CYBERCRIME AGAINST JUVENILES AND WOMEN IN INDIA THROUGH SOCIAL NETWORKING SITES

Abdul RoufNaik[1], Sankar D[2*]

[1]*VIT School of Law, VIT University, Chennai, Tamil Nadu, India, abdulroufnaik@gmail.com*
https://orcid.org/0009-0002-7633-5045
[2]*VIT School of Law, VIT University, Chennai, Tamil Nadu, India, sankar.d@vit.ac.in*
https://orcid.org/0009-0002-9209-232X

ABSTRACT

In recent years, the rapid growth of digital technology and widespread access to the internet has significantly impacted the lives of individuals, particularly juveniles and women. This paper explores the rising concern of cybercrime against juveniles and women in India, specifically focusing on incidents occurring through social networking sites. The study begins by examining the increasing prevalence of social networking platforms and their role in connecting people across diverse backgrounds. While these platforms offer opportunities for communication and networking, they also pose significant risks, particularly for vulnerable groups such as juveniles and women. The research aims to analyze the types of cybercrimes perpetrated against juveniles and women in the context of social networking sites, including but not limited to online harassment, cyberbullying, stalking, and dissemination of explicit content without consent. By presenting a comprehensive overview of the landscape of cybercrime against juveniles and women in India through social networking sites, this study aims to raise awareness, inform policy discussions, and contribute to developing strategies to safeguard vulnerable populations in the digital age. The findings of this research can serve as a valuable resource for policymakers, law enforcement agencies, and advocacy groups working towards creating a secure and inclusive online space for all.

1. INTRODUCTION

Juveniles and women are a sizable and fundamental section of the internet population. Indeed, youngsters will be more amiable and skilled with modern gadgets and programs than adults. However, regardless of whether juveniles and women are proficient users of web innovation and are aware of both dangers and methods for dealing with them, they do not have development in the sense of being able to assess the circumstances they encounter and the potential outcomes of their online activities.

The word Juvenile has been derived from the Latin word "juvenile," which means young. Although the words child and juvenile have been used interchangeably as both fall in the same age group, in common parlance, they are different. While the word child 'relates to the image of simplicity, innocence, and need for care & protection, the word juvenile is obdurate due to its relation with the court and the offense[1].

Juveniles are among the most active web users, and they are unfortunately vulnerable to a variety of threats. They spend a lot of time on the internet. Because the internet is a perplexing place, it exposes juveniles to the murky side of the world. This is evidenced by the increasing prevalence of cybercrimes in cyberspace, such as cyberwarfare, cyberterrorism, hacking, data theft, invasion of privacy, phishing attacks, intellectual property infringements, identity theft, and other computer-related crimes. Because of the secrecy and speed with which these crimes can be perpetrated online, cyberspace is an appealing medium for cybercriminals.

Data theft of private information, denial of service (DoS) attacks that interfere with services, email bombing, Trojan horse malware that infiltrates users' systems, and salami attacks that obtain bank account and credit card information are examples of cybercrimes committed against a business. Forgery, creating phony documents and signatures, and web jacking are examples of cybercrimes against society. The hacker fabricates a phony website and requests private information, including passwords.

During this critical stage of their development, juvenile people today face greater and more distinctive obstacles than ever before as they deal with the biological and psychological growth processes that characterize childhood and adolescence. For juveniles living in conflict zones, the obstacles are multiplied, as violent conflict, social disturbance, and psychological depression have a negative influence on all aspects of their lives. Violence is a detriment to a juvenile person's overall development. If these juveniles are unable to mature into responsible adults, they may constitute a threat to society as a whole, as fully functioning adults are required for a society to function successfully.

2. REVIEW OF LITERATURE

Violence against Juveniles and Women in Cyber World. The COVID-19 epidemic[2], which has proven to be a disaster, has claimed many lives and affected millions of people. Aside from the millions of deaths caused by the pandemic, it has been a difficult time for many people who have lost their jobs or had to close their businesses due to the lockdown, for families who have lost the sole wage earner, for children who have lost both parents at a young age, and for many others. However, this is not the case. Another disaster, cybercrime and mobile crime spread like a virus while people fought the pandemic. Several people used the internet and phones to express their dissatisfaction with the lockdown by tormenting others, while many more used these tools to keep themselves busy and distracted throughout the pandemic. During the epidemic, there was a sharp and rapid rise in cybercrime committed online.

Shan-a-Khuda and Schreuders (2019) have studied the local area variation in cybercrime victimization. The data for the study were collected from the recorded cybercrime incidents by the police in England. The study's results try to provide insight into cybercrime victimization and its relation to demographics and area variation.

The present research paper reveals that violence against Juveniles and women in our society is a violation of human rights, and it is not a new phenomenon. With the advancement of knowledge, many feminist scholars and NGOs have come forward with the aim of women's empowerment and trying to fight the violence against juveniles and women, but women are being exploited in every walk of their lives, and there is no end to their venerability. This paper presumes the cyber violence against juveniles and women and how it is impacting their social lives in the context of India. It highlights the reasons and forms of cybercrime and explores some suggestions on how to curb cybercrime against Juveniles and women. In

---

[1]AprajitaBharagava, Research Scholar, DAVV Indore (M.P.)

[2]Cybersecurity Ventures, "2019 official annual cybercrime report," 2019,https://www.herjavecgroup.com/the-2019- official-annual-cybercrime-report

India, juveniles and women netizens are still not open to immediately reporting cyber abuse or cyber-crime.

Saxena et al. (2012) have discussed the necessity of cyber security and the issues and challenges faced at organizational and personal levels. They have focused on various mechanisms to initiate large-scale awareness at the foundation level, for which they have advocated for changes in the education system. They have highlighted that the teachers are ignorant of cybersecurity threats and that no training or education regarding information security is provided to the students. Moreover, it is not practical even if provided, and students tend to forget that easily if it is not taught practically. They have also recommended improvements to be made at the classroom level to make students aware of cybercrime, hacking, and cyber theft.

A comprehensive review of existing literature will provide an understanding of the status of cybercrime against juveniles and women in India, including its causes and consequences. This will form the foundation for the research and help identify gaps in the current knowledge.

3. METHODOLOGY

This study adopted a purposive sampling method to focus on juveniles and women, who are recognized as the most vulnerable groups to cybercrime in India. A total of 120 respondents were selected across three states (Jammu & Kashmir, Tamil Nadu, and Delhi), comprising 70 women (aged 18–40) and 50 juveniles (aged 13–17). Primary data was collected using structured questionnaires and in-depth interviews conducted both online and offline. The questionnaire included sections on cybercrime exposure, awareness of cyber laws, reporting behavior, and psychological impact. Interviews provided qualitative insights into lived experiences, coping strategies, and perceived gaps in institutional responses.

Secondary data sources included reports from the National Crime Records Bureau (NCRB), the National Commission for Women (NCW), and peer-reviewed academic publications. For analysis, a mixed-method approach was adopted. Quantitative data from surveys were analyzed using descriptive statistics (frequency distribution and trend analysis), while qualitative data were examined thematically to identify recurring patterns, narratives, and gaps in policy implementation.

4. INDIA'S CYBERCRIMES: AN EVALUATION.

The number of cybercrimes in India has been on the rise. Technically proficient cybercriminals use new technology to participate in emerging crime trends. Cybercrimes are a terrible problem in India, costing the government and society a great deal. The more urgent problem is that thieves are frequently able to successfully hide their identity. The number of crimes reported in India between 2019 and 2024 is shown in Table No.1 However, because so many crimes go unreported, this does not give a true picture of the total number of crimes committed.

Table 1: Reported Crimes in India Since 2019-2024. Source: Business Standard (2024).

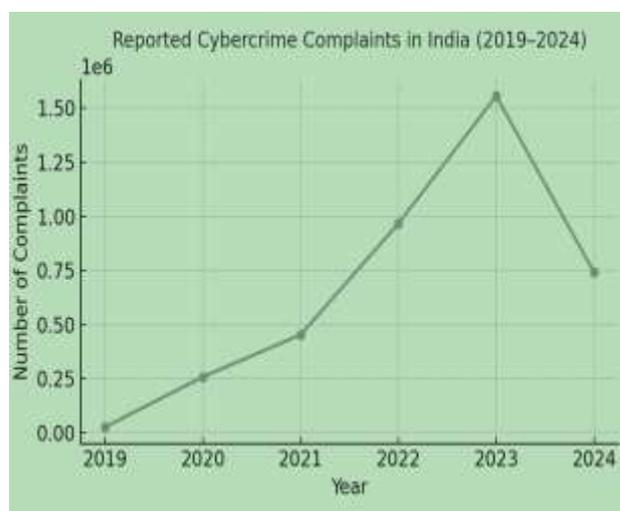| Year	Complaints were Recorded.
2019	26,049
2020	257,777
2021	452,414
2022	966,790
2023	1556,218
2024	740957(First Four Months of 2024)

Figure 1: Reported Cybercrime Complaints in India (2019–2024).

Cybercrime Victims: Juveniles and Women were the most vulnerable parts of society during the pandemic, making them simple targets for cybercriminals, whereas men and adults were victims of several cybercrime scams. Juveniles and Women were exposed to these crimes during the pandemic, in particular housewives and those who use social media.

The data from the 2021 A Special Reference to India published in the National Commission for Women show that after a lockdown, the number of cybercrime incidents against Juveniles and Women decreases. When India was badly affected by the second batch of COVID-19 and almost the entire country was subjected to rigorous lockdown restrictions in April, and May of 2021, the frequency of cybercrimes against Juveniles and Women

increased drastically in March and continued to raise.[3].

Finally, after the second pandemic wave passed and the lockdown restrictions were released in June, the frequency of cyber-attack occurrences started to diminish as well. This scenario lasted till July, as the lockdown restrictions were lifted. In earlier years, there were very few female victims of cybercrime, but during the pandemic and lockdown, this figure significantly increased.

Assessment of Cybercrimes Targeting Juveniles and Women: In India, since everyone now considers the internet to be essential, spending more time online makes one a target for criminals. People are susceptible to fraud or phishing assaults when using a variety of online services, including banking, file sharing, and e-commerce site buying. Phishing, pornography, cyberstalking, and cybersquatting account for the majority of cybercrimes recorded from India. Additionally, it was shown that the majority of information theft is typically committed by either current or former workers of the company.

Hackers commit approximately one-third of the information theft. The cybercrimes targeted against women are massively under-reported, as women in India are mostly unaware of such criminal offenses (Jain 2017; Chaudhary 2019). Women are blamed for outcomes over which they have no control. Even though women often are victims of cybercrimes, they prefer to maintain silence as honor is attached to female members of the family (Kaphle 2019; Chaudhary 2019). The innovations and technological advancements in India are the outcomes of initiatives such as Digital India, Bharat Net, and E-hospital to empower the citizens digitally. Digitalization has enhanced various sectors in India, such as the economy, education, and governance, but it has also increased cybercrimes exponentially every year (Sankhwar and Chaturvedi, 2018). Women voicing their opinions and taking a stand for their rights on the internet are ultimately cyberbullied, trolled, and threatened.

The number of cybercrime cases reported in India has been increasing significantly since 2019 onwards[4]

- 2019: 26,049 complaints
- 2020: 257,777 complaints
- 2021: 452,414 complaints
- 2022: 966,790 complaints
- 2023: 1,556,218 complaints

- First four months of 2024: Over 740,000 complaints

Some other details about cybercrime in India

- In the first four months of 2024, about 85% of the reports were related to online financial fraud.

Some of the most common types of cybercrime in India include

- Online investment fraud
- Gaming apps
- Algorithm manipulations
- Illegal lending apps
- Sextortion
- OTP scams
- The number of cybercrimes in India has increased significantly since 2019, especially during the pandemic.
- The most common form of cybercrime in India is financial fraud.

Juveniles and Women as the Victims of Cybercrimes People were forced to use the internet for social, professional, recreational, and educational purposes throughout the pandemic and lockdown. Working women began working from home using laptops, smartphones, and the internet. Women in school are forced to utilize the Internet for online homework and other academic activities.

Because the majority of women were using social networking sites and one or more online platforms for academic, professional, and entertainment objectives, the rate of cybercrime against women began to rise around this time. Criminals began to mentally and emotionally torture the victims because they couldn't physically harm them. After all, the entire country was under lockdown.

The report, for the first time, includes data on cyberstalking and cyberbullying of women. A total of 555 cases of cyberstalking and cyberbullying of women have been registered across India in 2017, with Maharashtra registering the most number of cases 301 among the states. Andhra Pradesh, with 48 cases, was second, and 27 cases were reported from Telangana and Haryana each, putting them in third place.

The report also mentions cyberstalking and cyberbullying cases against children. A total of seven cases were reported from across India, with three cases being reported from Maharashtra. Across

---

[3]The data from the 2021 A Special Reference to India published in National Commission for Women

[4]https://www.news18.com/news/india/cyber-crimes-in-india-spiked-nearly-nine-times-since-2013-up-topped-chart-in-2020-data-4210703.html

India, a total of 88 cybercrimes against Juveniles were reported.[5]

Women are most commonly exposed to the following Cyber Crimes

1) Phishing To make money during the lockdown, criminals send bogus e-mails containing a link to a specific webpage in an attempt to coerce the victim into entering personal information such as contact information and passwords or to infect the victim's device with dangerous viruses as soon as the link is clicked. These messages and emails appear to be genuine. The attackers then use the victim's bank account and other confidential information to conduct shady transactions from the victim's bank account to their own.

2) Pornography During the pandemic, offenders indulged in online sexual attacks against juveniles and women, altering the victim's image and using it in pornographic material.

Revenge Pornography example [6] In April 2015, a 21-year-old man was booked by the police in the Nargol village of Valsad (Gujarat) for allegedly spreading photographs of his teenage ex-girlfriend in compromising positions on popular social media websites. The pictures were reportedly taken on a mobile phone but were posted by the accused when the girl's parents were reportedly looking for a groom for the girl. The accused was charged with molestation under different sections of the Information Technology Act and the Protection of Children from Sexual Offences Act.

3) Cyberstalking Contacting or attempting to engage the victim through social media sites or phone conversations despite their clear lack of interest, writing messages on the victim's page (sometimes threatening in nature), and repeatedly bothering the victim with emails and phone calls were all part of it.

4) Cyber hacking People began reading the news online during the outbreak. False news and information are more prevalent now than ever before. The juveniles and women were victims of cyber hacking after clicking on fraudulent URLs. The spyware transferred all of their personal information to their phones, activated the microphone and camera, and shot intimate images and videos of them. The information and images are then used by criminals to commit extortion and other crimes.

5) Cyber-bullying This involves threatening the victim with rape, Sexual abuse, and murder, as well as making false, misleading, and abusive posts about the victim on social networking sites and demanding money to get them deleted. It also includes making cruel comments on the victim's social media pages. Digital or communication technology such as a computer, cell phone, or laptop is an example of digital or communication technology used for harassment and bullying.

6) Cybersex trafficking The victim does not physically engage with the perpetrator, which distinguishes it from physical sex trafficking. When a dealer broadcasts, records, or photographs a victim participating in sexual or personal behaviors from a central place, the content is sold online to sexual predators and customers. Juveniles and Women were coerced, misled, and blackmailed into participating in cybersex trafficking, which is sexual abuse for both of them.

Legal Provisions Regarding Cybercrime
The Bharatiya Nyaya Sanhita, 2023 (BNS)[7]

• **Section 75:** According to Section 75, a male who engages in any of the following acts demanding or pleading for sexual favors, showing pornography against a woman's will

• **Section 77:** Voyeurism is defined in Section 77 as the act of taking a photograph of a woman engaging in a private act and/or publishing it without the lady's permission

• **Section 78:** The addition of Section 78 states about stalking prohibition that covers online stalking.

• **Section 356(1):** To slander is to do something with the intent to harm someone's reputation. Defamation through the publication of an instant and unambiguous portrayal of imputation is punishable by up to two years in prison, a fine, or both when done with the intent to harm a woman's reputation.

• **Section 351(1):** Criminal intimidation occurs when a person is threatened with reputational injury to make her panic or force her to do what she ordinarily does or does not do.

• **Section 79:** Anyone who speaks, gestures, shows an object, or makes a sound with the intent that it be heard or seen by a female and offends her modesty or invades her privacy may be charged with violating this section and punished with up to three years of imprisonment and a fine.

---

[5]The National Crime Records Bureau (NCRB) on Monday night published its report on Crime in India in the year 2017

[6]Reagan Gavin Rasquinha / TNN / Apr 19, 2015 Times of India Newspaper.
[7]The Bharatiya Nyaya Sanhita, 2023.

5. THE INFORMATION TECHNOLOGY ACT 2000

It has been approved by the Indian Parliament and provides the legal framework for e-commerce in India. Cyber law is significant because it affects practically all elements of the Internet, WWW, and cyberspace transactions and activities. The Standing Committee made numerous recommendations, the most essential of which was that a cyber café owner keeps track of all visitors to his establishment as well as a list of websites they visited. It was created in an attempt to reduce cybercrime and simplify the quick identification of a cybercriminal. But this suggestion invades a net surfers' privacy and is dropped by the IT Ministry.

The Act was revised in 2008 to broaden its applicability. The term 'communication devices' was added to include cell phones, personal digital assistants, and other devices used to send text, videos, and so on. The term 'electronic signature' was coined and defined as a legally recognized method of executing signatures. By including the word "electronic," the BNS was changed to place electronic records and papers on par with physical records and documents. The parts dealing with the false entry in a record or false document, among other things, have been renamed 'electronic record and electronic document.' Following the establishment of the ITA, electronic records and papers were recognized.

The Information Technology Act 2000[8]

- **Section 66C:** Identity theft is a crime that is punishable under Section 66C of the IT Act. This provision would apply to scenarios of cyber hacking. According to this clause, whoever falsely or dishonestly uses another person's electronic signature, password, or other distinctive identifying feature risks up to three years in prison and a fine of up to Rs. 1 lakh.
- **Section 66E:** If someone's right to privacy is breached, Section 66E addresses that issue A person can face up to three years imprisonment and/or a fine for taking, sharing, or sending a picture of their private area without their consent or in a way that
- **Section 67:** Obscene content must not be published, transmitted, or made to be distributed under Section 67, which carries a maximum sentence of three years imprisonment or a fine for a first conviction

and up to 5 years imprisonment and a fine for the second.

- **Section 67A:** Publishing, transmitting, or aiding in the transfer of sexually explicit material is a misdemeanor under Section 67A, punishable by up to five years in prison and a fine for a first conviction and up to seven years of imprisonment and a fine for the subsequent conviction.

Power of Arrest Sec 80 of the IT act empowers police with vast powers to search premises and arrest suspected accused. This provision empowers police to arrest by way of preventive action, i.e., if police can suspect that a person is going to indulge in a cybercrime before he plunges into action, police officers can arrest him.

6. STEPS TAKEN BY THE GOVERNMENT

Ministry of Home Affairs dispatched a plan named 'Cyber Crime Prevention against Women and Children (CCPWC)' under which an online National Cyber Crime Reporting Portal (www.cybercrime.gov.in) was dispatched on 20th September 2018 to empower the general population to report cases relating to child pornography/kid sexual maltreatment material, assault/assault pictures or explicitly express substance. This entryway engages people, in general, to hold up grievances secretly or through the "Report and Track" alternative.

7. RESULTS

The findings showed that the researcher's study, which focused on women and children in India, was purposeful because it sought to comprehend cybercrimes from the viewpoints of women and children. The findings also showed that women and children update their personal information on social media, making it easier for cybercriminals to abuse it. Examining how well-informed the women and young people were about cybersecurity, cybercrimes, and cyber laws was important. This study revealed a complete lack of understanding regarding cybercrimes, cybersecurity, and cyber legislation. It was crucial to look at the women's and youths' level of knowledge regarding cybersecurity, cybercrimes, and cyber legislation. The results of this survey showed a total ignorance of cybersecurity, cybercrimes, and cyberlaw. This made it easier for scammers to locate their victims. As a result, fraudsters found their targets more easily.

---

8 The Information Technology Act 2000

Numerous academic researches supported the conclusion that the victim did not know the criminal in the majority of the cases. Additionally, it was discovered that the victim did not typically know the perpetrator. The same fact was also established by some earlier investigations. It was discovered that social media was the platform with the highest level of vulnerability. Researchers discovered in this study that women and young people believed social media was their primary exposure mode.

According to research on the causes of cybercrimes against women and children, the two main causes of the rise in cybercrimes are a lack of knowledge about cyber laws and a rise in mobile usage. Additionally, women and children were unaware of cybersecurity regulations; some women reported quitting social media following the incident. The low degree of knowledge regarding the TheBharatiya Nyaya Sanhita, 2023 (BNS) ability to punish offenders was another troublesome issue. Most women and children lack the awareness necessary to hold offenders accountable.

8. DISCUSSION

The findings reaffirm that women and juveniles remain disproportionately targeted in cyberspace due to increased digital dependency and insufficient awareness of cyber laws. The rise of cybercrimes during COVID-19 mirrors global patterns reported in studies from the UK, USA, and Southeast Asia, where lockdowns amplified online vulnerabilities. However, the Indian context is unique because cultural factors such as family honor, gender norms, and victim-blaming further silence victims and hinder reporting.

This study contributes original knowledge by highlighting how underreporting, coupled with poor digital literacy, creates a structural gap in cyber governance. Compared to international research that often focuses on technical cybersecurity, this paper emphasizes the socio-cultural dimension of cyber victimization in India.

8.1. Policy Implications

1. **Digital Literacy Programs** – Integration of cyber safety modules in school and college curricula, with special focus on adolescent girls.
2. **Gender-Sensitive Policing** – Training cybercrime units to handle cases involving women and juveniles with confidentiality and sensitivity.
3. **Community Awareness Campaigns** – Government and NGOs must jointly conduct campaigns to destigmatize reporting.
4. **Stricter Implementation of Laws** – Ensure effective enforcement of the IT Act 2000 and Bharatiya Nyaya Sanhita (2023) provisions.
5. **Public-Private Collaboration** – Social networking platforms must collaborate with law enforcement for faster takedown of harmful content and better victim redressal mechanisms.

According to the aforementioned findings, women and children are particularly at risk from hackers as a result of the growing use of mobile devices and the internet. The same fact has also been proved by numerous academic investigations. Furthermore, the findings indicate that consumers typically divulge personal information on a variety of websites. Because thieves may access personal information, this serves as a trigger for an increase in cybercrimes. Therefore, posting personal information on social networking sites is not safe because it could be misused.

The study has identified additional factors that contribute to the rise in cybercrimes, such as low computer literacy, ignorance of cyber laws, unemployment among educated youth, and a reduced conviction rate for cybercrimes. Our is such a controversial topic in our technological age. The degree of computer literacy should be significantly higher since people are so reliant on technology. Women would not be victims of numerous cybercrimes if they were aware of the various cyber regulations.

Furthermore, one of the main causes of the rise in cybercrimes is the unemployed, educated youth. In a densely populated nation like India, the dearth of employment possibilities deprives the educated youth of a means of securing their livelihood. As a result, some of them engage in online criminal activity. The results showed that women need to be educated about cyber security regulations and stop blaming the victim to primarily boost the reporting of cybercrime instances. A safer and more welcoming environment for women online can result from increased awareness of cybercrimes, which also encourages women to come forward and report the crime, potentially leading to the offender's legal penalty. In Indian society, victims who endure harassment rather than counseling are still stigmatized. It is important to note that the various social, financial, and psychological effects that cybercrimes have had on victims have also made them feel anxious and afraid. One of the main causes

of the rise in cybercrimes is the patriarchal and male-dominated nature of the internet.

Suggestions for Preventing Cybercrime Watch out for pointless or fraudulent phone or email messages.

1. Emails that request personal information should not be replied to.
2. Watch out for fraudulent websites that try to obtain your personal information.
3. Pay special attention to the privacy policies that are included with the software and posted on websites.
4. Make sure your email address is secure.
5. Put Secure Passwords to use.
6. A victim of cybercrime should notify the local cyber cell or a police station.
7. A complaint can also be submitted anonymously through the National Cybercrime
8. Reporting Portal.

9. CONCLUSION

Cybercrime against juveniles and women is high nowadays it is not limited to India, rather, it is a global phenomenon. Also, it is a huge matter of concern among developed as well as underdeveloped countries because of its continued growth. To reduce the crime rate of such cases, not only legislative changes are required, but also awareness is needed on a large scale, the parents of juveniles and adult girls should be more alert and aware of how to protect themselves from targeted online attacks. Cybercrime against juveniles and women as a whole is challenging, and its major

reasons are internet addiction and the usage of online social media platforms. Cybercrime against Juveniles and women in India is a complex issue that requires a multidisciplinary approach to understanding and addressing its underlying causes and consequences. This research outlines a systematic study to shed light on the phenomenon and evaluate the impact of cybercrime, ultimately contributing to the development of effective policies and interventions to control such types of heinous crimes in our society.

While a crime-free society is unattainable and merely a idealistic aspiration, there should be a continuing effort to implement rules that reduce criminality to a minimum. Legislators must go above and beyond to deter impostors because criminality related to electronic law-breaking is sure to expand, especially in a world that is becoming increasingly reliant on technology. Technology is typically a two-edged sword that can be used for both good and evil purposes.

No matter how much time juveniles and women spend online, they are likely to experience cyber violence. Therefore, it is essential to examine how violence affects the victim. Many cases remain unreported because the victim's thoughts are dominated by a fear of being isolated and victim-blaming. Furthermore, many cases are suppressed under the pretense of family honor. The victim experiences psychological effects from the suppression of cybercrimes, including worry, fear, depression, and withdrawal from online activities. To get over these kinds of consequences, victims frequently talk about their experiences with friends, family, and close acquaintances.

REFERENCES

Primary Source
TheBharatiya Nyaya Sanhita, 2023 (BNS) Indian Evidence Act, 1872
Information Technology Act,2000
Information Technology (Amendment) Act, 2008

188th Report, The Law Commission of India "Proposal for Constitution of Hi-Tech Fast-Track Commercial Divisions in High Courts," 2003.

Cybercrime Survey Report 2014, Forensic Technology Services, KMPG, https://www.kpmg.com/IN/en/IssuesAndInsights/ArticlesPublications/Documents/KPMG_Cyber_Crime_survey_report_2014.pdf.

Secondary Source Books

Brian, Loader and Douglas, Thomas, Cyber-Crime Law Enforcement, Security and Surveillance in the Information Age,(Routledge Publication, London, 2000)

Rd. Viswanathan Paranjape, Legal Dimensions of Cyber Crimes and Preventive Laws with Special Reference to India, (Central Law Agency Publication, 2010)

Rodney D. Ryder, Guide to Cyber Laws (Information Technology Act, 2000, E-commerce, Data Protection, and the Internet),(Wadhwa Publication, 2001)

Nandan Kamath, Law relating to Computers, Internet and E-commerce: A Guide to Cyber Laws and the Information Technology Act, 2000, (Universal Law Publishing Co., 2009)

D.P Mittal, Law of Information Technology(cyber law) with Information Technology (certifying authorities) rules,2000 (Taxmann Allied Services Pvt. Ltd., New Delhi,2000)

Vakul Sharma, Information Technology –law and practice (Universal law publication,3rd ed. , 2011) Dr. N Das Gupta, Cyber Crime in India- A comparative study (Eastern Law House,2016)

Article

Abhimanyu Behra, "Cyber Crime and Law in India," IJCC 16-30 (2010).

RohasNagpal, "Offences and penalties under the Information Technology Act, 2000", ITLJ, 15-32 (2002). Ramesh, "Pornography and Obscenity on the Web: Need a Strict Law," SCJ 20-25(2009).

Charlotte Decker, "Cyber Crime: An Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime", SCLR 959-1016 (2008).

S. Mishra and C.S. Panda," A Survey of Cybercrimes," IJCSET, (2015).

Websites

Organization of American States. (2017). U.S. Cyber Laws Overview. (visited on 01/10/2017). vle.du.ac.in/mod/book/print.php?id=9205&chapterid=13340 (visited on 02/10/2017).

NALSAR University. (2017). Cyber Law Learning Modules. (visited on 02/1o/2017). Securelist. (2017). Cybercrime and UK Computer Crime Legislation. (visited on 04/10/2017). UK Government. (2017). Cybercrime Policy Report. (visited on 05/10/2017).