Research Paper IMPACT FACTOR VALUE : 5.983 | E-ISSN NO : 2455-295X | VOLUME : 11 | ISSUE : 7 | JULY 2025

INCREASING CYBER CRIMES AMONG URBAN YOUTH IN INDIA: A SOCIOLOGICAL PERSPECTIVE

ANAMIKA SINGH KUSHWAHA [1] | PROF. RAMJEE PRASAD [2]

[1] RESEARCH SCHOLAR, DEPARTMENT OF SOCIOLOGY, D.A-V. (PG) COLLEGE, KANPUR.

[2] HEAD, DEPARTMENT OF SOCIOLOGY, D.A-V. (PG) COLLEGE, KANPUR.

ABSTRACT:

India's digital revolution, driven by initiatives like Digital India, has empowered urban youth aged 15–30, with over 70% regularly using smartphones and social media. However, this connectivity has fuelled a surge in cybercrimes, including cyber bullying, hacking, online fraud, cyber pornography, and social media impersonation, particularly in cities like Delhi and Mumbai. National Crime Records Bureau data from 2023 highlights a significant rise in cases involving young perpetrators and victims, driven by anonymity, peer pressure, economic instability, and limited digital literacy. These crimes cause emotional, financial, and social harm, disproportionately affecting young women and straining India's legal systems. Contributing factors include a generational digital divide, lack of cyber ethics education, and psychological stressors like academic pressure and unemployment. This article analyzes these sociological dimensions, revealing how urban anonymity and online subcultures normalize deviance. It proposes stronger cyber laws, youth-focused awareness campaigns, digital ethics in schools, and mental health support to foster responsible digital citizenship and curb cybercrime effectively.

KEYWORDS:

CYBERCRIME, URBAN YOUTH, DIGITAL LITERACY, SOCIAL MEDIA.

PAPER ACCEPTED DATE:	PAPER PUBLISHED DATE:
12th July 2025	13th July 2025

1. INTRODUCTION

India's rapid digital transformation has made it one of the world's fastest-growing digital economies, reshaping how people connect, work, and access information. With initiatives like Digital India and widespread access to affordable smartphones and mobile networks, over 70% of urban youth aged 15–30 are regular internet users, primarily through personal devices. This digital boom has empowered young people, boosting education, social connections, and entrepreneurial opportunities. However, it has also fueled a darker trend: a sharp rise in cybercrime among urban youth in cities like Delhi, Mumbai, Bengaluru, and Hyderabad. The internet's anonymity and global reach make it easy for youth to engage in cybercrimes like cyber bullying, online fraud, hacking, and identity theft, often driven by thrill-seeking, revenge, or financial gain. The National Crime Records Bureau (NCRB) reported a surge in cybercrime cases involving 18–30-year-olds in 2023, with metropolitan areas as hotspots. These crimes harm individuals and strain India's legal and ethical systems, challenging the safety of digital spaces.

Cybercrime's rise is tied to broader social changes in India's urban centres, where globalization and urbanization create both opportunities and pressures. Many urban youths face a gap between high aspirations and limited resources, leading to frustration and risky behaviour. Constant exposure to social media, influencer culture, and online gaming normalizes aggressive or unethical actions, as sensationalism often gains attention. Youth, still developing their moral compass, are particularly vulnerable to these influences, which can blur the line between fun and crime.

A generational digital divide worsens the issue. Parents, teachers, and policymakers often lack the tech know-how to guide or monitor youth online, leaving them with little oversight. This freedom, combined with psychological stressors like academic pressure, social media comparison, and career uncertainty, can push youth toward cybercrime as a way to cope, assert control, or gain validation. For some, exposure to dark web content or peer encouragement amplifies this risk.

India's response to youth cybercrime has gaps. The Information Technology Act of 2000, amended to address digital crimes, and sections of the Indian Penal Code cover offenses like fraud and defamation, but enforcement is inconsistent. Victims, especially women and minors, often hesitate to report crimes due to stigma or fear. Youth-friendly reporting systems and rehabilitative approaches are needed to prioritize education over punishment. Cybercrime includes hacking, identity theft, phishing, cyber bullying, and cyber stalking, often enabled by tools like encryption or the dark web, which make tracking criminals tough. For urban youth, ignorance of

legal boundaries—like sharing explicit content or unauthorized account access—adds complexity. Addressing this requires a mix of legal, tech, psychological, and social strategies.

This article aims to provide a comprehensive analysis of the sociological dimensions of increasing cybercrime among urban youth in India. It seeks to explore how socio-economic pressures, cultural dynamics, psychological conditions, and technological access converge to create an environment conducive to online deviance. By identifying patterns and root causes, this paper intends to propose practical interventions and policy recommendations to curb this growing threat.

2. THE URBAN YOUTH DEMOGRAPHIC IN INDIA

Urban youth in India, typically aged between 15 and 30, constitute over 35% of the urban population, translating to more than 150 million individuals, as per the Ministry of Statistics and Programme Implementation (MoSPI, 2023). This group is digitally empowered, with over 75% reported to have daily internet access, primarily through smartphones (IAMAI-Kantar ICUBE Report, 2023). Their use of the internet is multifaceted, including education, social media, online gaming, job searches, digital payments, and entertainment. Social media penetration is particularly high in urban India, with platforms like Instagram, WhatsApp, YouTube, and X (formerly Twitter) being extremely popular among this age group. According to the Digital India Report (2024), nearly 90% of urban youth use at least one social media platform daily. While this has opened avenues for communication and self-expression, it has also increased exposure to harmful content, online manipulation, misinformation, and cyber threats.

Furthermore, data from the National Crime Records Bureau (NCRB) 2023 indicates that nearly 60% of cybercrime offenders fall within the age group of 18–30 years, with the majority coming from urban or semi-urban settings. Metropolitan cities like Bengaluru, Mumbai, Delhi, and Hyderabad reported the highest incidence of cybercrime arrests involving youth. The data also revealed a rise in crimes related to social media abuse, financial frauds, and online defamation involving young individuals.

Urban anonymity and peer culture play significant roles. Unlike rural areas, urban neighbourhoods tend to lack the close-knit social fabric that often acts as a deterrent to deviance. This allows urban youth to explore online spaces more freely, often without sufficient parental or institutional oversight. Combined with rising aspirations, exposure to global culture, and an increasing dependence on digital validation, many urban youths find themselves vulnerable to risky online behaviour.

Employment instability further fuels the issue. The Centre for Monitoring Indian Economy (CMIE) reported a youth unemployment rate of over 16% in urban areas as of mid-2024. This economic pressure, coupled with the allure of quick digital money through scams, phishing, and fraud, acts as a catalyst for criminal activity. To compound the problem, there is limited digital ethics education in Indian schools and colleges. The National Education Policy (NEP) 2020 recommends the integration of digital citizenship and cyber hygiene, but implementation remains patchy. Without formal awareness and accountability frameworks, urban youth often do not realize the legal consequences of their digital actions until it is too late.

3. CAUSES OF INCREASING CYBERCRIME AMONG URBAN YOUTH

The surge in cybercrime among urban youth in India stems from a tangled web of technological, social, economic, psychological, and cultural influences. As India races toward digital transformation, young people in cities like Mumbai, Delhi, and Bangalore are increasingly connected, with smartphones and high-speed internet becoming as common as street vendors. Yet, this digital boom has a dark side, pulling some youth into illegal online activities, either as perpetrators or victims. The reasons are complex, ranging from easy access to technology to a lack of awareness about what's legal online, economic pressures, peer influence, and emotional struggles. Below, we explore these factors in a way that feels human and relatable, painting a picture of why cybercrime is gripping urban youth.

TECHNOLOGY: A DOUBLE-EDGED SWORD

India's push for a digital future, through initiatives like Digital India, has put smartphones and 4G or 5G connections in the hands of millions, even in modest urban households. For young people, this is a game-changer—social media, gaming, and endless apps are just a tap away. Urban youth, often called digital natives, dive into these platforms with enthusiasm, exploring everything from Instagram reels to coding forums. But here's the catch: while they're tech-savvy, many don't know the rules of the digital road. For example, a teenager might hack a friend's WhatsApp for a laugh or download pirated software, not realizing these actions could land them in legal trouble. Tools like VPNs or encrypted apps, easily available, make it tempting to cross lines sometimes just for the thrill.

The internet's vastness also means young users can stumble into shady corners without much effort. Picture a curious 17-year-old in Hyderabad finding a YouTube tutorial on phishing or a Reddit thread glorifying hackers. Without guidance from parents or schools, these platforms can glamorize cybercrime, making it seem like a cool, rebellious skill rather than a crime. The accessibility of technology, while empowering, opens doors to risky behavior when not paired with education on ethics or consequences.

NOT KNOWING WHAT'S WRONG

Many urban youths don't realize their online antics could be crimes. Sharing a doctored photo of a classmate, forwarding a private chat, or joining in on a "prank" that humiliates someone online often feels like harmless fun. But these actions can fall under cybercrime laws, like those

in India's IT Act, 2000. The problem? Most kids aren't taught what's illegal. Schools drill computer basics—how to use Excel or code a simple program—but rarely cover cyber ethics or the fact that cyber bullying can lead to jail time.

Misinformation adds fuel to the fire. Many young people believe they're untouchable online, thinking, "No one can trace me," or "I'm just a kid, so it's fine." Social media's cloak of anonymity makes them feel invincible, lowering the mental barrier to doing something risky, like sending a threatening message or trying to scam someone. Without clear education on digital responsibility, urban youth are left navigating a minefield blindfolded.

MONEY TROUBLES AND QUICK FIXES

Urban India is a pressure cooker for young people. With jobs scarce and competition fierce, even college graduates struggle to find stable work. The gap between what they dream of—fancy cars, trendy clothes, the influencer lifestyle—and their reality can be crushing. For some, cybercrime looks like an easy way out. Setting up a fake online store, sending phishing emails, or running a small scam can seem like a low-risk way to make quick cash. Stories of "genius" hackers making millions, splashed across news or social media, only make it more tempting.

Take a 20-year-old in Bangalore, stuck in a dead-end job, scrolling through Instagram and seeing influencers flaunt wealth. The dark web or a Telegram group might offer a "script" for stealing credit card details, promising big bucks with little effort. For youth feeling left behind by the system, cybercrime can feel like a rebellious middle finger to a society that's failed them.

PEER PRESSURE IN THE DIGITAL AGE

Friends have always influenced teens, but now its digital communities calling the shots. Platforms like Discord or Telegram are home to groups where hacking, trolling, or even cyber stalking is treated like a badge of honour. In these spaces, a 16-year-old might earn "clout" by cracking a password or spreading a viral meme that humiliates someone. These online subcultures celebrate deviance, making it feel normal or even admirable—to break digital rules.

In urban schools or colleges, tech-savvy cliques might form, daring each other to pull off small cybercrimes, like stealing data or pranking a teacher's email. What starts as a joke can spiral, as group dynamics push kids to take bigger risks to prove themselves. Once sucked into these circles, it's hard to back out without losing face or feeling isolated.

EMOTIONAL STRUGGLES FUELLING BAD CHOICES

Urban youth face intense pressure—ace exams, land a dream job, look cool online. This constant race can leave them stressed, anxious, or even depressed. For some, the internet is an escape, a place to vent or feel powerful. A teen feeling ignored might turn to cyberbullying to lash out, while another might hack a rival's account to settle a score. The anonymity of the internet makes it easy to act on impulses without facing immediate consequences.

Mental health support in India's cities is often out of reach—either too expensive or stigmatized. A young person grappling with loneliness or anger might not seek help, instead channelling their emotions into harmful online behaviour. For those craving attention, the instant fame of pulling off a bold online stunt—like a viral prank or a hack—can be addictive. Without proper support, these emotional struggles become a hidden driver of cybercrime.

4. TYPES OF CYBERCRIME PREVALENT AMONG URBAN YOUTH

As India's urban youth immerse themselves in the digital age, the internet has become a double-edged sword, offering both opportunities and risks. The accessibility of smartphones and high-speed internet in cities like Mumbai, Delhi, and Bangalore has led to a surge in cybercrimes, with young people often playing roles as both perpetrators and victims. These crimes range from emotionally damaging acts to financially motivated schemes, exploiting the anonymity and reach of digital platforms. Below are the key types of cybercrimes affecting urban youth:

Cyber bullying and Trolling: Cyber bullying involves using digital tools like social media, messaging apps, or forums to harass, mock, or intimidate others. Urban youth, deeply engaged on platforms like Instagram, Snapchat, and WhatsApp, frequently encounter or engage in this behaviour. Trolling, a related practice, entails posting provocative or hurtful comments to stir conflict or upset others. These acts can devastate victims, causing anxiety, depression, or even suicidal thoughts. For instance, a teenager in Delhi might face relentless taunts in a group chat, leading to social isolation. Organized cyber bullying campaigns, where groups target an individual, amplify the harm, leaving lasting emotional scars.

Hacking and Data Theft: Hacking involves breaching systems or devices to steal, alter, or destroy data without permission. For some urban youth, hacking starts as a curiosity-driven challenge but can escalate into serious crimes like stealing bank details or personal photos. Data theft is particularly rampant, with stolen information often sold on dark web marketplaces or used for blackmail. With free hacking tools widely available online, even amateurs with basic skills can cause significant damage. For example, a college student in Hyderabad might hack a peer's social media account to settle a personal score, unaware of the legal consequences.

Online Fraud and Phishing: Online fraud includes scams designed to trick people into parting with money or sensitive information. Phishing, a popular tactic, uses fake emails, texts, or websites that mimic trusted entities like banks or e-commerce platforms. Urban youth, eager for quick money or lured by fake job ads, often fall prey to or perpetrate these scams. The rise of digital wallets and online banking has made it easier for fraudsters to target vulnerable youth, who may lack financial literacy. A common scam involves fake internship offers that trick

students into sharing bank details, leading to significant losses.

Cyber Pornography: Cyber pornography encompasses the creation, sharing, or consumption of explicit content online. A troubling trend is the non-consensual sharing of intimate images, often called "revenge porn," where youth share private photos to humiliate or control others. This crime is fueled by peer pressure and the accessibility of adult content online. Some youth also stumble into legal trouble by unknowingly sharing illegal material. The emotional toll on victims, especially young women, is immense, often leading to shame and social exclusion.

Social Media Impersonation: Impersonation involves creating fake social media profiles using someone else's identity to deceive or harm. Urban youth may use these accounts to bully classmates, scam friends, or spread false rumours. For instance, a fake profile mimicking a popular student might be used to post embarrassing content, damaging their reputation. Victims face public humiliation and loss of trust, while perpetrators often underestimate the legal and social consequences of their actions.

5. SOCIOLOGICAL IMPLICATIONS

Erosion of Moral Values: The anonymity of the internet often strips away accountability, encouraging urban youth to act in ways they wouldn't offline. Without parental oversight or digital ethics education, many justify harmful actions like trolling or hacking as harmless pranks. This shift in moral standards fosters an online culture where deceit and aggression are normalized, weakening the ethical foundation of young people.

Impact on Victims: Victims of cybercrimes, often peers of the perpetrators, endure profound emotional and psychological harm. Cyber bullying or image leaks can lead to anxiety, depression, and social withdrawal. In extreme cases, victims may resort to self-harm or face academic setbacks. The personal nature of these attacks, especially when perpetrated by classmates, intensifies the trauma, leaving lasting scars.

Normalization of Deviance: social media often rewards deviant behaviour with likes, shares, or viral fame, making trolling or hacking seem acceptable. Group chats and memes glorify these acts, creating a culture where breaking rules is celebrated. This environment blurs the line between right and wrong, encouraging youth to push boundaries without fear of consequences.

Gendered Impact: Cybercrimes disproportionately harm girls and young women, who face cyber stalking, sexual harassment, or non-consensual image sharing. These acts reflect societal gender inequalities, with female victims often blamed or shamed, discouraging them from reporting incidents. This silence empowers perpetrators, highlighting the need for gender-sensitive policies and awareness campaigns tointre.

6. GOVERNMENT INITIATIVES AND POLICY FRAMEWORK

India has taken several initiatives at the national level to address the challenges posed by the increasing incidence of cybercrime, particularly among the urban youth. These government policies and frameworks aim to build a safer digital ecosystem by promoting cyber hygiene, enhancing legal enforcement, and fostering responsible digital citizenship. The key initiatives include:

Digital India Program: Launched in 2015, the Digital India initiative aims to transform India into a digitally empowered society and knowledge economy. While the program has significantly improved access to digital infrastructure and e-governance services, there is growing recognition of the need to incorporate cyber security awareness and safe internet usage into its objectives. As youth are major beneficiaries of this program, integrating modules on digital ethics, online safety, and cybercrime awareness can play a vital role in prevention.

Cyber Surakshit Bharat: This initiative, launched by the Ministry of Electronics and Information Technology (MeitY) in 2018, seeks to spread awareness about cybercrime and promote the importance of cyber hygiene. It focuses on training Chief Information Security Officers (CISOs) and government officials in cybersecurity practices. Although it primarily targets institutional stakeholders, expanding its reach to educational institutions and urban youth forums can enhance its preventive impact.

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021: These IT Rules mandate that digital platforms, including social media companies, must take down unlawful or harmful content within 24 hours of receiving a complaint. They also require platforms to appoint grievance officers and ensure greater transparency in operations. For urban youth, this translates into quicker responses to issues like cyber bullying, trolling, and impersonation. These rules empower users to report abuse and seek redressal, thus enhancing accountability in the digital space.

Indian Cyber Crime Coordination Centre (I4C): The I4C initiative under the Ministry of Home Affairs is aimed at creating an ecosystem to tackle cybercrime in a coordinated and comprehensive manner. It offers a national cybercrime reporting portal (www.cybercrime.gov.in), which allows individuals, including youth, to report online offenses. It also promotes capacity building for law enforcement agencies, digital forensics, and research on emerging cyber threats.

National Cyber Security Policy (NCSP): Though currently under revision, the existing National Cyber Security Policy provides a broad framework for protecting information infrastructure in cyberspace. It emphasizes promoting cyber awareness among citizens, developing human resources, and fostering public-private partnerships. The upcoming revised policy is expected to further strengthen safeguards for vulnerable groups such as youth.

7. CONCLUSION

Cybercrime among urban youth in India, fuelled by widespread internet and Smartphone use, is a growing issue driven by peer pressure, low digital literacy, and emotional instability. Anonymity online enables deviant acts like hacking or cyber bullying, as youth seek recognition or financial gain. Weak cyber laws and minimal supervision worsen the problem. Solutions require collaboration among government, schools, parents, and tech platforms to strengthen laws, promote digital ethics education, and provide mental health support. By fostering knowledge and empathy, we can empower youth to be responsible digital citizens, curbing cybercrime and ensuring a safer digital future.

REFERENCES

1. Chakraborty, A. (2020). Digital India and the youth: Challenges of cyber security. Journal of Emerging Technologies, 8(3), 55–67.

2. Kumar, P., & Sharma, R. (2021). Urbanization and youth deviance in India. Sociological Studies Quarterly, 12(1), 33–47.

3. Mehta, V. (2019). Peer influence and cybercrime behavior among students. Indian Journal of Psychology, 25(2), 78–89.

4. National Crime Records Bureau (NCRB). (2023). Crime in India Report. Ministry of Home Affairs, Government of India.

5. Patel, S., & Reddy, N. (2020). Mental health and online delinquency: A youth study. Psychological Trends in India, 11(4), 102–118.

6. Saxena, D. (2022). Cybercrime economy and unemployed youth: A rising trend. Economic Review of India, 18(2), 61–72.

7. Wall, D. S. (2007). Cybercrime: The transformation of crime in the information age. Polity Press.

8. Centre for Monitoring Indian Economy. (2024). Unemployment in India: A Statistical Profile. Retrieved from https://www.cmie.com/

9. Digital India Corporation. (2024). Digital India: Transforming India into a Digitally Empowered Society and Knowledge Economy. Ministry of Electronics and Information Technology, Government of India. Retrieved from https://digitalindia.gov.in/

10. Internet and Mobile Association of India (IAMAI) & Kantar. (2023). ICUBE 2023 Report: Digital Adoption and Usage Trends in India. Retrieved from https://www.iamai.in

11. Ministry of Statistics and Programme Implementation (MoSPI). (2023). Youth in India 2023. Government of India. Retrieved from https://www.mospi.gov.in

12. National Crime Records Bureau. (2023). Crime in India – Statistics on Cybercrime. Ministry of Home Affairs, Government of India. Retrieved from https://ncrb.gov.in/

13. National Education Policy (NEP). (2020). National Education Policy 2020. Ministry of Education, Government of India. Retrieved from https://www.education.gov.in