

Securing Justice to Victims of Crime Victimization in the Digital Environment

Neelam Yadav*

Abstract

“Every saint has a past, every criminal has a future”

Rights of the victim are the essential part of the Criminal Justice Administration. The 21st century has been defined by significant advancements in technology that have influenced the ways in which individuals engage with one another. The global digital age has enabled social, political, and economic aspects of human existence to be more easily facilitated. The web is usually described as an exquisite tool, an enticing place and a liberating experience. However, we must question: for whom? The usage of electronic devices has rapidly increased across all demographics. These changes have caused crime, particularly cybercrime, to significantly increase. The number of criminals who are adept at using the internet to commit crimes is expanding, and there is a chance that many people will fall victim to them. Technology development has led to an increase in the sophistication and complexity of crime, as well as a significant shift in how people view the world. Though crime against women is on an increase altogether fields being a victim of cybercrime may well be most traumatic experience for a women. The Indian parliament passed the Information Technology Act of 2000 with the aim of regulating cybercrime and safeguarding the technological infrastructure. It absolutely was the primary global law of India to deal penalties and punishments regarding digital crimes. Although research on cybercrime victimisation is relatively diverse, no bibliometric study has been found to introduce the landscape of this subject. Furthermore, the purpose of this research is to identify global collaborations and current gaps in cybercrime victimisation research. Through statistical evidence and visual findings, this study contributed a summary of the scholarly status of cybercrime victimisation.

Keywords: Cybercrime, cybercrime victimization, bibliometric analysis, technology, administration

INTRODUCTION

No doubt, the invention of computers and moreover, the invention of world wide web also known as Internet has been single greatest invention of 21st century. Almost every walk of our life has been affected with the emergence of Internet. Emergence of Internet has revolutionized the communication modes. Our lives have become entwined with the computers and Internet so much that in today's world, it is hard to imagine our lives without the internet or computers. Even the 2-year old child who does not know how to speak but knows how to navigate through videos on YouTube. Internet, has the potential to change our way of thinking about anything existing in the world and it is even doing that also. Various scientific experiments keep proving the same very often.

*Author for Correspondence

Neelam Yadav
E-mail: neelamydv@hotmail.com

Student, Department of Law, Maharshi Dayanand University,
Haryana, India

Received Date: November 04, 2022

Accepted Date: March 22, 2023

Published Date: April 05, 2023

Citation: Neelam Yadav. Securing justice to victims of crime victimization in the digital environment. National Journal of Cyber Security Law. 2023; 6(1): 32–38p.

Aforesaid being the reality, there are always two sides of a coin. The one side which is useful to mankind, however, there is another dark side, wherein, the same technology of Internet and computer are being used as a means to commit crimes. The anti-social elements are using the Internet to their advantage for committing offenses against the

innocent persons. Evidently, Internet has affected everything. It has faded the boundaries between Nations, changed the Government policies, changed the traditional warfare, took the medicines, treatments of diseases, injuries to an entire new level. Internet is not only revolutionizing, exciting, and helpful but it is also challenging, dark, unruly and incomprehensible and frightening. It is an established fact that, nowadays, almost all the electronic devices including computers, tablets, smartphones, watches etc. are internet enabled therefore, any man with a sinister intention could bring any nation or part of it to a halt or could disrupt the normal functioning of administrative system. Considering the dark side of internet, a new kind of crime has flourished and emerged. This is known as cybercrime. It includes under its ambit child pornography, software pirating, hacking, ransomware attacks, phishing, identity theft, bullying, spreading hate, cyber-stalking, etc. Combating the cybercrimes through laws is also an altogether different issue since this technology is fast-moving and very dynamic.

CYBER-CRIME AND VICTIMS OF CYBER CRIME: EXPLAINED

Cyber-Crime

The world has not always dealt with cybercrime since it is a recent phenomenon, therefore classical treaties for guidance are not available for ready reference. Recently, though some scholars have attempted to put the definition of cybercrime into words but there is none which is universally acceptable. Pertinently, in the Indian context, even though the word "cybercrime" has not been defined by any Act or legislation passed by Indian Parliament, it has been judicially interpreted in some judgements pronounced by Indian Courts of law. Typically, it is either the computer which is the intended victim of the crime or the computer which is employed in the commission of crime [1].

The scholars such as *Halder* and *Jaishankar* define cybercrimes as: Cybercrimes may be defined as "Offenses that are committed against individuals or groups of individuals with a criminal motive to intentionally damage the victim's reputation or cause the victim physical harm or emotional distress, or loss, directly or indirectly, using modern telecommunication networks such as the Internet (networks including but not limited to Chat rooms, emails, notice boards and groups) and mobile phones [2] (Bluetooth/SMS/MMS)"

We do not have any precise definition of cybercrime; however, following are the general definitions of term cybercrime:

According to the Oxford Dictionary, cybercrime refers to illegal activities that are conducted using computers or the internet. Cybercrime can be considered a subcategory of traditional crimes, where either the computer is the target or the perpetrator of the criminal act.

"Cybercrime refers to any criminal or other offence that is facilitated or involves the use of electronic communications or information systems, such as any device or the Internet, or any combination of them [3]."

Some other definitions include as: Cybercrime can be defined as any illegal behaviour that occurs on or through a computer, the internet, or any piece of technology recognized under the Information Technology Act. If we use a broader definition, we may say that cybercrime is any illicit conduct that uses a computer or the internet as a tool, a target, or both. Also, if a conventional crime is carried out via a computer or the Internet, it could also be considered a cybercrime [4].

Victims of Cyber Crime

The cyber victimization can be understood to mean in general terms as the experiencing of hostile actions while utilizing information and communication technology platforms including the internet, game consoles, and cell-phones [5]. Being the target of harmful online behaviours, such as harassing messages, derogatory comments, and/or embarrassing images, is one other aspect of cyber victimization. The worst of these are threats, innuendos, and blackmail. Studies have found that persons with physical

disabilities, intellectual disabilities, and chronic illnesses were the targets of cyberbullies who also caused depressive symptoms, anxiety, discomfort, somatic health issues, and self-harm. It is possible that even those who engage in cyberbullying struggle with social context, psychosomatic issues, and heightened emotional dysregulation [6].

Tragically, India had the 4th-highest number of cybercrime victims in the year 2021, according to a study by the Federal Bureau of Investigation in the United States (FBI). According to the aforesaid report, India ranked 4th with 3,131 victims of cybercrime, only behind the US, the UK, and Canada. The UK had 3.03 lakh casualties, compared to Canada's 5,788. With more than 4.66 lakh victims of cybercrime, the US topped the list [7]. Another pertinent statistics states that more than 59% out of the surveyed Indian adults were the victim of cybercrimes in the year 2020–21, as reported by a cyber security software company, Norton LifeLock [8]. Above brought data shows that the monster of cybercrime has spread far and wide clutching a considerable population.

During lockdown and COVID pandemic isolation, daily work, communications, and interactions were hampered and the only method to do daily business was online. Many people used the internet, social media, online dating, and online gaming and streaming for amusement and friendship. The recent COVID pandemic has provided the perfect window of opportunity, for the cybercrimes due the encouragement in work from home and resultantly, increased use of remote working tools. There have been reported cases/incidences, wherein hackers attempted or successfully took advantage of the pandemic itself to compromise person's devices or accounts.

MAJOR CATEGORIES OF CYBER CRIMES

Cyber Terrorism

"Cyber Terrorism" is essentially a fusion of terrorism and cyberspace. Government Police organizations are majorly concerned with such intrusions by the cyber terrorists upon the Government websites, data, or any other information pertaining to the State's security. A cyber terrorist is someone who uses computer-based attacks on computers, networks, or the data they contain to frighten or force a government or an organization to further their own political or social goals. A general definition of cyber terrorism is an act of terrorism carried out via computer or cyberspace resources. Cyber terrorism can affect everyone, including men, women, and children.

In India, the Cyber terrorism is punishable under the Information Technology Act, 2000 and amendment Act 2008, especially, section 66F of the IT Act deals with cyber terrorism and if convicted, the perpetrator may be punished for life imprisonment.

Cyber Pornography

Cyber pornography is the act of producing, displaying, disseminating, importing, or publishing obscene content, particularly material that depicts children having sex with adults. Pornography is a crime that has always been seen as one of the corrupt acts harming people. Customers use the internet to create sex, sexual life, sexual actions, and to orchestrate sexual exercises from a computer screen. There are several websites that display various filthy stuff, including photographs and short animated films, to sound recordings and stories [9].

Under Section 67 of the Information Technology Act, 2000 making, transmitting and distribution of cyber pornography is an offence. However, browsing and viewing online pornography is not punishable. Making, distributing and even browsing online Child Pornography is punishable under cyber laws. Besides the provisions of IT Act, 2000, section 292, 293, 294 of the Indian Penal Code and the Indecent Representation of Women (prohibition) Act, 1986 also deals with the pornographic offenses.

Child Cyber Pornography

Child cyber pornography is one of the contentious issues at the international level. Article 2 of the Optional Protocol defines child pornography as *"any portrayal, by whatever methods, of a child*

occupied with genuine or mimicked expresses sexual exercises or any portrayal of the sexual parts of a kid for principally sexual purposes [10]". Child pornography comprises behaviours like showing sexually explicit images of kids, which exposes these impressionable kids to inappropriate content, physical harassment, and harms their emotional senses. Being helpless and innocent, children need to be protected from the world of evil and dishonest people.

Laws punishing the Child Pornography include IT Act 2000, Indian Penal Code 1860, and The Protection of Child from Sexual Abuses Act, 2012.

Section 67B of the Information Technology Act, 2008 provides punishment for distributing or transmitting of material of youngsters occupied with explicitly express act, making content or advanced pictures or publicizing or advancing such material portraying kids in vulgar or disgusting way, who makes content or computerized pictures, gathers, looks for, peruses, downloads, promotes, advances, trades or disseminates material in any electronic shape, develops, tempts or initiates kids to online association with at least one kid for and on explicitly unequivocal act or in a way that may outrage on the first conviction, a sensible adult on the computer resource shall be punished with imprisonment of either description for a term that may extend to 5 years and a fine that may extend to Rs. 10 lakh, and on the second or subsequent conviction, with imprisonment of either description for a term that may extend to 7 years and a fine that may extend to Rs. 10 lakh. For the purposes of this section, "children" refers to anyone under the age of 18 years.

The Protection of Child from Sexual Abuses Act, 2012 also provides for punishment regarding child pornography. Section 13 to 15 provides for punishment for using a child for pornographic purposes and punishment for storage of pornographic material involving a child.

In *Kamlesh Vaswani v. Union of India* [11], it was held that websites showing child pornography, especially of children between the ages of 14 and 18 years, should be completely outlawed and prohibited.

In this ground breaking decision of Hon'ble Court, *Avinash Bajaj v. State* [12], the operator of the website was detained because of a user's advertising to sell the DPS sex scandal video. Despite the fact that Avinash was detained in accordance with Section 67 of the Information Technology Act, the video was not posted on the digital platform. In response to this case, the Intermediary rules were adopted in 2011, which provide that an intermediary will not be held accountable if they take reasonable steps to guarantee that offensive information is not exposed on their portal [13].

Cyberstalking

Cyber-stalking is the practise of using technology to instil fear or anxiety for another person's safety. Cyberstalking is a pattern of behaviour that occurs repeatedly over time, violates an individual's right to privacy, and creates a sense of fear or intimidation. Cyberstalkers commonly use social media, online databases, search engines, and other digital tools to harass, stalk, and terrorize their victims [14]. Surprisingly, cyberstalking is almost never carried out by a stranger; instead, it is most frequently done by someone the target is close to or works with. The aggressor, for instance, can be an ex-girlfriend or ex-boyfriend, former friend, former coworker, or acquaintance who wishes to possess, dominate, frighten, threaten, or even hurt the other person. They frequently have access to specific private data, accounts, inboxes, or other private knowledge about their target's daily activities, lifestyle, or life decisions [15].

The remedy against the cyber stalking in India has been covered under the two major laws viz., Information technology Act, 2000 and other is Criminal law amendment Act 2013. Basically, section 67 of IT Act, 2000 provides for the punishment for the cyber stalking. However, it is Criminal Law amendment Act 2013 which specifically deals with the offence of Cyber stalking. The said amendment

made several changes in the laws dealing with the offences against the women. One such section is Section 354D of IPC, which states that “*any man who*:

- Contacts and follows a woman or attempts to contact such woman to proselytize personal communication repeatedly despite of being clear indication of disinterest by such woman or;
- Observe the use of a woman over the internet, instant messages, e-mail or any other form of electronic communication is the offence of stalking” [16].

Besides the above, a complaint can also be filed under the section 500 of the Indian Penal Code that deals with defamation. This section can be applied in case of cyber stalking in India if the stalker forges the victim’s personal information to post an obscene message or comment on any electronic media. Section 500 criminalizes publishing any false statement against a person or harming the person’s reputation and provides punishment for any such act with imprisonment up to 2 years, fine or both [17].

Sexting has become a common practise among young children these days, which refers to the practise of sending and receiving sexually explicit and obscene pictures via mobile phone, which is accessible to child pornographers due to the cyber space. Therefore, this sexting must be avoided because anything which is connected to the net is prone to being hacked and misused.

SUGGESTIONS FOR PREVENTING CYBER CRIME

In order to protect the general public from the cybercrimes, it is imperative that there is cooperative collaboration between law enforcement departments, the information technology businesses, internet service providers and the international security organizations. It is always to be kept in mind that the conventional methods of fighting crime are useless against the cybercrimes. Cybercrimes are not limited by the physical boundaries, borders and these crime transcend the national boundaries.

Cybercrimes encompass various types of crimes, as discussed above. Consequently, effective measures are required to prevent and combat these crimes.

Use Strong Passwords

The easiest way of protecting self from the cyber fraud is to always use strong passwords and be very alert while choosing password for social media account, internet banking etc. One must avoid writing down password in piece of paper.

Secured Social Media Ids

In today’s world wherein everyone is on the social media platform (Facebook, Twitter, LinkedIn, Quora, Reels, Shorts, YouTube, etc.), it has become quite easy to fall prey to the perpetrators. One of main reasons is the making social media ids public wherein any stranger gets access to the timeline of individual and there is likelihood of misusing the public photos, videos etc. As a result, make sure to keep your social networking profiles (Facebook, Twitter, YouTube, and so on) private. Ensure to double-check your security settings and exercise caution when sharing information online. Remember that once something is posted on the Internet, it becomes permanent.

Secure your Mobiles, Ipads etc.

Mobile phones are things which are always with us and which often contain several intimate details/information. Since, mobiles are connected to internet, therefore, it is prone to the hacking or vulnerable to the attack of malicious ransomware, viruses. We must exercise extreme caution when downloading apps from the app store. It is also crucial that we keep our operating system of mobile or ipad, tab updated. Mobile phone should always be under lock screen. Otherwise, if you misplace your phone or set it down for a few moments, anyone can access all of your personal information on it. Someone could even install malicious software that uses your GPS to track your every move.

Protect Your Data

In the Indian context, there has been a comprehensive data protection law which has been in practice since 2018. It was recommended by the Justice Srikrishna, ret’d. Subsequently it was reviewed by the

Joint Committee of Parliament also and tabled, thereafter, in the Parliament, in the year 2021. Prior to withdrawal of the said bill by the ruling Government for re-introducing, the Personal Data Protection Bill contemplated a comprehensive legal framework *inter alia*, to regulate the online space, laws relating to data privacy, cyber security, telecom regulations. Therefore, it could be said that Government is taking all the necessary steps for protecting the general public from the cybercrime [18].

Use of Computer with Latest Updates

One should always keep the computer systems updated with the latest software and virus protections software. The manufacturers of the computers keep researching for making our systems more and more safe while online therefore we should not dilly dally in updating our systems and promptly install and update. The main advantage of regular updating of system minimises chances of attacks on the system by the sinister hackers etc.

CONCLUSION AND RECOMMENDATIONS

It is evident that with more individuals becoming active online, there have been even more cases of cyberattacks. This broadly covers the internet users being victims of crimes, stalking, bullying, assault, harassment, and trolling online. Blinded by the business gains, social media websites, and apps promote infinite scrolls for online entertainment in an effort to increase customer engagement, rather these websites, and apps should have some constructive ideas or measures such as resources for psychiatric assistance, offer trauma therapy, and police online material, additionally. Psychological assistance should be given to the victims and witnesses. Actions should go beyond the frequently pointless and distressing demands for justice or responsibility. There should be formulation and promotion of anti-cyber victimisation policies across all digital platforms. Regular impact quizzes and polls to see, and evaluate the impact of these policies. The responsibility of fostering prosocial behaviour should fall on all websites that facilitate online communication.

REFERENCES

1. Cyber Crime and Its Classification. [Online]. <https://www.bbau.ac.in/dept/Law/TM/1.pdf>, accessed on 18.09.2022
2. Debarati Halder, Jaishankar K. (2010). Cyber Victimization in India: A baseline survey report. [Online]. <https://deliverypdf.ssrn.com/delivery.php?ID=735105085006005014090064112001079106120009055009062036075096118085093108127079085094009013096038009044113127093124092100124064031087031066093111006122099022002125125095077054020084083067011069092010104065104085116106030095106001119079107108082073102117&EXT=pdf&INDEX=TRUE>; Accessed on 18.09.2022
3. Cybercrime. Cybercrime definition. [Online]. <http://cybercrime.org.za/definition>; Accessed on 18.09.2022
4. Vishi Aggarwal, Shruti. Cybercrime Victims: A Comprehensive Study. Int J Creat Res Thoughts (IJCRT). 2018 Apr; 6(2): 640–648. ISSN: 2320-2882.
5. Sheikh Shoib, Sharad Philip, Seema Bista, Fahimeh Saeed, Sana Javed, Dorottya Ori, Adil Bashir, Miyuru Chandradasa. Cyber victimization during the covid-19 pandemic: a syndemic looming large. Health Sci Rep. 2022 Mar; 5(2): E528. <https://onlinelibrary.wiley.com/doi/full/10.1002/hsr2.528>; Accessed on 19.09.2022)
6. Id.
7. Federal Bureau of Investigation. (2021). Internet Crime Report 2021. [Online]. FBI's Internet Crime Complaint Center (IC3). https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf; Accessed on 19.09.2022
8. Norton Life Lock. 2021-Norton-Cyber-Safety-Insights-Report. [Online]. 2021-Norton-Cyber-Safety-Insights-Report_IN-Cybercrime-Incidence-and-Impact.jpeg, Accessed on 19.09.2022
9. Yashika Arora, Bhawna Sharma. The Dark Side of Cyber Pornography. Acclaims. 2018; 4: 1–11. <http://www.penacclaims.com/wp-content/uploads/2018/12/Bhawna-Sharma.pdf>; Accessed on 19.09.2022

10. OHCHR. (2023). Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography [Online]. [cited 2023 Apr 29]. Available from: <https://www.ohchr.org/en/instruments-mechanisms/instruments/optional-protocol-convention-rights-child-sale-children-child#:~:text=%28c%29%20Child%20pornography%20means%20any,child%20for%20primarily%20sexual%20purposes>
11. Kamlesh Vaswani v. Union of India (2014) 6 SCC 705.
12. Avinash Bajaj v. State, 29 May, 2008 (India), (<https://indiankanoon.org/doc/309722/>)
13. Supra
14. Cyber-bullying: Research Center, (<https://cyberbullying.org/cyberstalking>; Accessed on 19.09.2022)
15. Id.
16. Supra at 11
17. Supra at 9
18. Soumyarendra Barik. (2022). Explained: Why the Govt has withdrawn the Personal Data Protection Bill, and what happens now. The Indian Express. Online Available from: <https://indianexpress.com/article/explained/explained-sci-tech/personal-data-protection-bill-withdrawal-reason-impact-explained-8070495/>.