International Journal of Advanced and Applied Sciences

Journal homepage: http://www.ijaas.in

International Journal of Advanced and Applied Sciences
iase
ISSN 2313-626X
E-ISSN 2313-3724 [Q3]
Publisher: Institute of Advanced Science Extension (IASE)
http://ijaas.in/

India's Legal Framework on Cybercrime Against Women and Children: Progress and Persistent Challenges

Dr. Priyanka Gupta [1*]

[1] Assistant Professor, Department of Law, NIMS University, Rajasthan, India

ARTICLE INFO

Article history:
Received: 28-09-2025
Received in revised form: 04-10-2025
Accepted: 03-11-2025

Keywords:

Cybercrime Protection, Women and Children Safety, Legal Safeguards, Digital Harassment, Online Exploitation.

ABSTRACT

Cybercrime has emerged as a pervasive threat in India, disproportionately affecting women and children who are especially vulnerable in the digital environment. This paper examines India's legal framework addressing cyber offences against these groups, focusing on key provisions under the Information Technology Act, 2000, the Indian Penal Code, and recent legislative and policy initiatives aimed at enhancing online safety. While significant progress has been made such as strengthened penalties for cyber harassment, child sexual abuse material (CSAM), and online stalking gaps persist in enforcement, technological capacity, and victim support mechanisms. Challenges including underreporting, investigative delays, jurisdictional complexities, and inadequate digital literacy continue to hinder effective implementation of existing laws. The analysis underscores the need for a more holistic approach that integrates legal reform, technological innovation, awareness programmes, and institutional capacity-building to ensure meaningful protection for women and children in India's rapidly evolving digital landscape.

Introduction

Cybercrime includes a broad range of offenses, from financial fraud to cyber bullying, hacking, and online harassment. Unfortunately, women have been disproportionately affected by cybercrime in India, where cyber offenses against women have increased rapidly in recent years. Cybercrime has severe consequences for women in India, both in terms of mental and physical health. With the rise of social media and online platforms, cyber bullying and online harassment have become widespread in India, targeting women in particular. Women face cyber threats like stalking, identity theft, and revenge pornography, leading to severe mental distress and emotional trauma. According to a study by the National Commission for Women, 54.8% of women have experienced cyber harassment, while 26% of them have reported cases of morphed images or videos. Moreover, cybercrime has also had a significant economic impact on women, with many women losing their jobs or experiencing financial losses due to online fraud. The different types of cybercrimes against women in India include online harassment, cyber bullying, online stalking, revenge pornography, and cyber financial fraud. Online harassment involves sending threatening or offensive messages or comments on social media platforms, while cyber bullying is the use of technology to harass, humiliate, or intimidate someone [1]. Online stalking is a pattern of repeated online harassment that involves following, monitoring, or tracking someone's online activity. Revenge pornography involves the distribution of sexually explicit images or videos without the victim's consent, while cyber financial fraud includes online phishing, credit card fraud, and other forms of online financial scams. The current state of cyber security in India is a cause for concern, with India ranking among the top five countries in the world for cybercrime. Despite the government's efforts to strengthen cyber security laws and regulations, there are still significant gaps in implementing cyber security measures in India. The lack of awareness and knowledge about cyber security among the general public and law enforcement agencies also exacerbates the problem. Moreover, the increasing use of technology and the internet has led to an increase in the number of cybercrimes, making it challenging to address the issue effectively.

The different types of cybercrimes, including online harassment, cyber bullying, online stalking, revenge pornography, and cyber financial fraud, require immediate attention from the government, law enforcement agencies, and civil society organizations. There is a need for a comprehensive approach to addressing cybercrime, including increasing public awareness, strengthening cyber security laws and regulations, and providing support2 to victims of cybercrime.

Cyber-crimes against women in India are a growing concern, with a significant impact on women's mental and physical health, as well as their economic wellbeing. The different types of cyber-crimes against women include online harassment, cyber stalking, cyber bullying, revenge porn, and financial fraud. Online harassment is one of the most common forms of cybercrime against women in India. It involves the use of digital platforms to send threatening, abusive, or offensive messages or comments to women. According to a study by the National Commission for Women, 54.8% of women have experienced cyber harassment [2]. Online harassment can lead to significant mental distress, anxiety, and fear among women, making them feel unsafe and vulnerable. Cyber stalking is another type of cybercrime that women in India face. It refers to a pattern of repeated online harassment that involves following, monitoring, or tracking someone's online activity. Cyber stalkers use various digital platforms like social media, emails, and messaging apps to stalk and harass their victims. According to a report by the Cyber Crime Cell of the Mumbai Police, there has been a 91%3 increase in cyber stalking cases in India in the past year.

Cyber bullying can take many forms, including spreading rumors, posting offensive messages, and sharing embarrassing photos or videos. A survey by the Cyber and Media Cell of the Delhi Police found that 40% of cyber bullying victims in India were women. Revenge porn is a particularly heinous form of cybercrime against women in India. It involves the distribution of sexually explicit images or videos without the victim's consent, often as an act of revenge or blackmail. According to a report by the Cyber Peace Foundation, there has been a 148% increase in revenge porn cases in India in the past year. Revenge porn can lead to severe mental and emotional trauma, as well as damage to a woman's reputation. Cyber financial fraud is also a growing concern for women in India. With the rise of online transactions, cyber criminals have found new ways to defraud unsuspecting victims [3]. Cyber financial fraud includes online phishing, credit card fraud, and other forms of online financial scams. According to a report by the Reserve Bank of India, there has been a significant increase in online banking fraud in India in the past year.

These forms of violence often spill over into cyberspace, where perpetrators use technology to harass, stalk, or blackmail their victims. In many cases, the perpetrators are known to the victims, such as intimate partners or family members. According to a report by the National Crime Records Bureau, over 93%5 of rape cases in India were committed by someone known to the victim. Patriarchal attitudes in Indian society also contribute to the prevalence of cybercrimes against women. The patriarchal system promotes male dominance and control over women, leading to a culture of misogyny, victim-blaming, and discrimination. These attitudes often manifest in cyberspace, where women are subjected to online harassment, trolling, and abuse. Women who speak up against harassment or violence are often accused of bringing shame to their families or communities. The lack of support from family and society can deter women from reporting cyber-crimes. The lack of awareness about cyber security is another contributing factor to the prevalence of cyber-crimes against women in India. Many women in India lack basic knowledge about safe online practices, such as creating strong passwords, avoiding phishing scams, and using privacy settings. This lack of awareness makes them vulnerable to cyber-attacks, such as identity theft, financial fraud, and data breaches. The absence of comprehensive cyber security policies and laws also makes it difficult for women to seek justice and protection.

Cyber Crime Laws in India The rise of cyber-crimes against women in India has led to the development of a legal framework to address these crimes. The legal framework in India includes several laws and regulations, including the Information Technology Act, 2000, the Indian Penal Code, and the Protection of Women from Domestic Violence Act, 2005. Let's take a closer look at these laws and regulations The Information Technology Act, 2000 (IT Act) is the primary law that deals with cyber-crimes in India [4]. The IT Act was enacted to provide legal recognition for electronic transactions and to facilitate e-governance. The IT Act includes provisions that deal with cyber-crimes against women, such as hacking, identity theft, and electronic stalking. The IT Act also provides for the establishment of cyber-crime investigation cells in every state to investigate and prosecute cyber-crimes. The Indian Penal Code (IPC) is the primary criminal law in India. The IPC includes provisions that deal with crimes against women, such as rape, sexual harassment, and domestic violence. The IPC has been amended to include provisions that deal with cyber-crimes against women, such as voyeurism, cyber stalking, and dissemination of sexually explicit material [5]. The IPC also provides for punishment for abetment to cyber-crimes against women.

Literature review

Agarwal, M. (2022) [1]**:** *Cybercrimes against women in India: A review of literature Journal of Criminology and Criminal Justice, 14(1), 71–84* Agarwal presents a comprehensive literature review analyzing existing research on cybercrimes targeting women in India. The study identifies gaps in legal responses and highlights recurring themes such as online harassment, blackmail, and gender-based digital violence.

Abbasi, A., & Abbasi, M. (2022) [2]**:** *Cybercrimes against women: A global perspective Journal of Cyber Security and Law, 7(1), 1–16* This paper explores cybercrimes against women from a global standpoint, comparing legal frameworks and responses in various countries. It emphasizes the universal nature of online gender-based violence and advocates for stronger international collaboration.

National Crime Records Bureau (2022) [3]**:** *Cybercrime in India, 2020 Ministry of Home Affairs, Government of India* An official statistical report providing detailed data on cybercrime incidents in India, including crimes specifically targeting women. It is a vital resource for understanding crime trends and informing policy decisions.

Arora, P., & Arora, A. (2021) [4]**:** *Cybercrime against women in India: A study of trends and patterns Journal of Cyber Security and Digital Law, 6(1), 1–18* This study tracks recent patterns in cybercrimes against Indian women, highlighting increases in cyber-stalking, revenge porn, and fake profiles. It combines quantitative data with legal commentary.

Bhuyan, M., & Das, P. (2021) [5]**:** *Cybercrimes against women in South Asia: A study of trends and patterns Journal of Cyber Security and Digital Law, 6(2), 1–18* The authors present a comparative analysis of South Asian countries, emphasizing socio-cultural factors that influence the prevalence and reporting of cybercrimes against women.

Gupta, S. (2021) [6]**:** *Cybercrimes against women in India: A study of the challenges and opportunities Journal of Law, Technology and Policy, 14(2), 1–22* Gupta discusses challenges such as legal loopholes, delayed justice, and underreporting. The study also highlights opportunities for reform through digital literacy and community policing.

Kumar, A., & Yadav, A. (2021) [7]**:** *Cybercrimes against women: A study of the challenges and opportunities Journal of Law, Technology and Policy, 14(3), 1–22* This paper offers a multidisciplinary approach to the issue, incorporating insights from law, technology, and social policy. The authors stress the role of proactive governance and tech-based solutions.

Chaturvedi, S., & Mishra, A. (2020) [8]**:** *Cybercrimes against women in India: A study of the modus operandi and impact Journal of Law, Policy and Globalization, 64, 103–117* Focused on how cybercrimes are committed, this study breaks down technical methods used by perpetrators, such as phishing and digital impersonation, and discusses their psychological and social effects on victims.

Das, S., & Bhattacharyya, S. (2020) [9]**:** *Cybercrimes against women in India and Bangladesh: A comparative study Journal of Law, Policy and Globalization, 65, 113–128* This cross-border study compares legislative responses and victim support systems in India and Bangladesh, revealing common weaknesses in enforcement and cultural barriers to justice.

Dixit, A. (2019) [10]**:** *Cybercrimes against women in India: A study of the legal and social dimensions Journal of Criminology and Criminal Justice, 11(2), 159–176* Dixit examines both legal provisions and societal attitudes toward victims. The research finds a disconnect between law and enforcement, often leaving victims with limited recourse.

Gupta, A., & Singh, S. (2019) [11]**:** *Cybercrimes against women: A global perspective Journal of Criminology and Criminal Justice, 11(3), 235–252* A global comparative analysis that outlines various international legal frameworks, this paper identifies best practices and benchmarks that India and similar countries could adopt.

United Nations (2019) [12]**:** *Cyber Violence Against Women and Girls: A Global Overview UN Women* This official UN report offers a global overview of online violence targeting women. It emphasizes the need for gender-sensitive digital policy and coordinated global actions to protect vulnerable groups.

Methodology

Re-chipping and cloning of mobile phones

The electronic serial number (ESN) of an analogue, or the International Mobile-Electronic Identity number (IMEI) of a digital, mobile phone is its unique identity and was originally intended to be inviolably incorporated into the phone [6]. However, the security features which protect the number can be overcome and a new set of numbers installed. The change of identity is called ‘re-chipping’ and can be achieved on analogue phones in a number of ways. Sometimes, the ESN can be altered directly from the keypad using supposedly secret combinations of keystrokes; in other cases, connection to a computer can allow the phone chip to be re- programmed. The software to do this is available via advertisements in specialist magazines or even available free over the Internet [7]. Re-chipping is not illegal and was started to bypass the service providers when reconnecting a secondhand phone, replacing a faulty one or upgrading to a new phone. Once available, however, the equipment could be readily applied to give a stolen phone a new identity so it can be connected to a network, and to clone another mobile phone.

A clone is an analogue mobile phone which has been programmed to impersonate one owned by a legitimate subscriber by using its ESN and telephone number (these numbers are usually obtained by interception with a ‘scanner’ radio, theft of a dealer’s or service provider’s records or directly from the impersonated phone) [8].

Mobile cloning is copying the identity of one mobile telephone to another mobile telephone Mobile cloning is also known as cell phone piracy and has been taking place throughout the world since decades. Mobile phones have become a major part of our everyday life. On the one hand, India’s mobile phone market has grown rapidly in the last decade on the back of falling phone tariffs and handset prices, making it one of the fastest growing markets globally. On the other the number of mobile phone subscribers is exceeding that of fixed-line users [9].

Today millions of mobile phones users, be it Global System for Mobile communication (GSM) or Code Division Multiple Access (CDMA), run the risk of having their phones cloned. And the worst part is that there isn’t much that you can do to prevent this. Such crime first came to light in India in January, 2005 when the Delhi police arrested a person with 20 cell phones, a laptop, a SIM scanner, and a writer. The accused was running an exchange illegally where ii he cloned CDMA based phones. He used software for the cloning and provided cheap international calls to Indian immigrants in west Asia. A similar racket came to light in Mumbai resulting in the arrest of four mobile dealers. Each year, the mobile phone industry loses millions of dollars in revenue because of the criminal actions of persons who are able to reconfigure mobile phones so that their calls are billed to other phones owned by innocent third persons. Often these cloned phones are used to place hundreds of calls, often long distance, even to foreign countries, resulting in thousands of dollars in air time and long distance charges. Cellular telephone companies do not require their customers to pay for any charges illegally made to their account, no matter how great the cost [10].

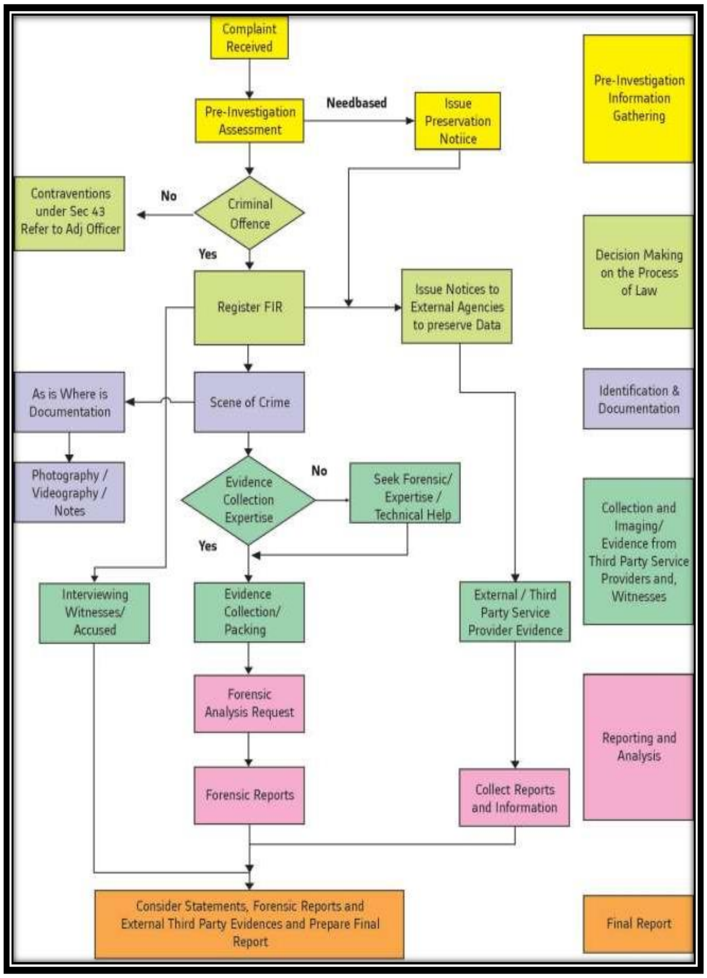
Complaint Received
Pre-Investigation Assessment
Needbased
Issue Preservation Notiice
Pre-Investigation Information Gathering
Contraventions under Sec 43 Refer to Adj Officer
No
Criminal Offence
Yes
Register FIR
Issue Notices to External Agencies to preserve Data
Decision Making on the Process of Law
As is Where is Documentation
Scene of Crime
Identification & Documentation
Photography / Videography / Notes
Evidence Collection Expertise
No
Seek Forensic/ Expertise / Technical Help
Yes
Collection and Imaging/ Evidence from Third Party Service Providers and, Witnesses
Interviewing Witnesses/ Accused
Evidence Collection/ Packing
External / Third Party Service Provider Evidence
Forensic Analysis Request
Reporting and Analysis
Forensic Reports
Collect Reports and Information
Consider Statements, Forensic Reports and External Third Party Evidences and Prepare Final Report
Final Report

Figure 1: Flow Chart for Digital Crime Investigation Under ITAA 2008

Many criminals use cloned cellular telephones for illegal activities, because their calls are not billed to them, and are therefore much more difficult to trace. This phenomenon is especially prevalent in drug crimes. Drug dealers need to be in constant contact with their sources of supply and their confederates on the streets. Traffickers acquire cloned phones at a minimum cost, make dozens of calls, and then throw the phone away after as little 'as a day' use. In the same way, criminals who pose a threat to our national security, such as terrorists, have been known to use cloned phones to thwart law enforcement efforts aimed at tracking their whereabouts [11].

SMS spoofing

SMS spoofing is like e-mail spoofing, which looks to originate from your acquainted number but in reality it is spoofed, and send from some evil minded individual. We can take this by an example. Suppose if a woman receive a Short Messaging Service (SMS) in her cellphone in the middle of a night from the mobile of her spouse asking her to bring cash as he has met with an accident. The chances are that she would check the mobile number and if she confirms that the cell is her husband's then she would rush out with cash. If this could be the response then the chances are that she is not aware of "Mobile Spoofing". Using web-based software, a cybercriminal could send anyone a message from any person's cell without even touching his mobile and no cellular service provider can say that it was a spoofed or faked one.

The aim of the Act seems to be covering governance and facilitating commerce by providing infrastructural facilities for creation, promotion and use of digital signatures as also providing for electronic records. Further the aim of IT Act was to make a shift from the paper based system to electronic system whereby the communication and storage of data would be through the electronic media rather than on the paper [12].

Legal recognition of electronic records and digital signatures authentication and retention of electronic records has been incorporated in the IT Act. Legal recognition to records, files or documents that are retained in electronic form, has been provided in the Act. Public institutions and government departments have been empowered to issue electronic licenses and permits and this is the way for electronic governance and thus the way for electronic governance has been covered. A legal framework has been established by the Act for providing the setting up of a public key infrastructure. As regards the appointment, powers and function of the Controller of Certifying Authorities, provisions have been provided there in and also the duties of the subscribers have been provided. Offences like tempering with computer source document, hacking and publication of obscene information's have been made punishable. The Act also has provided for the establishment of special tribunals Cyber Regulation Appellate Tribunal.

Table 1: Information Technology Act 2000/2008 PUNISHMENT (Amendment)

IT ACT	Information Technology Act 2000/2008 (Amendment)	PUNISHMENT
65	Tampering with Computer Source Code	3 year &/or fine upto 2 lakh
65 B	Admissibility of Electronic Records	Indian Evidence Act
66	Hacking	5 lakh/ 3 year
66 B	Stolen Computers etc.	3 year & or fine upto 1 Lakh
66 C	Identity Theft and Personation	3 year & fine upto 1 lakh
66 D	Punishment for cheating by personation by using computer resource	3 year & fine upto 1 lakh
66 E	Violation of Privacy	3 year &/or fine upto 2 Lakh
66 F	Cyber Terrorism	Life time
67	Publishing Obscene Material	1. 3 year & 5 lakh 2. 5 year & 10 lakh
67 A	Publishing Sexually Explicit Act	1. 5 year & fine upto 10 lakh 2. 7 year & fine upto 10 Lakh

67 B	Publishing Child Pornography	1. 5 year & fine upto 10 lakh 2. 7 year & fine upto 10 Lakh
67 C	Prevention and retention of information by intermediaries	3 year/fine
68	Non-compliance with Controller's Order	2 year & or 1 lakh
69	Failure to Decrypt Information	
69 A	Blocking and Interception of Information	7 year & fine
69 B	Power to authorized to monitor & collect traffic data or information through any computer resources for cyber security	3 year/fine
70	Accessing Protected System	10 year and fine
70 B	Service provider fail to provide data	1 year/fine

Another salient feature of the Act is that the courts while interpreting the IT Act, have to bear in mind that though “the focus is paperless means of communication, it is not intended save, as otherwise expressly provided in the IT Act, to alter fundamental doctrines and requirements of paper based communication.” Because the model law represents a compromise of paper based documentation and communication and electronic means of communication and the states were allowed to adopt their domestic legislations to developments in communication technology applicable to trade law without necessitating the wholesale removal of the paper based requirements or disturbing the legal concepts and approaches underlying those requirements [13]. The States have also been given a mandate by the model law to exclude any transaction from the Act.

The Information Technology Act, 2000 has been substantially amended by the Information Technology (Amendment) Act, 2008 whereby numerous cyber-crimes have been added to the law. After the amendments, the-I.T. Act, 2000 defines the maximum number of offences, after the

Indian Penal Code, 1860. The I.T. Act, 2000 can now be said to be a quasi-penal statute. The dominant theme of the I.T. Act, 2000 after amendments introduced therein by the I.T (Amendment) Act , 2008, is its penal character. Since penal statutes have far reaching implications on personal liberty, it is imperatively necessary to critically examine and test the various offences defined by law, on the touchstones of reasonableness, necessity, and implications from the social and the individual's perspective [14].

Section 43 of the act envisages the penalty for the damages to the computer, computer system, etc. under this section; clauses have been identified for which the person, so misusing, damaging or making unauthorized use of a computer, computer system o computer network, may be held liable for the offences and may be made to pay compensation to the person who has been adversely affected by his misdeeds.

Two Pal ghar Girls arrested for Facebook Post

Two young women were arrested on charges of "promoting enmity between classes" and "sending offensive messages through a communication service," after one posted, and the other 'liked,' a message on Facebook, questioning the Mumbai band h that followed Shiv Sena leader Bal Thackeray's death. The Post Reads as "With all respect, every day, thousands of people die, but still the world moves on," read the message posted by 21- year old Shaheen Dhada and 'liked' by 20-year old Renu Srinivasan from Palghar. The post continued: "Just due to one politician died a natural death, everyone just goes bonkers. They should know we are resilient by force, not by choice. When was the last time, did anyone showed some respect or even a two-minute silence for Shaheed Bhagat Singh, Azad, Sukhdev or any of the people because of whom we are free-living Indians? Respect is earned, given, and definitely not forced. Today, Mumbai shuts down due to fear, not due to respect." The women were earlier booked for hurting religious sentiments under Section 505(2) of the Indian Penal Code, along with Section 66A of the Information Technology Act.

Result

The Ministers of Justice or Ministers or Attorneys General of the Americas in the Organization of American States (OAS) recommended in Peru in 1999 the establishment of a group of governmental experts on cybercrime. At a meeting in

Trinidad and Tobago in 2002 recommendations were adopted giving the Group of Experts the following mandate: "To consider the preparation of pertinent inter-American legal instruments and model legislation for the purpose of strengthening hemispheric cooperation in combating cybercrime, considering standards relating to privacy, the protection of information, procedural aspects, and crime prevention."

Consideration of recommendations was discussed at a meeting in Washington D.C., June, 2003 The Fifth Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas in Washington D.C. on April, 2004, approved conclusions and recommendations to the General Assembly of the OAS, including as follows: "That Member States evaluate the advisability of implementing the principles of the Council of Europe Convention on Cybercrime (2001), and consider the possibility of acceding to that convention."

The General Assembly of the Organization of American States requested at the Meeting on June 7, 2005, the Permanent Council to convene the meeting of the Group of Governmental Experts on Cybercrime. The Organization of American States, in cooperation with the Council of Europe and Spain, organized a conference in Madrid on December, 2005 [15].

Table 2: Some of The Best Safety Apps For Women In India.

App	**Download**	**Rating**
Life360-Family Locator	50,000,000+	4.5
bSafe	500,000+	3.7
Watch.Me	100,000+	3.8
Shake2Safety	100,000+	3.7
Himmat Plus	50,000+	4.4

My SafetyPin	50,000+	3.9
Smart24x7	50,000+	3.0
Raksha	10,000+	4.4
Chilla	10,000+	4.2
Rescuer	5,000+	4.4

Acknowledge the importance of the only international treaty in this field: the Convention on Cybercrime which is open to all States as well as the importance of strengthening the international legal framework; Strongly encourage States to consider the possibility of becoming Parties to this Convention in order to make use of effective and compatible laws and tools to fight cybercrime, at domestic level and on behalf of international cooperation; Recognize the need of pursuing cooperation, providing technical assistance and organizing similar events in other regions of the world.

The Permanent Council of the Organization of American States resolved on December 15, 2005, that the Group of Governmental Experts on Cybercrime should meet on February 27-28, 2006, for the purpose of carrying out the mandates referred to in the conclusions and recommendations of the Fifth Meeting of Ministers of Justice on April 28-30, 2004.The Group of Governmental Experts on Cybercrime met in Washington D.C. February 27- 28, 2006.

The Asia Pacific Economic Cooperation

The Ministers and Leaders of the Asia Pacific Economic Cooperation (APEC) have at a meeting in 2002 made a commitment to: “Endeavour to enact a comprehensive set of laws relating to cyber security and cybercrime that are consistent with the provisions of international legal instruments, including United Nations General Assembly Resolution 55/63 (2000) and Convention on Cybercrime (2001) by October 2003.” After the 9/11 attacks on the U. S., the APEC Leaders issued a Statement on Counter Terrorism, condemning terrorist attacks and considering it urgent to reinforce collaboration at different layers to fight against terrorism. The Leaders called for reinforcing APEC activities to protect critical infrastructure.

In a Ministerial Meeting in Santiago, Chile, November 2004 it was agreed to strengthen the respective economies ability to combat cybercrime by enacting domestic legislation consistent with the provisions of international legal instruments, including the Convention on Cybercrime (2001), and relevant United Nations General Assembly Resolutions.

In 1985 OECD has listed number of document included unauthorized access, damage to computer data or computer programmes, computer sabotage, unauthorized interception, and computer espionage as offences against confidentiality and integrity. The Organization for Economic Cooperation and Development officially approved the Guidelines for Consumer Protection in the Context of Electronic Commerce, representing member states' consensus in the area of consumer protection for e-commerce. The OECD adopted Guidelines for the Security of Information Systems and Networks in July 2002, calling on member governments to "establish a heightened priority for security planning and management", and to "promote a culture of security among all participants as a means of protecting information systems and networks". The guidelines established nine principles, including awareness, responsibility, response, ethics, democracy, risk assessment, security design and implementation, security management, and reassessment.

United Nations

The United Nations (UN) comprises a multitude of agencies, a number of which have an interest in discrete issues. The International Telecommunications Union, for example, has promoted global standards in relation to lawful intercept capabilities for law enforcement access. As a truly global intergovernmental institution, the perspective of UN agencies inevitably tends to encompass to a greater extent the needs of developing countries than the organizations discussed above.

One particular area of concern has been to assist developing countries to establish the capacity and expertise to be able to deal effectively with computer crime issues. To support such initiatives, the UN published a

'Manual on the prevention and control of computer-related crime' in 1994. The Manual examines the need for substantive and procedural law reforms, crime prevention through data security, and international cooperation.

A Resolution on combating the criminal misuse of information technologies was adopted by the General Assembly on December 4, 2000 (A/res/55/63), including as follows: States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies; Legal systems should protect the confidentiality, integrity, and availability of data and computer systems from unauthorized impairment and ensure that criminal abuse is penalized.

In the area of child protection, the United Nations Children's Fund (UNICEF), with the support of the Office of the High Commissioner for Human Rights, has taken a particular interest in child pornography, under its Convention on the Rights of the Child In 2000, an 'Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography' was adopted, entering into force in January 2002, although the UK has not ratified the Optional Protocol.

This formulation would seem broad enough to cover virtual images created without directly involving a child. The Protocol calls upon States to criminal lise the 'producing, distributing, disseminating, importing, exporting, offering, selling or possessing' or such material.

Table 3: Legal Frameworks, Challenges, and Recommendations For Addressing Cybercrime

Aspect	**Details**
Cybercrime Types Affecting Women and Children	Cyber bullying, online harassment, identity theft, cyber stalking, child pornography, and online exploitation.
Legal Framework in India	**N formation Technology Act, 2000 (IT Act)**: Addresses cybercrimes like cyber bullying and identity theft.

	- **Indian Penal Code (IPC)**: Sections on sexual harassment, voyeurism, and child sexual abuse material (Section 67B). - **Protection of Children from Sexual Offences Act (POCSO)**: Protection against online exploitation and abuse of children.
Key Legal Safeguards	**Section 66A of IT Act** (repealed in 2015): Previously dealt with offensive online content. - **Section 354C & 354D of IPC**: Addresses voyeurism and stalking online. - **Cyber Crime Cells**: Set up to address and investigate online crimes.
Challenges in Enforcement	**Lack of Specialized Law Enforcement**: Insufficient training for police in handling cybercrimes, especially those related to women and children. - **Jurisdictional Issues**: Cross-border nature of cybercrimes complicates enforcement. - **Delayed Legal Process**: Slow judicial processes in addressing digital crimes.
Challenges for Victims	**Fear of Social Stigma and Victim Blaming**: Women and children hesitate to report cybercrimes due to societal judgment. - **Lack of Digital Literacy**: Many victims, especially women and children, lack awareness about how to safeguard themselves online or seek help.

To date, computer crime issues have only been the subject of express resolutions from the United Nations General Assembly on two occasions. In 1990, the General Assembly endorsed the recommendations of the Eighth United Nations Congress on the

Prevention of Crime and the 'treatment of Offenders, which included a resolution on computer-related crimes'. In 2001, a second General Assembly resolution was adopted, 'Combating the criminal misuse of information technologies'. The resolution made a series of general recommendations to Member States concerning the need to eliminate safe havens and to improve cooperation between national law enforcement agencies.

Most recently, computer-related crime was one of the topics considered during a workshop at the Eleventh United Nations Congress on Crime Prevention and Criminal Justice, held in Bangkok in April 2005.

Every person in this country in one way or the other is using or becoming part of the cyber world. Every technology has its advantages and disadvantages, so does the information and communication technology. The advent of information technology has made our work easier but also it makes us vulnerable to number of crimes which are committed over the internet medium. The main problem lies with the control of cybercrime is that it is committed in borderless world and regulated by national laws, where the law is still struggling to define and redefine the boundaries for the control of cyber-crimes.

We require international co-operation and international Harmonization in controlling the menance of online criminal activities. The cyber-crime is far different from conventional crimes, so it is very hard for the law enforcement agencies to deal with the cyber-crime with the same old approach. We need to have different outlook and adequate knowledge and training for the law enforcement agencies to control the rising cyber-crimes. The conventional approach while dealing with the cyber-crime is the biggest reason why this new variety of crime is posing challenge to the legal regime in every country. The enactment of the Information Technology Act, 2000 as specific legislation to control the cyber-crime as well as providing protection to e-commerce is the step in the right direction by the government of India.

Conclusion

The rise of the internet and digital technologies has brought numerous benefits, but it has also given rise to alarming new threats, particularly in the form of cybercrime against women and children. In India, women and children are increasingly vulnerable to various forms of online abuse, including cyber stalking, sextortion, online harassment, child pornography, and cyber bullying. These crimes not only cause psychological trauma but can also lead to serious long-term consequences for the victims. As digital spaces continue to expand, it is crucial to assess the legal safeguards in place and the challenges that hinder the effective protection of vulnerable populations. India has made strides in addressing cybercrime through legislation such as the Information Technology Act, 2000 (IT Act, 2000), and the Indian Penal Code (IPC), which include provisions for offenses like cyber stalking, identity theft, and the distribution of child sexual abuse material (CSAM). Specific sections, like Section 66E (violation of privacy) and Section 67B (punishment for publishing or transmitting child pornography), aim to provide a legal framework for protecting women and children from online exploitation Moreover, recent reforms such as the Criminal Law (Amendment) Act, 2018, have strengthened provisions against sexual offenses and have broadened the scope of cyber harassment and cyber stalking. Despite these legal advancements, significant challenges persist. Underreporting of cybercrimes remains a major issue, as victims—especially women and children are often hesitant to come forward due to social stigma, fear of retribution, or a lack of awareness of legal rights. Furthermore, law enforcement agencies often lack the expertise, resources, and technological tools to effectively investigate and prosecute cybercrimes, especially those involving advanced technologies like social media platforms, encryption, and dark web activities. The complex and often anonymous nature of cybercrimes complicates the identification and apprehension of perpetrators. Criminals can operate across borders, making it difficult for Indian authorities to engage in cross-border cooperation and enforce laws effectively. The global nature of the internet further complicates the ability to safeguard victims, as offenders can often exploit legal loopholes in different jurisdictions. Additionally, legal safeguards remain insufficient in addressing the nuances of online abuse, particularly when it comes to issues like cyber grooming, revenge porn, and online trafficking. There is also a lack of comprehensive protection for victims, including the provision of mental health support and rehabilitation services. Women and children who face online abuse often experience prolonged psychological harm, which is not always adequately recognized or addressed by the law.

Reference

1. Agarwal, M. (2022). Cybercrimes against women in India: A review of literature. Journal of Criminology and Criminal Justice, 14(1), 71-84.
2. Arora, P., & Arora, A. (2021). Cybercrime against women in India: A study of trends and patterns. Journal of Cyber Security and Digital Law, 6(1), 1-18.
3. Chaturvedi, S., & Mishra, A. (2020). Cybercrimes against women in India: A study of the modus operandi and impact. Journal of Law, Policy and Globalization, 64, 103- 117.
4. Dixit, A. (2019). Cybercrimes against women in India: A study of the legal and social dimensions. Journal of Criminology and Criminal Justice, 11(2), 159-176.
5. Gupta, S. (2021). Cybercrimes against women in India: A study of the challenges and opportunities. Journal of Law, Technology and Policy, 14(2), 1-22.
6. Abbasi, A., & Abbasi, M. (2022). Cybercrimes against women: A global perspective. Journal of Cyber Security and Law, 7(1), 1-16.
7. Bhuyan, M., & Das, P. (2021). Cybercrimes against women in South Asia: A study of trends and patterns. Journal of Cyber Security and Digital Law, 6(2), 1-18.
8. Das, S., & Bhattacharyya, S. (2020). Cybercrimes against women in India and Bangladesh: A comparative study. Journal of Law, Policy and Globalization, 65, 113- 128.
9. Gupta, A., & Singh, S. (2019). Cybercrimes against women: A global perspective. Journal of Criminology and Criminal Justice, 11(3), 235-252.
10. Kumar, A., & Yadav, A. (2021). Cybercrimes against women: A study of the challenges and opportunities. Journal of Law, Technology and Policy, 14(3), 1-22.
11. National Crime Records Bureau. (2022). Cybercrime in India, 2020. Ministry of Home Affairs, Government of India.
12. United Nations. (2019). Cyber violence against women and girls: A global overview. United Nations Women.
13. Kumar, A., & Yadav, A. (2021). Cybercrimes against women: A

study of the challenges and opportunities. Journal of Law, Technology and Policy, 14(3), 1-22.

14. National Crime Records Bureau. (2022). Cybercrime in India, 2020. Ministry of Home Affairs, Government of India.

15. United Nations. (2019). Cyber violence against women and girls: A global overview. United Nations Women.