

Upgraded Technology in Social-Media: A Major Threat to Women and Children for Cyber-victimisation in Cyberspace

Shobhana Mudaliyar¹, Aayush Bokade²

¹ Administrative Officer, Rashtriya Raksha University

² PhD Scholar, Rashtriya Raksha University

Abstract - Globally, the importance of social media platforms represents widespread among the youth and the general population in the modern age. Although the internet has facilitated incomparable opportunities for communication, sharing information, and social networking, it has also created new platforms for criminal activities in cyberspace. Cybercrimes represent the developing class of offences that are spreading across developing nations such as India, due to considerable internet infiltration and weak regulatory frameworks. With the help of technological advancements that facilitate new approaches to cyber threats, there has been a significant variation in the threat vectors and patterns in the victimisation. Social media platforms like YouTube, Instagram, Twitter, Facebook, Telegram, and Snapchat have become the vectors for cybercriminal threats and activities as the offenders exploit the social media platforms to obtain private gain. Notably, when compared to men, women and children in regions with significantly lower levels of safety and awareness from police regarding cybercrime, such as India, are more vulnerable to online victimisation. The paper examines motivations underlying cybercrimes against women and children, including black financial gain, private gain, private revenge, intimate exploitation, extortion, defamation, and harassment. The examination is based on the five established criminological theories: such as, Intergroup Emotion Theory, Choice Theory, Social Dominance Theory, Routine Activity Theory, and Space Transition Theory. This study also reviews the cybercrime legislation in India, particularly the Information Technology Act of 2000 and its amendments, along with a comparison of International Approaches. This paper concludes with preventive measures and recommendations for policy development, institutional reforms, and strategies to protect individual privacy to address the developing harm of cybercrime against the weak population such as women and children in India.

Keywords: *Cyberspace, Cybercrime, Social Media, Cybervictimisation, Gender-Based Violence, Digital Safety, Criminological Theory*

INTRODUCTION

The Internet has become one of the most transformative technological developments in the history of human communication. With the arrival of worldwide connectivity, geographical boundaries have collapsed, transforming the world into what is usually termed the “global village”. This interconnected environment has created exceptional opportunities for both personal and professional relationships across borders and has reshaped interactions and the information shared (Halder & Jaishankar, 2009). The Internet has served as a democratising force by providing access to information and various forms of empowerment across different aspects of society, including women who have faced forced restrictions on participation in public events and on expressing their own ideas (Halder & Jaishankar, 2009). Nonetheless, this technological advantage comes with an enormous price to pay. The very infrastructure that enables positive connectivity also increases the possibilities of committing crimes, taking advantage of people through different means, and hurting them. Women, in particular, face unique risks in cyberspace. In India, women suffer from misery due to things like gender-related discrimination, lack of legislative support, and a low level of knowledge of law enforcement authorities about the phenomenon (Halder & Jaishankar, 2011). Moreover, given that India is a country with a strongly patriarchal society and traditional social organisation, women are extensively exposed to this problem (Halder & Jaishankar, 2011). Social stigma mostly falls on women in the country who find themselves in such a position, making their suffering even more severe and painful. Finally, India does not have strong anti-cybercrime legislation and enforcement compared to Western countries (Halder & Jaishankar, 2011).

In June of 2016, the United Nations Human Rights Council recognised access to the internet as a basic human right, which indicates that the internet is important in current society. At the same time, the recognition of this fact raises some important questions: how can this basic human right be exercised in such institutions known for the patriarchal reality associated with constant violence, bullying, and discrimination of women in both physical and digital worlds? Meanwhile, the Ministry of Women and Child Development in India made a statement indicating that the ministry is aware of the nature of cybercrimes against women and children and the fact that a need exists for checks and balances of these forms of crime. The present paper tackles these issues and analyses the psychological, criminological and legal aspects of cybervictimisation. The paper outlines the general types of motivators of cybercrimes committed against vulnerable groups of people, such as economic gain, personal revenge, modesty insults, extortion, sexual criminality, defamation, hate crime and their manifestations. Apart from this, the present paper analyses the latest trends in law in cybercrime in India and worldwide and shows the already developed ways to deal with this crime.

AIM AND OBJECTIVES

This paper has the following specific aims and objectives.

- To investigate the patterns of children's and women's victimisation in the domains of cybersecurity, focusing on their experiences in India and other technologically advanced contexts;
- To interpret the psychological and criminological theories behind the behaviour of cybercriminals and the pattern of their victimisation.
- To familiarise with the legal Regulations related to cybercrime in India; comparison of the provisions of the Information Technology Act, 2000 and its subsequent amendments with laws in other countries.
- To understand the main factors driving cybercriminals to commit crimes against women and children.
- To provide evidence concerning the facts of incidents of cybercrime aimed at vulnerable populations.
- To give recommendations regarding the measures for preventing and fighting against cybercrimes.
- To promote understanding of the issue of digital security among victims, vulnerable populations, law enforcement officials, and legislators.

THEORETICAL PERSPECTIVES ON CYBERCRIME

To understand cybercriminal conduct and victimisation, theoretical concepts derived from recognised criminology and psychology theories should be utilised, as per their extension to the digital environment. The theories described in this section will facilitate a relatively better understanding of several types of cybercrimes aimed at vulnerable social groups.

Intergroup Emotion Theory

According to Intergroup Emotion Theory (IET), people assess various events and emotional stimuli based on their social identities. If a certain social identity is activated, people will likely interpret events with reference to its consequences for their group rather than the individual self. In the cases of cyberbullying and cybercrime, hate and derogatory messages may create substantial emotional reactions influenced by group belonging. The issue of intergroup relations is constantly changing, which means that people continuously evaluate changes in their social conditions that will result in the strengthening or weakening of their emotional responses (Smith et al., 2015). This theory can be effectively used in the context of cybercrime aimed at designated categories of people, like women who face systematic harassment that is gender-based in essence.

Choice Theory

Choice Theory is a theory developed in the field of psychology and counselling that stresses that people have choices in how they behave through agency. The theory asserts that people have little control over the actions of others. In this respect, Choice Theory emphasises personal responsibility for one's choices and discourages attempts to manipulate or control the decisions of others. The implications for cybercrime are that people acting as both perpetrators and victims of cybercrime behave deliberately through agency, making choices in response to different events.

Social Dominance Theory

Originally, Social Dominance Theory (SDT) was established to explain inequalities in social hierarchies and power structures. In the realm of cybercrime, SDT illustrates how cyberbullying, as a form of online abuse, is used by cyberbullies to create fear, shame, and powerlessness in their victims, thus dominating them and controlling them socially. The anonymity and distance provided by the internet might worsen the aggression of a cyberbully and his cruelty, for he does not see the emotional reactions of the victim, thus removing any obstacles to his behaviour. According to SDT, when a victim is perceived as resistant, a bully can

increase the violence of his actions, while the opposite is true, as victims who are aware of the attack and do not react or get back to the aggressor might stop the bully from dominating them. Nevertheless, vulnerable groups of young people lack emotional competence to ignore the harmful messages directed towards them, therefore exposing them to the risk of being dominated through cyberspace and psychological damage.

Routine Activities Theory

RAT theory is considered an important theoretical framework in criminology. According to it, predatory crime occurs when three conditions coincide at the same time and place; these are motivated offender, a potential victim and lack of capable guardianship or supervision. In relation to cybercrime, RAT theory suggests that any online space, where the potential victim is unprotected is a dangerous area for crime. Criminals use opportunities provided to them by technology and perpetrate crimes in situations of anonymity and low honorability. In addition to that the RAT theory makes it possible to identify trends and tendencies in victimisation. It also helps identify programming before it occurs and allows law enforcement professionals to carry out preventive measures aimed at the vulnerable populations. Knowledge of lifestyles of cyber victims and non-cyber victims helps understand the differences in their exposure to motivated offenders and level of parental or institutional supervision. Women and children without computer knowledge and monitoring from parents and institutions are most suitable for cybercriminals (Cohen and Felson, 1979).

Space Transition Theory

The Space Transition Theory, formulated by Jaishankar (2008), is the only theory in the criminology discipline that focuses on cybercrime. The theory states that people behave differently as they move from physical to digital space and highlights conformity and non-conformity of behaviour, which is evident in these different spaces. The theory states that the individual who represses criminal tendencies in the physical world because of social constraints, status, or fear of being caught can do wrong things in cyberspace due to the anonymity and lesser degree of social control there. The theory explains the seven principles that show why and how cybercrime is committed.

- Individuals with suppressed criminal propensities in the tangible world have a greater likelihood of engaging in cybercriminal behaviours in virtual environments, where status and position constraints are lifted.
- The ability to adapt personal identity, the phenomenon of being anonymous, along with the minimisation of the effectiveness of deterrence in the cyberworld makes it easier for criminals to commit unlawful acts in cyberspace.
- Crimes committed online can also be transposed to the real world and vice versa.
- The episodic forays into cyberspace together with the ever-changing spatio-temporal nature of digital environments provide perpetrators with numerous chances to escape from nearly every crime.
- People who have never met in real life may unite online to commit a crime in the real world, while people who are connected in real life might cooperate in cyberspace.
- People coming from closed societies have higher chances of committing cybercriminal activities than those from open societies.
- The conflict between values in the real world and cyberspace may lead to criminal activities as people deal with two competing ethical infrastructures.

The Space Transition Theory has been the subject of considerable academic validation, asserting its position as the most prominent theoretical framework in the field of cyber criminology (Jaishankar, 2008, 2010). According to this theory, women and children are more likely to become victims of cybercrime than men due to the challenging circumstances created in the patriarchal environment in India that ensures justice is done by both local and foreign criminals.

CYBERSPACE AND VULNERABILITY: GENDER DIMENSION

The virtual environment known as cyberspace utilises the internet as the most basic form of technology along with the advancement of Information and Communication Technologies. The field of cyberspace is rapidly developing due to the numerous breakthroughs made in computer hardware over the years. In contrast with the physical environment, cyberspace overcomes the limitations of time and space, allowing each person to connect and send messages without delay. Most importantly, researchers point out that cyberspace is much less adherent to laws and regulations compared to real life and thus has less chance of being punished or arrested (Halder & Jaishankar, 2009).

The process of globalisation has transformed the way information is circulated and the way markets operate. Like other developing countries, India has benefitted from informational globalisation, and hence, has witnessed rapid growth in its information technology sector, which has experienced double-digit growth rates in recent times. Still, such technological growth has brought in

some new concerns related to safety and privacy. Comprehensive research done by the Boston Consulting Group in collaboration with the Retailers Association of India identified significant gender differences in terms of internet access. About 29% of internet users in India are female, and 71% are male. Such an unequal distribution leads to the increased vulnerability of women towards cybercrimes. Women entering cyberspace are often thought to be “invading” or “trespassing” on the territory that belongs to men, especially if they hold a specific opinion about certain disputed issues. According to 2015’s Observer Research Foundation report, there was low participation of women in political discussions occurring on Twitter in India, just like in the offline political process. It was stated that a great number of women users deleted their online accounts after being subjected to online abuse and harassment (Halder & Jaishankar 2011).

Cybercrime is defined as criminal conduct carried out using computers and internet resources, where actions considered illegal can be prosecuted according to existing laws. Understanding the perpetration of cybercrime against women calls for both knowledge of technical characteristics of computers and awareness of gender-based social systems within which these technologies are used. It is essential to appreciate the vulnerability of women in cyberspace not just as a technical issue but as a manifestation of overall inequalities between genders embedded in the patriarchal social framework existing in real life (Halder & Jaishankar, 2011).

SOCIAL MEDIA PLATFORMS AND CYBERCRIME VECTORS

The term “social media” indicates the technology that enables sharing ideas and exchanging information in virtual communities. It has been estimated from recent statistics that the total number of people living on Earth is around 7.7 billion. Among them, 3.5 billion people have the possibility of using the internet. The rapid development of technology has contributed significantly to changing how people communicate with each other. The first social media site to reach the target of 1 million unique monthly users was MySpace, thus marking the birth of social media in its contemporary definition. After that, MySpace, as well as other social networks, such as Facebook, YouTube, and Reddit, have existed for more than 10 years. TikTok is the latest confirmation of this tendency, having appeared in September 2016 and reached more than 500 million users by mid-2018. At the same time, other social networks, such as Myspace, Hi5, and Friendster, have experienced serious downsides, with MySpace being the most visited website in the USA in 2006 and then disappearing from the market generally. The major social media platforms that have lasted through the last few years have undergone substantial transformation; For instance, Twitter used to be a platform that would not allow users to share videos and photographs, but since the year 2011, it has enabled multimedia content sharing, with visual media which currently constitutes over 50% of Twitter's viewed content (Halder & Jaishankar, 2011)

The fast expansion of social media and the diversity of platforms have opened the pathways for many criminal activities. The volume of user data available from all these social networks, coupled with the low possibility of anonymity detection, high accessibility of the platforms, and inconsistent law enforcement around the world, makes social media a good instrument for committing cybercrimes against women and children. Criminals take advantage of social media in a variety of ways for their criminal activities, such as financial fraud, identity theft, damage to reputation, sexual abuse, and psychological manipulation

CYBERVICTIMISATION OF WOMEN AND CHILDREN

The shift of modern society to digitalisation raises the issue of digital inclusion, as it has come to be regarded as a necessary factor enabling participation and gaining access to opportunities. Having said that, while the digital inclusion entails different risks for different demographic groups, all genders are prone to online violence and abuse, but women go through this in a more mortal manner and with a difference sexual undercurrent. Online threats and violence targeting women are usually sexual and rooted in anti-female ideas that strengthen the patriarchal power structure. Studies show the increase over time regarding the cybercrimes committed against women and children, which is confirmed by the statistics provided by the National Crime Records Bureau (NCRB) and the measures of legislative nature taken with the aim of stopping cybercrime (Sankhwar et al., 2024).

Tradition has seen women occupying a subordinate position in the societal structure as an effect of patriarchal social framework with limited autonomy and expression in society. In the context of internet usage, especially in socially suppressed societies, women and girls showcase a greater susceptibility to gender specific sexual harassment or abuse. The increase in vulnerability to abuse can be due to various factors such as women being digitally illiterate in developing nations; lack of parental or institutional supervision; non-availability of digital safety education; unwillingness to report to the law enforcement agencies; and continuation of offline gender-related violence in online settings. According to a report conveyed by the National Commission for Women (India), 54 per cent of women have experienced cybercrime. The impact of cyber victimisation on women and girls has been proven by the number of psychological issues related to being exposed to such abuse, such as anxiety level, depression, thoughts about suicide and reactions to traumatic events (Sankhwar, 2014).

LANDMARK CASES IN INDIAN CYBERCRIME LAW

Jurisprudential decisions rendered by Indian courts have cast light on legal principles and evidentiary standards adopted in cases of cybercrimes against women. This section emphasises the core cases highlighting substantial developments in Indian jurisprudence of cybercrime and showing victimisation patterns, along with those available for victims' relief.

Case 1: Yogesh Prabhu V. State of Maharashtra (2015)

India's first cyberstalking conviction was obtained in Maharashtra when it comes to Yogesh Prabhu in July 2015, which was decided by Additional Chief Metropolitan Magistrate M.R. Natu. The first cyberstalking case was initiated in 2009, when the complainant was communicating online with Prabhu. When Prabhu proposed marriage and was refused, she cut off all communications with him and also unsubscribed him from her social profile due to her perception of Prabhu's abnormal conduct. Despite her assertion of her disassociation from him, Prabhu continued viewing her social profile and using electronic means to monitor her. Later, the complainant was receiving emails from an anonymous account consisting of obscene pictures with lewd videos.

The complainant tried ignoring the lewd emails but when she kept receiving these emails, she lodged a police complaint. The cyber-crime investigation cell took charge of investigation, tracked the Internet protocol address of the computer from the firm where Prabhu worked, and filed a detailed 200 page charge sheet in September 2009. Eight persons, Prabhu's colleagues, cyber crime technical analysts, officials and the complainant herself appeared and were examined. Prabhu was Later convicted under section 509 of the India Penal Code (insulting the modesty of any women through word, gesture or acts) and Section 66E of the Information technology Act, 2008 (privacy violation). The court was unable to convict him under section 354D of the India Penal Code (Stalking was introduced in 2013) because the law cannot be applied retrospectively. This case set important precedents for gathering digital evidence, locating an IP address, and joint prosecution by institutions (Duggal, 2019).

Case 2: Suhas Katti v. State of Tamil Nadu (2004)

India's first-ever conviction for cyberpornography was achieved in Chennai in 2004 with the prosecution and conviction of Suhas Katti. The case involved a divorced woman laying a police complaint against a man who repeatedly sent obscene, defamatory and offensive messages through Yahoo messaging services after the woman refused a marriage proposal. The offender created a false email account that appeared to be in the victim's name, used it to circulate offensive messages and interacted with strangers who, through unsolicited telephone calls, solicited sex. Filing of the police complaint took place in February 2004 and within less than seven months, the cybercrime cell convicted Katti. The anthology of sentences handed down to Katti is like this: 2 years rigorous imprisonment, fining Rs. 500 under Section 469 (forgery with an intent to harm reputation) of the IPC; 1 year rigorous imprisonment and fining Rs. 4000 under Section 67 of the Information Technology Act of 2000 (Publishing obscene material through electronic means). The latter sentences were to run concurrently which meant two years of imprisonment required. Also, this was the first case of its kind that set the important precedent about the event of email ICQ impersonation, chemically defamatory electronic communications as well as the concurrent use of various provisions of the IPC and the IT Act, 2000 (Duggal, 2019).

Case 3: Saddam Hussain v. State of Madhya Pradesh

This matter was the culmination of a very serious sexual violation in which the accused took the victim's pictures in a completely non-consensual situation. What makes this case quite different from others is that, apart from the violation of privacy, the accused further blackmailed and extorted the victim with the pictures. The victim, who was the woman, filed a written submission of the criminal complaint with a view on IPC, the Section 354D (Stalking), Section 507 (Criminal Intimidation by Anonymous Communication), and IT Act Section 66A (later held unconstitutional). Legal representatives of the victim approached Madhya Pradesh High Court seeking a dismissal of the case on the grounds of a settlement. The High Court however decided that these criminal acts could not be classified as personal disputes settled through a resolution but instead as violations of criminal law against society. The court pointed out that society's interest in punishing cyber-stalking and related cyber-crimes was at stake here. So, such criminal proceedings could not be dismissed because parties have reached a separate agreement. This decision made it clear that women and children's crimes, in particular, cyber-related victimisation, represent public wrongs and because of this society-related harm not just a victim's choice of a matter.

In their overall effect, these three landmark cases are indicative of new trends in the judiciary for how to deal with cybercrime. One of the lessons from these cases is the need for the use of digital forensic evidence by law enforcers and the importance of collaboration between law enforcement agencies. At the same time, the willingness of the government to protect victims from cyber-attacks on women and girls through the institutional setup is being demonstrated in these cases. Also, the cases

make it clear that though lawmakers have created various laws to punish computer criminal activities, the implementation of those laws is not uniform and the victim-supportive services are lacking at many levels.

CYBERCRIME LEGISLATION: INDIA AND COMPARATIVE PERSPECTIVES

Information Technology Act, 2000 (India)

The passage of the Information Technology Act (ITA-2000) in 2000, effective October 17 2000 marked India's definitive shift from paper to digitally-mediated processes on the legal and transactional levels. The law gave statutory recognition to electronic records and digital signatures, allowing the possibility of doing business, electronic government, and online managing of government records. Through Section 6 of ITA 2000, the law empowers authorities to digitally file applications, permits, and forms thereby transforming the nature and scope of government services. Section 7 allows government bodies to keep official documents in digital format instead of paper records which would allow archival and retrieval of the documents to be much more efficient. The Act takes the "bridging provision" principle to stipulate that in all the legal procedures requiring the signing of documents and making records (e.g. signing and keeping a record of agreement), the same requirements can be fulfilled by the use of digital alternatives in the prescribed electronic format. So through this provision of the Act, the whole set of Indian's legal system has been extended to the realm of electronic transactions, except for five categories that have been explicitly excluded by the Ministry of Law and Justice (2000): negotiable instruments (with cheques being excluded), power of attorney, trust deeds, Wills, and contracts about the sale or conveyance of immovable property.

The Information Technology Amendment Act, 2008 (ITAA-2008) is an Act passed by both Houses of Parliament on December 23 - 24, 2008, and the President gave the assent on February 5, 2009. The Act came into operation on October 27, 2009. The amendment substantially expended cybercrime provision and introduced heightened penalties for emerging threat vectors. Key provisions include:

Section 67: Prohibits publishing or disseminating through electronic means any material that is regarded as indecent, immoral and disgusting. Maximum penalty - three years imprisonment and/or fine Rs.5 lakhs for the first conviction; five years imprisonment and/or fine Rs. 10 lakhs for subsequent convictions.

Section 66-A: Transmission of messages or e-mails to others through electronic communication or e-mail spoofing that is meant to deceive recipients about the true source of the mail or communication is made a punishable act under this section. Maximum punishment - three years imprisonment and/or fine. [Note: this provision But was scrapped as being unconstitutional by the Supreme Court in *Shreya Singhal v. Union of India* (2015); it was held to infringe on the rights of free speech guaranteed by Article 19.]

Section 66-B: Dishonestly taking possession or keeping stolen computer equipment or communication device is penalised under this section of the Act. Maximum - three years imprisonment and/or fine up to Rs. 1 lakh.

Section 66-C: Identity theft and misuse of electronic signature have been addressed under this section. The section also includes instances where somebody is not entitled to access a person's password or a person's electronic signature or both. Maximum punishment - three years imprisonment and/or fine.

Section 66-D: Cheating through impersonation using use of computer resources or communication devices has been made a criminal offence under this Act. Maximum penalty - three years imprisonment and fine extending to Rs. 1 lakh.

Section 66-E: Publishing or disseminating private photographs of a person without the person's consent is a prohibited act. Maximum penalty - three years imprisonment and/or fine up to Rs. 2 lakhs.

Section 66-F: Defines the term cyber-terrorism as accessing a computer for a purpose which has the effect of a threat to India's unity integrity security or sovereignty or causing or threatening to cause a system which denies access to authorised persons (e.g. hackers or terrorists). Maximum penalty - life imprisonment.

Section 67-A: Transmission or publication of sexually explicit material in electronic form is criminalised. First conviction under this section: the maximum punishment is three years imprisonment and/or Rs 5 lakhs fine. Subsequent conviction: up to seven years imprisonment or Rs 10 lakhs fine whichever is higher

Section 67-B: This section deals with the publication or distribution of material that shows Children engaged in sexual activity. Under this section: First conviction- up to five years imprisonment and or fine to the extent of Rs 10 lakhs. (i) Subsequent offences: seven years imprisonment or fine of Rs 10 lakhs.

Section 72: Violation of provisions in contracts for privacy and secrecy is dealt with under this section.

Section 72-A: This section puts a criminal law against information that a person has acquired through an illegal contract.

The Complementary Indian Penal Code (IPC) provisions have a role in cybercrime, like Sections 354D (Stalking), Section 509 (Insult to the modesty), and Section 441 (Criminal trespass). Really cybercrime is being addressed by multiple statutes indicates

that the Law-makers have recognized cybercrime as an intersection with traditional criminal law (Ministry of Law and Justice, 2000; The Law Institute, 2026).

International Cybercrime Legislation

Cybercrime legislative approaches differ around the world. Nations like the USA, UK, and Western countries in general have implemented well-rounded cybercrime laws with good enforcement agencies and plenty of resources. Yet a comparison of different countries around the world still shows some differences - prosecution ideas are varying as well as evidentiary requirements and victim support provisions. India has developed a cybercrime law which is very extensive about statute, but still encounters various hurdles in their implementation. They face insufficient cybercrime investigation staff, lack of digital forensics knowledge among law enforcement, uneven awareness of victim's legal redress, and lack of coordination between jurisdictions in dealing with cases involving foreign criminals. These weaknesses call for measures for building up human resources, inter-agency collaboration, victim support, and a continuing dedication to cybercrime prevention (Halder & Jaishankar, 2011).

Preventive Measures and Cybersecurity Strategies

Cybercrime against women and children is on the rise even with security measures in place. A lack of proper implementation of cybersecurity measures has become obvious through several reasons like a gap in the digital literacy among the more vulnerable demographics, no real understanding of the digital threats, limited technical capabilities to apply protection measures, specific gender hurdles in the way reporting and help-seeking go; also, law enforcement lacks enough institutional skills to deal with cybercrime at a response level. Preventing cybercrime has to be an approach that involves not just individuals and their families but also institutions, and the whole society has to work in harmony.

Individual and Household Protective Measures

- Make very strong passwords for all online accounts so that they are unique, with an uppercase letter, lowercase letter combination, numbers, and a special character.
- Use two-step Verification (Multi-Factor Authentication) on important account(s) - it adds a layer of security preventing unauthorised users from accessing even if they have got hold of your password.
- Keep updating your security package and your operating system; set automatic updates to defend against the ones already recognized.
- Be careful about what's being revealed on a personal level at social media - the most damaging data like a home address, phone numbers, information about family, and financial details.
- Set up social media privacy settings and limit friends-only; keep them in your sight.
- Don't get caught trying to do something you shouldn't do over a wireless network that's open for everyone, even less so if you're doing something you'll have to hide from an entity like a bank. You can take the help of a Virtual Private Network (VPN) if you absolutely must use a public network connection).
- Be careful about links as well as the attached files you've got from suspicious or unknown email senders; only those whom you can verify are safe should be downloaded and opened.
- Teach your family about online scams that target the elderly, children & women and other types of cybercrime.
- Save cyberstalking and harassment material by taking screenshots, saving conversations, keeping records & if required report this evidence to the Police.
- Use parental control or web filter programs Mainly for the ones under 18 in a family but also inform other members of the family if any monitoring is taking place.

Institutional and Organisational Responses

Educational institutions, corporations, and government organisations should set up cybersecurity setups as well as digital safety policies. Some of the institutional measures that can be used include:

- Organising cybersecurity awareness campaigns for staff and students focused on issues like email security, password practices, phishing awareness, recognition of phishing emails, and appropriate handling of confidential or sensitive information.
- Creating digital usage policies of the organisation that clearly define staff and student expectations on appropriate use of email, internet, and social media.

- Designating official channels in writing for employees to report cyberstalking, cyber harassment or other security issues anonymously, i.e. without fear of retaliation or adverse consequences
- Specialisation and development of a law enforcement cybercrime unit, providing sufficient manpower and equipment, and cooperating with the specialist cybercrime units of law enforcement organisations.
- Trauma-informed victim support service development and providing, including counseling, legal advocacy, and coordination with policing.
- Detecting and fixing security issues through regular internal cybersecurity audits and vulnerability assessments.
- Making cooperation and collaboration between victim-focused organisations working on digital safety and with non-profit organisations (NGOs).

Policy and Legislation Recommendations

Legislative and executive branches of the government must make cybercrime prevention one of their top priorities and work on policy proposals to ensure that:

- Detection and investigation of cybercrime will require the recruitment of specialists as well as additional training and equipment of law enforcement.
- Organising and offering comprehensive digital literacy programs with special emphasis placed upon women and girls who reside in the most remote and least digitalised communities.
- Establishing training programmes for judges in the field of cybercrime and evidence procedures with digital content.
- Due to a fear of re-traumatisation after a prolonged time being victim of crime, vulnerable victims such as women and children deserve special cybercrime law court proceedings where the duration could be shorter and/or not very long.
- Introducing full victim support programs covering a wide range from mental health counseling and legal aid to financial assistance of victims and when necessary to their protection even after they have given their testimonies at courts.
- Launch cybercrime prevention and information awareness initiatives explaining to the public about cybersecurity, ways of spotting cybercrime, the process of reporting, and information on assistance for victims.
- The law has to be drafted to different areas of the world can be united in the fight against cybercrime, while it is necessary for governments to sign agreements that can help police investigation at different places or even at several international levels.
- Doing a long study to determine how cybercrime is prevalent, what patterns of victimisation the criminals have, why criminals perpetrate offences, which factors make a crime happen, and if any interventions (measures) have a positive effect in order for legislation to be based on facts and research, i.e. evidence-based legislation.

CONCLUSION

Women and children are increasingly targets of cybercrime, a trend that should cause serious concern for society at large legislation as well as public health professionals, mostly since some developing countries still have very inefficient law enforcement apparatuses and weak state support. Five major theories, namely Intergroup Emotion Theory, Choice Theory, Social Dominance Theory, Routine Activities Theory, and Space Transition Theory, have been combined within an integrated criminological and psychological structure in the paper to account for the victim's susceptibility and the criminal's motives. The findings show that cybercriminal behaviour is not simply a technological matter at an individual level but, it is mainly reflective of the deep-rooted and gendered imbalance of power and the patriarchal social arrangement that govern both the virtual and the real world. Cybercrime against women and children is a fast-growing problem, even though some legislative changes have been made, as evident by National Crime Records Bureau records and judgments in Indian courts. The Information Technology Act of 2000, amended in 2008, brings for a complete set of rules covering aspects like cybercrime investigations and the courts. But, the problem is that not every court uses them effectively, nor are the victim support services good enough nor can most of the people in India afford to make a living without being digitally illiterate. For instance, the State of Maharashtra vs. Yogesh Prabhu, the State of Tamil Nadu vs. Suhas Katti, and the State of Madhya Pradesh vs. Saddam Hussain are three major cases that have been studied and show how the legal system still doesn't quite protect the vulnerable victims from the harm of the cybercrimes they have been subject to, but also set precedents.

Fighting cybercrime is a societal problem so solving it will require actions at many levels. Personal protective tactics, although very useful, will not do the trick if not supported by changes in the system or in the making of a law. The law enforcement

sector would require large investments to increase capacity through specialized trainings, Mainly in cybercrime detection, as well as digital forensics equipment. Courts will need specialized training to be able to handle cybercrime cases effectively and understand the various types of digital evidence. Schools and educational centers should incorporate courses on understanding the risks posed by social media, online safety, etc. Civil society groups would need to be supported so that they can provide victims with help services and also do outreach work to educate and raise awareness. The key is that the State Policy has a role to play in cyberbullying/cybercrime issues and that cyberbullying and/or cybercrime prevention work has not only to be a part of the security agenda but a very important one as a matter of fact. The government should be willing to commit substantial financial resources to prevent, enforce and support victims when there has been a case of cyber victim. The study should cover some areas like the psychology of cybercriminals, different reasons for victims being open about cybercrime vs. keeping silent, assessment of the impacts of interventions and, in particular, dimensions that reflect how the social situation is affected by the different aspects of life - like social status, religion, and sexuality - for the person to become a cyber victim. There is a growing need for legal setups and international collaboration against cybercriminals who are exploiting the loopholes of different countries' jurisdictions. It is a fact that society is getting more into a totally digital world which cannot be rolled back; Still, the security and wellbeing of women and children online depend heavily on a world-wide, sustained and coordinated commitment to prevent such incidents, catch the perpetrators and support the victims.

REFERENCES

- [1] Social Media, Technology, and the Cybervictimisation of Women and Children in India.
- [2] Bajpai, S., Jain, N., & Samtani, K. (2015, April 23). The Changing Connected Consumer in India. BCG Global. <https://www.bcg.com/publications/2015/globalization-technology-digital-changing-connected-consumer-in-india>
- [3] Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, 44(4), 588. <https://doi.org/10.2307/2094589>
- [4] Duggal, P. (2019). LINKING OF AADHAAR CONNECTING WITH SOCIAL MEDIA AND CONNECTED LEGALITIES FACIAL RECOGNITION IN INDIA -SOME LEGAL CHALLENGES Dr. Pavan Duggal.
- [5] Halder, D., & Jaishankar Karuppannan. (2009). Cyber socializing and victimisation of women. *Temida*, 12(3), 5–26. <https://doi.org/10.2298/TEM0903005H>
- [6] (2021). Online Child Sexual Exploitation. <https://doi.org/10.1007/978-3-030-66654-5>
- [7] Akhtar, S., & Bhowmik, M. (2025). Digital Violence: The Rise of Online Gender-Based Violence Against Women in the Age of Social Media. *International Journal For Multidisciplinary Research*. <https://doi.org/10.36948/ijfmr.2025.v07i02.41785>
- [8] Champion, A. R., Oswald, F., Khera, D., & Pedersen, C. L. (2021). Examining the Gendered Impacts of Technology-Facilitated Sexual Violence: A Mixed Methods Approach. *Archives of Sexual Behavior*, 51, 1607 - 1624. <https://doi.org/10.1007/s10508-021-02226-y>
- [9] Henry, N., & Powell, A. (2018). Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research. *Trauma, Violence, & Abuse*, 19, 195 - 208. <https://doi.org/10.1177/1524838016650189>
- [10] Henry, N., Flynn, A., & Powell, A. (2020). Technology-Facilitated Domestic and Sexual Violence: A Review. *Violence Against Women*, 26, 1828 - 1854. <https://doi.org/10.1177/1077801219875821>
- [11] Hong, M. (2024). The impact of social media in child sexual abuse. *Journal of Paediatrics and Child Health*, 60. <https://doi.org/10.1111/jpc.16638>
- [12] Leukfeldt, E. R., & Yar, M. (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior*, 37, 263 - 280. <https://doi.org/10.1080/01639625.2015.1012409>
- [13] Lorenzo-Dus, N., Evans, C., & Mullineux-Morgan, R. (2023). Online Child Sexual Grooming Discourse. <https://doi.org/10.1017/9781009314626>
- [14] M., V., Balamurugan, G., Sevak, S., Gurung, K., G., B., X., S., P. T., & S., T. (2024). Silent Screams: A Narrative Review of Cyberbullying Among Indian Adolescents. *Cureus*, 16. <https://doi.org/10.7759/cureus.66292>
- [15] Mulaah, C. J., Musa, A. Z. B., & Ibharim, N. S. B. (2025). Child Protection and Vulnerability in the Context of Uncensored Social Media. *International Journal of Social Science and Human Research*. <https://doi.org/10.47191/ijsshr/v8-i8-76>
- [16] Özaşçılar, M., Çalıcı, C., & Vakhitova, Z. I. (2024). Examining cybercrime victimisation among Turkish women using routine activity theory. *Crime Prevention and Community Safety*, 26, 112 - 128. <https://doi.org/10.1057/s41300-024-00201-y>
- [17] P, N., & Jegadeeshwaran, M. (2023). An Empirical Study on Cyber Crimes Against Women and Children in India. *International Journal of Advanced Research in Science, Communication and Technology*. <https://doi.org/10.48175/ijarset-11327>
- [18] Powell, A., & Henry, N. (2019). Technology-Facilitated Sexual Violence Victimization: Results From an Online Survey of Australian Adults. *Journal of Interpersonal Violence*, 34, 3637 - 3665. <https://doi.org/10.1177/0886260516672055>
- [19] Reyns, B. W., Henson, B., & Fisher, B. (2011). Being Pursued Online. *Criminal Justice and Behavior*, 38, 1149 - 1169. <https://doi.org/10.1177/0093854811421448>
- [20] Upadhyay, R. (2025). Harassment of women on social media in India. *INTERNATIONAL JOURNAL OF AGRICULTURAL SCIENCES*. <https://doi.org/10.15740/has/ijas/21.2/363-368>
- [21] Wefers, S., Dieseth, T., George, E., Øverland, I., Jolapara, J., McAree, C., & Findlater, D. (2024). Understanding and Deterring Online Child Grooming: A Qualitative Study. *Sexual Offending: Theory, Research, and Prevention*, 19. <https://doi.org/10.5964/sotrap.13147>
- [22] Cyber Crime in India and Its Effect on Society - ProQuest. (2026). Proquest.Com. <https://www.proquest.com/docview/2314605298>
- [23] Putra Siregar, Y. A., Jannah, R., Yunindya, W. A., & Luthfia, A. (2026). Breaking the silence: how social media campaigns shape public awareness of child sexual violence in Indonesia. *JPPi (Jurnal Penelitian Pendidikan Indonesia)*, 12(1), 322–336. <https://doi.org/10.29210/020266706>