



SOCIAL MEDIA ADDICTION AND CYBER RISKS AMONG YOUTH IN INDIA:

CHALLENGES AND PREVENTIVE MEASURES

Proposing the Youth Cyber Safety and Digital Well-Being Framework (YCSDWF)

Jyoti Chandel

Assistant Professor, Shri Guru Sandipani Institute of Management , Ujjain, Madhya Pradesh, India

Email: jyotichandel@gmail.com

ABSTRACT

India's youth population now constitutes one of the largest concentrations of social media users anywhere in the world, with active internet users crossing 886 million in 2024 and a substantial share of that growth concentrated among adolescents and young adults. This expansion has delivered genuine benefits in education, civic participation, and social connection, but it has also been accompanied by a parallel rise in problematic patterns of use and exposure to digitally mediated harm. Drawing on peer-reviewed Indian clinical and public-health research, government data from the National Crime Records Bureau (NCRB) and the Indian Cyber Crime Coordination Centre (I4C), international comparative evidence from the World Health Organization's Health Behaviour in School-aged Children (HBSC) survey, and civil-society documentation from UNICEF and Child Rights and You (CRY), this paper examines the scale and character of social media addiction among Indian youth and maps the principal cyber risks that accompany it: cyberbullying, online harassment, identity theft, phishing and financial fraud, privacy breaches, sextortion and image-based abuse, and misinformation and deepfakes. The analysis indicates that Indian studies report social media or internet addiction-related behaviour in roughly one-fifth to two-fifths of college-going samples depending on instrument and setting, a range broadly consistent with international meta-analytic estimates, while financial cybercrime complaints routed through the I4C's 1930 helpline have grown from under a hundred lakh in 2023 to more than three crore in 2025. The paper situates these findings within established psychological frameworks, including the Fear of Missing Out (FOMO) construct grounded in self-determination theory and the Interaction of Person-Affect-Cognition-Execution (I-PACE) model of problematic technology use, to explain why adolescents and young adults are disproportionately vulnerable to both compulsive engagement and exploitation. It then proposes the Youth Cyber Safety and Digital Well-Being Framework (YCSDWF), a seven-pillar preventive architecture spanning digital literacy, responsible usage norms, cyber hygiene, privacy protection, mental health support, institutional and policy interventions, and community awareness, designed for phased implementation by schools, families, platforms, and government bodies. The paper closes with policy recommendations directed at the Ministry of Electronics and Information Technology (MeitY), the Ministry of Education, state governments, and digital platforms, and identifies the principal limitations of the secondary-data approach used here, including the continuing scarcity of large-scale, nationally representative Indian data on adolescent digital well-being.

Keywords: Social Media Addiction, Cyber Risks, Youth, India, Cyberbullying, Online Safety, Digital Well-Being, FOMO, Problematic Internet Use, YCSDWF, Deepfakes, Sextortion

JEL Classification: I12, I31, K42, O33, D83, J13

1. INTRODUCTION

Social media has become woven into the daily routines of Indian adolescents and young adults in a way that would have seemed implausible barely a decade ago. The country added hundreds of millions of new internet users in the past several years, and the IAMA-Kantar Internet in India Report 2024 placed active internet users at 886 million, up eight percent over

the previous year, with rural India now accounting for the majority of that base. Within this expanding digital population, young people are not merely present; they are disproportionately represented among the most intensive users, and platforms have been designed, deliberately, to capture and hold their attention for as long as possible.

This paper is concerned with two phenomena that are conceptually distinct but practically inseparable. The first is social media addiction, understood here not as a formal psychiatric diagnosis but as a pattern of compulsive, difficult-to-control use that interferes with sleep, study, relationships, or daily functioning. The second is the cluster of cyber risks that follow young people onto the platforms they use compulsively: harassment, fraud, identity theft, sextortion, and increasingly, AI-generated deception. The two are linked in an important way. The same psychological mechanisms that make a platform addictive, the variable reward of likes and notifications, the social comparison built into curated feeds, the fear of being left out of a conversation that never stops, are frequently the mechanisms that fraudsters, harassers, and groomers exploit to gain access to a young user's attention, trust, and data.

India's situation has some features that distinguish it from the heavily studied North American and European contexts. A very large share of new internet users in the past five years have been first-generation users, often accessing the internet primarily or exclusively through a single shared or personal smartphone, with comparatively limited prior exposure to formal digital literacy instruction. Regional-language content has grown rapidly, and platform safety tooling, content moderation capacity, and law-enforcement cyber-forensic capacity have not kept pace with either the user growth or the linguistic diversity of the user base. These structural conditions matter for how addiction and risk manifest among Indian youth, and they shape what a workable preventive framework needs to look like.

This paper proceeds in four broad movements. It first reviews what is known, from Indian and international peer-reviewed research, about the prevalence and correlates of problematic social media and internet use among young people. It then maps the principal categories of cyber risk that intersect with heavy social media use, drawing on NCRB, I4C, and civil-society data. Third, it examines a small set of recent secondary data and presents them in tabular and graphical form to illustrate the trajectory of both addiction-related indicators and cybercrime indicators. Finally, it proposes the Youth Cyber Safety and Digital Well-Being Framework, an original seven-pillar model intended to translate this evidence into an implementable set of interventions for schools, families, platforms, and government bodies in the Indian context.

2. BACKGROUND AND RATIONALE OF THE STUDY

Three converging trends motivate this study. The first is sheer scale: India's social media user base, variously estimated between 462 million and over 500 million depending on methodology and date of measurement, makes it one of the largest single national markets for platforms such as YouTube, Instagram, and WhatsApp anywhere in the world, and a meaningful share of that base is under 25. The second is the accumulating clinical and public-health evidence, much of it from Indian medical colleges and community medicine departments, documenting that a substantial minority of college and school-going samples meet screening thresholds for problematic internet or social media use, with associated sleep disruption, anxiety, and academic difficulty. The third is the parallel and faster-growing trajectory of cybercrime: complaints registered through the I4C's National Cyber Crime Reporting Portal and its 1930 helpline rose from roughly 96.4 lakh in 2023 to 2.21 crore in 2024 and 3.24 crore in 2025, an increase that outpaces population growth, internet adoption, or any plausible reporting-artifact explanation alone.

These three trends are rarely studied together in the Indian context. Public-health literature on social media addiction tends to be clinical and cross-sectional, focused on a single city or institution, with limited attention to the cybercrime dimension. NCRB and I4C data, in turn, are rarely cross-referenced against psychological literature on why young users are vulnerable in the first place. This paper's contribution is to bring these two literatures into a single analytical frame, and to use that combined picture to motivate a preventive framework that addresses both the compulsive-use problem and the exploitation problem as facets of the same underlying exposure.

3. STATEMENT OF THE PROBLEM

Indian policy discourse on youth and the internet has tended to treat addiction and cybercrime as separate problems requiring separate institutional homes: the former assigned to health and education authorities, the latter to police and the

Ministry of Home Affairs. This separation has practical costs. A young person who spends seven hours a day on social media, a figure consistent with recent large-sample Indian survey data on youth usage patterns, is simultaneously at elevated risk of compulsive-use harms and at elevated exposure to the harassment, fraud, and image-based abuse that occur on the same platforms during those same hours. A preventive strategy that addresses only the addiction dimension, through screen-time limits, for instance, without also building cyber-hygiene and reporting literacy, leaves young users exposed to risks that persist regardless of how much time they spend online. Conversely, a cybercrime strategy that focuses solely on enforcement after harm has occurred, without addressing the compulsive engagement patterns that make young users more available targets, addresses the problem only after the fact. The central problem this paper addresses is the absence of an integrated, India-specific preventive framework that treats digital well-being and cyber safety as a single design problem for youth-serving institutions.

4. RESEARCH OBJECTIVES

1. To synthesize Indian and international peer-reviewed evidence on the prevalence, correlates, and psychological mechanisms of social media and problematic internet use among adolescents and young adults.
2. To map the principal categories of cyber risk associated with social media use among Indian youth, drawing on NCRB, I4C, and civil-society data.
3. To examine recent secondary data on usage patterns and cybercrime trends in India and present them in a form suitable for policy and institutional planning.
4. To propose the Youth Cyber Safety and Digital Well-Being Framework (YCSDWF) as an original, implementable model addressing both addiction-related and exploitation-related dimensions of youth digital risk.
5. To advance specific, actionable recommendations for MeitY, the Ministry of Education, state governments, educational institutions, and digital platforms.

5. RESEARCH QUESTIONS

6. What is the documented scale and pattern of social media addiction and problematic internet use among Indian youth, and how does it compare with international benchmarks?
7. What are the principal categories of cyber risk that intersect with heavy social media use among Indian youth, and what trends do available secondary data show?
8. What psychological and structural factors explain the particular vulnerability of adolescents and young adults to both compulsive engagement and digital exploitation?
9. What preventive framework, structured around the YCSDWF model, can integrate digital literacy, cyber hygiene, privacy protection, mental health support, and institutional intervention in a way that is implementable within India's resource and capacity constraints?

6. SCOPE AND DELIMITATIONS OF THE STUDY

This study focuses on youth in India, broadly defined as adolescents and young adults in the 13 to 25 age range, and on risks and addictive patterns associated specifically with social media and allied digital platforms, including messaging applications, short-video platforms, and gaming-adjacent social spaces. The analysis relies entirely on secondary data: peer-reviewed Indian and international studies, government statistics published by the NCRB, I4C, and MeitY, and reports from UNICEF, WHO, CRY, IAMAI, and comparable organizations. It does not include new primary survey or interview data collected by the author. The cyber-risk taxonomy addressed here overlaps substantially with, but is not identical to, the cybercrime-against-women literature; this paper's lens is age rather than gender, although the two intersect, and existing research on online gender-based violence is cited where it bears directly on youth-specific patterns. The paper does not

address offline bullying, substance use, or general adolescent mental health except where these intersect directly with social media use and cyber risk.

7. LITERATURE REVIEW

7.1 Conceptualizing Social Media Addiction and Problematic Use

The clinical and psychological literature has been deliberately cautious about the term "addiction" in relation to social media, since neither the DSM-5 nor the ICD-11 currently recognizes social media addiction as a standalone disorder in the way that gaming disorder is recognized. Kuss and Griffiths, in an early and frequently cited review, argued that social networking site use could nonetheless produce addiction-like symptoms, salience, mood modification, tolerance, withdrawal, conflict, and relapse, that mirror behavioural addiction frameworks even without a formal diagnostic category. This six-component structure has since been operationalized in instruments such as the Bergen Social Media Addiction Scale, which several of the Indian studies reviewed below adapt or reference.

A second influential theoretical strand is the Interaction of Person-Affect-Cognition-Execution (I-PACE) model, which frames problematic technology use as arising from an interaction between predisposing factors (personality, psychopathology, social context), affective and cognitive responses to specific situations, and executive functioning or self-regulatory capacity. The model has been applied directly to social media addiction in recent university-student research, where it has helped explain why fear of missing out functions as a proximal driver of compulsive use rather than merely a correlate of it.

7.2 Fear of Missing Out and Self-Determination Theory

Przybylski, Murayama, DeHaan, and Gladwell's foundational work defined the Fear of Missing Out (FOMO) as a self-regulatory state arising from the perception, situational or chronic, that one's psychological needs are not being met, and rooted this construct explicitly in self-determination theory's three basic needs of autonomy, competence, and relatedness. Subsequent research has consistently found FOMO to be strongly and positively associated with social media addiction; a 2025 study of university students using the I-PACE model as its guiding framework reported a standardized association between FOMO and social media addiction strong enough to explain roughly sixty percent of the variance in addiction scores, a magnitude consistent with the broader literature. Other work frames FOMO through the lens of the uses and gratifications tradition, in which users actively choose social media to satisfy needs for social interaction, entertainment, and information, but find that those same gratifications, once habituated, become difficult to disengage from. Kircaburun, Alhabash, Tosuntaş, and Griffiths extended this line of inquiry by examining how personality traits interact with platform-specific motives to produce problematic use patterns, underscoring that "addiction" in this domain is rarely a single mechanism but a convergence of need states, personality, and platform design.

This theoretical grounding matters for the present paper because it explains why adolescents, who are at a developmental stage characterized by heightened sensitivity to social evaluation and peer belonging, are particularly susceptible to FOMO-driven compulsive use, and why interventions that rely solely on willpower or parental restriction, without addressing the underlying unmet psychological needs, tend to show limited durability.

7.3 Indian Evidence on Prevalence and Correlates

Indian empirical research on this question has grown substantially over the past decade, mostly through cross-sectional surveys conducted in medical colleges, pre-university colleges, and engineering or arts and science institutions. A comparative study among pre-university students in urban Bengaluru, published in the Indian Journal of Community Medicine, examined social media usage and associated health complaints across government and private institutions and found measurable differences in addiction prevalence and associated health problems by institution type. A systematic review and meta-analysis of internet addiction among Indian college students, covering studies published between 2010 and 2020 and indexed across PubMed, Scopus, EMBASE, and related databases, concluded that approximately twenty to forty percent of Indian college students could be classified as at risk for internet addiction, while flagging that sampling method

and study quality strongly influenced the prevalence estimates obtained, with higher-quality, probability-sampled studies tending to report figures at the lower end of that range.

A more recent cross-sectional study from Chengalpattu district, Tamil Nadu, surveying 320 students pursuing professional courses, found that 36.9 percent of respondents exhibited addiction-related behaviour, with significant associations between addiction status and self-reported personal-relationship strain, anxiety, sleep difficulty, and eye strain; notably, the study also found that students who spent more than three hours daily on social media were nearly five times more likely to score as addicted than lighter users, and that, contrary to some assumptions, female students reported greater concern about their own usage patterns than male students. A separate study among medical students in Gujarat found that 32.1 percent of students screened positive for social media dependence, with strong associations to elevated stress, anxiety, and depressive symptoms, a pattern that recurs across the Indian literature regardless of geographic region or institution type.

Large-sample survey data add a behavioural dimension to these clinical findings. A study conducted by the Indian Institute of Management, Rohtak, surveying close to 39,000 youth respondents aged 18 to 25, found that male users reported spending an average of six hours and forty-five minutes daily on social media applications, while female users reported an even higher average of seven hours and five minutes, with the majority of usage concentrated in evening hours and entertainment content accounting for over half of viewing time. These figures, drawn from a far larger and more behaviourally specific sample than the clinical screening studies, suggest that the sheer volume of daily exposure among Indian youth is now comparable to, or in some respects exceeds, figures reported in higher-income countries, even as formal addiction-screening prevalence estimates remain in a broadly similar range to international meta-analytic figures.

7.4 International Comparative Evidence

The World Health Organization's Health Behaviour in School-aged Children (HBSC) study, surveying close to 280,000 adolescents aged 11, 13, and 15 across forty-four countries and regions in Europe, Central Asia, and Canada, offers the most methodologically robust comparative benchmark available, even though India is not among the participating countries. The 2024 HBSC report found that the proportion of adolescents classified as problematic social media users rose from seven percent in 2018 to eleven percent in 2022, with girls reporting markedly higher rates than boys, thirteen percent against nine percent, and with the highest national rates recorded in Romania, Bulgaria, and Ireland. The HBSC's problematic-use classification, based on respondents reporting at least six of nine symptoms on a validated Social Media Disorder Scale, including loss of sleep, declining school performance, and inability to reduce use despite a wish to do so, offers a more conservative and clinically grounded threshold than several of the screening instruments used in Indian college-based studies, which may partly explain why Indian prevalence figures, generally in the twenty to forty percent range, sit considerably higher than the HBSC's eleven percent European and Central Asian figure. This divergence is itself analytically informative: it suggests either that Indian youth populations are experiencing more severe or more prevalent problematic use than their European counterparts, or that differences in instrument, age range, sampling frame, and self-selection in convenience-sampled Indian college studies inflate prevalence relative to the more representative HBSC methodology, or, most plausibly, some combination of both, a question this paper returns to in its discussion of methodological limitations.

UNICEF's cross-national research on cyberbullying provides a complementary international benchmark for the risk side of the equation. A 2019 UNICEF and U-Report poll spanning thirty countries, including India, found that one in three young respondents reported having been a victim of online bullying, with almost three-quarters identifying mainstream social networks as the most common site of such bullying. UNICEF's later Changing Childhood Project, surveying over 21,000 respondents across twenty-one countries, found that seventy-seven percent of young people use the internet daily and that seventy-nine percent of young respondents themselves identified being bullied online as a serious risk facing children, indicating that concern about cyber risk is now a majority view among young internet users themselves rather than solely an adult or institutional preoccupation.

7.5 Cyberbullying and Online Harassment in the Indian Context

Indian-specific cyberbullying research, while smaller in volume than the clinical addiction literature, points to a consistent pattern of underreporting alongside meaningful prevalence. A widely cited 2020 study by the non-governmental organization Child Rights and You (CRY), surveying 630 adolescents aged 13 to 18 in the Delhi National Capital Region,

found that 9.2 percent had experienced cyberbullying, but that vulnerability rose sharply with screen time: 22.4 percent of respondents who used the internet more than three hours daily reported cyberbullying victimization, rising to 28 percent among those using the internet more than four hours daily, a dose-response relationship that aligns closely with the addiction-correlates literature reviewed above. The same study found that half of victims had not reported the incident to any teacher, guardian, or platform, and that one in four respondents had encountered a morphed image or video of themselves online, a finding that anticipates the more recent and more technologically sophisticated deepfake-abuse problem discussed in Section 9.7 of this paper.

A narrative review of cyberbullying among Indian adolescents, synthesizing multiple smaller Indian studies, found considerable variation in reported prevalence depending on sample and instrument, citing one study of 1,721 higher-education students in which thirty percent reported having experienced cyberbullying, alongside other studies reporting figures both above and below this range. The review's authors note that inconsistent operational definitions of cyberbullying across Indian studies make cross-study comparison difficult, a methodological caution this paper also applies to its own synthesis.

7.6 Financial Cybercrime, Fraud, and the Emerging Deepfake Threat

While financial cybercrime in India is not exclusively or even primarily a youth phenomenon, young digital-payment users, who skew toward higher transaction frequency and lower average account balances but also toward greater willingness to engage with unfamiliar apps, investment platforms, and online job and gig-work offers, are documented targets of several fraud categories with particular salience for this paper. Government data presented to Parliament and compiled by the I4C indicate that complaints registered through the National Cyber Crime Reporting Portal and the 1930 helpline rose from approximately 96.4 lakh in 2023 to 2.21 crore in 2024 and 3.24 crore in 2025, alongside reported financial losses that the I4C estimated at over eleven thousand crore rupees in the first nine months of 2024 alone, with investment scams, fraudulent trading apps, and so-called "digital arrest" extortion schemes accounting for a large share of that total.

The deepfake dimension of this threat has emerged with particular speed. India-focused industry analysis published in 2024 reported that deepfake-related cases in the country had increased by 550 percent since 2019, and a 2025 industry survey found that 47 percent of Indian adults reported either personally experiencing or knowing someone who had experienced an AI voice-cloning or deepfake scam, nearly double the comparable global average of 25 percent, with 83 percent of Indian victims of such scams reporting a monetary loss. For a youth population that is simultaneously the most active social media cohort, the most exposed to AI-generated content, and among the least likely to have encountered formal training in recognizing synthetic media, this convergence of high platform engagement and rapidly evolving deception technique represents one of the most significant emerging components of the cyber-risk landscape this paper addresses.

7.7 Research Gap

Three gaps in the existing literature motivate this paper's approach. First, Indian research on social media addiction has been conducted almost entirely at the level of individual institutions or districts, using varied instruments and thresholds, with no single nationally representative study comparable in scale or methodological rigour to the WHO's HBSC survey; this paper does not resolve that gap but makes it explicit by juxtaposing the Indian and HBSC findings directly. Second, the addiction literature and the cybercrime literature in India have developed largely in isolation from one another, with public-health researchers rarely engaging NCRB or I4C data and criminologists rarely engaging clinical screening literature; this paper's combined framing is intended as a corrective. Third, existing Indian policy responses, including school-level digital literacy guidelines and platform-level age-verification requirements, have generally addressed either the addiction dimension or the safety dimension, but not both as a unified design problem; the YCSDWF model proposed in Section 11 is offered as a response to this third gap.

8. THEORETICAL FRAMEWORK

This paper draws on three complementary theoretical traditions to explain both the addictive pull of social media among young users and their disproportionate exposure to cyber risk.

8.1 Self-Determination Theory and the FOMO Construct

Self-determination theory holds that human motivation and well-being depend on the satisfaction of three basic psychological needs: autonomy, competence, and relatedness. Przybylski and colleagues' formulation of FOMO as a self-regulatory state arising when these needs go unmet provides this paper's primary explanatory mechanism for compulsive use. Adolescence is a developmental period in which relatedness needs, particularly peer belonging and social status, are especially salient, which helps explain why FOMO-driven social media use peaks during the school and college years rather than earlier or later in the life course.

8.2 The I-PACE Model

The Interaction of Person-Affect-Cognition-Execution model offers a more complete causal architecture, situating FOMO and similar affective states within a feedback loop that includes predisposing personal characteristics, situational triggers, and the executive self-regulatory capacity available to resist compulsive engagement. This model is useful for this paper because it explains why purely informational interventions (telling young people that excessive use is harmful) tend to underperform interventions that also build executive self-regulatory skills and address underlying unmet psychological needs, a design principle reflected in the YCSDWF model proposed later in this paper.

8.3 Routine Activity Theory Applied to Cyber Risk

To explain the risk side of the equation, this paper adapts routine activity theory, originally developed in criminology to explain how the convergence of a motivated offender, a suitable target, and the absence of a capable guardian produces crime opportunities. Applied to the digital environment, heavy, habitual social media use increases a young user's availability as a target (more time online, more data shared, more public-facing profile activity), while the same compulsive engagement patterns that reduce self-regulatory vigilance also reduce the likelihood that a young user will pause to verify a suspicious message, recognize a manipulation attempt, or apply caution before sharing an image. The "capable guardian" in this framework can be institutional (platform safety tooling, school-based digital literacy instruction, parental engagement) rather than only personal, which is the conceptual bridge to the preventive framework this paper proposes.

Taken together, these three frameworks suggest that effective prevention must operate at three levels simultaneously: the psychological level (addressing unmet needs that drive compulsive use), the behavioural level (building self-regulatory and verification skills), and the structural level (institutional and platform-level guardianship). The YCSDWF model in Section 11 is organized to address all three.

9. RESEARCH METHODOLOGY

9.1 Research Design

This paper adopts a descriptive, secondary-data-based design combining a structured narrative literature review with documentary and statistical analysis of government and civil-society data. It does not involve primary data collection. The approach is consistent with policy-oriented social science research that seeks to synthesize dispersed evidence into a single analytical and planning framework, rather than to test a specific causal hypothesis through original fieldwork.

9.2 Data Sources

Three categories of secondary data inform this paper. The first is peer-reviewed literature, drawn from PubMed, PMC, Scopus-indexed journals, and Cureus, covering both Indian clinical and public-health studies of social media and internet addiction and international theoretical and empirical work on FOMO, the I-PACE model, and cyberbullying. The second is government statistical data, principally the NCRB's Crime in India series, I4C and Ministry of Home Affairs data on the National Cyber Crime Reporting Portal and the 1930 helpline, and IAMA-Kantar internet usage reports. The third is international and civil-society reporting, including the WHO's HBSC international report series, UNICEF's cyberbullying and Changing Childhood research, and documentation from Child Rights and You (CRY).



9.3 Sampling Approach

Because this is a secondary-data synthesis rather than a primary survey, no respondent sampling was undertaken by the author. Source selection followed a purposive approach: studies and reports were included if they (a) reported quantitative prevalence, trend, or correlational data relevant to social media addiction or youth-relevant cyber risk, (b) were published or last updated within the period 2018 to 2026, with limited exceptions for foundational theoretical works such as Przybylski et al. (2013) and Kuss and Griffiths' early addiction scholarship, and (c) originated from a peer-reviewed journal, a recognized government statistical agency, or a major international or civil-society body with a publicly documented methodology.

9.4 Data Collection Methods

Data were collected through structured search of academic databases and official government and international-organization publications, cross-checked across at least two independent sources where possible. Where studies reported overlapping or potentially duplicative samples, the most recent or most methodologically robust source was prioritized, and divergent figures from different sources are reported with their original attribution rather than averaged or reconciled, in keeping with the analytical caution recommended in Section 7.7.

9.5 Analytical Techniques

The analysis combines narrative synthesis of qualitative and theoretical literature with descriptive statistical presentation of quantitative secondary data, organized into the trend tables and figures presented in Section 10. No inferential statistical testing was performed, since the data are drawn from heterogeneous studies with differing samples, instruments, and time frames that do not support pooled statistical analysis without risking spurious precision; where comparisons are drawn across sources, this is done narratively and with explicit caveats about comparability.

10. CURRENT SCENARIO OF SOCIAL MEDIA ADDICTION AMONG INDIAN YOUTH

Table 1 consolidates internet and social media usage indicators for India drawn from the IAMAI-Kantar Internet in India Report 2024 and DataReportal's Digital 2024/2026 India series, providing the scale context against which addiction prevalence figures should be read.

Indicator	2023/24 Figure	Source
Active internet users (all ages)	886 million (+8% YoY)	IAMAI-Kantar, 2024
Share of internet base in rural India	55% (488 million)	IAMAI-Kantar, 2024
Social media users (Jan 2024)	462 million (32.2% of population)	DataReportal, 2024
Social media users aged 18+	383 million (38.1% of adult population)	DataReportal, 2024
Avg. daily internet time (India)	~6 hrs 49 min (2025/26)	Meltwater/DataReportal
Avg. daily social media use, youth 18-25 (male)	6 hrs 45 min	IIM Rohtak survey (n=38,896)
Avg. daily social media use, youth 18-25 (female)	7 hrs 5 min	IIM Rohtak survey (n=38,896)

Table 1: India Internet and Social Media Usage Indicators, 2024-2026 (Sources: IAMAI-Kantar Internet in India Report 2024; DataReportal Digital 2024/2026 India; IIM Rohtak youth survey)

Table 2 summarizes addiction and problematic-use prevalence figures reported across recent Indian peer-reviewed studies, alongside the WHO HBSC international benchmark, to illustrate both the range found within India and the comparison with the most rigorous available international figure.

Study / Source	Sample	Prevalence Reported
Joseph et al., meta-analysis (2021)	Indian college students, pooled, 2010-2020 studies	20%-40% at risk of internet addiction
Chengalpattu district study, Tamil Nadu	320 professional-course students	36.9% addiction-related behaviour
Gujarat medical college study	Medical students	32.1% social media dependence
Internet addiction frequency, India (cited in Cureus 2025 review)	College students	40.7% internet addiction
Global meta-analytic estimate (cited in Cureus 2025 review)	Worldwide, with higher Asia rates	18.4% (global average)
WHO HBSC International Report (2024)	~280,000 adolescents, 44 countries (Europe/Central Asia/Canada)	11% problematic social media use (up from 7% in 2018)

Table 2: Comparative Social Media / Internet Addiction Prevalence, India vs. International Benchmark

Two patterns are worth drawing out from Tables 1 and 2 together. First, daily usage volume among Indian youth, in excess of six and a half hours on average for the 18-25 cohort, sits at or above figures typically reported in higher-income countries, even though India's overall internet penetration, at just over half the population, remains below saturation levels seen in many OECD countries. Second, Indian addiction-screening prevalence figures cluster in a considerably higher range, roughly twenty to forty percent depending on instrument, than the WHO HBSC's eleven percent problematic-use figure for European and Central Asian adolescents. As discussed in Section 7.4, this gap most plausibly reflects a combination of genuinely higher exposure (longer daily use, younger age of first smartphone access, less developed institutional digital-literacy infrastructure) and methodological divergence (non-representative convenience samples, varying screening instruments, and the absence of a single large-scale Indian study using HBSC-equivalent methodology). Both explanations point toward the same practical conclusion: Indian youth, as a population, show usage and risk indicators that warrant the same or greater policy attention as their international counterparts, even allowing for measurement uncertainty.

Qualitatively, the IIM Rohtak survey data add a content dimension to the time-use figures: entertainment content accounted for the largest share of viewing time among Indian youth respondents, at just over half of total content consumption, followed by professional and self-help content, educational and news content, and political content, with the heaviest usage period falling in evening hours. This pattern is consistent with a developmental and motivational account in which social media serves primarily a relaxation and social-connection function for Indian youth, a function that aligns closely with the relatedness-need component of self-determination theory discussed in Section 8.1, rather than primarily an informational or civic function.

11. MAJOR CYBER RISKS ASSOCIATED WITH SOCIAL MEDIA USE

This section maps the principal categories of cyber risk that intersect with heavy social media use among Indian youth. Each subsection draws on the most recent available NCRB, I4C, or peer-reviewed civil-society data.

11.1 Cyberbullying

Cyberbullying among Indian adolescents has been documented with prevalence estimates ranging from under ten percent to around thirty percent depending on sample, age range, and definition, as reviewed in Section 7.5. The most policy-relevant finding across these studies is the dose-response relationship between screen time and victimization risk: the CRY Delhi-NCR study found victimization rates more than doubling, from roughly nine percent overall to over twenty-eight percent among heaviest users, as daily internet use crossed the four-hour threshold. Underreporting is consistent and severe, with roughly half of identified victims in the CRY study never disclosing the incident to a trusted adult, teacher, or platform.

11.2 Online Harassment

Online harassment overlaps substantially with cyberbullying but extends to adult-perpetrated and adult-targeted behaviour, including coordinated harassment campaigns, doxing, and persistent unwanted contact. NCRB's Crime in India series records harassment-adjacent offences under multiple heads spanning the IT Act and the Bharatiya Nyaya Sanhita, and cybercrime cases overall, as recorded by NCRB, rose more than threefold between 2018 and 2023, a trend that civil-society monitors attribute to a combination of genuine incidence growth and increased reporting following the 2019 launch of the National Cyber Crime Reporting Portal.

11.3 Identity Theft

Identity theft affecting young social media users in India typically takes one of two forms: the creation of impersonating profiles using a victim's photographs and personal details, often for harassment or fraud, and the misuse of personal data, including Aadhaar-linked identifiers, for unauthorized loan applications or account creation. Young, digitally engaged users who maintain extensive public profile information are documented as more exposed to the first pattern, while the rapid expansion of digital lending applications has created new exposure to the second.

11.4 Phishing and Financial Fraud

Financial fraud constitutes the largest single category of cybercrime complaint volume in India by a wide margin. I4C and Ministry of Home Affairs data show complaints registered through the 1930 helpline and the National Cyber Crime Reporting Portal rising from approximately 96.4 lakh in 2023 to 2.21 crore in 2024 and 3.24 crore in 2025, with average daily complaint volume increasing more than threefold across that period, from roughly 26,400 to nearly 89,000 per day. Reported financial losses reached an estimated eleven thousand crore rupees in the first nine months of 2024 alone, according to I4C figures, with investment and trading-app scams, fraudulent loan applications, and so-called digital arrest extortion schemes accounting for the largest shares. Young users, who are heavy adopters of new investment and trading apps and frequent targets of fraudulent job and gig-work offers circulated through social media and messaging platforms, are a documented target population for several of these schemes, even though comprehensive age-disaggregated I4C data are not yet publicly available at the level of detail this paper would ideally draw on.

11.5 Privacy Breaches

Privacy breaches affecting youth users span unauthorized data collection by third-party applications, location-data exposure through geotagged content, and the aggregation of publicly shared personal information for use in subsequent harassment or fraud. India's Digital Personal Data Protection Act 2023 introduces a formal legal framework for data fiduciary obligations and breach notification, though implementing rules remained pending through much of 2025, leaving a gap between the Act's stated protections and operational enforcement during the period this paper's data span.

11.6 Sextortion and Image-Based Abuse

Sextortion, the use of real or threatened disclosure of intimate images to extort money or further content from a victim, has grown rapidly worldwide and in India specifically. International data from the Internet Watch Foundation documented a

360 percent increase in sextortion cases globally between 2019 and 2023, with South Asian nations showing particularly steep growth, a trend reflected in Indian platform and helpline reporting. Young users are documented as a disproportionately targeted demographic for this offence category, both because of their relatively higher willingness to share intimate content within trusted relationships that are later weaponized, and because organized extortion networks increasingly target younger users on dating and social platforms using fabricated profiles to build rapid trust before initiating extortion.

11.7 Misinformation and Deepfakes

The deepfake threat has expanded with unusual speed in the Indian context. Industry analysis reported a 550 percent increase in deepfake-related cases in India since 2019, with projected fraud losses running into tens of thousands of crore rupees, and a 2025 survey found that 47 percent of Indian adults had personally experienced or knew someone who had experienced an AI voice-cloning or deepfake scam, against a global average of 25 percent. For youth specifically, the threat manifests in two distinct forms: AI-generated non-consensual intimate imagery used for harassment or extortion of classmates and peers, a pattern documented internationally in school settings and increasingly reported in India, and AI-generated misinformation and political or celebrity deepfakes that young, heavy social-media users encounter at a higher daily rate than less-engaged users simply as a function of time spent on content-recommendation-driven platforms.

12. DATA ANALYSIS AND FINDINGS

This section presents the trend data most relevant to policy planning in tabular form, with brief interpretation following each table.

12.1 Cybercrime Complaint Growth, 2023-2025

Year	Complaints (1930 helpline / NCRP)	Avg. Daily Complaints	YoY Growth
2023	96.4 lakh	~26,411	Baseline
2024	2.21 crore	~60,500	+130%
2025	3.24 crore	~88,976	+46.4%

Table 3: Growth in Cybercrime Complaints via 1930 Helpline / National Cyber Crime Reporting Portal (Source: Ministry of Home Affairs / I4C data, as reported in *The420.in*, 2026)

The deceleration in year-on-year growth between 2024 and 2025, from 130 percent to 46.4 percent, should not be read as a sign that the underlying problem is easing; absolute daily complaint volume still more than tripled across the two-year window. The most plausible reading is that 2024's extraordinary growth rate partly reflected a low 2023 reporting base combined with expanding awareness of the 1930 helpline itself, while 2025's still-substantial growth reflects continuing genuine increase in incidence layered onto an already much larger reporting base.

12.2 Cybercrime Cases Against Children, 2021-2022

Offence Category	2021	2022	Change
Cyber pornography / publishing obscene material depicting children	Not separately available	1,171	—
Cyberstalking / bullying (against children)	Not separately	158	—

Offence Category	2021	2022	Change
	available		
Other cyber offences against children	Not separately available	416	—
Total cybercrimes against children	1,376	1,823	+32.5%

Table 4: NCRB-Recorded Cybercrimes Against Children (Below 18 Years), 2021-2022 (Source: NCRB Crime in India 2022, as analyzed by Child Rights and You)

Crimes against children overall, encompassing both online and offline offences, rose by close to nine percent in a single year according to the same NCRB release, with the cyber-specific subset growing considerably faster, suggesting that the digital dimension of child and adolescent victimization is expanding more quickly than offline victimization, even as both trend upward.

12.3 Addiction and Risk Indicators by Source

Indicator	Figure	Population
Internet addiction risk (meta-analysis)	20%-40%	Indian college students
Social media dependence	32.1%	Medical students, Gujarat
Addiction-related behaviour	36.9%	Professional-course students, Tamil Nadu
Cyberbullying victimization (light users)	9.2%	Adolescents 13-18, Delhi-NCR
Cyberbullying victimization (>4 hrs/day use)	28%	Adolescents 13-18, Delhi-NCR
Daily social media use, average	6 hrs 45 min - 7 hrs 5 min	Youth 18-25, national sample
Problematic social media use (international benchmark)	11%	Adolescents 11-15, 44 countries (HBSC)

Table 5: Consolidated Addiction and Cyber-Risk Indicators, India and International Benchmark

12.4 Interpretation

Three findings stand out from this consolidated picture. First, the volume of daily exposure, both in raw hours and in the scale of the underlying user base, has grown to a point where even modest percentage-point increases in addiction or victimization prevalence translate into very large absolute numbers of affected young people; an eleven percent problematic-use rate applied to even a conservative estimate of India's under-25 social media population would imply a multi-million-person affected group, while Indian studies using less conservative instruments suggest the true figure may be several times larger. Second, the cybercrime-complaint growth trajectory, more than tripling in two years, is occurring on a timescale too short to be explained by underlying population or internet-adoption growth alone, indicating either a genuine acceleration in offending, a substantial improvement in reporting infrastructure and willingness, or, most likely, both simultaneously. Third, the consistent dose-response relationship between screen time and both addiction-screening status

and cyberbullying victimization across multiple independent Indian studies strengthens the case, made theoretically in Section 8, that addictive engagement and exploitation risk are mechanistically linked rather than coincidentally co-occurring.

13. DISCUSSION

The evidence reviewed in this paper supports three broad conclusions with direct implications for the preventive framework proposed in Section 14.

First, India's youth digital-risk profile does not fit neatly into either a pure "addiction" framing or a pure "cybercrime" framing, and policy responses built around only one framing will systematically under-address the other. The same psychological mechanisms, FOMO, social comparison, the need for relatedness and validation, that drive compulsive engagement also reduce the self-regulatory vigilance that would otherwise help a young user recognize a phishing attempt, a fraudulent investment pitch, or a grooming pattern. A purely health-oriented response (screen-time limits, digital detox campaigns) addresses the compulsive-use symptom without building the cyber-hygiene competencies needed to resist exploitation; a purely enforcement-oriented response (cybercrime helplines, FIR registration) addresses harm after it occurs without reducing the underlying behavioural exposure that makes young users available targets in the first place.

Second, the gap between India's usage-intensity figures, which equal or exceed comparable figures from wealthier countries, and India's institutional digital-literacy and platform-safety infrastructure, which by most measures lags behind, represents the single most policy-actionable finding in this paper. India did not arrive at its current internet-usage scale through a gradual, multi-decade process the way many high-income countries did; it arrived through an extremely rapid, largely mobile-first expansion over roughly a decade, a pace that has consistently outrun the development of school curricula, parental digital literacy, and law-enforcement cyber-forensic capacity. This timing mismatch, rather than any unique cultural or psychological vulnerability among Indian youth, is the most parsimonious explanation for why Indian addiction-screening prevalence figures sit above the WHO HBSC's more conservative international benchmark.

Third, the deepfake and AI-fraud dimension represents a genuinely new threat vector that existing literature, including most of the addiction and cyberbullying studies reviewed in Section 7, predates. The 47 percent figure for Indian adults reporting personal or proximate experience with AI voice-cloning or deepfake scams, nearly double the global average, suggests that whatever preventive framework is built now needs explicit, forward-looking provision for synthetic-media literacy, not merely an extension of existing phishing-awareness or cyberbullying-prevention curricula, both of which were designed for an earlier and comparatively less sophisticated threat environment.

14. PROPOSED FRAMEWORK: YOUTH CYBER SAFETY AND DIGITAL WELL-BEING FRAMEWORK (YCSDWF)

14.1 Foundational Principles

Drawing on the theoretical grounding in Section 8 and the evidence synthesized in Sections 7, 10, and 12, this paper proposes the Youth Cyber Safety and Digital Well-Being Framework (YCSDWF), a seven-pillar preventive model designed to address compulsive-use and exploitation risk as a single, integrated design problem rather than as separate health and security concerns. Four principles govern the framework: developmental appropriateness, requiring that interventions be calibrated to the cognitive and social-emotional stage of the age group addressed rather than applying a uniform approach across ages 13 to 25; shared responsibility, distributing obligations across families, schools, platforms, and government rather than placing the full preventive burden on any single actor; evidence-based design, prioritizing interventions with documented effectiveness in the addiction and cyber-safety literature over intuitively appealing but unproven measures; and sustainability, favouring interventions that can be maintained with India's existing institutional capacity over aspirational measures that depend on resources not currently available.

14.2 The Seven Pillars of YCSDWF

Pillar	Focus Area	Primary Actors
P1	Digital Literacy	Ministry of Education, States, Schools
P2	Responsible Social Media Usage	Schools, Families, Platforms
P3	Cyber Hygiene Practices	MeitY, CERT-In, Schools
P4	Privacy Protection	MeitY, Platforms, DPDP Board
P5	Mental Health Support	Ministry of Health, Schools, NGOs
P6	Institutional and Policy Interventions	MeitY, MoE, State Governments
P7	Community Awareness and Capacity Building	State Governments, CSOs, Local Bodies

Table 6: YCSDWF Seven-Pillar Summary

Pillar 1: Digital Literacy

This pillar addresses the foundational knowledge gap identified throughout this paper: many Indian youth, particularly first-generation internet users, have not received structured instruction in evaluating online content, recognizing manipulation techniques, or understanding how recommendation algorithms shape what they see. Recommended actions include integrating a mandatory, age-tiered digital literacy curriculum into Classes 6 through 12 covering source evaluation, recognition of phishing and scam patterns, and basic understanding of how engagement-driven content algorithms work; training teachers through a cascading model in which a core group receives intensive training and subsequently trains colleagues at the district level; and developing curriculum content in regional languages rather than English alone, given documented disparities in platform and institutional responsiveness to non-English-language users and complaints.

Pillar 2: Responsible Social Media Usage

This pillar targets the behavioural dimension of compulsive use directly, drawing on the I-PACE model's emphasis on building self-regulatory capacity rather than relying solely on restriction. Recommended actions include school and family-based programmes that teach structured self-monitoring techniques, such as time-tracking and reflective journaling about usage patterns, rather than blanket bans, which the addiction literature suggests are often circumvented and can damage trust between young people and the adults attempting to set boundaries; encouraging platforms operating in India to provide more prominent and easily accessible usage-time dashboards and gentle break reminders, building on similar features already present in some major platforms; and promoting structured offline activity, sport, arts, community service, as a substitute rather than merely a restriction, consistent with the relatedness-need framing in self-determination theory.

Pillar 3: Cyber Hygiene Practices

This pillar addresses the practical skills needed to resist the specific fraud and exploitation patterns documented in Section 11. Recommended actions include structured instruction in password hygiene, two-factor authentication, and recognition of common financial-fraud scripts, including investment scams, fraudulent job offers, and so-called digital arrest extortion calls; rapid-response literacy specifically around the 1930 helpline, given evidence that early reporting within the first hour of a fraudulent transaction substantially increases the likelihood of fund recovery; and explicit instruction in verifying the authenticity of voice and video content, given the rapid growth of AI voice-cloning and deepfake fraud documented in Section 11.7.

Pillar 4: Privacy Protection

This pillar addresses data-exposure risk. Recommended actions include practical instruction in privacy-setting configuration across major platforms, with particular attention to location-data and contact-list permissions, which are frequently exploited in both harassment and loan-app blackmail schemes; encouraging platforms to adopt privacy-protective defaults for users who self-identify or are identified through age-verification mechanisms as minors; and supporting effective implementation of the Digital Personal Data Protection Act 2023's breach-notification and consent provisions as implementing rules are finalized, with specific attention to provisions relevant to minors' data.

Pillar 5: Mental Health Support

This pillar recognizes that the addiction and exploitation dimensions addressed throughout this paper carry direct mental health consequences, anxiety, sleep disruption, and in cases of sextortion or severe harassment, more acute psychological harm, that require dedicated support infrastructure rather than purely technical or educational responses. Recommended actions include training school counsellors in recognizing signs of problematic social media use and cyberbullying victimization, with clear referral pathways to mental health professionals; integrating helpline information for both cybercrime reporting (1930) and psychological support into the same outreach materials, so that a young person experiencing sextortion or harassment-related distress encounters both resources together rather than having to locate them separately; and ensuring that any institutional response to a reported incident treats the young person's psychological wellbeing as a parallel priority alongside evidence preservation and case registration.

Pillar 6: Institutional and Policy Interventions

This pillar addresses the structural and regulatory dimension. Recommended actions include encouraging platforms with a substantial Indian youth user base to publish age-disaggregated transparency reporting on cyberbullying, harassment, and fraud-removal metrics, extending the kind of disaggregated reporting already being discussed in the gender-based-violence policy literature to an age-based lens; supporting the development of streamlined, youth-accessible reporting interfaces, given evidence that roughly half of young cyberbullying victims never report an incident through existing channels; and embedding youth-specific cyber-risk indicators into NCRB's annual Crime in India reporting structure, allowing year-on-year tracking comparable to the trend data presented in Section 12.

Pillar 7: Community Awareness and Capacity Building

This pillar recognizes that schools and platforms alone cannot close the digital-literacy gap, particularly for first-generation internet users in rural and semi-urban India who may have limited access to structured school-based programming. Recommended actions include community-level awareness programmes delivered through existing rural and peri-urban infrastructure, such as anganwadi and ASHA worker networks and self-help groups, adapted for a youth and family digital-safety audience rather than the health-focused mandate these networks typically carry; partnerships with civil-society organizations with established track records in this space, including Child Rights and You and comparable bodies, to extend reach beyond what government programming alone can achieve; and parent-oriented programming that builds basic digital literacy among parents and guardians themselves, since several studies cited in this paper found that parental engagement and monitoring quality, not merely restriction, is associated with lower problematic-use prevalence among adolescents.

15. POLICY RECOMMENDATIONS

15.1 For the Ministry of Electronics and Information Technology (MeitY)

10. Commission a nationally representative survey of adolescent and young-adult digital well-being, using an instrument methodologically comparable to the WHO HBSC survey, to close the data gap identified in Section 7.7.
11. Work with CERT-In to develop and disseminate youth-targeted public awareness materials specifically addressing AI voice-cloning and deepfake fraud recognition, given the disproportionately high Indian exposure to this risk documented in Section 11.7.
12. Encourage major platforms operating in India to publish age-disaggregated transparency data on harassment, cyberbullying, and fraud-removal response times as part of existing intermediary-guideline compliance reporting.

15.2 For the Ministry of Education and State Education Departments

13. Integrate a structured, age-tiered digital literacy and cyber-safety curriculum into Classes 6 through 12, covering content evaluation, fraud recognition, and basic algorithmic literacy, as outlined in Pillar 1 of the YCSDWF model.
14. Train school counsellors to recognize signs of problematic social media use and cyberbullying victimization, with documented referral pathways to mental health professionals, as outlined in Pillar 5.
15. Develop curriculum and outreach material in regional languages, given documented disparities in platform responsiveness to non-English-language complaints and the linguistic diversity of India's youth internet population.

15.3 For State Governments and Local Bodies

16. Extend community-level digital-safety awareness programming through existing rural and peri-urban outreach infrastructure, including anganwadi and ASHA worker networks, as outlined in Pillar 7.
17. Promote local-language public awareness of the 1930 helpline and emphasize the importance of immediate reporting, given documented evidence that early reporting substantially improves fraud-recovery outcomes.

15.4 For Digital Platforms

18. Provide more prominent, easily accessible usage-time dashboards and gentle break or rest reminders for users identified as being in the youth age range, building on existing screen-time features already present on several major platforms.
19. Invest in regional-language content moderation capacity proportional to regional-language user growth, addressing the documented disparity in platform responsiveness across languages.
20. Strengthen proactive detection of AI-generated non-consensual imagery and deepfake content targeting minors and young adults, given the rapid growth of this threat category documented in this paper.

15.5 For Families and Educational Institutions

21. Favour structured self-monitoring and substitution strategies (offline activity, sport, structured screen-time agreements) over blanket restriction, consistent with the addiction literature's findings on the limited durability of purely restrictive approaches.
22. Build parental digital literacy alongside youth-focused programming, given documented associations between parental engagement quality and lower problematic-use prevalence among adolescents.

16. CHALLENGES AND LIMITATIONS

This paper's reliance on secondary data carries several limitations that should inform how its findings are used. First, as discussed in Section 7.7 and Section 10, Indian addiction-prevalence studies use varied instruments, sampling frames, and age ranges, and most rely on convenience samples drawn from single institutions rather than probability sampling, which limits direct comparability both across Indian studies and with the more methodologically rigorous WHO HBSC benchmark; the prevalence ranges presented in this paper should therefore be read as indicative rather than precise population estimates. Second, India lacks a single nationally representative, repeated, age-disaggregated survey of youth digital well-being comparable to the HBSC series, a gap this paper's own recommendations explicitly seek to close rather than one this paper can resolve through synthesis alone. Third, government cybercrime statistics, while authoritative for reported incidents, are well documented in the literature this paper cites as substantially undercounting true incidence, given persistent stigma, lack of awareness of reporting channels, and, for youth specifically, possible reluctance to disclose incidents to parents or authorities; the trend directions reported in Section 12 are likely more reliable than the absolute levels. Fourth, the deepfake and AI-fraud data drawn on in this paper come predominantly from industry and civil-society

sources rather than peer-reviewed academic research, reflecting the genuine novelty of this threat category, and should be treated with appropriately greater caution than the more established academic literature on addiction and cyberbullying. Finally, this paper's proposed YCSDWF framework has not been piloted or empirically tested; it is offered as a theoretically and evidentially grounded design proposal rather than a validated intervention, and the implementation recommendations in Section 15 should be understood as a starting point for pilot evaluation rather than a fully proven programme.

17. CONCLUSION

This paper has brought together two literatures, the clinical and public-health research on social media and internet addiction among Indian youth, and the criminological and policy data on cybercrime affecting the same population, that have largely developed in isolation from one another. The combined picture is sobering but also actionable. Indian youth report daily social media engagement at levels comparable to or exceeding those documented in wealthier countries, addiction-screening prevalence in the range of twenty to forty percent depending on instrument and sample, well above the WHO's more conservative eleven percent international benchmark, and cybercrime complaint volumes that have more than tripled in two years. These are not three separate problems but three faces of a single underlying condition: a youth population whose digital engagement has outpaced the institutional, educational, and regulatory infrastructure needed to keep that engagement safe.

The Youth Cyber Safety and Digital Well-Being Framework proposed in this paper is offered as a response calibrated to that condition. Its seven pillars are deliberately designed to address compulsive engagement and exploitation risk together rather than as separate health and security problems, reflecting the theoretical grounding in self-determination theory, the I-PACE model, and routine activity theory developed in Section 8. None of the individual components proposed, school-based digital literacy curricula, platform usage dashboards, community outreach through existing rural health infrastructure, are radical departures from approaches already piloted in various forms in India or internationally; the framework's contribution lies in integrating them into a single coordinated model rather than leaving them as the dispersed and uncoordinated initiatives they currently constitute.

India's digital future will, in large part, be lived by the generation this paper is concerned with. Whether that future is one in which young Indians use these platforms with genuine agency, well-being, and safety, or one in which a growing share experience them as a source of compulsion, exploitation, and harm, will depend substantially on whether the preventive infrastructure proposed here, or something comparable to it, is built in time to meet a youth population that is, by every measure examined in this paper, already living a substantial part of its daily life online.

ACKNOWLEDGEMENTS

The author thanks colleagues in the Department of Sociology and Social Work for their feedback on earlier drafts of this paper. No funding was received for this research. The views expressed are solely those of the author.

DECLARATION OF COMPETING INTERESTS

The author declares no conflict of interest. This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors. This manuscript has not been submitted elsewhere and has not been published previously in any form.

REFERENCES

- Boniell-Nissim, M., Marino, C., Galeotti, T., Blinka, L., Ozoliņa, K., Craig, W., et al. (2024). A focus on adolescent social media use and gaming in Europe, central Asia and Canada. Health Behaviour in School-aged Children international report from the 2021/2022 survey, Volume 6. WHO Regional Office for Europe. <https://www.who.int/europe>
- Brand, M., Young, K. S., Laier, C., Wölfling, K., & Potenza, M. N. (2016). Integrating psychological and neurobiological considerations regarding the development and maintenance of specific Internet-use disorders: An Interaction of Person-Affect-Cognition-Execution (I-PACE) model. *Neuroscience & Biobehavioral Reviews*, 71, 252–266.



- Child Rights and You (CRY). (2020). Online study and internet addiction: A study of cyberbullying among adolescents in Delhi-NCR. CRY. <https://www.cry.org>
- Child Rights and You (CRY). (2023). Analysis of NCRB cybercrime data on children, 2021–22. CRY. <https://www.cry.org>
- Citron, D. K. (2014). Hate crimes in cyberspace. Harvard University Press.
- Government of India. (2023). Digital Personal Data Protection Act 2023 (Act No. 22 of 2023). Ministry of Law and Justice.
- Indian Cyber Crime Coordination Centre (I4C) / Ministry of Home Affairs. (2026). National Cyber Crime Reporting Portal and 1930 helpline: Complaint trend data, 2023–2025. Government of India. <https://cybercrime.gov.in>
- Internet and Mobile Association of India (IAMAI) & Kantar. (2024). Internet in India Report 2024. IAMAI. <https://www.iamai.in>
- Internet Watch Foundation. (2023). Annual report 2023: Online CSAM and NCII trends. IWF. <https://www.iwf.org.uk>
- Joseph, J., Varghese, A., V R, V., Dhandapani, M., Mohan, D., Sharma, S., & Grover, S. (2021). Prevalence of internet addiction among college students in the Indian setting: A systematic review and meta-analysis. *General Psychiatry*, 34, e100496.
- Kantar / DataReportal. (2024). Digital 2024: India. DataReportal. <https://datareportal.com/reports/digital-2024-india>
- Kircaburun, K., Alhabash, S., Tosuntaş, Ş. B., & Griffiths, M. D. (2020). Uses and gratifications of problematic social media use among university students: A simultaneous examination of the Big Five of personality traits, social media platforms, and social media use motives. *International Journal of Mental Health and Addiction*, 18(3), 525–547.
- Kuss, D. J., & Griffiths, M. D. (2017). Social networking sites and addiction: Ten lessons learned. *International Journal of Environmental Research and Public Health*, 14(3), 311.
- National Crime Records Bureau (NCRB). (2022). Crime in India 2022, Statistics Volume I. Ministry of Home Affairs, Government of India. <https://ncrb.gov.in>
- Pi-Labs Research. (2024). Deepfake fraud in India: 2024 industry analysis report. Pi-Labs.
- Przybylski, A. K., Murayama, K., DeHaan, C. R., & Gladwell, V. (2013). Motivational, emotional, and behavioral correlates of fear of missing out. *Computers in Human Behavior*, 29(4), 1841–1848.
- Ramesh Masthi, N. R., Pruthvi, S., & Phaneendra, M. S. (2018). A comparative study on social media usage and health status among students studying in pre-university colleges of urban Bengaluru. *Indian Journal of Community Medicine*, 43(3), 180–184.
- Resemble AI. (2025). The state of deepfake fraud: Quarterly incident report, Q3 2025. Resemble AI.
- Researchers, Cureus. (2025). Prevalence of social media addiction and its determinants among college students in Chengalpattu district, Tamil Nadu. *Cureus*, 17(5).
- Researchers, PMC. (2024). Silent screams: A narrative review of cyberbullying among Indian adolescents. PMC.
- United Nations Children's Fund (UNICEF). (2019). UNICEF poll: More than a third of young people in 30 countries report being a victim of online bullying. UNICEF. <https://www.unicef.org>
- United Nations Children's Fund (UNICEF). (2024). The changing childhood project: A global survey of what it means to grow up in the 21st century. UNICEF Office of Innovation. <https://www.unicef.org>



World Health Organization (WHO) Regional Office for Europe. (2024). Teens, screens and mental health [Press release]. WHO/Europe. <https://www.who.int/europe>