

# STATE-WISE TRENDS AND PATTERNS OF CYBERCRIMES AGAINST CHILDREN IN INDIA: AN EMPIRICAL ANALYSIS OF NCRB DATA FROM 2017 TO 2021

**Dr Pradip Kumar Kashyap**

*Assistant Professor, CGC University, Mohali , Email: pradiprgnul@gmail.com*

---

## **Abstract**

Cybercrimes against children have emerged as a major public safety and child protection concern due to the rapid expansion of digital technologies and online communication. Understanding temporal and regional patterns of these offences is essential for developing effective prevention and policy strategies. This study aimed to examine state-wise trends, geographical distribution, offence patterns, and the relationship between child population and reported cybercrime cases against children in India. *Methods:* A quantitative retrospective analysis was conducted using secondary data obtained from the National Crime Records Bureau (NCRB) covering all Indian States and Union Territories from 2017 to 2021. Descriptive statistics, trend analysis, Pearson correlation, and simple linear regression were performed to evaluate temporal changes and determinants of reported cybercrime cases. A total of 3,103 cybercrime cases against children were reported during the study period, increasing from 88 cases in 2017 to 1,376 cases in 2021. Cyber pornography and obscene material constituted the largest offence category (59.94%), followed by other cybercrimes (26.94%). Maharashtra, Uttar Pradesh, Kerala, and Karnataka accounted for more than half of all reported cases. Child population showed a significant positive association with reported cybercrime cases ( $p < 0.001$ ), although the regression model explained only 15.88% of the observed variation. The findings demonstrate a substantial increase in cybercrimes against children in India and underscore the need for strengthened legal enforcement, digital literacy initiatives, child-centred cyber safety policies, and coordinated institutional responses to address emerging online threats.

**Keywords:** cybercrime against children, National Crime Records Bureau, child online safety, cybersecurity, India

## 1. INTRODUCTION

Digital technologies have changed the way people communicate, learn, trade and interact with each other around the globe. Global access to information and online services has greatly improved due to the increasing penetration of the Internet, and considerable use of smart phones. Cybercrimes by exploiting children to access the Internet have also been enabled by these technological advances. Children are growing up in an online world, engaging in online learning, social networking, gaming and digital communication, which increases their risk of being cyberstalked, cyberbullied, groomed, having their identities stolen or distribution of child sexual abuse material. Cybercrimes targeting children are a pressing issue for governments, law-enforcement, and child protection bodies globally, as they have significant psychological, emotional, and social impacts (Al-Hakimi & Nur, 2023; Fourie, 2020).

Children have opportunities and risks in the digital environment. Internet sites can help children learn, create, and connect socially, but can also expose children to bad material, inappropriate privacy disclosures, financial scams, and technology-based exploitation. Stoilova et al. (2021) highlight a complex digital environment where opportunities and significant safety risks are all present in children's online experiences. Therefore, a multi-sectoral approach, combining legal measures, measures for online protection, supervision of parents and guardians, educational institutions and digital literacy programmes is necessary. Good governance of digital technologies has therefore come to be a critical aspect of contemporary cyber security and public policy (Flyverbom et al., 2019).

In the last decade, India has seen the remarkable digital transformation, marked by the growth of Internet connectivity, its low-cost mobile technologies, along with government initiatives that have encouraged digital inclusion. While these advancements have contributed to economic and social development, they have also raised the threats that vulnerable populations face from cyber-attacks. With the development of digital infrastructure, more people can engage in online activities, while at the same time allowing for a larger attack surface on cybercriminals using anonymous and borderless digital space (Feng & Qi, 2024). Child-based cybercrime is a serious legal and social issue among the various types of cybercrime. Cybercrimes against minors, including cyber pornography, cyber stalking, cyber bullying, fake social media profile creation, online gaming related offences, and others have been reported to be on the rise in various states of India (Karthik, 2023).

Due to the extended closure of schools and the greater amount of online learning, followed by the COVID-19 pandemic, children's reliance on digital platforms has further increased, exposing them to a significantly higher amount of Internet time. This change provided further opportunities for cybercriminals and marked a significant rise in cybercrime offenses targeting children (Matthews et al., 2025). During the pandemic period, there was an increase in cyber offences against minors which necessitated further strengthening of preventive measures, raising awareness about digital information and development of better mechanisms for the enforcement of cyber laws, noted Sharma and Kataria (2022). While cybercrime against children is on the rise and the awareness of these offences is growing, there remains a significant variation in the reporting and occurrence of cybercrime across the region, including variations in access to digital technologies, reporting behaviour, policing resources and legal awareness.

While there were some studies done before on the trends in cybercrime in India, they mostly concentrated on broad cybercrime or geographical studies in India, which has neglected the holistic study of crimes against children on a state-wise basis (Padmavathy, 2018). Thus, empirical evidence on the variations across states and Union territories and changes over time in the distribution of various types of cybercrimes against children is limited. The official datasets of NCRB offer a good chance to fill this research void by systematically analysing reliable and standardised crime data reported by law enforcement agencies.

Hence, the present study aims at analysing the NCRB data for the period of 2017 to 2021 to analyse the trends and pattern of cybercrimes against children in India at the state level. Specifically, this study examines the trends in reported incidents over time, looks at the state-by-state distribution of the primary categories of cybercrime and tries to explain regional differences that could guide future policy actions. The results are likely to be added to the ever-expanding body of literature on cyber law, child protection and digital governance, and will offer concrete evidence to policy makers, law enforcement and child protection authorities to help enhance the measures put in place to protect children in the rapidly changing digital environment in India.

### Research Objectives

To analyze temporal trends in cybercrimes against children across Indian states and Union Territories from 2017 to 2021.

To compare the state-wise distribution of major categories of cybercrimes against children.

To identify regional disparities and provide evidence-based recommendations for strengthening child cyber protection in India.

## 2. METHODOLOGY

### 2.1 Study Design

The study used quantitative analysis, retrospective, and observational research design. This study was of an empirical nature and studied the temporal and geographical variations in cybercrimes against children in the Indian States and Union Territories. The study measured trends, made comparisons among types of crime and compared regional differences across five years without changing any of the study variables.

### 2.2 Data Source

The secondary data used for the analysis were collected from the National Crime Records Bureau (NCRB), Government of India, the "Cyber Crimes Against Children (IPC & SLL), Table 9A.11" for the period of 2017 to 2021 (Tikhute, 2023). The information in the dataset covers data reported by the states on cybercrimes committed against children, such as cyber pornography, cyberstalking, cyberbullying, fake profiles, cybercrimes involving on-line gaming and other cybercrimes. Estimates of child population based on the 2011 Census were also provided to enable comparative analysis

between States/UTs.

### 2.3 Study Variables

The dependent variable was the number of cybercrimes reported against children. Independent variables were State/Union Territory and year of reporting (2017-2021). Others analytical variables included individual types of cybercrime, such as cyber pornography, cyberstalking, cyberbullying, fake profiles, online gaming-related offences and other cybercrime. Data on children was included as a contextual variable to compare regional variation in reported crime incidents.

### 2.4 Data Preparation

Preprocessing and statistical analysis were performed using the dataset in MS Excel and Python. Data quality assessment included checking variable names, deduplication, checking consistency of variables across reporting years, and finding missing or inconsistent values. All data were coded in the same manner for variables, and all numerical data were checked before statistical analysis. Reported variables in the dataset were obtained from an official and trusted source of government data, which meant no imputation procedures were necessary.

### 2.5 Statistical Analysis

Descriptive statistics were calculated to present the summary of the data such as frequencies, percentages, mean, standard deviation, minimum and maximum values. The trends in reported cybercrimes were analysed over years to assess the temporal changes from 2017 to 2021. Comparative analysis with other States/ Union Territories was done to highlight the differences between the States/UTs and to understand the contribution of each cybercrime category to the overall burden of reported offences.

Pearson correlation analysis was conducted to test the relationship between continuous study variables and simple linear regression was used to test the association between child population and reported cybercrime cases. The use of data visualization techniques, such as line graphs, bar charts, scatter plots with linear regression lines, and correlation heatmaps, has been used to display temporal trends, geographical distributions and statistical relationships. Python was used for statistical analysis, and a 5% significance level ( $p < 0.05$ ) was applied to determine the statistical significance.

### 2.6 Ethical Considerations

No human subject or personally identifiable information was used in the study, and it relied on secondary data made available by the National Crime Records Bureau. Therefore, formal ethical approval and informed consent were not necessary. The research was carried out in accordance with the accepted principles of research integrity, transparency and responsible use of publicly available government information.

## 3. RESULTS

### 3.1 Descriptive Statistics

A total of 180 State/UT-year observations were analyzed from 2017 to 2021. In all, there were 3,103 cybercrime incidents against children in the study period. The mean number of cases of cybercrime per observation was 17.24, the standard deviation of 38.56 and the maximum number of 207 cases (as shown in Table 1). The largest number of cases were for cyber pornography (1,860 cases), followed by other cybercrimes (836 cases) and cyber stalking or bullying (355 cases). High standard deviations and low median values suggest strong right skewness in the distributions, and that there was a significant clustering of cases in a few States and Union Territories.

**Table 1. Descriptive Statistics of Cybercrime Variables, 2017–2021**

| Variable                                       | N   | Mean  | SD    | Minimum | Median | Maximum | Total |
|------------------------------------------------|-----|-------|-------|---------|--------|---------|-------|
| Cyber blackmailing, threatening, or harassment | 180 | 0.19  | 1.16  | 0       | 0      | 14      | 34    |
| Fake profile                                   | 180 | 0.09  | 0.43  | 0       | 0      | 3       | 17    |
| Cyber pornography or obscene material          | 180 | 10.33 | 29.25 | 0       | 0      | 161     | 1,860 |
| Cyber stalking or bullying                     | 180 | 1.97  | 7.77  | 0       | 0      | 69      | 355   |
| Internet crimes through online games           | 180 | 0.01  | 0.07  | 0       | 0      | 1       | 1     |
| Other cybercrimes                              | 180 | 4.64  | 9.65  | 0       | 1      | 72      | 836   |
| Total cybercrimes                              | 180 | 17.24 | 38.56 | 0       | 2      | 207     | 3,103 |

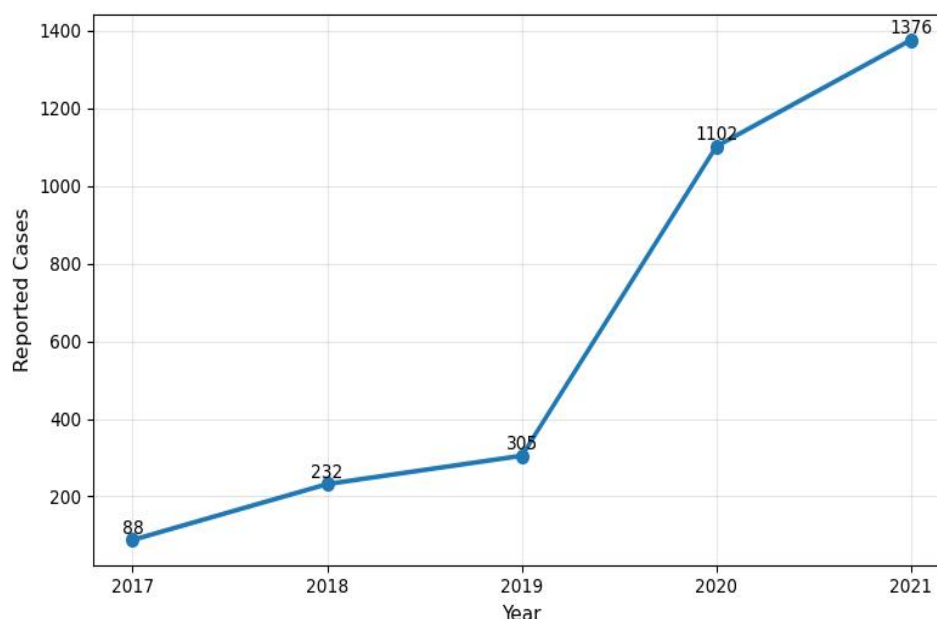
### 3.2 Annual Trends in Cybercrimes Against Children

There was a significant rise in the number of reported crimes against children from 2017 to 2021. The number of total cases rose from 88 in 2017 to 1,376 in 2021 as indicated in Table 2. The greatest annual growth rate was seen in 2020 with the number of cases increasing by 261.31% from 305 cases in 2019 to 1,102 cases in 2020. It is also observed that the mean number of cases per State/UT also got higher from 2.44 in 2017 to 38.22 in 2021. The data in Table 2 shows that there was a significant increase in reported cases following 2019 in the annual pattern (Figure 1).

**Table 2. Annual Trends in Cybercrimes Against Children in India**

| Year | Total cases | Mean cases | SD   | Maximum annual cases | Annual change (%) |
|------|-------------|------------|------|----------------------|-------------------|
| 2017 | 88          | 2.44       | 5.45 | 27                   | —                 |

|      |       |       |       |     |        |
|------|-------|-------|-------|-----|--------|
| 2018 | 232   | 6.44  | 11.42 | 57  | 163.64 |
| 2019 | 305   | 8.47  | 19.86 | 98  | 31.47  |
| 2020 | 1,102 | 30.61 | 53.71 | 207 | 261.31 |
| 2021 | 1,376 | 38.22 | 55.70 | 168 | 24.86  |



**Figure 1. Annual Trend of Reported Cybercrimes Against Children in India (2017–2021)**

### 3.3 State-Wise Distribution of Cybercrime Cases

Incidences of cybercrime were very unevenly distributed throughout the country. Table 3 shows that Maharashtra had the maximum number of cumulative cases at 529 cases accounting for 17.05 % of the national cases. Uttar Pradesh, with 426 cases, followed by Kerala (344 cases) and Karnataka (343 cases). These four States combined had 52.92% of the total number of reported cases. Assam had 198 cases and Delhi had 181 cases which were relatively high. A few States and UTs had either one case or no case during the study period, in contrast to the rest of the States. The distribution of reported cybercrime cases in the rankings in Table 3 is therefore clearly skewed among a few jurisdictions.

**Table 3. State-Wise Distribution of Cybercrimes Against Children, 2017–2021**

| Rank | State/UT                  | Total cases | Mean annual cases | Maximum annual cases | Percentage of total |
|------|---------------------------|-------------|-------------------|----------------------|---------------------|
| 1    | Maharashtra               | 529         | 105.80            | 207                  | 17.05               |
| 2    | Uttar Pradesh             | 426         | 85.20             | 197                  | 13.73               |
| 3    | Kerala                    | 344         | 68.80             | 163                  | 11.09               |
| 4    | Karnataka                 | 343         | 68.60             | 164                  | 11.05               |
| 5    | Assam                     | 198         | 39.60             | 136                  | 6.38                |
| 6    | Delhi                     | 181         | 36.20             | 162                  | 5.83                |
| 7    | Andhra Pradesh            | 139         | 27.80             | 65                   | 4.48                |
| 8    | Odisha                    | 131         | 26.20             | 71                   | 4.22                |
| 9    | Chhattisgarh              | 125         | 25.00             | 88                   | 4.03                |
| 10   | Madhya Pradesh            | 124         | 24.80             | 45                   | 4.00                |
| 11   | Gujarat                   | 98          | 19.60             | 43                   | 3.16                |
| 12   | Punjab                    | 83          | 16.60             | 63                   | 2.67                |
| 13   | Rajasthan                 | 74          | 14.80             | 33                   | 2.38                |
| 14   | Tamil Nadu                | 67          | 13.40             | 35                   | 2.16                |
| 15   | Haryana                   | 44          | 8.80              | 33                   | 1.42                |
| 16   | West Bengal               | 40          | 8.00              | 19                   | 1.29                |
| 17   | Himachal Pradesh          | 38          | 7.60              | 19                   | 1.22                |
| 18   | Uttarakhand               | 36          | 7.20              | 23                   | 1.16                |
| 19   | Telangana                 | 31          | 6.20              | 17                   | 1.00                |
| 20   | Goa                       | 11          | 2.20              | 3                    | 0.35                |
| 21   | Jharkhand                 | 10          | 2.00              | 6                    | 0.32                |
| 22   | Manipur                   | 7           | 1.40              | 3                    | 0.23                |
| 23   | Jammu & Kashmir           | 6           | 1.20              | 4                    | 0.19                |
| 24   | Meghalaya                 | 4           | 0.80              | 3                    | 0.13                |
| 25   | Andaman & Nicobar Islands | 4           | 0.80              | 2                    | 0.13                |

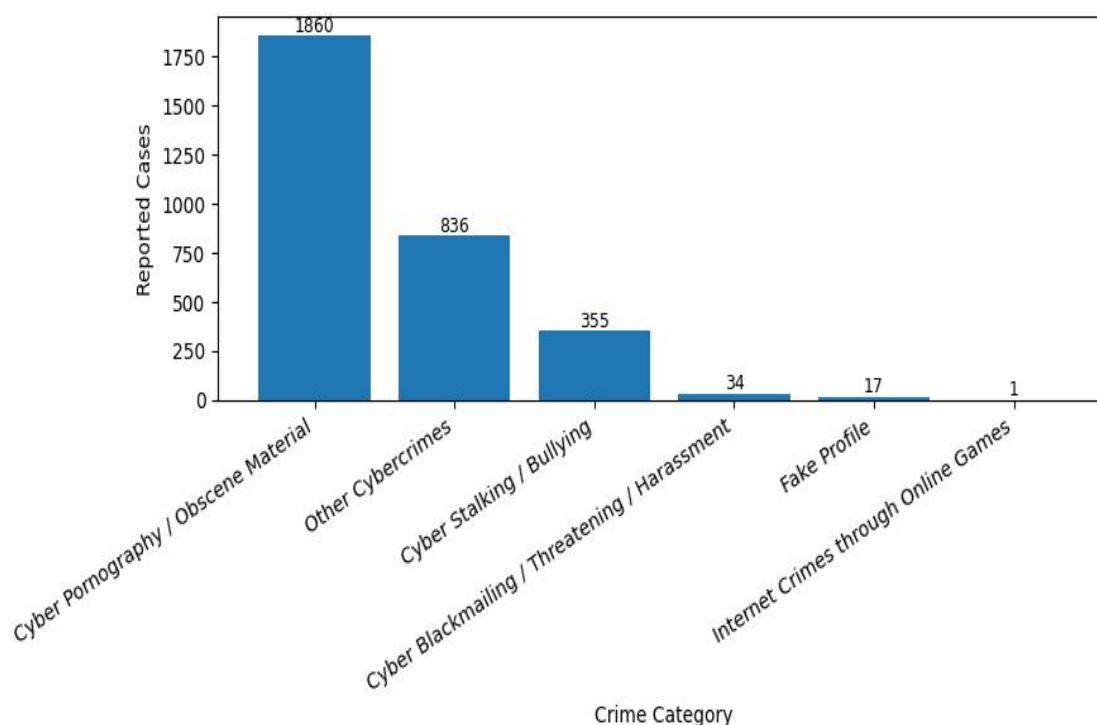
|       |                                      |   |      |   |      |
|-------|--------------------------------------|---|------|---|------|
| 26    | Bihar                                | 3 | 0.60 | 2 | 0.10 |
| 27    | Chandigarh                           | 3 | 0.60 | 3 | 0.10 |
| 28    | Arunachal Pradesh                    | 1 | 0.20 | 1 | 0.03 |
| 29    | Sikkim                               | 1 | 0.20 | 1 | 0.03 |
| 30    | Mizoram                              | 1 | 0.20 | 1 | 0.03 |
| 31    | Tripura                              | 1 | 0.20 | 1 | 0.03 |
| 32–38 | Remaining States/UTs with zero cases | 0 | 0.00 | 0 | 0.00 |

### 3.4 Distribution of Cybercrime Categories

Table 4 indicates that the leading category of offences is cyber pornography and publication of obscene material (1,860 offences or 59.94% of total offences). Other cybercrimes were 26.94% and cyber stalking or bullying was 11.44%. Combined, the burden of cyber blackmailing, threatening or harassment, fake profiles and internet crimes committed in online games accounted for below 2% of the total burden (Figure 2). Cyber pornography and other cybercrimes accounted for 86.88% of the total number of reported cases as shown in Table 4.

**Table 4. Distribution of Cybercrime Categories, 2017–2021**

| Crime category                                 | Total cases | Percentage (%) |
|------------------------------------------------|-------------|----------------|
| Cyber pornography or obscene material          | 1,860       | 59.94          |
| Other cybercrimes                              | 836         | 26.94          |
| Cyber stalking or bullying                     | 355         | 11.44          |
| Cyber blackmailing, threatening, or harassment | 34          | 1.10           |
| Fake profile                                   | 17          | 0.55           |
| Internet crimes through online games           | 1           | 0.03           |
| Total                                          | 3,103       | 100.00         |



**Figure 2. Distribution of Major Cybercrime Categories Against Children in India (2017–2021)**

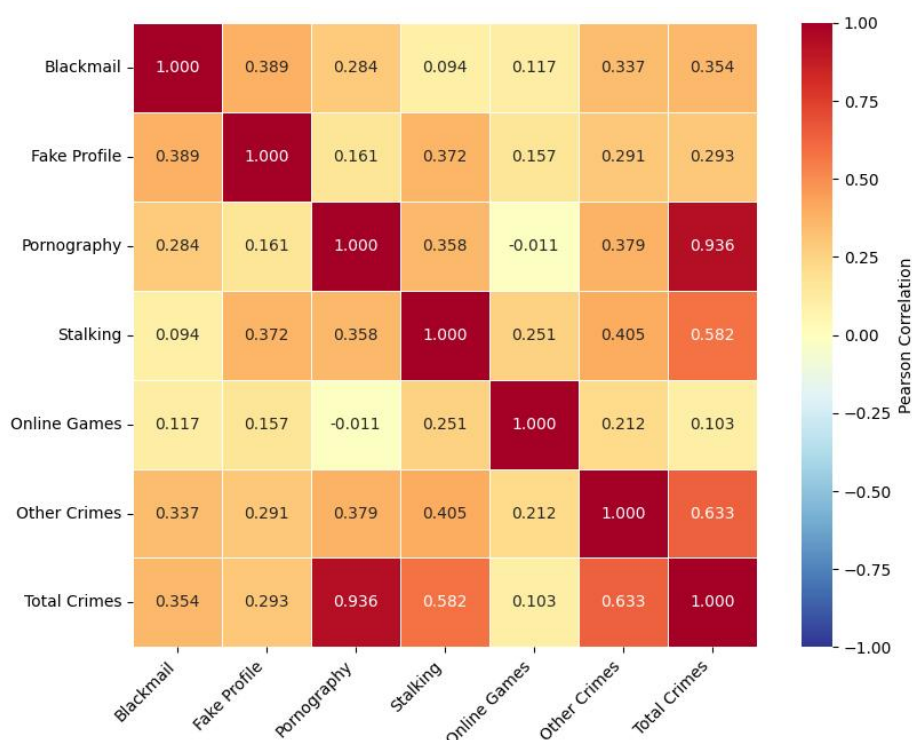
### 3.5 Correlation Analysis

Pearson's correlation coefficients are shown in Table 5. There was a very high positive correlation ( $r = 0.936$ ) between total cybercrime and cyber pornography or obscene material. Relationships were also positive between total cases and other cybercrimes ( $r = 0.633$ ), and cyber stalking or bullying ( $r = 0.582$ ). Positive correlations were found to be comparatively weak between total cybercrimes and cyber blackmailing/harassment ( $r = 0.354$ ) and fake-profile offences

( $r = 0.293$ ). The total number of cases had a very small association with Internet crimes via online games ( $r = 0.103$ ). Table 5 shows that cyber pornography was the highest contributor to the overall differences in cybercrime cases reported, statistically (Figure 3).

**Table 5. Pearson Correlation Matrix of Cybercrime Variables**

| Variable                      | Blackmail | Fake profile | Pornography | Stalking | Online games | Other crimes | Total crimes |
|-------------------------------|-----------|--------------|-------------|----------|--------------|--------------|--------------|
| Cyber blackmail or harassment | 1.000     | 0.389        | 0.284       | 0.094    | 0.117        | 0.337        | 0.354        |
| Fake profile                  | 0.389     | 1.000        | 0.161       | 0.372    | 0.157        | 0.291        | 0.293        |
| Cyber pornography             | 0.284     | 0.161        | 1.000       | 0.358    | -0.011       | 0.379        | 0.936        |
| Cyber stalking or bullying    | 0.094     | 0.372        | 0.358       | 1.000    | 0.251        | 0.405        | 0.582        |
| Online gaming crimes          | 0.117     | 0.157        | -0.011      | 0.251    | 1.000        | 0.212        | 0.103        |
| Other cybercrimes             | 0.337     | 0.291        | 0.379       | 0.405    | 0.212        | 1.000        | 0.633        |
| Total cybercrimes             | 0.354     | 0.293        | 0.936       | 0.582    | 0.103        | 0.633        | 1.000        |



**Figure 3. Pearson Correlation Heatmap of Cybercrime Categories Against Children in India (2017–2021)**

### 3.6 Linear Regression Analysis

A simple linear regression model was estimated to investigate the association between child population and total reported cybercrime cases. Child population was a positive and statistically significant predictor of reported cybercrime cases as presented in Table 6 ( $B = 0.0906$ ,  $t = 5.6651$ ,  $p < 0.001$ ). This coefficient suggests that for a one-lakh increase in the child population, the reported cases are estimated to increase by around 0.091, while keeping all the other factors in the model fixed. The intercept was not significant at 5% level ( $p = 0.0668$ ).

**Table 6. Regression Coefficients for Child Population and Total Cybercrime Cases**

| Predictor                 | Coefficient (B) | Standard error | t-value | p-value |
|---------------------------|-----------------|----------------|---------|---------|
| Constant                  | 6.3479          | 3.4415         | 1.8445  | 0.0668  |
| Child population in lakhs | 0.0906          | 0.0160         | 5.6651  | <0.001  |

Overall regression model was statistically significant (Table 7:  $F(1,170) = 32.09$ ,  $p < 0.001$ ). The model accounted for

15.88% variance in the total cybercrime cases and the adjusted  $R^2$  value was 0.1539. The population of children accounted for much of the variation in reported cases, but the relatively low explanatory power suggests that other factors not included in the model were a major reason for much of the variation in reported cases.

**Table 7. Regression Model Summary and ANOVA**

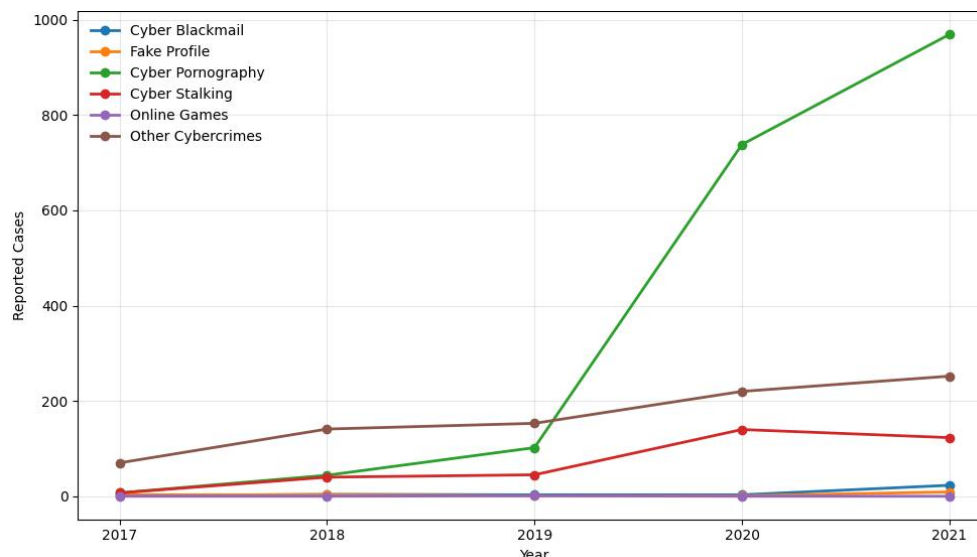
| Source     | Sum of squares | df  | Mean square | F       | p-value |
|------------|----------------|-----|-------------|---------|---------|
| Regression | 41,860.4092    | 1   | 41,860.4092 | 32.0928 | <0.001  |
| Residual   | 221,740.3059   | 170 | 1,304.3547  | —       | —       |
| Total      | 263,600.7151   | 171 | —           | —       | —       |

### 3.7 Year-Wise Trends in Cybercrime Categories

Table 8 shows the distribution of cybercrime categories by year. The number of cases of cyber pornography or obscene-material offences rose from 7 in 2017 to 969 cases in 2021. The greatest increase was from 2019 to 2020, from 102 to 738. The number of other cybercrime cases rose from 70 cases in 2017 to 252 cases in 2021. The number of cyber-stalking/bullies also grew significantly, from 7 cases in 2017 to 140 in 2020 and 123 in 2021. Both cyber blackmailing and fake-profile offences were relatively rare, with both types on the rise in 2021 (Figure 4). As seen in Table 8, the national rise post 2019 was largely attributable to a significant rise in cyber pornography offences.

**Table 8. Year-Wise Distribution of Cybercrime Categories**

| Year  | Cyber blackmail | Fake profile | Cyber pornography | Cyber stalking | Online games | Other cybercrimes | Total |
|-------|-----------------|--------------|-------------------|----------------|--------------|-------------------|-------|
| 2017  | 1               | 3            | 7                 | 7              | 0            | 70                | 88    |
| 2018  | 4               | 3            | 44                | 40             | 0            | 141               | 232   |
| 2019  | 3               | 1            | 102               | 45             | 1            | 153               | 305   |
| 2020  | 3               | 1            | 738               | 140            | 0            | 220               | 1,102 |
| 2021  | 23              | 9            | 969               | 123            | 0            | 252               | 1,376 |
| Total | 34              | 17           | 1,860             | 355            | 1            | 836               | 3,103 |



**Figure 4. Year-wise Trends in Major Categories of Cybercrimes Against Children in India (2017–2021)**

### 4. Discussion

This study focused on the temporal, geographical and category-wise trend of cybercrime against children in Indian States and Union Territories between the years of 2017 to 2021. The results show that the number of cases reported has risen dramatically, from 88 cases in 2017 to 1,376 cases in 2021. There were increases in recorded cases, the greatest of which happened from 2019 to 2020, with recorded cases rising by over 260%. This trend indicates that cybercrime against children was increasingly becoming a speedy child-protection and cybersecurity issue between 2002 and 2013. The escalating use of digital technologies, reliance on the internet and the evolving nature of cyber threats have ushered in new opportunities for perpetrators to exploit vulnerable users, such as children, including children and young people

(Kuzior et al., 2024).

This rise following 2019 may be attributed to the increased utilization of digital platforms during the COVID-19 pandemic, which saw children increasingly relying on digital learning, social media, games, and digital communication. However, an increase in the number of cases should not only be seen as an increase in victimization rates (Ali et al., 2022). They could also be due to better reporting mechanisms, increased awareness, shifts in police practice around registration and increased awareness of online offences against children. Fear and stigma, not knowing who to report to, or lack of legal knowledge can all have a negative impact on cybercrime reporting. They can be particularly significant for children, who are often vulnerable and rely on adults to recognise and report on online harms (Sikra et al., 2023).

There were also significant inter-state variations. The states of Maharashtra, Uttar Pradesh, Kerala and Karnataka combined recorded over half of the reported cases. The disparities could be linked to different child populations, Internet penetration, urbanization rates, policing ability, digital literacy and access to cybercrime reporting mechanisms. Child population was a significant predictor of total cases but only accounted for 15.88% of the variance. This suggests that regional differences cannot only be attributed to population size and that technological, socioeconomic and institutional factors are also relevant. National aggregations can mask large regional disparities, therefore state-level analysis is necessary. (Baumeister et al., 2024).

Nearly 60% of all offences recorded were related to cyber pornography and obscene material about children, and the former had the highest correlation with the total number of cybercrime offences. This discovery highlights technology-facilitating sexual exploitation as the key factor contributing to the country's rise. Offences committed in this manner are legal and investigative difficulties due to the fact that digital content can be generated, copied, transmitted and saved on a variety of platforms and in various jurisdictions. While the POCSO Act offers significant legal safeguards for children against sexual offences, its implementation has faced a number of obstacles, including the reporting of sex crimes, their investigation, the support for victims, and the coordination of the institutions that might be called upon to intervene (Maity & Chakraborty, 2023; Pattath et al., 2023). The Information Technology Act also needs to be constantly reviewed to meet the evolving modes of cybercrime and cyber-evidence (Madhusudan, 2024).

The results substantiate the need for a multi-faceted approach to children's online safety including law enforcement, digital literacy, platform accountability, school-based prevention, and victim support systems. The 4Cs framework (content, contact, conduct and contract risks) provides a good foundation for the development of comprehensive protection policies (Jang & Ko, 2023). Child-care providers and teachers should also be trained to identify warning signs and appropriately respond to cyberbullying, exploitation and online harassment (Briggs, 2020). In general, there is a need for better inter-agency coordination, dedicated cybercrime units, reporting mechanisms that are child-friendly, and evidence-based digital safety policies to enhance the safety of children in India's rapidly changing digital landscape.

## 5. Conclusion

This study comprehensively examines the cybercrime against children from the National Crime Records Bureau data from 2017 to 2021 in Indian States and Union Territories. The results show that there has been a significant rise in the number of reported cases over the period of the study, with the steepest increase after 2019. Cyber pornography and obscene content publishing was the biggest offence category, and there was a clear geographical disparity between "hot spots" and a sub-dominant number of states that saw a high proportion of reported offences. The correlation between child population and reported cybercrime cases shows that child population is a contributing factor to the distribution of reported cybercrime cases. However, the fit of the regression model points towards other factors including the role of technology access, reporting, institutional capacity and wider socioeconomic issues. The results indicate that there is a need for better legal enforcement, better cybercrime reporting, better cybercrime forensic skills, and more coordinated child protection strategies at the law-enforcement, educational, technology and policy levels. Continuous progress in digital literacy initiatives among children, parents and teachers, as well as the constant evolution of the cybersecurity legal framework and institutional procedures, will be key to combat new threats that are appearing online. This study provides solid empirical data to the body of research on child cyber safety and provides some practical takeaways that can inform evidence-based policy making and help boost the national response to protecting children in an increasingly digital world.

## Reference

1. Al-Hakimi, A., & Nur, M. (2023). Cybercrime Threats in Technology Era. *Journal of Computer Science & Computational Mathematics*, 13(1), 21-30.
2. Ali, M. K., Pearson-Stuttard, J., Selvin, E., & Gregg, E. W. (2022). Interpreting global trends in type 2 diabetes complications and mortality. *Diabetologia*, 65(1), 3-13.
3. Baumeister, C., Leiva-León, D., & Sims, E. (2024). Tracking weekly state-level economic conditions. *Review of Economics and Statistics*, 106(2), 483-504.
4. Briggs, F. (2020). *Child protection: A guide for teachers and child care professionals*. Routledge.
5. Feng, J., & Qi, S. (2024). Digital infrastructure expansion and economic growth in Asian countries. *Journal of Business and Economic Options*, 7(2), 27-32.
6. Flyverbom, M., Deibert, R., & Matten, D. (2019). The governance of digital technology, big data, and the internet: New roles and responsibilities for business. *Business & Society*, 58(1), 3-19.
7. Fourie, L. (2020). Protecting children in the digital society. *Childhood Vulnerabilities in South Africa: Some Ethical Perspectives*, 229-272.
8. Jang, Y., & Ko, B. (2023). Online safety for children and youth under the 4Cs framework—A focus on digital policies in Australia, Canada, and the UK. *Children*, 10(8), 1415.
9. Karthik, R. (2023). A Critical Analysis on Cyber Crimes against Children in India. *Indian J. Integrated Rsch. L.*, 3, Volume-6 | Issue-1 | February, 2026

- 1.
10. Kuzior, A., Tiutiunyk, I., Zielińska, A., & Kelemen, R. (2024). Cybersecurity and cybercrime: Current trends and threats. *Journal of International Studies* (2071-8330), 17(2).
11. Madhusudan, V. V. (2024). A Critical Analysis of Information Technology Act, 2000 with Reference to Cyber Offence and Cyber Security. *Issue 2 Int'l JL Mgmt. & Human.*, 7, 2529.
12. Maity, S., & Chakraborty, P. R. (2023). Implications of the POCSO Act and determinants of child sexual abuse in India: insights at the state level. *Humanities and Social Sciences Communications*, 10(1), 6.
13. Matthews, T., Bursztein, E., Kelley, P. G., Kissner, L., Kramm, A., Oplinger, A., ... & Consolvo, S. (2025). Supporting the digital safety of at-risk users: Lessons learned from 9+ years of research and training. *ACM Transactions on Computer-Human Interaction*, 32(3), 1-39.
14. Padmavathy, R. D. (2018). Cybercrime in India: a trend analysis specific to north east. *Aayushi Int Interdiscip J*, 5(4), 88-96.
15. Pattath, A. R., Saju, J. M., Choudhary, S. K., Singh, U. P., Dev, K., & Mittal, A. K. (2023). Pocso act (2012): A critical assessment after a decade of its enactment & enforcement. *International Journal of Medical Toxicology & Legal Medicine*, 26(1and2), 73-89.
16. Sharma, B., & Kataria, G. (2022). Surge in Cybercrime against Children in India amid the Pandemic. *Issue 5 Int'l JL Mgmt. & Human.*, 5, 1279.
17. Sikra, J., Renaud, K. V., & Thomas, D. R. (2023). UK cybercrime, victims and reporting: A systematic review. *Commonwealth Cybercrime Journal*, 1(1), 28-59.
18. Stoilova, M., Livingstone, S., & Khazbak, R. (2021). Investigating Risks and Opportunities for Children in a Digital World: A rapid review of the evidence on children's internet use and outcomes.
19. Tikhute, Vishal (2023), "NCRB cyber-crimes against children in India from year 2017 to 2021 (compiled dataset)", Mendeley Data, V2, doi: 10.17632/mc7wsp8v9y.2