

**INTERNATIONAL JOURNAL OF LEGAL AFFAIRS AND
EXPLORATION**

Volume 2| Issue 3

2024

CYBERBULLYING AND IT'S IMPACT ON OUR YOUTH

Chetan Hingsley

1st Year BA LL.B Student from V.S.S.D College

ABSTRACT

With the rapid advancement of technology, its applications have expanded significantly. Alongside this growth, there has been a surge in competition among IT industries, leading to reductions in internet tariffs and the availability of affordable smartphones. This has made technology accessible to people across different economic classes. However, this increased use of technology has also brought about various forms of cybercrime in society, such as cyberbullying, cyber stalking, cheating, and fraud. In India, cyberbullying is on the rise and has become a significant issue. Cyberbullying involves intentionally insulting or harassing someone on social media platforms like WhatsApp, Facebook, Instagram, and Twitter, with teenagers and adolescents often being the primary targets. The aim of researcher in this paper is to analyse existing research papers, articles, and websites to understand different aspects of cyberbullying, including its causes, effects, and potential remedies. By doing so, we hope to shed light on this growing problem and its implications for youth, harassment, and mental health.

Key Words: *Cybercrime, Cyberbullying, Youth, Harassment, Mental Health.*

1. INTRODUCTION

In today's digital era, communication channels like email, websites, and online applications have become indispensable tools for connectivity among individuals. These platforms facilitate the exchange of various forms of data, including images and other materials, contributing significantly to our interconnectedness. While these technological advancements offer immense benefits, they also bring undesirable elements into the picture.

The advent of information technology has opened up new economic and social opportunities, but it has also posed challenges to our security and privacy. We find ourselves deeply integrated into the realm of IT, with nearly everyone using digital devices and gadgets. This interconnectedness extends beyond individuals to encompass entire social systems, forming what is commonly referred to as the "internet of things." This digital revolution has led to significant improvements in our quality of life, with automation becoming increasingly prevalent. However, it has also raised concerns about safety and privacy. One of the most pressing challenges in this digital age is the

prevalence of cyber threats, especially among the youth demographic. With approximately 27.5% of the Indian population falling within the age group of 15–29 years, online risks such as addiction, cyberbullying, and sexual solicitation are widespread.¹ In recent years, there has been a significant surge in cybercrime rates, with a notable increase of 24.4%. According to a NCRB report,² law enforcement agencies have made strides in apprehending cyber criminals, many of whom are young adults. Over 55% of Indians in the 16-36 age group were hit by cybercrime.³ The rise in cybercrime among youth can be attributed to various factors, with the pursuit of 'easy money' being a predominant cause. The allure of quick financial gain often leads young individuals to engage in nefarious activities. Additionally, the prevalent culture of materialism and attention-seeking behaviour exacerbates the situation, pushing some youths towards committing heinous crimes. Disturbingly, even highly educated and qualified teenagers have been found to be involved in such criminal activities. The rate of youth involvement in cybercrime has surged by 40%, with a significant portion of these crimes—nearly 56%—being perpetrated by individuals aged between 16 and 25 years.

While the root causes of youth involvement in cybercrime may not always be apparent, several contributing factors have been identified. These include factors such as unemployment, the desire to fit into social groups, and a craving for attention. These societal pressures, coupled with the accessibility of technology and the allure of easy money, create a fertile ground for cybercrime among the youth population.

However, solely blaming the youth for these crimes would be unjust. In many cases, young individuals themselves are victims of circumstances. The scarcity of job opportunities often drives qualified young people to resort to criminal activities as a means of survival. Additionally, peer pressure plays a significant role, pushing teenagers to pursue easy money and seek attention through extravagant displays of wealth.

The lack of proper upbringing and inadequate attention given to youngsters contribute to their susceptibility to negative influences. Addressing these issues requires comprehensive changes in our education system and social awareness initiatives. Young people are a vulnerable group and

¹ Ms. Pooja and Dr. Aditi Vats, "The Growing Threat of Cyberbullying in India" 11 *IJERED* 85 (2023).

² Cybercrime rates in India, available at: <https://ncrb.gov.in/> (last visited on March 16, 2024).

³ Statistics of age group, available at: <https://shorturl.at/aktSQ> (last visited on March 16, 2024).

require nurturing and protection. They need time and compassionate guidance to navigate the complexities of life.⁴

While no approach can guarantee the complete elimination of youth involvement in cybercrime, proactive measures can significantly reduce the risk. Stringent law enforcement and a robust judiciary system can act as deterrents for young individuals contemplating criminal activities. However, waiting for others to improve the situation is not enough. Each of us has a responsibility to take proactive steps to safeguard our communities and prevent the exploitation of vulnerable youth.

2. WHAT DO WE KNOW ABOUT CYBER CRIME?

Cybercrime has evolved into a global issue, affecting every country without exemption. Surprisingly, the first recorded instances of cybercrime trace back to as early as 1820, occurring in India, Japan, and China. Today, one of the most significant challenges posed by cybercrime is pornography. Under Section 67 of the Information Technology (IT) Act, 2000, the creation, transmission, and distribution of cyber pornography are considered criminal offences. However, merely browsing and viewing online pornography do not warrant punishment. Conversely, the production, distribution, and even browsing of online child pornography are punishable under cyber laws. Shockingly, there are approximately 100,000 websites offering illegal child pornography.

In a recent case in Bhopal, a youth was apprehended for his involvement in a WhatsApp group that shared videos of child pornography. Upon investigation, the crime branch uncovered numerous messages containing coded language, indicative of demands for child pornography content from the accused.⁵ Cybercrime encompasses various criminal activities perpetrated using internet connections or computers as instruments. Several factors contribute to the prevalence of cybercrime, including the ease of storing large quantities of data in small spaces, the accessibility of information, the complexity of cyber operations, negligence, and challenges associated with preserving evidence.

⁴ Dr Dimpy Mahanta and Sulakshana Khatoniyar, "Cyberbullying and Its Impact on Mental Health of Adolescents" 14 *IRA-International Journal of Management & Social Sciences* 1 (2019).

⁵ This news, available at: <http://surl.li/rrecn> (last visited on March 18, 2024).

Various types of Cyber Crimes:

- *Crackers*: Individuals who create computer viruses.
- *Hackers*: Those who explore other computer systems for educational purposes.
- *Pranksters*: Individuals who engage in tricks or practical jokes online.
- *Career criminals*: Individuals who earn their income through cybercrime.
- *Harassment*: Cyberbullying that occurs through the internet.

Computer spam refers to the dissemination of unsolicited commercial advertisements online via emails, often carrying viruses or other harmful programs. Addressing cybercrime requires a thorough analysis of their behaviour and understanding their impacts on different levels of society. Therefore, it's essential to comprehend Cyber Crimes in the current era and their effects on society, considering future trends.

Another prevalent cybercrime is Phishing, which is just one of many fraudulent activities on the internet. Phishing involves tricking individuals into disclosing their personal financial information to unauthorised entities. These attacks can occur through various means, including voice, email, or telephone.

In Kolkata, the tragic death of a 17-year-old student due to cyberbullying serves as a stark reminder of the rising prevalence of Cyber Crimes.⁶ A recent study by TCS revealed alarming statistics, indicating that Kolkata has a high addiction rate to Facebook, with 85% of teens having an account on the platform. These incidents underscore the urgent need for greater awareness and measures to combat cybercrime effectively.⁷

3. RESEARCH METHODOLOGY

This research follows a structured approach, including literature review, survey-based research, and data collection from reputable sources like NCRB, TCS, TOI, Business Standard, and various research papers. Both primary and secondary data were utilised, with questionnaires administered to 1000 youth offenders from various states in India to gather primary data.

⁶ This news, available at: <http://surl.li/rregi> (last visited on March 18, 2024).

⁷ Statistics, available at: <https://www.tcs.com/> (last visited on March 18, 2024).

4. SOCIAL NETWORKING SITES

The study conducted on popular social media platforms like Facebook, Twitter, and Instagram focused on understanding views regarding trust and privacy concerns related to sharing information and forming new relationships. Interestingly, the research revealed that there is little variation in privacy concerns across these platforms, with most prominent members being willing to share information freely.⁸

These findings suggest that, regardless of the social media platform, privacy and trust are not significant factors when it comes to exchanging information or building relationships among members. Additionally, the study highlighted that adults also utilise social networking sites to connect with family and friends, often using online platforms to bridge gaps with distant relatives. Among the primary reasons people join social networking sites, the influence of peers, particularly for women, emerged as a significant factor. In contrast, men were less influenced by friends or family when deciding to join a social networking site.

Furthermore, the study revealed that psychologically, teenagers with an overenthusiastic disposition tend to spend more time on social networking sites and exhibit higher levels of addictive behaviour towards these platforms.

5. CYBER CRIMES AND SOCIAL NETWORKING SITES

The focus now shifts towards social media users equipped with the ability to monitor social media data streams for signs of high tension, which can be investigated to detect deviations from the 'norm,' typically characterised by low tension levels. These indicators encompass community crimes, inadequacies, and population analyses, providing a diverse representation of both 'terrestrial' and 'cyber' streets. In conclusion, this approach to identifying 'neighbourhood infirmities' offers a means of establishing official foundations of civil unrest by referencing user-generated versions of social media and their connections to other curated social and commercial data. Scholars have highlighted that spending time on social media networking sites is one of the most common activities among today's children and youngsters. Gaming sites, virtual worlds, video platforms like YouTube, and blogs serve as gateways for entertainment and interaction, experiencing tremendous growth in recent years. However, it's imperative for parents to be aware

⁸ Mofoluke Ibidunni Akoja and Eyitemi Adrian Doyle, "Privacy Concerns Of Facebook Applications Users" 10 *CJBASS* 1 (2020).

of the social media environment, as not all platforms provide safe backgrounds for children and adolescents.

The significant disparity between reported instances of cybercrimes each year and the relatively small number of known trials raises questions about the quality of criminological evidence regarding cybercrimes. This gap underscores the need for a closer examination of how public perceptions of cybercrimes are formed and the resulting ambiguities.

This section delves into the varying conceptualizations of cybercrime before addressing tensions in the creation of criminological awareness, which has led to disconnect between public demands for internet safety and its actual implementation. Scholars have also underscored the prevalence of youth violence, with assassination being the second leading cause of death among young people. Exposure to violence has detrimental effects on youth mental health, academic performance, and interpersonal relationships. Moreover, youth violence, including victimisation, mob violence, and self-directed violence, is increasingly manifesting in virtual spaces, posing significant challenges for online safety.

An example of cybercrime in Bengaluru highlights the misuse of a college principal's name in an email scam. A fraudster created an email account in the name of the principal of St. Joseph College autonomous, soliciting donations for a charitable cause. This incident underscores the need for heightened vigilance against cybercrimes and underscores the importance of cybersecurity measures.⁹

6. CYBER CRIMES AND ITS IMPACT ON YOUTH

Studies have demonstrated that the implementation of effective policies and educational programs can significantly enhance youth and individuals' ability to defend themselves online. It is crucial for young people to exercise caution when communicating with others online and refrain from sharing personal information with unfamiliar or untrustworthy individuals. Further analysis of social networking website access and deceptive online behaviours among youth, along with their familiarity with misleading internet practices, can raise awareness about teenagers' online activities and behaviours. With this understanding, better safety and security measures and strategies can be developed to safeguard teenagers online.

⁹ This news, available at [:http://surl.li/rrfrd](http://surl.li/rrfrd) (last visited on March 18, 2024).

Cybercrime has emerged as a major issue over the past two decades, with youth populations being particularly vulnerable targets. Factors such as age, gender, education, financial status, and experiences of forceful victimisation are associated with cybercrime victimisation. Offline social networks serve as a protective factor against cybercrime harassment among females, while young individuals engaged in cyber activities are more susceptible to future victimisation.

An incident in Delhi highlights the impact of cyber-related behaviour on real-world actions. A call centre employee was arrested after fleeing with an iPhone to create high-quality TikTok videos. The individual responded to an online advertisement for the sale of an iPhone and met the seller near Preet Vihar Traffic Signal. However, during the exchange, the respondent diverted the seller's attention and fled with the phone. This incident underscores the importance of vigilance against cyber-related crimes and the need for heightened awareness about online safety measures.

7. WHAT MOTIVATE SOME YOUNG PEOPLE TO BECOME CYBER CRIMINALS

It's commonly understood that cybercriminals are often driven by financial gain. However, it appears that this isn't always the primary motivation for young cybercriminals when they take their first steps into the 'dark side.' For instance, a compelling report by the National Crime Agency (NCA) in the UK revealed that many young cybercriminals are not necessarily motivated by financial rewards. Instead, factors such as perceptions from their peers, popularity within online forums, and a sense of accomplishment play a more significant role.¹⁰

According to the report, "The sense of achievement at completing a challenge, and gaining recognition from peers, are the primary motivations for those involved in cybercriminal activities." The report includes testimony from an 18-year-old who was arrested for unauthorised access to a government website. At the time of his arrest, the individual stated, "I did it to impress the people in the hacking community, to show them I had the skills to pull it off... I wanted to prove myself." This insight sheds light on the complex motivations driving young individuals toward cybercriminal activities and underscores the importance of understanding these factors in addressing and preventing cybercrime among youth.

¹⁰ Report, available at :<https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime> (last visited on March 18, 2024).

8. A SENSE OF IMPUNITY?

Another significant factor that attracts many youngsters to the world of cybercrime is the belief that it is not considered a crime in the traditional sense, and they are unlikely to face arrest for carrying out cyber-attacks.

According to the National Crime Agency (NCA), many teenagers involved in cybercrime do not have prior convictions for traditional crimes, which contributes to their perception of low risk regarding law enforcement intervention. This perception leads to a false sense of security among young cyber attackers.

This perception is further reinforced by the accessibility of online resources that provide easy entry into cybercriminal activities. Beginners often start by engaging in activities like cheating in video games or modifying games, before progressing to forums dedicated to cyber attacks where such activities are openly discussed.

The ease of entry into cybercrime is facilitated by the availability of tools such as Booters and Remote Access Trojans (RATs), which can be obtained with minimal or no payment. Additionally, step-by-step tutorials and video guides make it effortless for beginners to break the law. Once they have crossed this threshold, subsequent criminal activities become increasingly easier. However, the NCA believes that mentorship and early intervention can deter young people from entering the world of cybercrime. Guidance from a mentor and timely intervention can help steer these individuals away from criminal activities. Interestingly, discussions about the law and its consequences are rare in cybercriminal forums. If the topic does arise, it is quickly dismissed. These teenagers often only become aware of the consequences of their actions when someone they know is arrested for similar offences. This lack of awareness about the legal ramifications further perpetuates their involvement in cybercrime.

The individuals who participated in the study expressed a lack of guidance from mentors to steer them towards a more positive path and away from cybercrime. Instead, they often found themselves influenced by notorious cybercriminals who mastermind society's most complex attacks. The NCA highlighted the transformative impact of positive mentorship on former offenders who managed to leave behind their criminal activities and pursue education or careers in technology. These individuals credited their positive turnaround to mentors who provided them with the opportunity to utilise their skills for constructive purposes. However, the study also revealed a weakness in this aspect, as opportunities to channel skills towards positive endeavours

are not always readily available. In the field of technology, there is a constant demand for cybersecurity professionals, yet there remains a shortage of qualified individuals to fill these roles.

It's not uncommon for security professionals to have dabbled in hacking during their youth, often for recreational purposes, before deciding to pursue a career in the corporate world. However, the question arises whether it is prudent to hire someone with a history of cybercriminal activity, even if they have reformed and possess valuable skills.

In conclusion, the report underscores the alarming ease with which young people can become involved in cybercrime, often perceiving it as a risk-free endeavour. In a recent incident in Hyderabad, a youth employed at a hotel and a student were arrested for uploading nude videos and photos of a 23-year-old woman on social media platforms, harassing her and soliciting sexual favours and money. The accused had been in a relationship with the victim during their hotel management course, and the arrest occurred after the accused downloaded the victim's videos and photos and uploaded them to another pornographic website. This incident highlights the serious consequences of cyber harassment and the need for robust measures to combat such crimes.¹¹

9. WHY SHOULD PARENTS OF TEENAGERS BE CONCERNED ABOUT CYBER CRIME?

Cybercrime isn't just a concern for parents and teachers; it affects schools and educational institutions as a whole. In today's interconnected world, it's challenging to avoid the digital realm entirely. However, some may underestimate the profound impact of cybercrime on social conditions. With the proliferation of social media, cybercriminals have found new avenues to perpetrate their crimes. Platforms like Facebook, Twitter, Instagram, Snap chat, and WhatsApp have become targets for cybercrime. Recognizing this threat, social media companies have implemented detection mechanisms and sought legal support from experts in social law networks. Many children are introduced to the digital world at an early age, becoming adept at navigating social networks, managing social media, and utilising technology to solve everyday problems. They exhibit a natural curiosity and eagerness to explore, much like previous generations.

¹¹ This news, available at :<http://surl.li/rrgrh> (last visited on March 18, 2024).

Today's youth are often comfortable sharing intricate details of their lives on platforms like Twitter, Facebook, Instagram, and Snapchat. They may engage in impulsive or insensitive behaviour online, joining online clubs and forums, chatting with strangers, and sharing personal information on their devices. Unfortunately, this makes them vulnerable targets for cybercriminals, posing risks not only to themselves but also to their families and loved ones.

Now if you are a parent of young teen, and concerned about his/her wellbeing, here are some ways to protect your child from cyber crimes

- a) *Acknowledge the Reality of Cyber Crimes:*** It's crucial to recognize that cybercrimes exist, and no one is immune, not even your child. Even individuals with extensive knowledge in cybersecurity have fallen victim to online traps. Everything shared online can potentially be accessed by data hackers and malware specialists. There's no safe zone online, whether it's social media, e-commerce platforms, or peer-to-peer sites.
- b) *Report Cyber Crimes Promptly:*** Encourage your child to report any instances of cyberbullying or online harassment immediately. Cyberbullies often prey on fears and insecurities to prevent their actions from being reported. By promptly informing the authorities, you can aid in the apprehension of cybercriminals, no matter how significant or minor the incident may seem.
- c) *Educate Your Child on Safe Online Practices:*** Teach your child to avoid visiting and sharing information on unreliable websites. While anonymity may seem appealing, it can also pose significant risks, as users may not know who is monitoring their activities or their intentions. Many students fall into the trap of accessing freebies, files, and media through questionable sources, unknowingly exposing themselves to cybercrime.
- d) *Foster Awareness of Cybercrime:*** Many students are unaware of the severity of cybercrimes. As a parent, it's essential to engage in frequent conversations with your child about the nature of cybercrime and potential vulnerabilities online. Alert them to situations where they may be susceptible to cybercrime and encourage open communication about their online activities.
- e) *Monitor Your Child's Online Activity:*** While respecting your child's privacy, keep an eye on their online behaviour for any red flags indicating potential risks. Maintain open and ongoing communication with your child, creating a safe environment where they feel comfortable confiding in you about any problems they encounter online.

Cybercrime poses a significant threat as perpetrators can act anonymously, targeting vulnerable populations, including children. With teenagers increasingly addicted to social media platforms, they become easy targets for cybercriminals. Parents often struggle to protect their children from cybercrimes due to a lack of awareness about available legal remedies under national and international law.

10. ONLINE OFFENCES AGAINST CHILDREN ARE COVERED BY A SERIES OF LEGISLATION

Legal Framework:

The Protection of Children from Sexual Offences (POCSO) Act, 2012, is a critical legislation that specifically addresses sexual offences against children. It criminalizes various cybercrimes targeting children, including child pornography, cyberbullying, cyber stalking, defamation, grooming, hacking, identity theft, online child trafficking, online extortion, sexual harassment, and violation of privacy.¹² Additionally, the Information Technology (IT) Act, 2000, serves as the primary law dealing with cybercrimes against both children and adults in India.¹³ It is complemented by various rules formulated under it. Furthermore, the Indian Penal Code (IPC), 1860, offers protection against all crimes, covering certain cybercrimes that are modern variants of traditional offences such as theft, cheating, forgery, mischief, and defamation.¹⁴ In some instances, the accused may face charges under multiple provisions of IPC, POCSO, and the IT Act, with the punishment being determined by the provision carrying the highest penalty.

Lack of Awareness:

Despite the existence of these laws, there is a serious lack of awareness among key stakeholders, including parents, teachers, law enforcement officials, and policymakers. It is imperative that government initiatives aimed at enhancing online child safety are accompanied by widespread knowledge of the law, effective implementation, and comprehensive legislative review. In a recent incident in Hyderabad, a 24-year-old private employee from Tadipatri, Anantapur, was arrested by the Rachakonda police for harassing a married woman. The accused, who befriended the victim on Facebook, developed a close relationship with her and began sending obscene photographs and abusive messages when she stopped responding to his calls. He even threatened to morph her

¹² The Protection of Children from Sexual Offences (POCSO) Act, 2012 (Act 32 of 2012).

¹³ Information Technology (IT) Act, 2000 (Act 32 of 2012).

¹⁴ Indian Penal Code (IPC), 1860 (Act 45 of 1860).

photos and post them on social media if she continued to ignore him.¹⁵ This case underscores the urgent need for robust enforcement of cybercrime laws to protect individuals, especially vulnerable groups like children and women, from online harassment and exploitation.

11. CONCLUSION

While not everyone falls victim to cybercrimes, the reality is that everyone is susceptible to them. Cybercrimes can be perpetrated by individuals ranging from as young as 12 years old to as old as 67 years old, and they can occur across vast distances without the victim even realising they are being targeted. In today's digital age, criminals no longer need to physically rob banks or be present at a crime scene; instead, they exploit the convenience and anonymity provided by technology to commit various forms of cybercrime. To prevent cyber stalking and other forms of online harassment, individuals should be cautious about sharing personal information online, as doing so is akin to revealing one's identity to strangers in a public space. It's crucial to avoid sending pictures to strangers or unknown chat contacts, as there have been instances of picture misuse. Additionally, using up-to-date antivirus software can help safeguard against virus attacks, and regularly backing up data can mitigate the risk of data loss due to virus corruption.

Furthermore, individuals should refrain from sharing credit card numbers with unfamiliar websites or individuals to prevent fraud. Parents should monitor the websites their children access to protect them from potential harassment. Employing security programs that provide control over cookies and prevent unauthorised data collection by websites can also enhance online safety. Website owners should remain vigilant about monitoring website traffic and identifying any irregularities or security breaches.

Overall, it's essential to engage in discussions about the importance of information security awareness and behaviour, and to consider various methods for delivering this awareness effectively to end-users. By staying informed and implementing proactive measures, individuals can reduce their susceptibility to cybercrimes and contribute to a safer online environment for everyone.

¹⁵ This news, available at :<http://surl.li/rrini> (last visited on March 18, 2024).