Cyber Stalking Victimisation of Women: Evaluating the Effectiveness of Current Laws in India from Restorative Justice and Therapeutic Jurisprudential Perspectives

Debarati Halder*

Victimisation of women through cyber stalking is one of the most serious crimes against women. Many countries including India have developed laws regulating cyber stalking. This article argues that since both, restorative justice (RJ) and therapeutic jurisprudence (TJ) are victim oriented, the issue of cyber stalking of women may be dealt with by RJ process and the laws in this regard must be analysed by the legal actors with a background in RJ and TJ philosophy. India had earlier taken up therapeutic punishment policy to enforce rights of the accused. But the modern principles of TJ have still not been considered in the RJ background in cyber stalking cases. This article therefore examines whether RJ and TJ principles can replace retributive principles for cyber stalking victimisation. It also examines the Indian cyber stalking law from RJ and TJ perspectives to assess its effectiveness for victims.

Key words: cyber stalking, restorative justice, therapeutic jurisprudence, victimisation of women.

*Debarati Halder is an advocate. She is the managing director of Centre for cyber victim counselling (www.cybervictims.org) and the vice president of kids and teens division, Working to Halt Online Abuse (www.haltabuse.org). She is presently pursuing her PhD from National Law School India University (NLSIU), Bangalore. E-mail: Debaratihalder@gmail.com.
Introduction

In the last decade, victimisation of women has taken a different dimension due to misuse of digital communication technology which has now become a new way for perpetrators to harass women. 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 shame the victim. Assuming that the impact of cyber graphical victimisation can be devastating on women and girls, many policy making bodies, including the European Union, had framed policies and guidelines to create laws to penalise creation, production and publication of child pornographic materials. The understanding in this regard is also expanding to cover creation, production and publication of revenge pornographic materials on the internet as well (Halder, Jaishankar, 2010, 2011; Citron, Franks, 2014). Textual victimisation on the other hand, may include cyber bullying, trolling, email harassment, cyber stalking, etc. While both textual and graphical victimisation may create huge defamation and public shaming for the victims, textual victimisation, when carried out by way of cyber stalking, may be more personal and may create more traumatising effects on victims as the stalkers aim to create threat in the minds of their victims (Ellison, Akdeniz, 1998).

Recent statistics on cyber victimisation show that women victims generally outnumber male victims when it comes to cyber stalking victimisation. Cumulative statistics released by Working to Halt Online Abuse (WHOA), organisation which deals with cyber stalking, showed that out of 4043 victims who contacted WHOA in the period of 2000-2013, 70% were women. Recently released UN Broadband Commission Report for Digital Development Working group on Broadband and Gender, also, showed that women from the age group of 18-24 are at high risk of being abused on internet by way of cyber stalking (UN Report, 2015: 16). Several studies have been carried out to

---

show the method and impact of cyber stalking on university students, young and adult individuals, including children, women and men (Jaishankar, Uma Sankary, 2005; Pittaro, 2008; Salter, Bryden, 2009; Pittaro 2010). Almost all of these researches suggest that cyber stalking may be an interpersonal crime and the impact may be graver on women. Depending on the nature and the impact of cyber stalking especially on women, several countries, including United States of America (US) and United Kingdom (UK), have made specific laws to regulate cyber stalking. India has joined this league only in the mid 2013 when the Criminal Law Amendment Act, 2013 was introduced as a result of a brutal gang rape in Delhi. This article argues that the current Indian law cannot sufficiently address victims’ needs. On the other hand, restorative justice (RJ) and therapeutic jurisprudence (TJ) are victim oriented approaches. Therefore, if the current law adopts these approaches, the needs of the victims may be addressed better.

Restorative justice emphasises upon repairing the harm through mediation involving the victim, offender and the legal actors, including judges, lawyers, and mediators to solve the problem amicably. This is especially because RJ involves emotional intelligence and communicative techniques, including understanding and empathy of the legal actors (King, 2008). Lately, practitioners and researchers have started feeling that RJ can prove to be a better option to deal with violence against women when compared to retributive justice which pronounces harsh punishments for offenders and may turn extremely traumatising for women victims of interpersonal abuse, especially when they may be forced to testify against their abusive partners in front of the police and the courts (Goodmarks, 2014). On the contrary, restorative process is victim centred and can be deployed at the victim’s request, it gives more power to the victim as a victim and not as a mere ‘witness’ who may not have much saying in the redresses process taken up by the court. Cyber stalking being a newly recognised form of violence against women involving intimate partners as one of the categories of harassers, may be considered to be dealt with by RJ process.

Therapeutic jurisprudence, on the other hand, emphasises upon law’s positive effect on the healing process. As Wexler and Winick (2008: 4) explained, “an interdisciplinary approach to legal scholarship that has a law reform

agenda, therapeutic jurisprudence seeks to assess the therapeutic and counter-therapeutic consequences of the law and how it is applied, as well as to increase the former and diminish the latter. It is an approach to the law that uses the tools of the behavioural sciences to assess the law’s therapeutic effects and, when consistent with other important legal values, to reshape law and legal processes in ways that can improve the psychological functioning and emotional wellbeing of the individuals affected.”

This article argues that the particular laws and the legal process fail to see what the victim wants. It must be understood that laws regulating cyber stalking must also include the victim’s needs which may not necessarily be harsh punishment to the offender, but may also include healing the trauma through proper restorative process.

It is interesting to note that several researches on cyber stalking regulations have highlighted law’s scope to regulate specific behaviours as cyber stalking, the gap which hampers the proper detection and retributive process, etc. (Basu, 2013; Hazelwood, Koon-Magnin, 2013). However, there is rarely any research on effectiveness of laws on the healing process in the cases of cyber stalking victimisation of women. This article aims to fulfil this gap. The goal of this article is to evaluate existing law on cyber stalking in India in the perspective of RJ and TJ. Whether the cyber stalking laws in India have this therapeutic jurisprudential approach in them? What are the prime motives of these laws? Whether the existing laws are anti-therapeutic? What are the primary needs of the victims of cyber stalking and whether these laws can meet these needs? Whether these laws have effectively criminalised cyber stalking? This article aims to research on these issues. The article is divided into five parts including the introduction. The second part deals with definitions of cyber stalking and finds out why the issue must be perceived as different from offline stalking. The third part deals with victimological aspects of cyber stalking. The fourth part deals with positive and negative aspects of the Indian cyber stalking law from the victimological perspectives and the fifth part deals with as how RJ and TJ principles may be involved to make the cyber stalking regulations more effective for the victims in India.
Defining cyber stalking

Academic and legal definitions of cyber stalking

Academically, the concept of cyber stalking has been construed mainly as a behavioural misconduct conveyed by digital communication technology. Bocij, Griffiths and McFarlane (2002: 5) define cyber stalking as “a group of behaviours in which an individual, group of individuals or organization, uses information and communications technology to harass one or more individuals. Such behaviours may include, but are not limited 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”. According to Baer, “Cyber stalking in particular is composed of words alone and therefore stands more distinctly as apart as a crime of accumulation” (Baer, 2010: 154).

According to Brenner, “in a sense, cyber stalking and cyber harassment are lineal descendants of the obscene or annoying telephone call offenses that were created roughly a century ago, to address harms resulting from the misuse of a nineteenth century technology” (Brenner, 2004: 14). Ellison and Akdeniz (1998) had construed the term cyber stalking as online harassment, which may include various digitally harassing behaviours, including sending junk mails, computer viruses, impersonating the victim, etc.

It may be noted that, legally, cyber stalking was recognised as an offence only in the early 1990s. Stalking through cyber space was criminalised by Michigan in 1993 through Michigan Criminal Code. The term ‘cyber staking’ is still not defined by any particular legal provision in the UK. Provisions including Ss.2-7 of the Protection from Harassment Act (PHA), 1987 are presently used as the regulatory provision for stalking and cyber stak-

---

4 See for details Michigan Criminal Code, Stalking: Section 28.643(8), definitions. 1993 section 411h. www.haltabuse.org/resources/laws/michigan.shtml, page accessed 12.12.2013. Later, the Federal law also developed anti-cyber stalking law through “Violence Against Women and Department of Justice Reauthorization Act, 2005”, which amended Section 2261A (2) of Title 18, USC through Section 114, which specifically deals with stalking including cyber stalking.


king. However, the Crown Prosecution Service (CPS) provides an exhaustive definition of cyber stalking based upon the framework of S2A (3).

As it may be seen from the above, all definitions (academic as well as legal) perceived cyber stalking as harassment carried out digitally, which may necessarily infringe the privacy of the victim. The legal definitions of cyber stalking that are discussed above derive their conceptualisations from laws meant for physical stalking. Before January 2013 there was no recognised legal definition of stalking or cyber stalking in India. The concept of cyber stalking neither received any new academic understanding in India until 2010, when Halder and Jaishankar (2010: 12) provided a functional definition of cyber stalking which is as follows: “In one word, when ‘following’ is added by mens rea to commit harm and it is successfully digitally carried out, we can say cyber stalking has happened”.

Stalking was legally recognised as an offence in India through S.354D of the Indian Penal Code which was inserted through the Criminal Law Amendment Act, 2013. The provision defined stalking in the following words: “Any man who follows a woman or contacts or attempts to contact such woman to foster personal interaction repeatedly despite a clear indication of disinterest by such woman or whoever monitors the use by a woman of the internet, email or any other form of electronic communication or watches or spies a person in a manner that results in fear of violence or serious alarm or distress, in the mind of such woman or interferes with the mental peace of such woman, commits the offence of stalking.” It may be noted that the above provision was made specifically as a ‘women centric law’ and the wordings of this law have put much emphasis on the infringement of privacy by way of monitoring and stalking, which creates fear from violence, serious alarm or distress. It therefore provides a three dimensional explanation to stalking: (i) despite her disinterest, physically persuading a woman repeatedly by conducting in such a way that may create fear in her, may interfere with her peace of mind, (ii) monitoring her digital whereabouts, communications, etc. by digital conducts which create serious threat, alarm or interfere with her mental peace, and (iii) spying or watching her to in order to pose a harm to her. As such, unlike other existing provisions on cyber stalking in other jurisdictions such as the US, this law has not put much emphasis on harassing communi-

---

7 Criminal Law (Amendment) Ordinance, 2013, Section 6.
cation which is also considered as stalking behaviour by many legal scholars, such as Bocij, Griffiths and McFarlane (2002), Brenner (2004) and Baer (2010).

*Why cyber stalking must be perceived as different from physical stalking*

From the academic and legal definitions discussed above, it can be seen that there are distinguishing factors which differ cyber stalking from physical stalking (Williams, 2009; Pittaro, 2010; Reyns, 2010). These may be summed up as follows:

**Digital mode of pursuing:** Unlike physical stalking, cyber stalking may not need the perpetrator and the victim to stay in near proximity. Cyber stalking necessarily infringes privacy through digital behaviour of pursuance with the help of communication which is made with the intention of creating a feeling of fear or psychological trauma that may make the victim restless, impatient or suffer from sleeplessness or eating disorder due to acquit anxiety (Jaishankar, Uma Shankary, 2005, Pittaro, 2008). The nature of cyber stalking can best be described through the explanation offered by Reyns (2010). He suggests that the four component parts of cyber stalking include repeatedly contacting the victim even after the perpetrator has been asked to stop; sending harassing or annoying communication to the victim, sending unwanted sexual advances to the victim and sending physical threats to the victim. Thus, it can be seen that the core mode of cyber stalking is pursuing of the victim digitally with intent to infringe her privacy against her will. Here lies the main distinctive feature of cyber stalking, which makes it different from physical stalking. This persuading stage can be described as shadowing of the victim. The process of shadowing includes accessing vital information of the victim including her personal as well as workplace data. It may be noted that such data may float in the internet due to ever increasing data contribution by the users themselves to the internet through various social media and web platforms like Facebook, Twitter, LinkedIn, and search engines like Google, which provide free services, as well as paid services such as mobile networking apps. The workplace data of an individual may also be available in the internet due to certain corporate policies and practices, which need the information about employees to be published in the company websites. Such personal, as well as workplace data can be easily accessed if searched in the internet with key words denoting his/her name, email id, workplace, school and university or even his/her mobile phone numbers (Gelman, 2009).
Negative online socialising: As such, pursuing or shadowing the victim or data mining about the victim can turn into an offensive behaviour when the information gathered is used to keep ‘unwanted’ contact with the victim. Analysing the literature on cyber stalking, it can be seen that this unwanted contact can be done in two ways (i) in a constructive manner whereby the stalker builds up personal communication with the victim through emails or chats, social media, or text messages or even phone calls (Brenner, 2004; Baer, 2010); and (ii) in a destructive manner, whereby the stalker monitors the victim by reaching out to her email id, social media profile, and takes up several harassing behaviours, such as hacking the profiles, identity theft, accessing the computer to establish a forceful contact with the victim and to gain direct control over the online activities, as well as real life activities of the victim (Bocij, Griffiths, McFarlane, 2002). Unwanted contact by means of constructive way as well as destructive way can therefore be done by way of negative online socialising, which is opposite to positive online socialising. Traditionally, negative socialisation means a phenomenon which “occurs when others use punishment, harsh criticism or anger, to try to teach us a lesson, and often we come to dislike both negative socialisation and the people who impose it on us.”

Choice of the victims for being accessible: It may also be noted that the social media, email/message/digital communication service providers and search engines may be parts of a wider database which can share the information of the user if the user wishes so (Armbarst et al., 2009); for example, a Facebook user can log into Academia.edu, a site meant for sharing academic interests, scholarly articles published by the users themselves, with the username and password used for his/her Facebook profile. In Academia.edu, the user’s profile may appear either in brief as he/she may wish to show, or the way Facebook profile briefly describes him/her. The user can further be

---

followed by people interested in the same subject, colleagues, students, friends of the students, etc. Such followers can get to see not only the professional profile of the user, but also the Facebook link and user email id if the user wishes to include them in his/her profile. Similarly, a Twitter account can be used to log into storyfy.com through which users can share their experiences, trending news, etc; it can also use hash tag in the similar fashion as in Twitter, and it provides further opportunity to share the ‘story’ through Facebook, Twitter, Google+ or LinkedIn. All that the user needs to do is to confirm participation in the site through his /her email id. As such, the social media and the cloud attached to it, carry on ‘commodification of personal information’(Tavani, Grodzinsky, 2002) and, nonetheless, it can provide a wider platform to carry out pursuing activity for cyber stalking through data mining and “reality mining”.9 This can be extremely fatal as has been proved in the case of Amy Boyer stalking case, where Boyer’s stalker gained sufficient personal information about her from the internet, constructed two websites providing false information about her and eventually murdered her (Tavani, Grodzinsky, 2002). But it needs to be remembered that cyber technology has developed hugely since 1999s when Amy’s stalker took to cyber space to get the details about his victim. In 2015, the liability of such ‘commodification of personal information’ is shared between the users, as well as the social media which are used by the users. Due to Due Diligence laws and Safe Habor Policies of the US, the tortuous liability of the social media and internet search engines has become even more limited, shifting the burden of protecting the privacy more to the users themselves.

Offender-victim relationship: Cyber stalking differs from physical stalking if seen from the perspective of offender-victim relationship in the light of lifestyle-routine activity theory. It rather fits into the theory of ‘cyber lifestyle-routine activity’ as has been explained by Reyns, Henson and Fisher (2011), which is the expanded form of lifestyle-routine activity theory to cover online victimisation cases, especially cyber stalking victimisation. In cases of cyber stalking victimisation, online deviance may have larger effect for causation of crime compared to online exposure of the victim and proximity of the victim-offender, target attractiveness and lack of guardianship (Reyns, Henson, Fisher, 2011). The term “Reality mining” was coined by Sandy Pentland and as Erica Orange has briefed the explanation of the term, it “refers to the collection and analysis of technology based data as it relates to human social behaviour” (Orange, 2009). Available at: www.minnesotafuturists.pbworks.com/f/JA2009_Orange.pdf, page accessed on 12.12.2013.
2011). But these factors may have their significant effects as well. Online deviance may increase due to enormous data swelling in the internet, which makes it easier for the perpetrator to target his victim/s even though victim may not herself expose unnecessary information to allure the perpetrator directly.

**Changing motive of the stalker:** It must also be noted that digitally pursuing or shadowing alone may not make the pursuer an offender of cyber stalking. Such ‘shadowing’ by the stalker, if accompanied by an ill motive, may fall into the category of cyber stalking. As the academic and legal definitions suggest, to attract the penal provisions meant for cyber stalking, pursuing or shadowing must be done with an intention to monitor the victim digitally as well as in real life in some cases. This understanding makes regulating the behaviour of digitally pursuing challenging. This is especially so in cases when the pursuer or shadower shadows his target, who may be a celebrity, in the course of simple fan following and not for obsessive monitoring and stalking of the celebrity (Wykes, 2007). Digitally pursuing or monitoring the victim fits in the concept of cyber stalking only when the perpetrator starts making his victim aware of such pursuing or shadowing or monitoring by communicating with his victim, which may be perceived as annoying, unwanted or threatening by the victim.

**Victimological aspects of cyber stalking**

**Impact of cyber stalking**

Even though it is an accepted fact that there is no universal definition of cyber stalking (Reyns, 2010), almost all the academic and legal definitions of cyber stalking from all jurisdictions strike in the same cord of harassment and harassing communication along with privacy infringement when it comes to conceptualising cyber stalking. It can be seen that on the cyber space, threat, harassment or distress or infringement of privacy is ‘communicated’ only when the perpetrator executes the same either by directly communicating with the victim or with the help of known and unknown users including the *aide stalkers* (Halder, 2013a: 77) through negative online socialisation. This stage may

---

10 For definitions of cyber stalking provided in laws from various jurisdictions, see links provided in footnotes 6 and 7.

11 Halder (2013b) explains aide stalkers as people who are not directly related to the victim. They could be the friends and acquaintances of the actual predator who wishes to monitor
also include offensive behaviours including, bullying, trolling or creation of fake avatars\textsuperscript{12} and spreading such fake avatars to websites meant for pornography (Pittaro, 2010). This is especially done by the cyber stalker either by him/herself or through aide Stalkers (Halder, 2013a: 77) with an aim to turn these websites as proxy stalkers whereby these sites may continuously send the victim obscene mails, pop-up notices, etc. (Pittaro, 2010).\textsuperscript{13} Such continued offensive behaviour by the stalker/s may create extremely negative impact on the victim. Continuous harassing, threatening phone calls or emails or negative online socialising may make the victims panicked and extremely concerned about their reputation. Stalking and consequent negative online socialising may also cause loss of job, hamper family life and damage reputation of women in the marriage market (Halder, Jaishankar, 2011). Additionally, women victims may suffer secondary harassment with the police or the courts due to poor understanding of the nature of the offence by the police officers, lawyers or judges (Halder, Jaishankar, 2011) or due to complete helpless situation faced by the courts or the police where the stalker/s or aide stalkers or the websites are situated outside the country. It may also make the victims to take extreme steps including suicide or they may suffer withdrawal symptoms.\textsuperscript{14}

\textsuperscript{12} Halder (2013a: 197) defines fake Avatars as “a false representation of the victim which is created by the perpetrator through digital technology with or without the visual images of the victim and which carry verbal information about the victim which may or may not be fully true and it is created and floated in the internet to intentionally malign the character of the victim and to mislead the viewers about the victim’s original identity.”

\textsuperscript{13} One such example could be United States vs. Sayer (U.S. v. Sayer, 2012 WL 2180577 (U.S. District Court for the District of Maine, where the defendant Sayer misused the personal information of the victim to build up online advertisements, fake profiles, etc. to exhibit the victim as a sex-object. The court rightly held that such conducts amount to unprotected conduct and speech and attracts Ss.2261A. For more details see Young, 2013.

\textsuperscript{14} From the personal experience of the author as cyber crime victim counselor.
Specific needs of the victims of cyber stalking

Basically, the needs of the victims of cyber stalking may be threefold: (i) in case the stalker is anonymous, to know the actual identity of the stalker, (ii) and irrespective of whether the stalker is known or unknown to the victim, to prevent the stalker from contacting her and (iii) pull down the offensive posts, websites, messages, etc. that may have been spread about the victim as part of negative online socialisation to create fear in the mind of the victim. In case of victimisation by anonymous stalker/s, victims often want to take up irrational coping methods like contacting the amateur hackers to hack and track the actual identity of the stalker (Halder, Jaishankar, 2015). Even when the stalker is known to the victim, she may want to take up irrational coping method to hack the stalker’s email id, social media profile or even digital devices, like the laptop or mobile phone, not only to prevent him from contacting through such profiles, but also to permanently erase any information, communication or photograph of the victim, which may help the stalker to continue with cyber stalking. The victims may take up such irrational coping methods out of fear of more harassment by the stalker or because of frustration due to no cooperation from the websites concerned, or because of lack of confidence in the criminal justice system, especially when the police may refuse to help the victim or the perpetrator continues to harass the victim even after the victim has approached the courts and the initial no-contact period has got over or the stalker may be out on bail. The last point as mentioned above is vital to develop new restorative process as well as better cyber stalking laws with TJ approach (Halder, Jaishankar, 2015)

Positive and negative aspects of S.354D of the Indian Penal Code from victimological perspectives

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, publica-

---

15 This is from the general observation of the author as a cyber crime victim counselor.
tion, transmission of obscene materials) (Singh, 2013); 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 (Verma, 2009). S.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.

a) Limited scope

It must be noted that S.354D of the Indian Penal Code protects women from men. Creators of this law failed to take note of famous cases like that of Megan Meier, where the perpetrator was a woman victimising another young woman. This provision has acquired more characteristics of anti-harassment law of the UK with some shadows of the US laws on stalking. Noticeably, this provision does not define cyber stalking, the concept of which is hidden in the wordings of the text, especially in the second explanation of the course of conduct which amounts to stalking. A clear reading of the clause (1) of the Section would show that the language of the provision indicates that physical and online stalking can be a combined act, or separate acts. The language in the first clause extends the scope of the law to a person who can be the perpetrator and who is (i) known to the victim and who may be in a

---

16 This particular provision was declared unconstitutional by the Supreme Court of India in 2015 for its vagueness in the case of Shreya Singhal vs. Union of India WP. (criminal) no. 167 of 2012, www.supremecourtofindia.nic.in/FileServer/2015-03-24_1427183283.pdf, page accessed on 27.3.2015.

17 Meir was a victim of cyber bullying in MySpace by another woman Lori Drew, who bullied Meir in the disguise of a teenage boy. Meir committed suicide due to the bullying. Drew was acquitted. Later, a Bill was proposed to amend Title 18, USC in respect to cyber bullying, which was popularly known as H.R.1966 (111th) Megan Meir Cyber bullying Prevention Act. See the full text at: www.govtrack.us/congress/bills/111/hr1966/text, page accessed on 27.3.2015.
relationship with the victim including personal or professional relationship, and such person may have access to the private data or private internet activities of the victim with the knowledge of the victim, or (ii) unknown to the victim, who may not be in any prior relationship and who may try to access the privacy of the victim and also breach the privacy and confidentiality of the victim. The language also broadly extends its scope to ‘aide stalkers’ and data mining by the perpetrator when it includes monitoring the web-space, computer, etc. by the victim and watching or spying the victim. But S.354D does not explicitly mention about interstate stalker as has been mentioned in Ss.2261A of USC18. This makes the question of jurisdiction a critical issue.

b) Regulatory reliefs do not cover the full concept of cyber stalking

Further, it may be noted that clause (1) of Section 354D of the IPC highlights the motive of the act of stalking, which includes fostering personal interaction or monitoring the usage of the internet, email or any other form of electronic communication or watching or spying his/her victim to actually cause fear of violence or serious alarm or distress of interfering the mental peace of the victim. This provision thus reflects the causing of the fear factor. But, unfortunately, this law provides regulatory relief for only a part of the whole concept of cyber stalking, i.e. invasion of privacy, and not the full concept, which includes invasion of privacy and also communicating the threat. This provision does not directly indicate the patterns as how the victim can be ‘monitored’, ‘watched’ or ‘spied’ when she is being cyber stalked. It neither includes any direct ‘third party’ liability when the aide stalker is involved. A clear reading of the patterns of victimisation as has been provided in S.354D may suggest that this Section has touched the notion of breaching of privacy (including the concept of secrecy and personal space), through monitoring, watching, spying of the internet, emails, online communication, etc. But, it becomes the responsibility of the courts to broaden the meaning of this particular provision since there were no Amy Boyer’s or Sayer’s case in India to show how the privacy of the victim in real life as well as in virtual life can be infringed by harassing communication and conducts. It needs to be understood that in India, the concept of ‘conduct’ has not been critically examined by the courts in the backdrop of cyber stalking cases. It is obvious that when the courts have to consider ‘conducts’ for justifying the role of anti cyber stalking law, the activities of the victim cannot be overlooked. The
courts in the US have interpreted the meaning of the term ‘conduct’ in relation to cyber stalking as a holistic term involving the online behaviour of the perpetrator and the communication carried on by him/her with a particular purpose which caused the victim to feel distressed, or afraid. In India, the court’s understanding of the victim’s rights and responsibilities towards using the ‘ignore’, ‘blocking’ options as has been provided by the service providers still needs to be nurtured when it comes to cyber stalking cases. This is especially so when online activities of the victims may constitute positive or negative online socialising, which can help the stalker. Further, S.354D of the IPC does neither proscribe the mannerisms as how the stalker should not use such online conducts, communication and real life information of the victim to fulfil his purpose; i.e., to create distress or fear for the victim.

The scope of S.354D of the IPC in preventing data mining may be further challenged by other existing laws, such as S.3 of the Information Technology (the reasonable security practices and procedures and sensitive data or information) Rules 2011, which regulates privacy to personal data including sensitive personal data. This is especially important as the provision S.3 states that this section would not cover information which are publicly available in the web; which are already revealed to any individual or the public by way of Right to Information Act, or any information which is already revealed to

---

18 For instance, consider the case of United States vs. Cassidy, 814 F. Supp 2D 574 (D. md. 2011) where the defendant was allegedly conducting cyber stalking through negative socialising; i.e. creating a fake Twitter account through which he had directed numerous Tweets to the victim and her religious centre. See more in Young, 2013: 61. The court emphasised on the victim’s choices to ‘ignore’ the blog posts or Tweets when they are not directed to a ‘captive audience’ and made in the public forums. Interpretation of harassing conduct in the back drop of cyber stalking has also been done in the same line by the courts in the UK; consider the cases of Majrowski vs. Guys & St. Thomas NHS trust [2006] UKHL 34; [2006] ICR 1199 HL and Conn vs. Sunderland City Council([2007] EWCA Civ 1492, [2007] 2 All ER (D) 99), where the court held that simple conduct which would not amount to criminal conduct, would not attract the PHA (Salter, Bryden, 2009). However, it depends upon the courts to build up the difference between conducts which may be categorised as ‘civil conduct’ which may escape the heavy liability as that of criminal conducts which may attract heavy punishment in PHA.

19 Section 3 of the Rules state that sensitive personal data would mean the following: “(i) password; (ii) financial information such as Bank account or credit card or debit card or other payment instrument details; (iii) physical, physiological and mental health condition; (iv) sexual orientation; (v) medical records and history; (vi) Biometric information; (vii) any detail relating to the above clauses as provided to body corporate for providing service; and (viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise".

---
the public by any other laws. Now, it needs to be understood that the internet is also serving the purpose of creating ‘naming and shaming’ pages. In India this can become a particular problem especially when the victims can be women who are involved in professions including governance of the country, including mainstream politics or bureaucrats, who need to compulsorily reveal their data regarding assets. Such public data may also include residential information and data regarding children. Further, many celebrity women, film, TV, sports, news-media persona have their Twitter or Facebook accounts open for public viewing. The social media can neither be held liable for data mining as such users may have consciously as well as consensually opted for minimum privacy policy and thereby contributed more personal data. Such profiles can very well aide in stalking activities including data mining. This had been proved in the case of Sagarika Ghosh, a noted woman journalist, who was viciously trolled in Twitter, threatened with gang-rape and her daughter’s name and school information were made public (Arya, 2013).

\[c\) Unwanted surveillance and victimisation

S.354D suffers from another major drawback when it comes to regulating the privacy of the victim and conduct and communication of the prospective harasser; the proviso clause to S.354D of the IPC has excluded specific persons from being accused of stalking when it is done under specific circumstances. This is again a clear resemblance of the prosecutorial guidance as has been proved in the case of Sagarika Ghosh, a noted woman journalist, who was viciously trolled in Twitter, threatened with gang-rape and her daughter’s name and school information were made public (Arya, 2013).\[20\]

---

20 In relation to this, it further becomes important to highlight the following principles regarding openness of the data in the popular social media: Facebook principles declare that the primary objective of the site is to “make the world more open and transparent, which we believe will create greater understanding and connection”. The ten principles of Facebook are (i) freedom to share and connect, (ii) ownership and control of information, (iii) free flow of information, (iv) fundamental equality regarding the application of these principles, (v) social value, (vi) open platforms and standards, (vii) fundamental service, (viii) common welfare, (ix) transparent process and (x) one world.; Twitter in its “about” page discloses that it is “real time information network” that connects the users to “the latest stories, ideas, opinions and news’ of the user’s interest. The users can choose the profiles of personalities whom they like to “follow” and see his /her/their “Tweets”, information, photos, videos and conversations directly in the Tweets. The users can also contribute his /her stories, ideas, opinions etc through their own account “Tweets”; YouTube allows people to “discover, watch and share originally created videos”. It also provides forum for users “to connect, inform and inspire” and it acts like a “distribution platform for original content creators and advertisers”

21 The provison attached to S.354D states that the course of conduct will not amount to stalking if the person who pursued it shows (i) that it was pursued for the purpose of
been mentioned in S.4A of the PHA (inserted via amendment to the PHA by Protection of Freedoms Act, 2012) As such, the provisions which mention that when the breaching of privacy by way of monitoring internet usage or email or online communication or fostering relationship is done for preventing and detecting any crime by someone entrusted with the responsibility of detecting and preventing crime, or when it is done under “any law or comply with any condition or requirement imposed by any person under any law”, it actually opens the flood gate of ways of misusing the provision and breaching of the confidentiality and privacy of the victim and victimise her in arbitrary ways. The language of the third provision proves more dangerous when it says that the act of stalking may not be considered as a penal offence when the accused person proves that in the particular circumstances, the course of conduct was reasonable. Understandably, these provisions may safeguard activities to nab incidences of cyber terrorism or cyber phishing cases, especially when seen in the lights of Ss.69 of the Information Technology Act, which provides powers to issue directions for interception or monitoring or decryption of any information through any computer resource, or 69A of the Information Technology Act which provides power to issue directions for blocking for public access of any information through any computer resource, or 69B of the Information Technology Act which speaks about power to authorize to monitor and collect traffic data or information through any computer resource for cyber security. But the atrocious police activities against two women from Palghar for their alleged comments in the Facebook about deceased political leader Balasaheb Thackeray (Deshpande, Ahmed Ali, 2012) has proved that such open clauses of provisions may prove extremely dangerous for protection of freedom of speech and expression and also privacy of individuals, especially when S.354D of the IPC has been categorised as non-bailable offence with punishment for an imprisonment term amounting from one to three years and with fines.22 This makes the law anti-therapeutic in its nature.

22 This has been established by the amendment of the First Schedule to the Code of Criminal Procedure by the Criminal Law Amendment Act, 2013, No.13 of 2013.
d) Sentencing policy

S.354D of the IPC suffers from another major drawback in its sentencing policy. This provision has made cyber stalking essentially a criminal act and, as such, has prescribed criminal recourse for the same. The provision has made the offence of stalking (including cyber stalking) a cognizable, but bailable offence. As per this provision, it is punishable with imprisonment for a maximum period of three years with fine in the case of first conviction. However, for the second conviction, the offence has been made cognizable, non-bailable and punishable with imprisonment for a period of maximum five years with fine. In both cases, the provision has empowered “any magistrate” to try the offence. However, this provision as such, does not prescribe any civil remedy like the US or UK laws by ways of restraining orders, including no-contact orders which may prevent the stalker from contacting the victim. It is broadly understood that once the accused is arrested and imprisoned, his devices would be ceased by the police and he would not be allowed to use any means to communicate with the victim.

How can RJ and TJ help victims of cyber stalking?

From the above it may be seen that while the common goal of the cyber stalking laws from different jurisdictions, including the US, UK and India, is to criminalise the act of stalking and prohibit the continuation of the act by either imprisoning the offender (which will automatically debar him from contacting the victim due to restraining him in prison), or by granting no contact order as civil remedy (except India), none of the provisions specifically mention meeting victims’ other needs, including taking off the defamatory posts that may have been posted by the offender as part of cyber stalking, or tracking and finding out the real identity of the stalker in case of anonymous stalker. In general, these needs may be met only in the course of prosecution when the prosecution may need to establish the identity of the offender/s and solid proof of the offence. As the police, as a primary investigating agency, may need to get information from the websites hosted in other jurisdictions, which may have been used by the stalker/s, this process may be lengthy and time consuming. Such lengthy and complicated process may make the victims suffer secondary traumatisation (Halder, Jaishankar, 2011). Further,
victims may feel extremely discouraged to contact the lawyers due to heavy costs involved in running civil cases, even though they may badly need permanent restraining of the stalker from contacting them.

**How RJ and TJ may be involved for benefitting the victims?**

The primary need of the victims of cyber stalking is listening and believing them without victim blaming. RJ fulfils this need. Even though it is necessary to have a different set of laws to regulate cyber stalking than physical stalking, it may be seen that the psychological impact of the offence, as well as of the legal/court procedure on the victims may be quite similar to that of other dating violence or violence against women. Victims, especially women feel reluctant to report the offences to the police fearing humiliating interrogation and possible media highlight (Halder, Jaishankar, 2011). RJ methods have already created examples of successful victim-offender mediation for intimate partner abuse as well as offences against women (Umbreit, 1998; Grauwiler, Mills, 2015). RJ sees restoration of losses, including the dignity of the victims, and, as Braithwaite (1998) suggests, this can be done on the basis of personal accountability of the offenders and active community involvement (Umbreit, 1998). In cases of cyber stalking, RJ methods may be initiated right from the moment when the victim approaches the police. In India, such sort of victim-offender mediation has taken place in some rare cases of cyber harassments when the victim may have seek assistance from the police (Halder, 2013a: 275). But, such mediations, which are informal in nature, may generally end with asking the offenders to stop continuing the harassment or take off the contents from the website concerned. In general, no proper procedural actions are taken against the harassers in such cases. Harassers can neither be directed to pay for the losses suffered by the victim because, unlike the US or UK laws, Indian cyber stalking law does not have civil remedy whereby damages can be paid directly to the victims. It is because neither the victims may wish to register the cases through the formal procedures, nor

---

23 This is from the personal experience of the author as cyber victim counsellor.

24 Even though in India Section 43 of the Information Technology Act, 2000 (as amended in 2008) (penalty and compensation for computer, computer system, etc.) provides for civil remedy for computer related offences, it does not specifically mention about damages for cyber stalking.
the police may be interested to consider such cases worth registering as per the Criminal Procedure Code. We need to understand that internet communication technology provides anonymity and, hence, such informal mediation may be futile if the offender decides to come back in a new avatar to take revenge because such mediations do not necessarily involve ‘offender shaming’. Seeing from this aspect, it may be seen that S.354D of the Indian Penal Code is a half-baked law which may turn anti-therapeutic to victims due to the gap from the RJ aspects.

Given the fact that practices of police mediation already exist, S.354D of the Indian Penal Code may be made more victim-oriented if such process of mediation is included in the law as an alternative dispute resolution method in the RJ way. For achieving this, the stakeholders, including the courts, the lawyers and the police as the primary reporting agency, may consider adopting the following mechanisms which are influenced by the restorative justice principles:

1. Encouraging the victims to report the case according to proper norms as established by Criminal Procedure Code. At this stage, the victims may be made aware of the Victim Compensation Scheme, which enables the victims to claim compensation for any crime recognised by the Indian laws.  

In case the stalker is known to the victim, the police may arrange for pro-

---

25 S.35A of the Criminal Procedure Code of India speaks about victim compensation scheme. It states as follows: (1) Every State Government in co-ordination with the Central Government shall prepare a scheme for providing funds for the purpose of compensation to the victim or his dependents who have suffered loss or injury as a result of the crime and who require rehabilitation.

(2) Whenever a recommendation is made by the Court for compensation, the District Legal Service Authority or the State Legal Service Authority, as the case may be, shall decide the quantum of compensation to be awarded under the scheme referred to in sub-section (1).

(3) If the trial Court, at the conclusion of the trial, is satisfied, that the compensation awarded under section 357 is not adequate for such rehabilitation, or where the cases end in acquittal or discharge and the victim has to be rehabilitated, it may make recommendation for compensation.

(4) Where the offender is not traced or identified, but the victim is identified, and where no trial takes place, the victim or his dependents may make an application to the State or the District Legal Services Authority for award of compensation.

(5) On receipt of such recommendations or on the application under sub-section (4), the State or the District Legal Services Authority shall, after due enquiry award adequate compensation by completing the enquiry within two months.

(6) The State or the District Legal Services Authority, as the case may be, to alleviate the suffering of the victim, may order for immediate first-aid facility or medical benefits to be made available free of cost on the certificate of the police officer not below the rank of the
per mediation following the RJ principles if the victim wishes so. In such victim-offender mediation, the police may include stakeholders, including pro-bono lawyers, social workers who may be aware about cyber crimes and laws, counsellors and the victim; to let the victim speak about her victimisation and learn the different options for resolving the issue. Once the victim consents, the harasser may be called for mediation. He may then be counselled to be aware about the mistake he has done and why it should be stopped. He must then be asked to take off all of the offending contents as per the needs of the victim. If necessary, the police must extend their support in contacting the concerned websites to take down the offensive posts especially in cases where the posts may have become viral and the harasser may need to contact not only the search engines, but also multiple websites who may make profit out of the offending post. Further, he must also be made to understand that as a registered offender, he should not repeat his mistake in any other form to harass the victim.

2. The District Legal Services Authorities (DLSAs), which provide free legal aid, may consider creating awareness in this regard and encourage the victims to directly contact them for resolving the issues. Once the victim registers her case, the DLSA may arrange for victim-offender mediation with the consent of the victim in the similar manner as stated above. Such mediation can be facilitated by a judicial officer. Such mediation offered by DLSA should be encouraged more as the victim may avoid going to the police station in case she or her family fears for social taboo, which may be attracted due to frequent visits to the police station.

3. Restorative process by the DLSA or the police or the RJ practitioners can also include adopting positive anti-stalking procedures, such as positive Google bombing procedure (Citron, 2014), which may pull up only the positive and desired information about the victim in cases where the stalker is anonymous or where the stalker resides in different jurisdiction and no immediate help may be offered to stop the stalking due to necessary lengthy court procedures involved in extra-territorial matters. Such resto-

---

26 The DLSAs are judicial bodies constituted by the Legal Services Authorities Act, 1997. These bodies are headed by a presiding judge and also act as alternate dispute resolution forums. DLSAs are constituted to provide free legal services to any Indian citizen as has been categorized in Section12 of the Legal Services Authorities Act, 1997. This category, necessarily, includes women and children from all social and financial backgrounds.
rative process may include the victim’s family members or close friends to enforce no-contact orders by creating a virtual shield to protect the victim’s information from getting leaked to the stalker, as well as encouraging the victim to avoid and ignore the stalker’s harassing communications. The legal actors must also ensure that no contact orders be effective on the service providers who in spite of being notified about the court orders, continue to provide services for the perpetrator to create new accounts and carry on stalking activities against the victim.

It must be understood that once the law recognises cyber stalking as a criminal behaviour, it may fall into the category of therapeutic law. This is because such recognition of the unethical and illegal behaviour may instantly provide the sufferer the status of ‘victim’ in the eyes of the law and may instantly provide a healing touch to the victims. But it needs to be understood whether such therapeutic law can meet the expectations of RJ, because often such therapeutic approach may be challenged by court’s understanding regarding freedom of speech and its effect on the victim. This aspect is glaringly present even in US and UK laws and legal systems dealing with cyber stalking. Therefore, for achieving the goals of RJ and TJ, the laws must be expanded in terms of including alternative remedies to cover victim’s needs in the process as mentioned above. It is an unfortunate fact that even in India the concept of therapeutic jurisprudence had been taken up by the judges much earlier than the introduction and definition of the concept by Professor David Wexler in 1990’s. But the Indian understanding remained limited to the rights of the accused and therapeutic jurisprudence was never applied in its modern sense for the victims. In this cyber era, the situation has remained the same. In India, since the inception of S.354D, the law makers and the courts have failed to consider therapeutic jurisprudential approach for dealing with cyber stalking victimisation.

Conclusion and suggestion

Cyber stalking is essentially an emotional crime and, hence, it needs to be dealt with by way of restorative process along with therapeutic jurisprudential approach. If restorative process is included in the laws dealing with cyber stalking, the victims may be prevented from committing further harm in the course of saving themselves from their stalkers. Additionally, the restorative process may also find out ways to heal the damage suffered by the victim by including not only the offender himself, but also the web service providers. The laws criminalising cyber stalking may make the offender feel repent by making him understand about the illegalities of his behaviour in the course of cyber stalking. Simultaneously, if the laws are amended and expanded to cover the RJ approach, the victims may not only be healed of their psychological trauma, but by process of recourse, the offenders, including the web-service providers who may have secondarily breached the court orders, may take part in repairing the damage to the reputation of the victim by removing the offensive posts from the internet. The existing laws do prescribe for paying the penalties. As Citron (2014) suggested, similar to compensating the victims for hate speech on internet, this can be used to directly compensate the victims of cyber stalking if in the course of such cyber stalking she had suffered monetary loss. India must consider reforming its cyber stalking law to adopt such methods. But for this, the police, the lawyers, the judges and the counsellors must be trained properly to understand the RJ principles in the light of cyber victimisation. Restorative process may provide respite to women who fear breach of privacy during legal procedures. This is because restorative process allows the victim to choose a place for mediation and also the persons to be present for the restorative process from the options as may be suggested by the legal actors. This may not only ensure the fulfilment of goals set up by therapeutic jurisprudence, but may also encourage more women victims to report the crimes and seek for proper redress. Unless such process is adopted in India, the victims, especially women may never be able to get proper justice for cyber stalking victimisation.
References


Internet sources


Debarati Halder


128


Viktimizacija žena sajber proganjanjem: Procena efikasnosti postojećih zakona u Indiji iz ugla restorativne pravde i terapeutske jurisprudencije

Sajber proganjanje žena predstavlja jedno od najtežih krivičnih dela protiv žena. Mnoge države, uključujući Indiju, usvojile su zakone kojima se reguliše sajber proganjanje. Polazeći od toga da su restorativna pravda i terapeutska jurisprudencija pristupi orijentisani na žrtvu, u ovom radu se ističe da se slučajevima sajber proganjanja žena može baviti primenom restorativnih procesa, te da u tom smislu pravosudni organi treba da analiziraju zakone imajući u vidu filozofiju restorativne pravde i terapeutske jurisprudencije. Indija je već ranije razvila politiku terapeutskog kažnjavanja kako bi unapredila poštovanje prava optuženog. Ali, savremeni principi terapeutske jurisprudencije još uvek nisu razmatrani u kontekstu restorativnog pristupa slučajevima sajber proganjanja. Stoga se u ovom radu ispituje da li principi restorativne pravde i terapeutske jurisprudencije mogu da zamene retributivne principe u slučajevima viktimizacije sajber proganjanjem. Takođe, u radu se analiziraju odredbe indijskog zakonodavstva o sajber proganjanju iz ugla restorativne pravde i terapeutske jurisprudencije, kako bi se procenila njegova efikasnost posmatrano iz ugla žrtve.

Ključne reči: sajber proganjanje, restorativna pravda, terapeutska jurisprudencija, viktimizacija žena.