Page 2871 - 2883 **DOI:** *https://doij.org/10.10000/IJLMH.11813*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 4 | Issue 3

2021

Changing Paradigms of Victimization in Cybercrimes: An Analysis

RADHIKA MAHESHWARI[1]

ABSTRACT

In the 21st century, 'Internet' is our mantra for survival, more so at a time when our country is progressing towards the motto of "Digital India". The increase in the number of internet users has catalysed the darker side of internet usage. This 'darker side' is associated with crimes that the cyber space facilitates and harbours. The anonymity of the internet has impelled the offenders, strangers and friends alike, to trap people into a web of online victimization. Against this backdrop, the author has attempted to analyse the nature of victimization on the internet in relation to different theories, and thereafter, bring to forefront the issues and challenges that our legislative regime faces in reference to cyber offending.

Keywords: *victimization, cybercrimes, victimology.*

I. INTRODUCTION

The cynosure of this research paper pertains to the different facets of victimization in the digital arena. The paper unravels the contours of cybercrime victimization in India with the relevant theories and supporting reasons for the causes of internet crimes. As shall also be discussed in the subsequent sections, the scope of this paper is specifically restricted to cyber offences against the body and mind. Economic cyber offences the subject matter of which is usually tangible or intangible property, are categorically excluded from the ambit of this paper.

(A) Method of Study

The research methodology pursued by the author was an amalgamation of qualitative and quantitative data, with the infusion of an analysis from both primary and secondary sources. As a part of this research paper, a Survey was conducted by the author in order to analyse the trends in, and frequency of cases of offline sexual harassment and of cyber offences, particularly cyber stalking, cyber sexual abuse and harassment. The method of collection of data was through a questionnaire that was filled by the respondents through google forms. Majority of the respondents are college-going students from inter-disciplinary backgrounds.

[1] Author is a student at Bennett University, India.

 [ISSN 2581-5369]

The sample comprised a total of 61 respondents (n=61), out of which 41 were females and 20 were males. The age of the respondents majorly varied between 19-25, with one respondent being above 25 years. The Survey results have been used to supplement the theoretical postulations that have been analysed and put forth in this research paper by the author.

(B) Chapterization

The paper comprises a total of five chapters- Chapter I provides a general outline of the cyber offences in India. Chapter II deals with the scope of victimization in cyber space and why it is different in its form from victimization in traditional offending. The two sub-chapters under Chapter II delve into the causes behind the internet serving as a potential space for victimization and the impact caused to victims of cybercrimes, respectively. Chapter III pertains to how the already established victimological theories provide a skeletal structure for understanding cybercrimes in addition to new typologies factorizing cyber-victim characteristics. In Chapter IV that is divided into four sub-chapters, the author has provided a detailed analysis of the current legislations relating to cyber offences, and the ambiguities that prevail therein. Lastly, Chapter V proffers the concluding remarks on the issues discussed by the author.

II. CYBER-CRIMES IN INDIA: AN INSIGHT

Cybercrimes are offences that are committed through the use of a computer, mobile phone or a networked device. In other words, these are crimes that are perpetuated in the digital space over an internet connection. They can be clubbed into offences against property (primarily economic offences) and offences against the body/mind. The former includes crimes like cyber extortion, phishing, cyber frauds like credit card thefts, hacking of data, online piracy, while the latter includes offences like cyber bullying, cyber sexual harassment, cyber stalking, cyber defamation, and online child pornography, among others. The primary legislations which deal with cyber offences in India are the Information Technology Act, ("**IT Act**") and the Indian Penal Code, 1860, ("**IPC**"). The increase in the number of internet users in the country has been rapid, especially with the advent of Covid-19 which has invariably compelled almost every person to resort to the use of internet. The year 2020 saw nearly 700 million internet users[2] in India, which was a big jump from 493 million users in the year 2018,[3] and statistics show that these figures will only surge in the near future. The National Crime Records Bureau Data ("**NCRB**") for the year 2019 shows that about a total of 2,266 cases of cyber sexual

[2] Sandhya Keelery, *Number of Internet Users in India from 2015 to 2020 with a forecast until 2025*, STATISTA 2021, (Oct 16, 2020), https://www.statista.com/statistics/255146/number-of-internet-users-in-india/
[3] Id.

 [ISSN 2581-5369]

exploitation were registered during that year.[4] The actual numbers would unarguably be higher than the given statistics as a large number of cases of sexual abuse go unreported on account of various reasons. To give an example, in the Survey conducted by the author, out of the 61 respondents, 27 females and 6 males (about 53.1% in total) had been sexually harassed at some point of time. However, quite surprisingly, none of these incidences were reported to the police- 6.6% of them did not report because the abuser was a family member; 1.6% did not report because of the fear of consequences in terms of family reputation; 13.1% did not report because they were hesitant to do so due to other reasons, whereas, 34.4% did not give a reason for not reporting the abuse. These statistics can be used to perceive how cases are under-reported in large numbers when it comes to sexual abuse and exploitation, and a similar approach may also be adopted for understanding the scenario in case of cyber-crimes. In a research study conducted by CRY amongst adolescents in NCR, about 50 % of cyber bullying cases, and about 55.6% of morphed images cases went unreported.[5] While children and women remain the most vulnerable groups in respect of cyber offending in India, the internet has also taken a toll on men, trans men/women, and people from other gender groups.

III. RE-DEFINING VICTIMIZATION IN CYBER CRIMES

A 'victim' can be defined as a person who suffers any physical, emotional, mental, psychological or financial harm or injury as a result of an act or omission by another person that violates the law.[6] Victimization may be referred to as the process which includes the act or series of acts that cause harm to a person. Traditionally, victimological studies were conducted from the standpoint of the offender rather than the victim for analysing the crime patterns and the reasons for commission of crimes.[7] It was after World War II that the focus of victimologists shifted towards the people who were actually affected by the crimes.

The internet has essentially changed the manner in which offences are now committed. Over centuries, crimes were known to take place in a physical setting, whereby the offender and the victim are face to face with each other, or at least within a certain proximal distance with one another. However, this requirement of physical proximity is no longer true for offences that

[4] *Crime in India, 2019*, Statistics published by National Crime Records Bureau (Ministry of Home Affairs), (2019), xiv, See also pages 206-210 for specific category of cyber offences and corresponding statistics.
[5] Child Rights and You (CRY), *"Online Safety and Internet Connection- A study conducted amongst adolescents in Delhi-NCR*, 52-60, (Feb 2020), https://www.cry.org/wp-content/uploads/2020/02/Online-Safety-and-Internet-Addiction-p.pdf.
[6] United Nations Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power, 1985, Art 1.
[7] See generally Chapter titled 'Victimization' in ENCYCLOPEDIA OF QUALITY OF LIFE AND WELL-BEING RESEARCH by MARIA GIUSEPPINA MURATORE, 296-297 (Alex C. Michalos ed., Springer, Dordrecht), (2014).

take place over the internet. Consequentially, the nature of victimization in relation to cybercrimes also differs from the traditional notion of victimization. The renowned criminologist Prof. Jaishankar Karuppannan, in the book titled "An International Perspective on Contemporary Developments in Victimology", emphasized on the need to create a sub-discipline of Victimology altogether, i.e., *Cyber Victimology*. The reason quoted by him for this was that "cybercrime victimization is a *novel* form of victimization, and, cyber victimology would be directed in understanding internet crimes purely from the victim's perspective"[8] as opposed to the previously followed trends in case of traditional offences, whereby the State's interest was given pivotal importance. One of the most important factors that distinguishes and in fact renders cyber victimization highly treacherous is that in crimes that take place wholly in a physical setting, the victim often knows the offender.[9] However, in crimes that are committed with the internet as a medium, the offender is often not previously known to the victim. The circumstantial background preceding the actual offence in internet crimes is therefore, very different from that of traditional crimes. A second factor for taking a dynamic approach towards cyber victimization is that in many instances the victims endure the agony of both cyber offending and traditional offending from the same perpetrator- this is seen in cases whereby the offender uses social media networking to lure and persuade the victim, and subsequently sexually abuses/kidnaps/cheats/or murders the victim when they meet offline.[10]

Hence, the contours of cyber victimization require to be perceived from a different angle than the traditional notion of victimization. *Inter-personal cyber victimization* is a new typology that refers to acts committed against individual persons through the use of online communication mediums that may threaten, distress, harass, torment, or exploit the victim, often taking the form of violent crimes.[11]

(A) Cyber space as a Breeding Ground for Victims: Causes and Reasons

There persist certain factors that incentivise offenders to commit crimes under the covers of the internet. The '*Space Transition Theory*'[12] is one such development in the arena of cyber

[8] JAISHANKAR KARUPPANNAN, *Cyber Victimology: A New Sub-Discipline of the Twenty-First Century Victimology*, in AN INTERNATIONAL PERSPECTIVE ON CONTEMPORARY DEVELOPMENTS IN VICTIMOLOGY 3-19 (Joseph J., Jergenson S. eds.), (2020).

[9] The Survey results revealed that out of the 54.1% of the victims of sexual harassment, in 37.7% cases the offender was a known person to the victim, whereas 21.3% of them were harassed by strangers.

[10] See Pranav Kumar, *Priya Seth: Meet the Lady who killed her tinder date and cheated thousands*, VOXSPACE (July 7, 2018), https://www.voxspace.in/2018/07/07/priya-seth/

[11] See generally BILLY HENSON et al., *Cybercrime Victimization* in THE WILEY HANDBOOK ON PSYCHOLOGY OF VIOLENCE 553-570, (2016).

[12] JAISHANKAR KARUPPANNAN, *Space transition Theory of Cybercrimes*, in CRIMES OF THE INTERNET, (Frank Schmalleger & Michael Pittaro eds., Prentice Hall) 283-301, (2008); See generally JAISHANKAR KARUPPANNAN, *Establishing a Theory of Cyber Crimes*, International Journal of Cyber Criminology, 1 Issue 2, 7-9, (July 2007).

 [ISSN 2581-5369]

criminology that explains the causation of crimes on the internet may be perused to further one's understanding of cyber victimology. As per this theory, the behaviour of people is subject to change when they transition from the physical space to cyber space and vice-versa. *Differential behaviour of persons in varying spaces* is therefore a factor on which this theory is pre-supposed and postulated. The elements of this theory are: *firstly,* the digital space provides great scope for anonymity of persons, meaning thereby the offender can flexibly modify or hide his real identity in order to entice the victims. The strategy of anonymity is to some degree manoeuvred in this manner- the offender befriends the victim via social media-platforms like Facebook/Instagram, builds a certain connection with the victim, and eventually traps the victim in a web of abuse. For instance, in a recent case a 32-year-old man was found to have lured minor girls online on the premise that he was a rich businessman, and then subsequently sexually exploiting and blackmailing them with their compromised pictures.[13] The modus operandi followed by the offender in such cases often begins with an anonymous identity. *Secondly,* the nature of cyber space gives the offender more power and authority, that he/she otherwise wouldn't have offline. This, accompanied with the lack of a deterrent factor on the internet increases the propensity of a person to commit crimes virtually.

Therefore, from a theoretical viewpoint, the Space Transition Theory well explains the reasons as to why the internet serves as a breeding ground for the perpetuation of crimes and resultantly for increase in the number of victims. From a practical standpoint, cyber victimization can be attributed to other factors that propagate victimization. The usage of social media has taken the form of a 'norm' rather than a 'need' to use it. While there are legitimate reasons and purposes to the use of social media, it is often used merely because of the prevalence of peer pressure. The novel trend is such that children are often bullied or teased in school for *not using* a certain type of social media platform. It is also seen that people who are not on social media platforms like Instagram, Tinder, Facebook are often looked down upon or outclassed- this is especially prevalent amongst school children who often end up being victims of cyber bullying and harassment. Therefore, there is a certain negative *social facilitation* that can be associated with internet offences and victimization thereafter.

[13] Sunitha Rao R., *Man befriends minor girls on Instagram, sexually exploits them,* TIMES NOW NEWS, (April 8, 2021), https://timesofindia.indiatimes.com/city/bengaluru/bengaluru-man-befriends-minor-girls-on-instagram-sexually-exploits-them/articleshow/81965301.cms. See also Chayyanika Nigam, *Delhi schoolkids increasingly coming under attack from cyber bullies*, INDIA TODAY, (May 12, 2017), whereby the author writes about a Survey carried out by the Delhi Police The findings of the survey indicated that nearly 60% of the capital's school kids using social media faced the risk of cyberbullying that often led to serious crimes like rape and molestation, https://www.indiatoday.in/mail-today/story/delhi-schoolkids-increasingly-coming-under-attacks-by-cyber-bullies-976595-2017-05-12.

 [ISSN 2581-5369]

(B) The Impact of Harm on Victims of Cybercrimes

While the harm suffered by victims may be physical, emotional, or financial, this section particularly delineates the impact of emotional and psychological harm that victims face. In certain cases, the cybercrimes that are initiated virtually on the internet often end up with the victim being raped, murdered, or sexually harassed in the physical space. In these instances of cybercrimes, the impact and harm suffered by the victim is both physical and mental. For cyber offences take place without any physical contact between the offender and the victim (like cyber stalking, bullying, defamation), there may or may not be a physical harm in the real sense that may be caused to the victim. In such cases the crime event does have a total bearing on the mind of the victim. Since the likelihood of physical proximity in the offences taking place wholly in the digital space is almost nil, the victim is entirely subdued within an emotional bracket. One of the factors that increases the severity of the harm faced by cybercrime victims is due to the infinite scale on which the harm is propelled, i.e., the extent of circulation over the internet. In a matter of seconds over a hundred thousand people may be able to view the hurtful/embarrassing comments or pictures of the victim on the internet, a factor that is absent in cases of traditional crimes. It is often seen that victimization on the internet happens in subtle ways that evolves with time, especially amongst children who fail do perceive that they are in fact trapped in a web of cyber abuse. The Survey report also depicted that 54.1% of the respondents found it safer to talk to people through offline modes as compared online mediums, whereas only 19.7% respondents found online modes to be safer than offline modes. Resultantly, the magnitude of victimization is inevitably high in cyber offences.

The idea is not to categorize cyber offences as more dangerous or severe than offences committed in a physical space, but only to emphasize the importance of the fact that cybercrimes are equally harmful and deteriorating in terms of their impact on the victim, regardless of the degree of remoteness with which they are committed.

In various case studies[14] conducted by *Cyber Bullying, Awareness, Action & Prevention ("**Cyber B.A.A.P**.")*, it was revealed that the victims of cyber bullying, sextortion and online sexual abuse that were counselled by them showed drastic symptoms of behavioural changes that included social withdrawal from activities, feelings of anger towards family members, anxiety, depression, fear and shock, among others. In one instance, a 13-year-old fell prey to cyber bullying due to the posting of a picture on Instagram that attracted several nasty

[14] Case Studies conducted by *Cyber Bullying, Awareness, Action & Prevention ("Cyber B.A.A.P.")*, https://cyberbaap.org/case-studies/

 [ISSN 2581-5369]

comments, thus making her a subject of ridicule and mockery.[15] The victim had to attend counselling sessions for over five months due to extreme social withdrawal on her part. What may initially begin as a harmless teasing may consequently turn into internet shaming. Another study analysing victims of online sexual exploitation depicted that many of them portrayed similar mental health issues as those who were victims of physical or offline abuse, while a few of them were diagnosed for a lifelong post-traumatic stress disorder.[16] There are other instances whereby victims of persistent blackmailing for leaking of intimate images, of online harassment and sexual abuse have committed suicide[17] due to fear of social repercussions and mental agony following the offences. The news portals are replete with such cases that are only multiplying on an everyday basis.

Accordingly, an evaluation of the harm caused to cybercrime victims becomes pertinent in order to assess the kind of treatment to be given to the victim, the quantum of compensation, victim-specific concerns, the method of counselling and confrontation. For this, the victimization of persons must be perceived as a *"process"* rather than a single or series or *"events"* that took place. In this regard, there are four stages that form a part of the victimization process- "the pre-victimization stage; actual victimization; protection and transition, resolution and reorganization of the victim."[18] The psychological impact caused by actual victimization has to be healed and minimised in the protection stage. The specific psychological and emotional needs of cybercrime victims need to be assessed on a continuous basis with regular counselling and support until they are finally re-organized into the society. Several NGOs and Centres (like Cyber B.A.A.P., Cyber Peace Foundation, Centre for Cyber Victim Counselling etc.) are specifically engaged in providing relief measures and services to cybercrime victims in addition to sensitising the vulnerable groups prone to being victimized.

IV. APPLICABILITY OF VICTIMOLOGICAL THEORIES TO CYBER-CRIMES: OLD & NEW PERSPECTIVES

The 20th century saw the emergence of several theories like *positivist victimology* postulated by Hans Von Hentig and Benjamin Mendelsohn that primarily concentrated on victim

[15] *Id.*
[16] Billy Henson, *supra* note 11, at 567.
[17] See HM Chaitanya Swamy, *IAS aspirant blackmailed over 'nude videos' ends life*, DECCAN HERALD, (April 8, 2021, 12:57 am), https://www.deccanherald.com/city/bengaluru-crime/ias-aspirant-blackmailed-over-nude-videos-ends-life-971726.html; See also *Boys Locker Room case: Girl to face trial for abetment to suicide for 17-year-old boy's death*, Times Now News, (March 25, 2021, 9:22 am), https://www.timesnownews.com/delhi/article/bois-locker-room-case-girl-to-face-trial-for-abetment-to-suicide-over-17-year-old-boys-death/736906
[18] JAMES K. HILL, *Victims' Response to Trauma and Implications for Interventions: A Selected Review and Synthesis of the Literature*, Policy Centre for Victims Issues- Research and Statistics Division, 3-5, (Nov 2003).

culpability in respect of the crime committed, and developed victim categories who were more prone to being victimized. Fattah's victim typology scheme depicted the role of victims in crimes in terms of characteristics and behaviours. Whereas, *critical victimology* propounded by Mawby and Walklate critiqued the concept of victim precipitation and put forth a more holistic model that took into account the societal structure and inequalities that dictate individual actions leading to crimes. The question now arises that can these theories which were primarily developed by surveying predatory crimes like robbery and murder, also be applicable for understanding internet victimization and offending- *not necessarily so*. One of the primary reasons being that cybercrime offending no longer requires the physical convergence of time and space[19] of the victims and perpetrators, one of the factors on which the paramountcy of the theories was premised.

Due to the change in the context and nature of cyber offending as compared to traditional offending, different risk factors may be associated with the victims that may make them more prone to being victimised in the digital world. The *Routine Activities Theory* identifies *continuous online activity* like the use of e-mail/social media as a risk factor that enables digital convergence and hence "increases the individual risk of inter-personal victimization such as sexual abuse and harassment."[20] Certain activities like greater association with people online who engage in harassing others, sharing personal information with strangers on social media, regular online shopping etc., are some of the activities that are likely to increase the risk factor for victimization. The Survey that was conducted by the author reflected that about 16.4% of the respondents had shared their personal information, including pictures through online platforms with people they never knew offline. Sharing information with strangers may be termed as a typology or a victim-trait that may make a person more prone to being victimized.

Another identified risk factor is the *low self-control* of persons when it comes to the use of internet. As per a Study[21] conducted, the "low self-control" factor was measured in reference to certain independent variables like prudence, fairness, fearfulness, flexibility, social self-esteem, patience and inquisitiveness, among others,[22] that indicated *inter alia* a high risk of being victimized online, especially if the person possessed more IT skills. While these results

[19] LORRAINE WOLHUTER, et al, VICTIMOLOGY: VICTIMIZATION AND VICTIM RIGHTS, Chapter 2, (1st edn.) 15, (2008). See also "Routine-Activity Theory" by Cohen and Felson, page 589.

[20] Thomas J. Holt & Adam M. Bossler, CYBERCRIME IN PROGRESS- THEORY AND PREVENTION OF TECHNOLOGY-ENABLED OFFENCES, (Routledge- Taylor & Francis Group), (2016). See generally BILLY HENSON, *Routine Activities- The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 469-489, (2020).

[21] MARLEEN WEULEN KRANENBARG, et al., *Offending and Victimization in the Digital Age: Comparing Correlates of Cybercrime and Traditional Offending-Only, Victimization-Only and the Victimization-Offending Overlap*, (Taylor & Francis Online) 40 Issue 1, 40-55, (2019).

[22] *Id.*

cannot be generalised due to differences in social demographics, they definitely provide a new direction and scope for further studies in cyber victimization.

From the above discussion, it can well be argued that while the outer fabric and model of the victim theories/typology may remain the same in respect of cybercrimes, their content has to be perceived in a different context than that of traditional victimization. For instance, the Routine Activities Theory now being used to analyse daily-routine activities as a factor for cyber victimization, was initially developed by Cohen and Felson and later by Fattah in respect of traditional crimes. However, one anomaly that can be culled out from the risk-factors stated above is that they hint towards victim precipitation or victim-blaming to a certain extent- whether in reference to the excessive use of social media or sharing information with unknown persons online, and delineate why certain persons serve as potential targets of online crimes. This may in effect negate the entire idea of a pro-victim approach in contemporary times, whereby efforts are being directed towards formulating a victim-friendly justice system.

V. THE EXISTING LEGAL FRAMEWORK FOR CYBERCRIMES: AN ANALYSIS

The laws pertaining to cybercrime regime in India are seemingly inadequate and deficient. Our country lacks a comprehensive cyber legislation that specifically caters to offences taking place online, whether wholly or partially. Even the IT Act and the Indian Penal Code that contain certain provisions for online sexual offences are replete with loopholes, as will be discussed below.

(A) Lack of Gender-neutrality: A glaring Defect

One of the primary drawbacks in the existing laws is the absence of gender neutrality that is reflected under various sections. For instance, Sections 354C and 354D of the IPC, that pertain to the offences of capturing/disseminating images of a woman's private parts,[23] and stalking a woman on the internet,[24] respectively- these provisions penalise a man for committing the offences of said nature against a woman, but not vice versa. Males, as victims of sexual abuse and rape is a ground reality, though they often go unreported due to societal stigma and even the absence of any laws on the same. In this regard, it may also be pertinent to highlight forthwith the Survey report conducted by the author. Out of the 20 male respondents, about 8 of them had at some point of time been stalked by another person on social media to an extent that they felt threatened or distressed about it. Whereas, about 10 of the male respondents had been victims of online harassment which included inter alia the posting of hurtful/embarrassing

[23] Indian Penal Code, 1860, (Act No. 45 of 1860), § 354C.
[24] Indian Penal Code, 1860, (Act No. 45 of 1860), § 354D.

 [ISSN 2581-5369]

comments, information or rumours about them whether publicly on social media or privately via chat rooms. Further, about 31.1% of the respondents knew of a male friend/family member who was either bullied or abused in some form over social media. Numbers like 8 and 10, though small due to the limited scope of the survey cannot be seen with a blind eye. The figures of male victims of cyber abuse and harassment at the national level will most certainly be alarming, and require redressal through the creation of gender-neutral cyber laws.

(B) Incongruency between Sections 66E, 67 & 67A of the IT Act, 2000

Section 66E of the IT Act, 2000, criminalises the act of capturing, publishing or transmitting images of private areas of any person *without his/her consent*.[25] Whereas, Sections 67 and 67A make punishable the act of transmitting or publishing obscene material and sexually explicit act respectively, over the internet, whether with or without the person's consent.[26] While Sections 67 and 67A penalise the consensual as well as non-consensual transmission or publication of sexual images in the cyberspace, Section 66E penalises only the non-censual transmission of the images. There is a patent conflict in terms of consent between these provisions despite the subject matter of these sections which is practically the same. This essentially implies that the perpetrator may escape liability under Section 66E if it is proven that the victim had given consent for the taking and posting of her private images, while the same act may be rendered punishable under the other two sections.

(C) Sexting and the Law- The controversies that emerge

The word "sexting" is currently undefined under the Indian law. In layman terms, it can be defined as the "action or practice of sending sexually explicit photographs or messages via mobile phone."[27] In the Survey conducted, about 12.3% of the respondents agreed to sharing their nude photos with another person via the online platform. Sexting in India is a social reality that people resort to for expressing sexual intimacy by using internet as a medium. The legality of sexting however, is a gray area and a rather controversial one. The exchange of intimate images/videos between minors or between a minor and an adult whether with or without consent may take the form of child pornography and is punishable under Section 67B of the IT Act, 2000, and other provisions of POCSO Act, 2012.[28] Further, Section 66E makes punishable only the non-consensual transmission of sexually explicit images of a person. However, Sections 67 and 67A criminalise *any* transmission of sexual material, whether consensual or

[25] Information Technology Act, 2000, (Act No. 21 of 2000), § 66E.
[26] Information Technology Act, 2000, (Act No. 21 of 2000), § 67 and § 67A.
[27] Lexico (Oxford University Press) definition of "sexting", https://www.lexico.com/definition/sexting
[28] Information Technology Act, 2000, (Act No. 21 of 2000), § 67B, see also Sections 13, 14 and 15 of Prevention of Children from Sexual Offences Act, 2012 (POCSO).

 [ISSN 2581-5369]

otherwise. While Section 66E reasonably renders the non-consensual transmission as an offence, is the latter two provisions that activate controversies when it comes to sexting on account of criminalization of even consensual transmission and exchange of sexual images.

Sexting, when taking place between two "consenting adults" undeniably harms no third person or even the sender and receiver themselves, because the images and texts are exchanged in private chats and there is no 'public transmission' or publication on the internet of those images. Therefore, it can essentially be termed as a ***victimless crime***, whereby no harm or injury is caused to the persons who are privately engaged the said act. Criminalization of consensual adult sexting is a blow to the freedom of expression and also invades with the privacy of the adults in question. Consensual sexual intercourse between two adults in physical space is not an offence under law. A logical corollary to this would imply that the same acts taking place online through private chats should not be criminalized either.

Notwithstanding the argument regarding the freedom of sharing intimate images between consenting adults, it is pertinent to bring to light the downside of the standpoint taken above, that is majorly premised on the *misuse* of sexting. A consensual transmission of sexual images might often lead to an array of other cybercrimes like sextortion, cyber bullying and revenge porn,[29] whereby the receiver of those images leaks them or threatens to leak them to third parties either to extort more such images from the primary sender or even to get back at him/her. This creates a *victim-offender dichotomy*, whereby the primary sender who caused the images to be transmitted is labelled as an offender (though he/she is a victim of the secondary transmission) for causing the transmission in the first place. The complexities that may arise out of such issues require the legal contours of sexting to be set firm by directly incorporating it within the legislative framework, keeping in view the right to privacy and freedom of expression of persons, and the reasonable restrictions paralleling them.

(D) Detecting Crimes and Tracing Offenders in Cybercrimes: Gaps in the present law

Independent Cyber Crime Cells in every State are currently absent in our country. The Cyber Crime Investigation Cell operating under the CBI deals with the menace of online crimes nationally. Nevertheless, it is essential to open up these Cells in every State in order to effectively detect cyber criminals and trace them. Recently, an advisory was issued by the Madhya Pradesh Cyber Crime Cell against online video calling with unknown people on

[29] See Kimberley O'Connor, et al., *Sexting Legislation in the United States and Abroad: A Call for Uniformity*, International Journal of Cyber Criminology, 11 Issue 2, (Dec 2017); The article extensively dealt with the complex issues that arise in cases of sexting and the subsequent charging of offenders under the law.

 [ISSN 2581-5369]

account of about 200 people being honey-trapped for sharing of intimate images.[30] The taking of cognizance and pro-active measures for the issue is certainly a welcome step. However, there has to be some uniformity in action at the national level for addressing the gaps currently present. This can most certainly be done by establishing Cyber Crime Cells in all States/UTs in pursuance of protocols to be applied uniformly across the country, in addition to State-specific needs that may be present. Additionally, the law enforcement agencies face a challenge in terms of levelling-up with the new technology when it comes to tracing the offenders.

Yet another anomaly under the existing law is that the offence of cyber bullying has not been formally defined in any statute. Further, the offence of cyber stalking may be prosecuted under Section 354D of the IPC but is missing under the IT Act. Similarly, specific provisions for cyber defamation and online sexual harassment are also missing in the Act. With the increasing number of cybercrimes, it becomes pertinent to have specific laws for such offences, because in their absence the reporting and detection of offenders is ultimately defeated. In the case of ***Shibani Barik v. State of Odisha,***[31] the whereby the Orissa High Court specifically observed that-

> "*the IT Act, 2000, does impose an obligation upon such companies to take down content and exercise due diligence before uploading any content, but India lacks a specialized law to address the crime like cyber bullying. Another grim scenario often comes the fore is the traditional approach of the investigative machinery while dealing with such type of offences. Most of our investigating officers are neither well trained nor do they understand the nuances of cybercrime. It is imperative that the personnel engaged in investigation need to be imparted periodical training so as to upgrade their skill to investigate this kind of techno-legal issues. Further, improvement in the cyber intelligence, cyber forensics and cyber prosecution training are long overdue to boost the hitherto rickety cyber policing."*[32]

The above-quoted judgement precisely sums up the lacunae prevalent in the legislative framework. The pressing concerns relating to cybercrimes either require a substantial overhaul of the IT Act, 2000, in order to cope with recent trends in online predator behaviour, victim-specific needs and technical advancements, or, the creation of a new legislation altogether that

[30] The Free Press Journal, *MP Cyber Police advise against chatting with unknown person*, (March 30, 2021), https://www.freepressjournal.in/bhopal/honeytrap-madhya-pradesh-cyber-police-advise-against-video-chatting-with-unknown-person.
[31] Shibani Barik v. State of Odisha, 2020 (212) AIC 871.
[32] *Id*, para 11-12.

would specifically deal with cyber offences, the procedure of enforcement, collection of evidence and punishment thereafter.

VI. CONCLUSION

To conclude, the author opines that the seamless nature of the internet and the crimes being committed through its use has brought about a dire need to analyse cybercrimes differently from other crimes. The advent of internet is an irreversible phenomenon that has deeply penetrated every section of the society. The criminal opportunities in the digital space are accordingly on the rise. The permanent nature of the internet has the potential to alleviate the psychological impact of the cybercrime victims, because unlike human memory, data storage on the internet almost takes a perennial form. Since the scope of this paper was only restricted to the aspect of cyber victimization and parallel laws, the means and measures of protecting such victims were not specifically discussed. It is nevertheless crucial to identify the rights that victims of cyber offences have, particularly victims of sexual crimes. The Right to be Forgotten under the Personal Data Protection Bill, 2019, is one such right that may be availed by victims especially in cases of cyber defamation, of images posted online in furtherance of voyeurism, or abusive comments, whereby the victims may request the social media intermediaries or websites to remove the content from the internet. The Bill however, is yet to be passed. Apart from this, in light of the anomalies in the current laws as discussed in the paper, the exigency to bring about timely modifications in them cannot be stressed upon enough. Most pertinently, changes in the law must be in furtherance of the theories and factors that can be associated with cyber offending and victimization. In addition to filling the gaps, the law must provide for future contingencies in respect of cybercrimes that are currently ascertainable. We are not required to await another Nirbhaya victim in order to trigger the requisite amendments. Therefore, the author suggests that the cybercrime regime in India must be dealt with utmost pensiveness by the legislature at the earliest in order to address the gaps and challenges.

*****

 [ISSN 2581-5369]