Internet Ubiquity And Cybercrime Targeting Children In India

Bhavana Sharma[1], Prof. (Dr.) Gaurav Kataria[2]

[1] Ph.D. Research Scholar, School of Law, Lovely Professional University Phagwara,
Panjab, India.
[2]Professor, School of Law, Lovely Professional University Phagwara,
Panjab, India.
Email: [1]kaushikbhanu1994@gmail.com, [2]gaurav.26147@lpu.co.in

Abstract

The Internet is pivotal in exchanging information in this information age and technology. The impact of this phenomenon is felt in all areas of human life, among all age groups. Even though the Internet has fundamentally changed our society, information on the Internet is not free from illegal access or harm. Consequently, information security and safety have become our time's significant challenges. The rapid growth of internet users has resulted in increased cybercrime cases, which are not restricted by geographical limitations or national borders. The past few years have seen a significant increase in cybercrime cases in India, which is of grave concern since it negatively affects people's social and economic lives. Criminals are misusing computers and the Internet to commit crimes. Cyberspace and new technologies can lead to violence and harm against children and young people. Cybercriminals use the cyber world to abuse children, which is also a cybercrime. It includes producing, distributing, and using materials depicting child sexual abuse, online solicitation or grooming (securing the trust of children to lure them into situations where they may be harmed), and exposure to materials that can cause psychological harm, physical harm, or facilitate other detriments to children, harassment, and intimidation. As a result of cybercrime, children have become the latest victims. Cyberbullying and grooming online are illegal activities used by criminals to target children. Computers and the Internet are being used to commit crimes against children, including child exploitation, the production, distribution, and possession of child pornography; exposure to harmful content; grooming, harassment, and sexual abuse; and cyberbullying. Research on cybercrime is based on quantitative analysis. An extensive review of cybercrime in India has been conducted in this paper.

Keywords: Internet, Social Media, Cybercrime, Children, Cyberspace security.

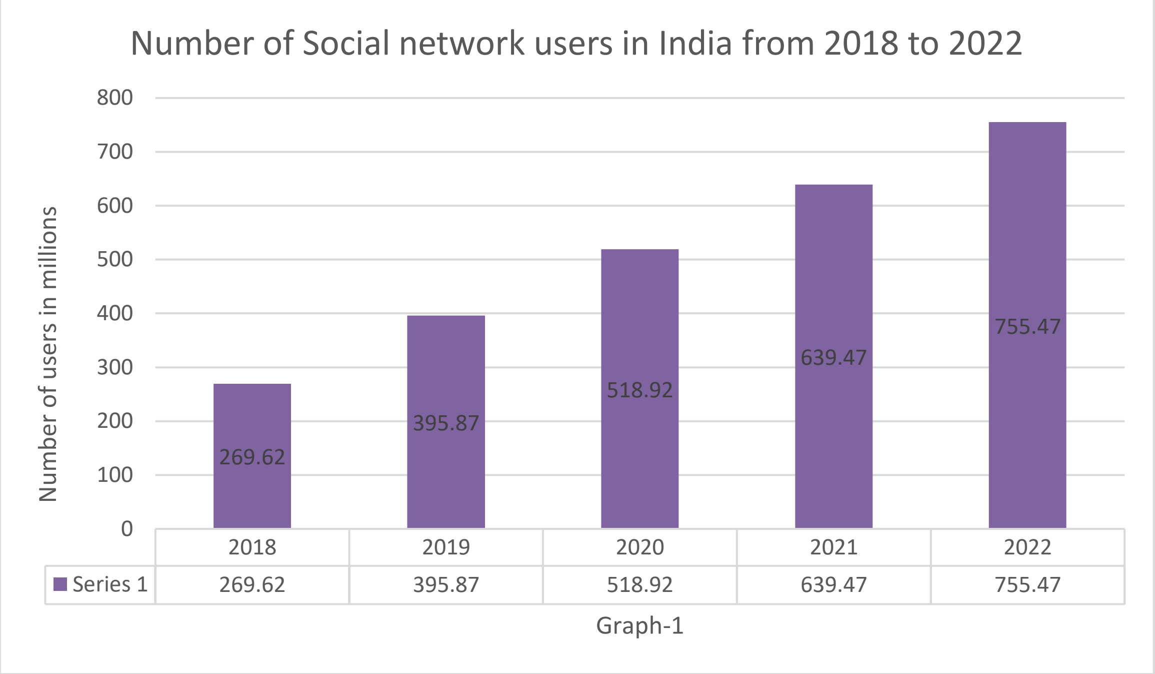
I. INTRODUCTION

In recent years, the number of daily active Internet users has increased as the Internet has become increasingly accessible to individuals throughout the world. Smartphones being affordable has enabled the digital population, especially in India, to access the internet through their mobile phones, even in rural areas, thereby increasing the percentage of internet users. The epidemic has also increased internet usage as people hunker down at home in quarantined countries, trying to avoid contracting the virus that appears to be rapidly spreading.

II. INTERNET USERS IN INDIA

India is the second largest online market in the world, after China, with more than 900 million internet users. The country's internet penetration was just around 50 percent, below the global average, despite a large number and a steady improvement in accessibility.The majority of the country's internet users access the internet through their mobile devices. The number of smartphone users in the United States is nearly equal to the number of internet users. There are several factors that contribute to India's high mobile internet usage, including the affordability of mobile data, the growing number of smartphone users, and their superior usability when compared to computers and tablets. However, despite a large number of internet users in the country, internet penetration levels have taken longer to catch up. Conversely, women in India have much lower internet access rates than men, and the disparity is even more significant in rural areas. Furthermore, older individuals' internet usage is reduced due to their online literacy and technological expertise. The digital footprint of India has considerable potential if women, the elderly, and rural residents are encouraged to use the Internet.

III.SOCIAL MEDIA USERS IN INDIA



Source: Statista.com

In the recent few years, India has recorded a grammatical growth in the users of social media. According to the latest data, India currently has more than 755 million social media users in 2022. Country was expected to be almost 1.5 billion in 2040 [Graph-1]. And this number is increasing every year at the rate of 4.2%. You will be surprised that, in line with the global average, Indian users spend an average of 2.4 hours on social media daily. (Source The Hindu) According to the Ministry of Electronic and Information Technology Government report, WhatsApp is the most used social media app in India. WhatsApp has 53 crore active users in India. After WhatsApp, YouTube and Facebook are the most used social media sites. **Social media has become a daily habit in most people's lives. Individuals across different age groups use social media platforms like Facebook, Instagram, YouTube, and Twitter for communication and networking. Young individuals aged 18-24 years spend excessive time on these applications – with Facebook and Instagram having 97.2 million and 69 million users from this age group alone in India, clearly showcasing growing dependency on social media. The constant use leads to exposure to risky content, changes in behavioural patterns, feeling of inferiority and even cyberbullying, resulting in grave mental health challenges and illnesses.**

According to UNICEF, 1 in 7 Indians aged 15 to 24 years feel depressed**. Depression** is linked to lack of self-esteem, poor concentration and other maladaptive symptoms, and can lead to difficulties in communication, failure to work or study productively, amplified risk of substance uses and abuse, as well as suicidal thoughts. One of the key risk factors for these prevalent rates of depression is social media.

IV. MOBILE USERS IN INDIA

The Indian smartphone industry has expanded to become one of the biggest smartphone markets in the world due to reasons including rising disposable income, cheaper internet, and the urge to always be connected. However, India's smartphone adoption rate is still very low when compared to other global markets. Due to the fact that a sizeable portion of the population either did not possess a phone or intended to upgrade from a feature phone to a smartphone, the demand for smartphones is expected to increase in the future. According to Deloittes's 2022 Global TMT (Technology, Media and Entertainment, Telecoms, 1billion smartphone users expecting in 2026, of which about 750 million are smartphone users 2022 in India. The apex child right body National Commission for protection of Child Right (NCPCR) in a study revealed that 59.2 percent of children use their smartphones/internet devices for chatting (using WhatsApp/Facebook/Instagram). While only 10.1 percent of children like use smartphones for online learning and education.

Cybercrime Data 2018 to 2022 (Till February)

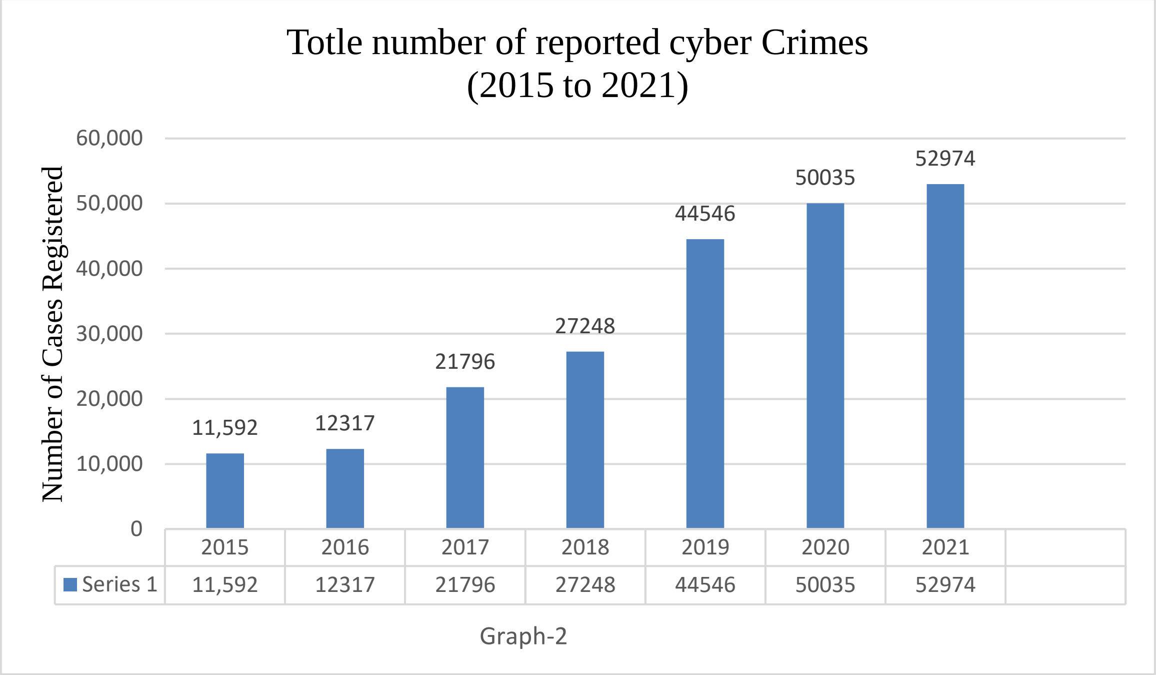
Table-1

Year	Total Cyber Incidents
2018	**2,08,456**
2019	**3,94,499**
2020	**11,58,208**
2021	**14,02,809**
2022(till feb)	**2,12,485**

India has emerged with the second largest internet population in the world, India was no exception to the digital village. While greater connectivity through the World Wide Web promises massive progress, it leaves our digital societies open to new vulnerabilities. Cybercrime knows no bounds and has evolved at the same pace as emerging technologies. The number of cybercrimes is increasing every year in the country, on the other hand, the nature of crimes ranges from small online frauds to large scale ones like lottery scams and sexual harassment, and material exploiting children. However, the most targeted cases have been reported in the banking sector and the financial segment. Due to Coronavirus, most of the services were done online, and due to this, people also faced many difficulties. This high risk has also spread to other areas. The latest of these include online grocery platform Big Basket with data from around 20 million users in November 2020.

Cybercrime cases have witnessed a steady spike since 2018. India reported 2,08,456 incidents in 2018; 3,94,499 incidents in 2019; 11,58,208 cases in 2020; 14,02,809 cases in 2021; and 2,12,485 incidents in the first two months of 2022[Table-1]. The above figures show that cybercrimes increased almost seven times between 2018 and 2021 and more sharply during the pandemic. A total of 17,560; 24,768, and 26,121 Indian websites were hacked in 2018, 2019, and 2020 respectively, CERT-In data. The National Crime Records Bureau (NCRB), however, presents a different set of data. According to NCRB, India reported 52,974 cybercrimes in 2021; 50,305 in 2020; 44,546 cases in 2019 and 27,248 cases in 2018. The year 2020 saw 4,047 cases of online banking fraud, 2,160 cases of ATM fraud, 1,194 credit/debit card fraud, and 1,093 OTP frauds. There were also 972 cases of cyber stalking/bullying of women and children and 578 cases of fake news on social media, NCRB data showed. Committing fraud was found to be the biggest motive and accounted for 30,142 out of the total 50,035 cases (60.02 per cent). This was followed by sexual exploitation (6.6 per cent) and extortion 4.9 per cent. Cybercrime rate was highest in Karnataka (16.2 per cent), followed by Telangana (13.4 per cent) and Assam (10.1 per cent).

More than 50,000 cases of cyber-crime were registered for the first time in 2020 to 2021



(Source: NCRB)

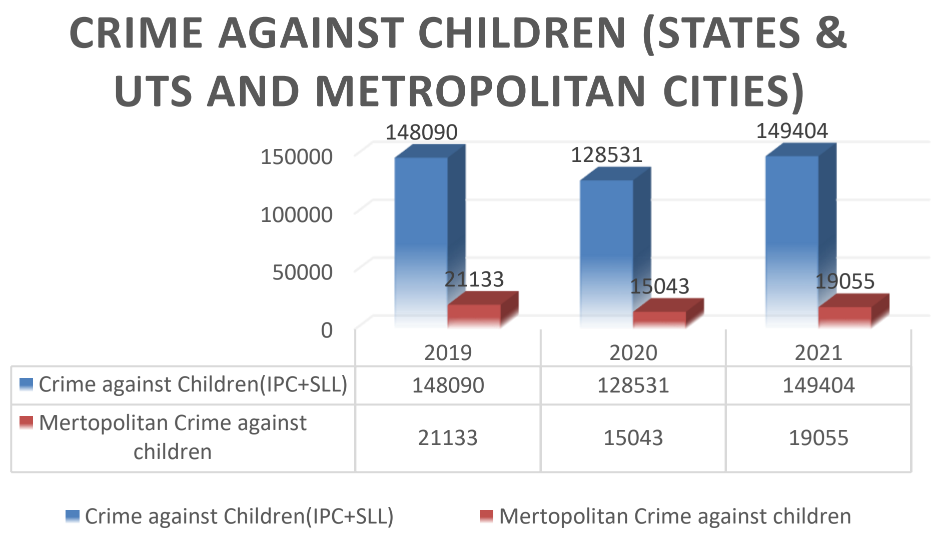
The National Crime Records Bureau (NCRB) has been publishing the data related to cyber-crimes in its annual Crime in India (CII) Report since 2002. The latest CII report for 2021 was released 22 August 2022, which puts the number of cases registered under cyber-crimes at more than 52,974. This is the first time that the number has crossed 50,000. A total of 52,974 cases were registered under Cyber Crimes, showing an increase of 5.9% in registration over 2020 (50,035 cases). Crime rate under this category increased from 3.7 in 2020 to 3.9 in 2021. During 2021, 60.8% of cyber-crime cases registered were for the motive of fraud (32,230 out of 52,974 cases) followed by sexual exploitation with 8.6% (4,555 cases) and Extortion with 5.4% (2,883 cases) [Graph-2].

The trend in the number of registered cybercrimes shows that there has been a significant increase in the number over the last few years. Only those cases registered with the police are reflected in the NCRB report. As with the increase in the number of documented cases of cybercrime, the rate of cybercrime has also increased to reach 3.9 per lakh population in 2021, up from 3.7 in 2020 and up from 3.3 in 2019. Before 2016, the rate of cybercrime was negligible. In 2016, the crime rate was just one per lakh population. Only one person out of one lakh people had reported a cybercrime.

V. CYBERCRIMES ARE REGISTERED UNDER THE IT ACT 2000, IPC & SLL.

Crime against Children

A total of 1,49,404 cases of crime against children were registered during 2021, showing an increase of 16.2% over 2020 (1,28,531 cases). [Graph-3] In percentage terms, major crime heads under ‘Crime Against Children’ during 2020 were Kidnapping & Abduction (45.0%) and Protection of Children from Sexual Offences Act, 2012 (38.1%), including child rape. The crime rate registered per lakh children population is 33.6 in 2021 in comparison with 28.9 in 2020. In Metropolitan cities, crime against children registered: A total of 19,055 cases of crime against children were registered during 2021, showing an increase in registration by 26.7% over 2020 (15,043 cases). In percentage terms, crime heads reporting a majority of cases under ‘Crime Against Children’ were kidnapping & abduction (56.6%), followed by Protection of Children from Sexual Offences Act, 2012 (30.8%).

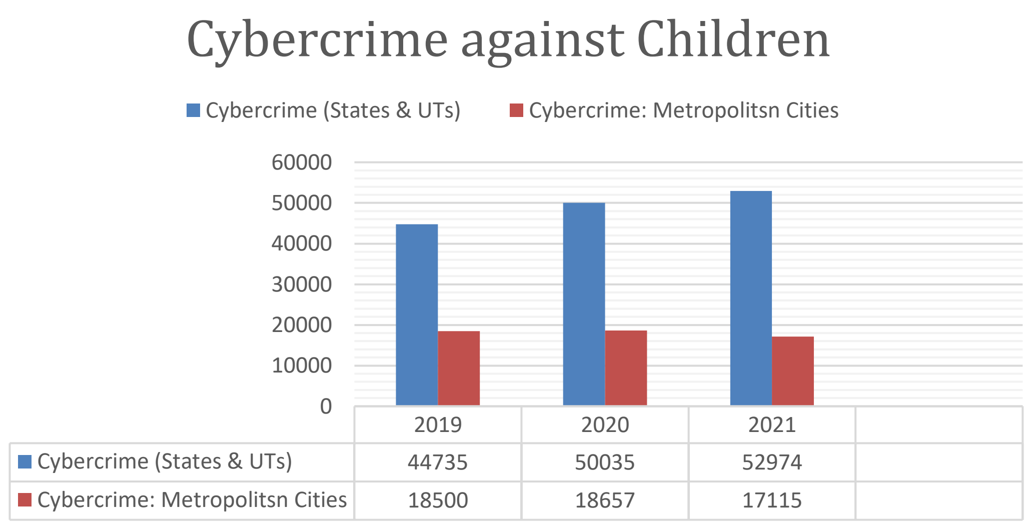


	2019	2020	2021
🟦 Crime against Children(IPC+SLL)	148090	128531	149404
🟥 Mertopolitan Crime against children	21133	15043	19055

GRAPH-3

Cybercrime against Children

A total of 52,974 cases registered under Cyber Crimes in 2021 is 18.91% more than the number in 2019, In reality, the rise in cybercrimes over the past several years may be seen in the trend in the number of registered cybercrimes. showing an increase of 5.87% in registration over 2020 (50,035 cases). The crime rate under this category increased from 3.7 in 2020 to 3.9 in 2021. In 2021, 60.8% of cyber-crime cases registered were for the motive of fraud (32,230 out of 52,974 cases), followed by sexual exploitation with 8.6% (4,555 cases) and Extortion with 5.4% (2,883 cases). [Graph-4] In Metropolitan cities, 17,115 cases have been registered under Cyber Crimes, showing a decline of 8.3% over 2020 (18,657 cases). The cybercrime rate has declined from 16.4 in 2020 to 15.0 in 2021. Crime head-wise cases revealed that Computer Related Offences (section 66 of IT Act) (8,513 points) formed the highest number of Cyber Crimes, accounting for 49.7% in 2021. [Graph-4]



	2019	2020	2021	
🟦 Cybercrime (States & UTs)	44735	50035	52974	
🟥 Cybercrime: Metropolitsn Cities	18500	18657	17115	

GRAPH-4

In 2017, comprehensive reporting of cybercrime statistics started.

Cybercrimes are a relatively new category in the NCRB's CII report compared to other crimes. As a result, this area has undergone several revisions over the past few years. Starting in 2017, the report made data on crime-head-wise cyber-crime cases available. Since 2017, there have been reports of detailed cybercrime data under the criminal headings of cyberterrorism, defamation, fraudulent profiles, and those targeting women and children covered under the Information and Technology Act of 2000. Since 2017, the report has now included information about internet scams, the spread of false information, and other topics.

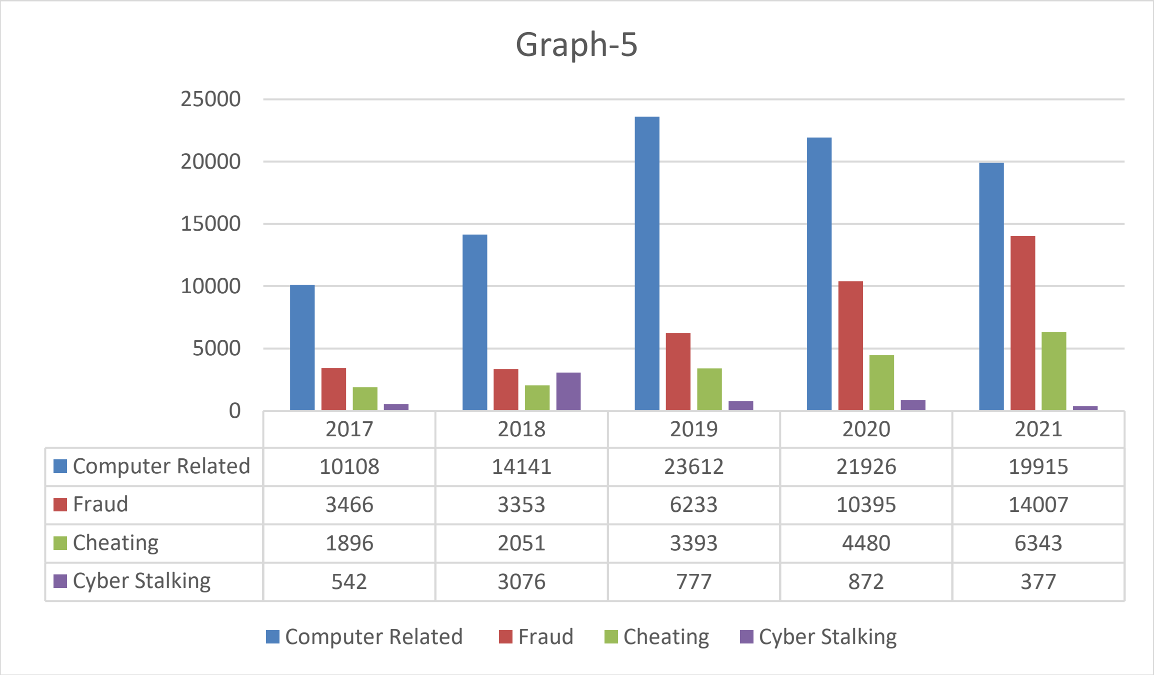
Cybercrimes are reported in accordance with the IT Act 2000, IPC, and SLL.

The IT Act of 2000 lays forth the rules for cybercrimes and the associated penalties. The IT Act of 2000 covers crimes using computers, cyberterrorism, aiding or attempting to commit crimes, publishing or transmitting pornographic or sexually explicit material, and tampering with computer source documents. However, the IT Act does not apply to all cybercrimes. The Indian Penal Code lists crimes connected to forgery, cheating, false news, data theft, defamation, etc. (IPC). Online gambling and lotteries are among the offenses covered by Special and Local Laws (SLL).

The number of computer-related offenses reported reduced in 2021 to less than 20,000 instances, which is 15.65% fewer than the amount in 2019 [Graph-5]. This is in contrast to the current trend. However, the number of fraud cases reported to the police more than quadrupled between 2018 and 2021. Between 2017 and 2021, the number of cases filed under the heading "Publication/transmission of obscene/sexually explicit conduct in electronic form" more than tripled. More than twice as many incidences of cheating have been reported. There was a 61% rise in cases reported under "Cyberstalking and bullying of women and children." Even though the number of forgery cases is tiny, it grew by over six times.[Graph-5] In only four years, the incidents involving "fake news on social media" more than tripled, crossing the 500 mark for the first time in 2020. However, in 2021, fewer than 200 examples of such false information were circulated. In the four years, there was a 45% rise in computer document tampering. In the meantime, incidences of cyber-threats and extortion reported decreased marginally. Less than 100 instances are reported annually under the other criminal headings, which make up less than 1.5% of total cases, including all SLL offenses. In contrast to a spike in incidents of cyberterrorism, online gambling, phony profiles, defamation, and counterfeiting, issues of data theft and those covered by the Trademarks Act and Copy Rights Act have dropped. The lockdown and increasing internet usage may be directly responsible for the rise in incidents of fraud, the transfer of offensive information, etc.[Graph-5A]

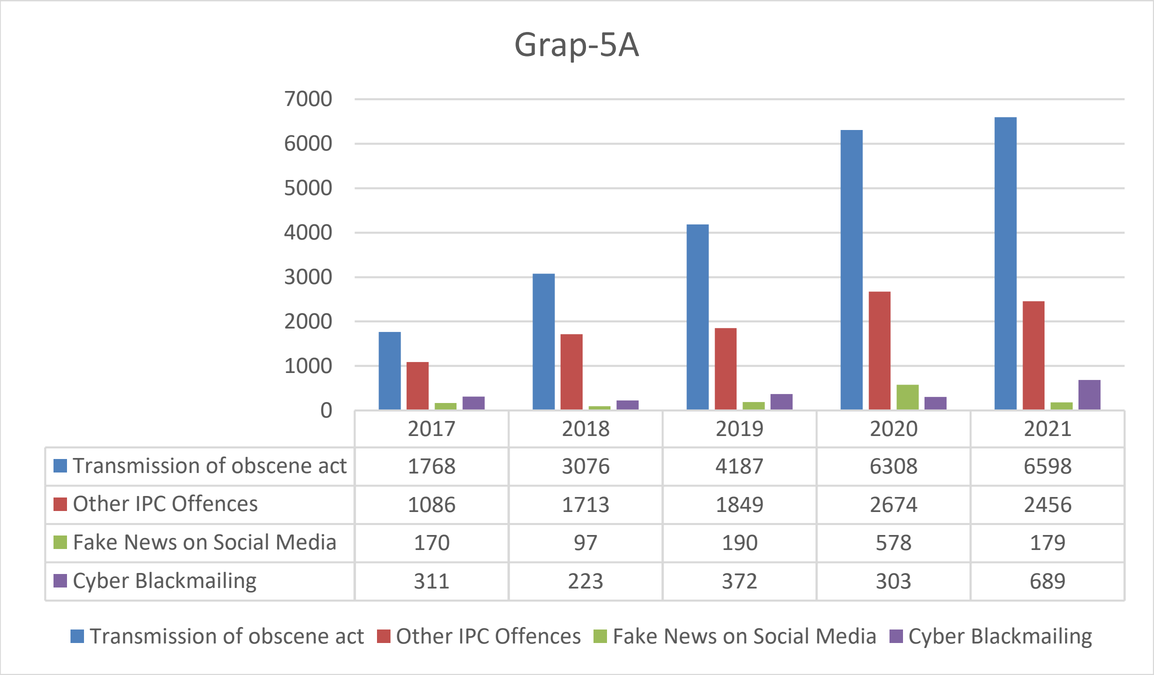
Crime-head wise trend in registered Cyber Crime against children

(2017 to 2021)



	2017	2018	2019	2020	2021
🟦 Computer Related	10108	14141	23612	21926	19915
🟥 Fraud	3466	3353	6233	10395	14007
🟩 Cheating	1896	2051	3393	4480	6343
🟪 Cyber Stalking	542	3076	777	872	377

Source: (NCRB)

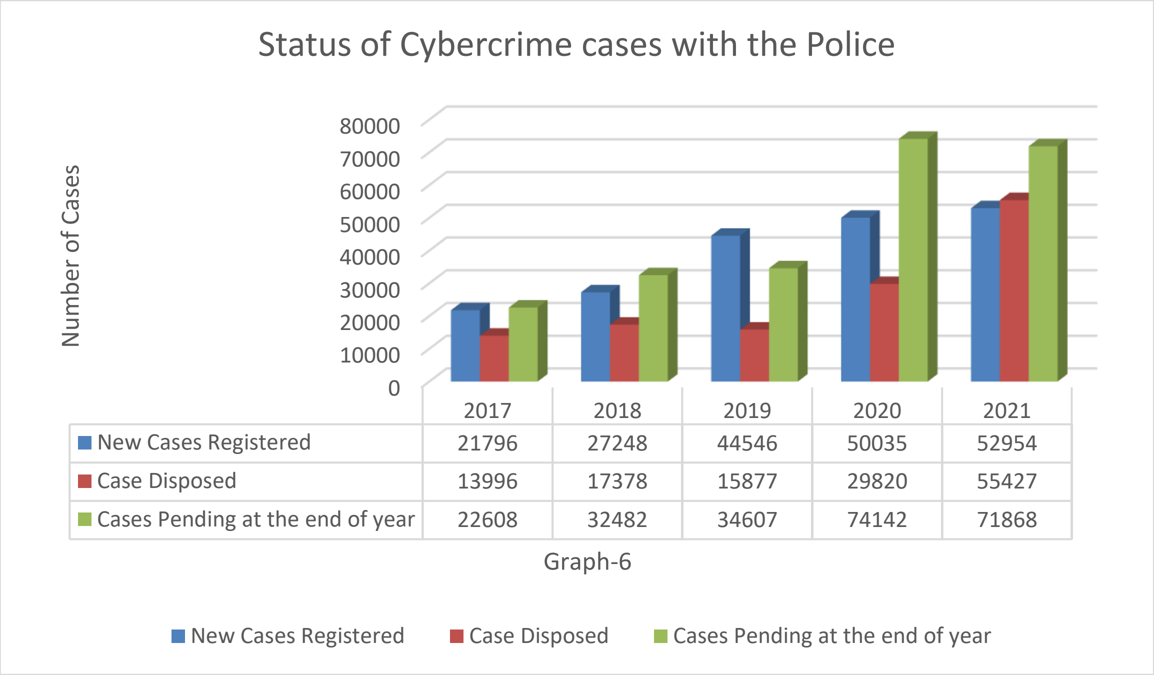


	2017	2018	2019	2020	2021
🟦 Transmission of obscene act	1768	3076	4187	6308	6598
🟥 Other IPC Offences	1086	1713	1849	2674	2456
🟩 Fake News on Social Media	170	97	190	578	179
🟪 Cyber Blackmailing	311	223	372	303	689

Source: (NCRB)

Status of Cybercrime Cases with the Police

The police have resolved 132,498 crimes between 2017 and 2021, while 1,96,579 additional cases were reported over that same period. In 2017, the disposal rate was at its lowest when fewer than 14,000 instances were disposed of. Even though the disposal rate has improved and about 60,000 cases were resolved in 2021, the pendency has grown due to the rise in the number of new possibilities. The pendency of cases is increasing annually since the disposal rate is lower than the registration rate. Consequently, from 22,608 instances in 2017 to 71,868 points in 2021, there were still open cybercrime cases at the end of the year, more than a three-fold increase in five years. [Graph-6]



	2017	2018	2019	2020	2021
🟦 New Cases Registered	21796	27248	44546	50035	52954
🟥 Case Disposed	13996	17378	15877	29820	55427
🟩 Cases Pending at the end of year	22608	32482	34607	74142	71868

Graph-6

Source: (NCRB)

The percentage of cases still pending at the end of the year relative to all investigated instances is known as the pendency percentage. The total number of cases under investigation includes those that were reopened for further examination as well as those that were carried over from the previous year. The number of pending cases has steadily risen over the past five years. According to the 2020 CII report, the number of pending cases under the IT Act's computer-related offenses category "Identity theft" was high. Most of the cases filed under "identity theft" are still open. For claims filed under the IPC's "counterfeiting" and "currency" categories, the pendency rate reached 90.9%, and for "defamation/morphing," it reached 90.5% [Graph-6].

VI. THE NECESSITY OF THE HOUR IS FOR CYBERCRIMES TO BE DEALT WITH QUICKLY

Cybercrimes have increased over time, and this trend is expected to continue as more people use the internet. Individuals who depend on the internet for various daily tasks might have difficulty coping with the epidemic-caused lockdown. The penalty will only increase if the disposal rate does not increase and catches up to the speed of newly reported crimes. The police force can only accomplish this if it is equipped with the proper equipment and resources.

VII. CONCLUSION

Currently, a large population of India uses social networking sites, which includes children. There is a lack of information among people about the use of social networking sites in India. Also, most social networking sites have servers abroad, making it challenging to get to the root of cybercrime in India. Children using social networking sites extensively are unaware of the danger of cybercrime. With children sharing their personal information on various social networking sites, hackers can easily hack into these social media accounts and misuse their data. Cybercrimes have increased manifold in recent years. The government has taken many steps to provide cyber security, but they have not proved effective. The government should make strict arrangements to comply with laws and make children and their parents aware of cyber laws. Also, to deal with cybercrimes, the police should be trained in the knowledge of new technology and knowledge of computers. Also, ensure the appointment and training of separate courts and judges for legal procedures related to cybercrimes. Children and young people's needs should be considered when developing Internet policy. Online risks, such as grooming and sexting, and other issues, such as exposure to harmful or illegal content, are areas of existing law and policy concern. Even though it is essential to keep children safe online, we should not ignore the positive impact the Internet can have on their growth and development. It is necessary to safeguard the younger generation from engaging in risky online behavior without denying them all the benefits of Internet access.

We must re-calibrate the balance between supervision or control and freedom of children and teenagers, as well as the roles of the various actors involved, especially children, parents, and the state, to ensure that autonomy is preserved while protecting individual and social welfare. Although the state's approach to cybercrime policy may be understandable, its effectiveness leaves much to be desired. In the current policy environment, the emphasis is overwhelmingly placed on criminal law approaches and surveillance, ignoring the opportunities that the Internet offers to today's youth in favour of only focusing on controlling risks through repression and supervision. Children are limited in their opportunities to grow, explore, make mistakes, and eventually benefit from those experiences when handling measures are in place, such as keeping them safe and preventing juvenile delinquency. A law or policy based on criminal law may not be effective and may even be counterproductive, so policymakers should consider alternatives seriously.

REFERENCE

1. "Internet Users in India - (Statistics and Facts) | 2022." https://findly.in/internet-users-in-india/#how-many-internet-users-in-india, Accessed 1 September. 2022
2. This text provides general information Statista assumes no liability for the information being complete or correct. Due to varying update cycles and Statistics Can Display More up-to-Date Data Than Referenced in the Text, “Topic: Internet Usage in India,” Statista, accessed September 13, 2022, https://www.statista.com/topics/2157/internet-usage-in-india/.
3. “India: Number of Internet Users 2040,” Statista, accessed September 19, 2022, https://www.statista.com/statistics/255146/number-of-internet-users-in-india/.
4. “India: Number of Social Network Users 2015-2040,” Statista, accessed September 22, 2022, https://www.statista.com/statistics/278407/number-of-social-network-users-in-india/.
5. Mental Health in India: Impact of Social Media on Young Indians,” The Indian Express, February 18, 2022, accessed September 20, 2022, https://indianexpress.com/article/lifestyle/health/mental-health-in-india-impact-of-social-media-on-young-indians-facebook-instagram-youtube-twitter-7778499/
6. “Search | Ministry of Electronics and Information Technology, Government of India,” accessed September 22, 2022, https://www.meity.gov.in/search/node/social%20media%20users.
7. This text provides general information Statista assumes no liability for the information being complete or correct. Due to varying update cycles and Statistics Can Display More up-to-Date Data Than Referenced in the Text, “Topic: Smartphone Market in India,” Statista, accessed September 22, 2022, https://www.statista.com/topics/4600/smartphone-market-in-india/.
8. Press Trust of India, “India to Have 1 Billion Smartphone Users by 2026: Deloitte Report,” last modified February 22, 2022, accessed September 22, 2022,

https://www.business-standard.com/article/current-affairs/india-to-have-1-billion-smartphone-users-by-2026-deloitte-report-122022200996_1.html.

9. "59.2 Pc Children Use Smartphones for Messaging, Only 10.1 Pc for Online Learning, Finds NCPCR Study," The Times of India, July 25, 2021, accessed September 22, 2022, https://timesofindia.indiatimes.com/education/news/59-2-pc-children-use-smartphones-for-messaging-only-10-1-pc-for-online-learning-finds-ncpcr-study/articleshow/84723977.cms#:~:text=NEW%20DELHI%3A%20The%20apex%20child%20rights%20body%20National,to%20use%20smartphones%20for%20online%20learning%20and%20education.

10. This text provides general information Statista assumes no liability for the information being complete or correct Due to irregular update cycles, and Statistics Can Display More up-to-Date Data Than Referenced in the Text, "Topic: Cyber Crime in India," Statista, accessed September 22, 2022, https://www.statista.com/topics/5054/cyber-crime-in-india/.

11. "Two Months of 2022 Saw More Cyber Crimes than Entire 2018: Why e-Fraud Is a Ticking Time Bomb," Zee News, accessed September 22, 2022, https://zeenews.india.com/technology/two-months-of-2022-saw-more-cyber-crimes-than-entire-2018-why-e-fraud-is-a-ticking-time-bomb-2458733.html.
"Two Months of 2022 Saw More Cyber Crimes than Entire 2018: Why e-Fraud Is a Ticking Time Bomb," Zee News, accessed September 22, 2022, https://zeenews.india.com/technology/two-months-of-2022-saw-more-cyber-crimes-than-entire-2018-why-e-fraud-is-a-ticking-time-bomb-2458733.html.

12. राष्ट्रीयअपराधरिकॉर्डब्यूरो, https://ncrb.gov.in/ (last visited Sep 22, 2022). (National Crime Record Bureau Ministry of Home Affairs)