



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

CYBER DELINQUENCY IN INDIA: A CRITICAL ANALYSIS OF EMERGING TRENDS, LEGAL CHALLENGES AND POLICY REFORMS

~ *Abhishek Suchari & Dr. Praveen Kumar Mall*

Abstract

Cyber Delinquency poses a significant challenge in India's rapidly expanding digital ecosystem, particularly emphasizing on juveniles who have a greater tendency to deviate and start doing unlawful act. The dependence on technology has led to new and evolving crimes especially done by youth such as circulating morphed videos or photos, online harassment, using artificial intelligence or deepfake technology. It can harm the victim in mental as well as psychological was, affecting the family and loved ones of both the victim and accused. In India there are various legal framework such as Bharatiya Saksha Sanhita 2023, Information Technology Act 2000, Juvenile Justice act. The domain of cybercrime is vast of which cyber delinquency is a part. Cyber Delinquency poses challenges such as investigative and prosecution challenges while proposing evidence based policy reform focusing on data prevention, digital literacy, child-centric cyber governance focusing on rehabilitation and addressing juvenile cyber offending in India

Keywords- Cybercrime, juveniles, policy reforms, cyberbullying, Cyber criminology

The 21st century has seen an unprecedented technological revolution. There has been a rapid rise of the Internet, smart phones, artificial intelligence, social networking platforms, and digital financial systems has altered every aspect of human life. Digital technologies are helped in the development in the field of communication, commerce, governance, education, health care and entertainment. These developments have brought significant changes and has also opened up opportunities for new forms of criminal behaviour.

Cyber delinquency represents the unlawful or antisocial behaviour committed by using computers, digital devices, or Internet-enabled technologies. It ranges from cyberbullying by adolescents to sophisticated financial fraud, hacking, identity theft, ransomware attacks, online child exploitation, cyber terrorism, and digital piracy.

Meaning, Concept, Scope and Nature of Cyber Delinquency -

According to Jaishankar in his book “Cyber Criminology” states “Cyber delinquency is deviant or illegal activity carried out by means of computers, digital networks, mobile devices or the Internet. It includes both juvenile and adult offenders that abuse information technology to breach legal and social norms.

Cybercrime, unlike conventional crimes, does not require physical presence. Victims can be found by offenders anywhere in the world, and they can be anonymous behind digital identities.”

Cyber Criminology is "the study of causation of crimes that occur in cyberspace and their impact in physical space."

The Scope of cybercrime is wide with includes crime against individual, crime against property, against children, women etc. Some of which are

- Crime against Individual- There are several cybercrime such as identity theft, cyber stalking, cyber bullying , online harassment etc.
- Crime against Property- Computer hacking, data theft, software privacy
- Crime against children- Child pornography, sexual exploitation, pedophilia
- Crime against Women- Fake social media account, image morphing, cyber harassment, online abuse
- Crime against organizations- data breaches, industrial espionage, corporate hacking, ransomware

Nature of cybercrime is that it is borderless, anonymity, highly technical, dynamic, difficult to detect, can be on a global level, high economic impact.

Growth of Internet and Digital technologies in India

The growth of digital technology has been both boon and bane for India while it has helped in fields such as digital banking, e-commerce, digital governance, online education, cloud

computing. It has helped in rapid internet penetration, affordable smartphone for every class of people.

Types of Juvenile Cyber offences

Though a exclusive classification cannot be proposed but can be categorized into-

- Unauthorized Access- young offenders may bypass passwords, alter websites, interfere with online services. The youngsters need to be trained to perceive hacking as a technical challenge rather than a criminal offence.
- Cyberbullying and Online harassment- its common form includes abusive messages, spreading false rumors, creating fake profiles, online threats, circulating offensive videos.
- Digital piracy- It refers to unauthorised downloading, uploading, copying, distributing of music, photo, videos and other digital content.
- Online Financial Fraud- It includes financial crimes such as phishing, identity theft, fake online shopping websites, gaming account fraud.
- Malware Development and distribution- It includes creating or distributing computer viruses, ransomware, spyware, keyloggers.
- Online sexual offences- It refers to sharing intimate images without consent, sextortion, online grooming, coercive sexual communication.
- Online Gaming offences- It includes offences such as hacking gaming server, stealing gaming accounts, virtual currency fraud, illegal trading of digital assets in game.
- Cyber Vandalism- It refers to website defacement, deleting digital information, damaging educational portals.

Difference between Cybercrime and Cyber Delinquency-

Cybercrime is as broad legal concept which refers to all unlawful acts committed while cyber delinquency refers to unlawful crimes committed by juveniles through use of digital technology.

Cybercrime refers to a broad concept including adult and juvenile offenders focusing upon criminal liability, governed by criminal law. Its punishment emphasizes on deterrence. On the other hand cyber delinquency refers to specialized branch of juvenile delinquency, primarily committed by children, it focuses upon juvenile behavior and rehabilitation. They are governed by criminal as well as cyber laws of a country.

Criminological Theories implication on Juvenile cyber delinquency

- Space Transition theory- is one of the first criminological theory to explain cybercrime. According to this theory, cyberspaces provides anonymity, identity flexibility, absence of immediate physical control, reduced fear of punishment. Its application on juvenile is that it tries to explain juvenile delinquency because juvenile tend to often create anonymous online identities, perceive online behavior as a game.
- Social Learning Theory- It was developed by Albert Bandura, who argues that criminal behavior is learned through observation, intimation, interaction with others. Juvenile may learn phishing techniques, online fraud, hacking techniques.
- Differential Association Theory- It was developed by Edwin Sutherland stating criminal behaviour can be learned through interaction. Youngster can easily join piracy communities, dark web network etc.
- Self-control Theory- Gottfredson and Hirschi state that low self-control individual are more likely to commit crimes. It can include cyberbullying, account hacking.
- Rational Choice Theory- It views offenders as decision makers who compare expected benefits against possible risks. Many Juveniles believe that police cannot trace them, fake account provide them anonymity.
- Neutralization Theory- It states that offenders justify unlawful conduct before or after the act is committed. Common justification include everyone downloads movies illegally, it was a joke etc.
- General Strain Theory- It postulates that crime can be result of frustration , to gain recognition, peer rejection, family conflict

Emerging Trends in Cyber Delinquency in India

India has undergone a significant shift over the last few decades. The digital revolution has helped in low cost of internet service, affordable smartphone for all classes , online education, social networking apps have altered the lifestyle of youth. The youth are among the most active internet user, online gamers, video streaming. These technological advancements have also increased the crime among the youth, creating new opportunities for juvenile cyber delinquency.

Instances such as cyberbullying, financial fraud , hacking, software piracy, cryptocurrency scams have increased in India as it is developing field. Unlike juvenile delinquency , these crimes are committed in anonymity, without any geographical boundary.

- Increasing Internet penetration among juveniles- The rapid spread of internet access among children and adolescents is one of the most important trends contributing to cyber delinquency in India. Smartphones availability, large availability of 4G and 5G connectivity, online education, and digital entertainment have led young people to spend several hours a day in cyberspace. According to the article Combating the Clutches of Cyber Delinquency in India, “Indian juveniles are increasingly normalizing excessive internet usage, without having a proper understanding of the legal or ethical implications of their online behaviour. Due to increased reliance on digital platforms, minors are at risk for both cyber victimization and cyber offending.”
- Rise of Cyberbullying and online harassment- Cyberbullying has emerged as a prevalent form of cyber delinquency. Common forms include trolling on social media, circulating fake or morphed photo or video, online defamation, abuse a person. Due to this victim suffer psychological as well as mental trauma
- Online Gaming and gaming related crimes- Online gaming is one of the fastest growing digital activities. It includes theft of gaming account, using it for fraud, identity personation etc.
- Sextortion and Image based sexual abuse- It is an emerging as well as disturbing trend which include fake friendship, social media platforms. Victim trust the offender who later blackmail, extort money or give any sexual favors.
- Juvenile Involvement in financial crimes- It includes UPI fraud, phishing , QR code scam, unauthorised digital transactions
- Digital Piracy and Copyright Violations- Youngsters frequently download or distribute movies, music, electronic books, video games etc. without any authorization from copyright owner.
- Social Media based Identity crimes- The use of social media applications such as WhatsApp, Facebook, telegram etc. have seen an increased offences such as fake profile, identity theft, account hacking, misinformation
- Artificial Intelligence and Deepfake Technology- It is one of the emerging form of crimes which include deepfake videos, voice cloning, AI generated fake photographs, AI assisted identity fraud.
- Dark Web and Anonymous Communication platforms- The increase use of virtual private network has increased in illegal software sharing , illicit online market, platforms such as onion peel.

- Cyber Delinquency through educational technology- It includes hacking online examination portals, plagiarism through AI tools, circulation of examination papers.

These persistent problems need to be looked upon as problems like inadequate cyber forensic infrastructure, shortage of trained professions , poor cyber awareness needs to be addressed.

Causes and Factors Responsible for Cyber Delinquency in India

The rapid expansion of digital technology has transformed the nature of juvenile delinquency. Cyber delinquency among adolescents is no longer confined to hacking or software piracy; it now includes cyberbullying, identity theft, online fraud, digital piracy, cyberstalking, sextortion, phishing, and social media abuse. The causes of cyber delinquency are multidimensional, involving psychological, social, economic, technological, and legal factors.

- Easy access to Digital Technology- With the digital revolution an age of cheap smartphone, access to everyone has led to experiment with online activities which can lead to unlawful behavior.
- Online Anonymity- It helps in lowering the feeling of personal accountability and social restraint. They believe as they are not face to face so they couldn't be caught.
- Curiosity and Technological experimentation- Many hackers initially enter cyberspace seeking intellectual challenges rather than financial gain
- Peer Influence and social learning- Juveniles learn online behaviors by observing their friends, peers, classmates, gaming communities. Social learning theory tells us that criminal behaviour is acquired through interaction with others.
- Lack of Cyber Awareness and Digital Ethics- Many youngsters do not realize that illegal downloading, creating fake social media accounts, sharing intimate photographs tend to constitute criminal offences.
- Weak Parental Supervision- Parents often provide their child with smartphones and internet access without keeping tab on the child or educating children about responsible digital behaviour.
- Psychological Factors- These include impulsive decision making, desire for excitement, need for recognition, frustration and anger.
- Online Gaming Environment- It creates virtual environment where youngsters anonymously interact with strangers across the world, can also create interaction with offenders.

- Weak Legal Awareness And Enforcement- Many juveniles believe online crimes are easily detectable, unlikely to result in punishment.
- Availability of Criminal Knowledge online- The youth can get information easily on internet like hacking tools, password cracking software.
- Normalization of minor cyber offences- Many adolescents do not regard digital piracy, downloading copyrighted material as cyber offences as they see that everyone is doing it.

Legal Framework governing Cyber Delinquency in India

There are various acts such as Information Technology Act 2000, Juvenile Justice(Care and Protection of Children) Act 2015, Bharatiya Nyaya Sanhita 2023, Bharatiya Nagarik Suraksha Sanhita 2023 Etc.

- Information Technology Act, 2000-The Information Technology Act, 2000 is India's principal legislation dealing with cyber offences. Although the Act does not contain separate provisions exclusively for juveniles, it applies equally where a child commits an offence through a computer or digital device. When the offender is below eighteen years of age, the provisions of the Juvenile Justice Act govern the procedure, rehabilitation, and adjudication.

Important provisions relevant to juvenile cyber delinquency include:

- “Section 43 – Unauthorized access to computer systems, downloading data, introducing viruses, damaging computer resources, and denial-of-service attacks.
- Section 65 – Tampering with computer source documents.
- Section 66 – Computer-related offences committed dishonestly or fraudulently.
- Section 66B – Receiving stolen computer resources or communication devices.
- Section 66C – Identity theft through misuse of passwords, digital signatures, or electronic authentication.
- Section 66D – Cheating by personation using computer resources, including phishing and online fraud.
- Section 66E – Violation of privacy through capturing or transmitting private images.
- Section 66F – Cyber terrorism.
- Section 67 – Publishing or transmitting obscene electronic material.
- Section 67A – Publishing sexually explicit material electronically.

- Section 67B – Publishing, browsing, collecting, or transmitting child sexual abuse material.”
- The Juvenile Justice (Care and Protection of Children) Act, 2015 provides the legal framework governing children alleged to have committed cyber offences. The Act is founded upon the principles of rehabilitation, reform, reintegration, child-friendly justice, best interests of the child.
- Bharatiya Nyaya Sanhita, 2023 (BNS)- The Bharatiya Nyaya Sanhita, 2023, which replaced the Indian Penal Code, complements the Information Technology Act by addressing conventional offences increasingly committed through digital means. Several offences frequently associated with cyber delinquency include cheating using digital platforms, forgery of electronic records, identity theft, criminal intimidation through electronic communication, publication of obscene content, defamation through social media, extortion, stalking, voyeurism, sexual harassment.
- Bharatiya Sakshya Adhiniyam, 2023 (BSA) Cyber offences depend almost entirely upon electronic evidence. The Bharatiya Sakshya Adhiniyam, 2023, replacing the Indian Evidence Act, modernizes evidentiary rules governing electronic records, emails, WhatsApp chats, CCTV footage, cloud storage, digital signatures, metadata, server logs, social media posts, electronic documents.
- Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS)- The BNSS replaces the Code of Criminal Procedure and governs the investigation, arrest, search, seizure, trial, and procedural safeguards relating to cyber offences. Important procedural features include: electronic registration of FIRs, electronic summons, use of audio-video recording during investigation, electronic documentation, digital forensic investigation, electronic production of evidence.

Challenges in Investigation and Prosecution

- Difficulty in identifying juvenile offenders- It includes challenges such as fake identities, using of virtual private network, proxy servers, public Wi-Fi networks etc.
- Problems in collecting and preservation of electronic evidence- Cyber offences depend upon browser history, CCTV footage, WhatsApp chats, metadata.
- Jurisdictional and Cross-Border offences- It is a major challenges as cyber offences can be done from any place across the globe.

- Rapid Technological Advancements- Evolution of technologies lead to new crimes such as AI based, Deepfake technology, blockchain etc.
- Inadequate Cyber Forensic Infrastructure- There are shortage of cyber forensic laboratories, forensic equipment, funding etc.
- Challenges in Proving Criminal Intention- The juveniles plead that they have done the act out of curiosity, as a joke or for entertainment purposes.
- Delayed Reporting of cyber offences- Many victims(youth) hesitate to report cyber offences due to embarrassment, fear of social stigma, reaction of parents.
- Limited cooperation from technology companies- The companies which have created social media platform, internet service providers do not cooperate which led to delay in obtaining information, privacy restrictions.

Policy Reforms and Recommendations

- Adopt a public health and consider whole society approach- According to Davidson and Farr, there shall be four level intervention of which first should primary prevention through awareness for all school children above 12 years. Secondly programs for 1st Time juvenile offender, then thirdly cyber-smart intervention programmed for children already involved in cybercrime and lastly post sentence community support.
- Strengthen Digital Literacy and Cyber Ethics Education
- Develop positive career pathways related to cyber talented youth
- Improve parental and community participation
- Strengthen multi-stakeholder collaboration- Coordination is needed between government agencies, schools ,technological companies , internet service providers.
- Enhance cybercrime legislation and juvenile specific policies
- Continuous training of professionals such as police officers, judges, prosecutors etc.
- Increase research and evidence based policy making which shall include long term research on youth cybercrime, evidence based legislation.
- Improve International cooperation.
- Awareness campaigns for the society.

Practical Impact Assessment

Cyber Delinquency has emerged as a evolving form of juvenile offending which demands a balanced legal and social approach. While India's framework such as IT Act 2000, JJA Act

2015 and other laws help in providing a foundation to address cyber offences but still significant challenges remain in various fields such as investigation, prosecution. A comprehensive approach which considers supervision of parents, digital awareness, law enforcement, technological safeguards are required. Adopting a child-centric multi-stake approach will help India to effectively combat cyber delinquency and protecting rights of young offenders.

The study makes a practical contribution by referring to the growing problems of cyber delinquency amongst juvenile in India. It also helps to identifying measures which can be implemented by policy maker, educational institutions, Law enforcement agencies highlights to move from a punitive approach towards a child centric framework. The study also provides a understanding of emerging forms of juvenile cyber offending which includes identity theft, digital privacy, online fraud, etc.

The findings are that there is a need to strengthen the information technology act, the juvenile justice (care and protection of children) act 2015 and BNS 2023 to accommodate this new type of crimes and cyber offenders. The educational solutions there should be research which should emphasize integration of cyber ethics, digital citizenship and online safety in school curriculum. It will help in reducing risky online behaviour among juveniles. There is also a need to teach parents and the community about internet, use its benefit and mishaps. The approach also provides an evidence based framework that can support future academic research, reforms, etc. The study also contributes to the development of a safer digital environment for children while reinforcing the principles of rehabilitation protection in juvenile Justice in India.

References

- Brenner, S. W. (2010). *Cybercrime: Criminal threats from cyberspace*. Praeger.
- Britz, M. T. (2013). *Computer forensics and cybercrime: An introduction* (3rd ed.). Pearson Education.
- Davidson, J., & Farr, R. (2026). *Pathways into and out of youth cybercrime: Research findings*. Routledge.
- Dutt, R., & Tayal, M. (2025). *Cybercrime and juvenile justice: Legal challenges and reforms*. *International Journal of Creative Research Thoughts*, 13(5).

- Gupta, C. (2022). Combating the clutches of cyber delinquency in India. *Indian Journal of Integrated Research in Law*, 2(1).
- Jaishankar, K. (Ed.). (2011). *Cyber criminology: Exploring internet crimes and criminal behavior*. CRC Press.
- Kirwan, G., & Power, A. (2012). *The psychology of cybercrime: Concepts and principles*. Information Science Reference (IGI Global).
- Onwuadiamu, G. (2025). Cybercrime in criminology: A systematic review of criminological theories, methods, and concepts. *Journal of Economic Criminology*, 8, 100136.
- Mall, P. K. (2026). Historical understanding and constitutional development of freedom of speech and expression under the Indian Constitution. *International Journal for Multidisciplinary Research (IJFMR)*, 8(1).
- Shipley, T. G., & Bowker, A. (2014). *Investigating internet crimes: An introduction to solving crimes in cyberspace*. Syngress/Elsevier.
- Yar, M., & Steinmetz, K. F. (2019). *Cybercrime and society* (3rd ed.). SAGE Publications.
- Bharatiya Nagarik Suraksha Sanhita, 2023 (Act No. 46 of 2023).
- Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023).
- Bharatiya Sakshya Adhiniyam, 2023 (Act No. 47 of 2023).
- Information Technology Act, 2000 (Act No. 21 of 2000).
- Juvenile Justice (Care and Protection of Children) Act, 2015 (Act No. 2 of 2016).