, EUROPEAN JOURNAL OF CRIME, CRIMINAL LAW AND CRIMINAL JUSTICE, Vol. 9/3, 209-232 (2001).

<sup>8</sup> See generally PAUL BOCIJ, MARK GRIFFITHS AND LEROY MCFARLANE, *Cyberstalking: A New Challenge for Criminal Law*, THE CRIMINAL LAWYER, 5, (2002).

<sup>9</sup> See generally DR. S.K. MOHAPATRA, *Victimisation of Women Under Cyberspace in Indian Environment*, in 2 (3 (1)) INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH, 221 July-September, 2015.

<sup>10</sup> See DEBARATI HALDER, *Cyber Stalking Victimisation of Women: Evaluating the Effectiveness of Current Laws in India from Restorative Justice and Therapeutic Jurisprudential Perspectives*, *Temida*, 104, (2015).

<sup>11</sup> See *Supra* note 2.

<sup>12</sup> See Comparison Statistics (2000-2013) released by WHOA, WHOA, available at [www.haltabuse.org/resources/stats/Cumulative2000-2013.pdf](http://www.haltabuse.org/resources/stats/Cumulative2000-2013.pdf) (last visited Mar. 13, 2017).

<sup>13</sup> See *Supra* note 6.

<sup>14</sup> See DEBARATI HALDER & H. JAISHANKAR, *Supra* note 2 at xv.

<sup>15</sup> See JUSTICE YATINDRA SINGH, *Cyber Laws*, 23 (2012).

<sup>16</sup> Section 509. Word, gesture or act intended to insult the modesty of a woman

Whoever, intending to insult the modesty of any woman, utters any word, makes any sound or gesture, or exhibits any object, intending that such word or sound shall be heard, or that such gesture or object shall be Seen, by such woman, or intrudes upon the privacy of such woman, shall be punished with simple imprisonment for a term which may extend to three years, and also with fine.

<sup>17</sup> See *Supra* note 6.

<sup>18</sup> DEBARATI HALDER, *Cyber Stalking Victimisation of Women: Evaluating the Effectiveness of Current Laws in India from Restorative Justice and Therapeutic Jurisprudential Perspectives*, *Temida*, 115, (2015).

<sup>19</sup> See generally NATIONAL CRIMES RECORD BUREAU (NCRB), available at <http://ncrb.nic.in/> (last visited Feb. 23, 2017).

<sup>20</sup> SANDHYA SOMAN, CYBERSTALKING MAKES FIRST ENTRY INTO LEGAL DEBATE, available at <http://epaper.timesofindia.com/Repository/ml.asp?Ref=VE9JQ0gvMjAxMy8wMy8xOCNBcjAwNDAY> (last visited Mar. 27, 2017).

<sup>21</sup> 2012 SCC OnLine Del 2673.

<sup>22</sup> See Cyber cell's first conviction: Man gets 3 years for sending obscene messages, stalking colleague, Indian Express, Jul. 4, 2015 available at <http://indianexpress.com/article/cities/mumbai/cyber-cells-first-conviction-man-gets-3-years-for-sending-obscene-messages-stalking-colleague/> (last visited Mar. 2, 2017).

<sup>23</sup> See Swati Mehta, *Cyber Forensics and Admissibility of Digital Evidence*, SUPREME COURT CASES, available at [http://www.supremecourtcases.com/index2.php?option=com\\_content&itemid=135&do\\_pdf=1&id=22821](http://www.supremecourtcases.com/index2.php?option=com_content&itemid=135&do_pdf=1&id=22821) (last visited Apr. 29, 2017).

<sup>24</sup> See generally Deepak Bade, *Cyber Forensics & Electronic Evidences: Challenges In Enforcement & Their Admissibility*, ACADEMIA.EDU, available at [https://www.academia.edu/3831495/Cyber\\_Forensics\\_and\\_Electronic\\_Evidences\\_Challenges\\_In\\_Enforcement\\_and\\_Their\\_Admissibility](https://www.academia.edu/3831495/Cyber_Forensics_and_Electronic_Evidences_Challenges_In_Enforcement_and_Their_Admissibility) (last visited May 1, 2017).

<sup>25</sup> See Erin E. Kenneally, *Confluence of Digital Evidence and the Law: On the Forensic Soundness of Live-Remote Digital Evidence Collection*, 5 UCLA J.L. & TECH. 1, 4 (2005).

<sup>26</sup> See generally Stefan Fafinski, *Access Denied: Computer Misuse In An Era of Technological Change*, 70(5) J. OF CRIM. L. 424, 430 (2006).

<sup>27</sup> See Cyber Forensics Trends and Developments in India 2014, available at <http://ptlb.in/cfrci/?p=98> (last visited Mar. 2, 2017).

<sup>28</sup> See NINA GODBOLE & SUNIT BELAPURE, *Cyber Security* 329 (2011).

<sup>29</sup> See generally CHRIS REED & JOHN ANGEL, *Computer Law* 319 (2004).

<sup>30</sup> See generally ANNE WALLACE, *Using Video Link to Take Forensic Evidence: Lessons from an Australian Case Study*, 17(3) INT. J. OF EVIDENCE & PROOF 221, 224 – 227 (2013).

<sup>31</sup> (2016) 15 SCC 485.

<sup>32</sup> See generally CD is a document under law, says SC, THE HINDU, Nov. 26, 2015, available at <http://www.thehindu.com/news/national/cd-is-a-document-under-law-says-sc/article7916647.ece> (last visited Apr. 17, 2017).

<sup>33</sup> See generally Tejas Karia, *Digital Evidence: An Indian Perspective*, INTERNATIONAL LAW OFFICE.COM, available at <http://www.internationallawoffice.com/newsletters/detail.aspx?g=93c76fe9-e156-470b-b84d-3f4cf73da391> (last visited Apr. 29, 2017).

<sup>34</sup> (2006) 7 SCC 607.

<sup>35</sup> (2006) 11 SCC 1.

<sup>36</sup> (2005) 11 SCC 600.

<sup>37</sup> (2003) 4 SCC 601.

<sup>38</sup> See generally 26/11 trial: David Headley deposes before Mumbai court via video conference, THE TIMES OF INDIA, Feb. 8, 2016, available at <http://timesofindia.indiatimes.com/india/26/11-trial-David-Headley-deposes-before-Mumbai-court-via-video-conference/articleshow/50895266.cms> (last visited Feb. 9, 2017).

<sup>39</sup> (2014) 10 SCC 473 : AIR 2015 SC 180.

<sup>40</sup> See FRANKLIN WITTER, LEGAL ASPECTS OF COLLECTING AND PRESERVING COMPUTER FORENSIC EVIDENCE, available at <http://www.giac.org/paper/gsec/636/legal-aspects-collecting-preserving-computer-forensic-evidence/101482> (last visited Mar. 28, 2017)

<sup>41</sup> See generally BILL NELSON, AMELIA PHILLIPS & CHRISTOPHER STEUART, *Guide to Computer Forensics and Investigation* 153 (2010)

<sup>42</sup> GURMANPREET KAUR, *Cyber Stalking and Victimization of Women: An Analytical Study, in Law as a Catalyst of Social Change in Present Scenario* (Bindu Jindal ed., 2016).

**Disclaimer:** While every effort is made to avoid any mistake or omission, this casenote/ headnote/ judgment/ act/ rule/ regulation/ circular/ notification is being circulated on the condition and understanding that the publisher would not be liable in any manner by reason of any mistake or omission or for any action taken or omitted to be taken or advice rendered or accepted on the basis of this casenote/ headnote/ judgment/ act/ rule/ regulation/ circular/ notification. All disputes will be subject exclusively to jurisdiction of courts, tribunals and forums at Lucknow only. The authenticity of this text must be verified from the original source.