Jus Corpus Law Journal
Open Access Law Journal – Copyright © 2026 – ISSN 2582-7820
Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

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

From Screen to Safeguards: Statutory Solutions for Involuntary and Unauthenticated Child Exposure

Khizrah Aziz[a] Sonu Kumar[b] Shashwat Dubey[c]

[a]Amity Law School, Amity University, Noida, India [b]Amity Law School, Amity University, Noida, India
[c]Amity Law School, Amity University, Noida, India

Received 08 October 2026; *Accepted* 09 November 2026; *Published* 13 November 2026

The unsupervised and unmoderated use of phones by children in India and across the world has become one of the most pressing child-protection concerns of this decade. This paper examines the problem of children being involuntarily and curiously exposed to sexually explicit, violent or age-inappropriate content through algorithmic pop-ups, autoplay features and inadequately filtered platforms. It situates the problem within the constitutional and statutory framework of the Protection of Children from Sexual Offences Act, 2012 the Information Technology Act, 2000; in addition to the Intermediary Guidelines Rules, 2021 the Juvenile Justice (Care and Protection of Children) Act, 2015; and the Digital Personal Data Protection Act, 2023. The paper also compares and evaluates responses in Australia, the United States, the European Union, the United Kingdom, China, South Korea and France and ends by proposing a legal model centred on a statutorily mandated verifiable parental-consent lock at the device and platform level, stronger intermediary due-diligence obligations and compulsory digital-literacy education as the most workable solution for India while acknowledging the enforcement difficulties faced by comparable jurisdictions.

Keywords: *child online safety, algorithmic due diligence, intermediary safe harbour, age verification, parental consent.*

INTRODUCTION

The mobile phone, a device primarily used by adults, is now the first and most constant companion of the Indian child. Toddlers who barely speak are given smartphones to calm them; school children receive phones for 'classes' that quietly evolve into gateways to social media, video sites and occasionally sexual content. What began as a tool of convenience for parents has evolved, in a decade, into what researchers term universal child exposure. I believe the law has not kept pace with technology, and the lack of an enforceable way to block access for minors, rather than a lack of a legal wish to protect children, is the primary legal gap that needs to be addressed. The right of a child to be protected from material is not simply a policy preference but a constitutional entitlement derived from Article 21 of the Constitution of India (the right to life and personal liberty, which includes a dignified childhood), Article 39(e) and (f)[1] and India's commitments under the United Nations Convention on the Rights of the Child 1989, of which India is a signatory.[2] This paper begins with the premise that unregulated mobile access for children's in effect a violation of child rights caused by a regulatory gap. The paper examines the existing framework in other countries and proposes a new law.

STATEMENT OF THE PROBLEMS

Early, ubiquitous and unsupervised exposure: Research studies conducted by pediatric associations, public health bodies and child-rights think tanks across India have identified a rising trend of free and unsupervised access to digital handheld devices by children at the most formative stage of cognitive and physiological development. Initially used as an accessory to indulge and pacify the child, the smartphone has become omnipresent in the child's everyday life. Starting with parents using the smartphone to keep the child quiet and occupied, the device was soon introduced into the child's learning curriculum as a result of the pandemic.

[1] Constitution of India 1950, art 21
[2] United Nations Convention on the Rights of the Child 1990

Once given free access to a non-native operating system and without parental locks and restrictions, the child's browsing activity and exposure become divorced from parental control. The child's path of least resistance is dictated by an algorithm that makes recommendations based on the watch time, engagement and retention metrics captured by the recommendation engine. The underlying business model of these third-party recommendation engines is designed to capture attention and maximise screen time by encouraging binge-watching and reducing the friction of switching content. As a result, millions of children are exposed to an unreviewed, unfettered and unsupervised digital ecosystem where the ability to discover and consume potentially harmful content is not restricted by parental controls or supervision.

POP-UPS AND AUTOPLAY: INVOLUNTARY EXPOSURE

An underlying fallacy in the current discourse on child safety and exposure is that the child is only exposed to undesirable content when they seek it out. A significant portion of child exposure is involuntary and is driven by the predatory advertising practices deployed by recommendation engines. Pop-up advertisements, autoplay banners and context-aware recommendation engines are designed to capture the child's attention by interrupting their current activity on the smartphone. This practice is prevalent across video-watching apps, browsers and games.

Irrespective of the innocuousness of the current activity, recommendation engines deploy targeted advertisements using context-based targeting, behavioural tracking, and intrusive pop-ups to interrupt the child. A young child who is innocently watching an online tutorial or nursery rhymes has no capacity to distinguish an innocuous advertisement from a predatory one that promotes graphic and explicit content. The ability to distinguish voluntary and involuntary exposure is critical in establishing the legal culpability of a child in accessing undesirable content. A child who is unable to distinguish between voluntary and involuntary exposure to undesirable content is not legally competent to give informed consent to the exposure. The child is legally incapable of providing informed consent to undesirable exposure, which significantly impacts the legal liability of the recommendation engines. By creating interfaces and mechanisms that expose children to involuntary exposure, the recommendation engines abdicate their responsibility as neutral intermediaries and become directly liable for the exposure.

PHYSICAL HEALTH AND TRAUMA

Unsupervised and prolonged exposure to digital handheld devices has caused physiological damage to multiple children, exposing them to long-term health complications. Healthcare professionals in medical colleges and government-run tertiary care hospitals have reported an upsurge in health issues affecting children:

Smartphone Vision Syndrome and Neurological Damage: Doctors in Jaipur have reported an increase in eye-related problems affecting children, which is primarily caused by viewing content on phones for 3–6 hours every day. Hospitals in Hyderabad have treated children exhibiting signs of Smartphone Vision Syndrome, which manifests in asthenopia (eye strain), photopsia (flashes of light), keratopathy (eye dryness), and temporary monocular and binocular blindness after exposure to blue light in dark rooms.[3]

Developmental Disorder and Arrested Expression: Doctors at Kurnool Government General Hospital have observed a peculiar connection between prolonged exposure to smartphones and developmental disorders. Affected children exhibit delayed speech, difficulty in social interaction, poor motor skills, and auditory processing disorders.[4]

Lithium-Ion Battery Explosion and Physical Trauma: Children who play mobile games and watch videos while charging their phones are at risk of sustaining serious physical trauma. Hospital emergency wards have witnessed an uptick in admissions of children with severe facial disfigurement, blast injuries, and eye injuries caused by the spontaneous combustion of lithium-ion batteries.

Neuro-Somatic Disorder and Physiological Dependence: Continued exposure to recommendation engines takes a toll on the neuro-somatic structure of an adolescent and causes physiological dependence on the reward loop of the algorithms. Case studies on smartphone addiction in Indian adolescents have shown that depriving a smartphone-

[3] 'Vision Impairments In Children On Rise From Cellphone Addiction, Says New Study By Jaipur Hospital' *ETV Bharat* (09 December 2025) <https://www.etvbharat.com/en/bharat/jaipur-hospital-report-says-mobile-phone-addiction-is-increasingly-becoming-a-serious-among-children-enn25120902781> accessed 06 October 2026

[4] 'Mobile Addiction Fuels Health Issues Among Children' *Deccan Chronicle* (15 July 2025) <https://www.deccanchronicle.com/southern-states/andhra-pradesh/mobile-addiction-fuels-health-issues-among-children-1891715> accessed 06 October 2026

dependent child of the device results in insomnia, hand-wringing, body tension, and physical aggression towards parents.

PSYCHOLOGICAL DAMAGE, LETHAL BEHAVIOUR AND DOMESTIC TRAGEDY

The exposure of children to unreviewed and unsupervised digital content damages their psychological well-being, causes undesirable behavioural shifts, and exposes them to lethal behaviour:

Predatory Challenges and Self-harm: A significant number of children across India have been exposed to predatory challenges and undesirable content online. The infamous Blue Whale Challenge resulted in the death of several children who engaged with the online interactive task. In Mumbai, 14-year-old Manpreet Sahani jumped to his death from a high-rise building in July 2017 after playing the Blue Whale game with his friends. In West Bengal, 14-year-old Aindril Pal was found dead at his home in August 2017 after engaging with the interactive challenge.

Lethal Domestic Dispute: Smartphone exposure can cause undesirable behavioural changes and turn an ordinary domestic dispute into a lethal one. In Bengaluru, a domestic dispute between parents of a 14-year-old student named Tejas turned fatal in November 2024.[5]

Hardware Loan and Psychological Breakdown: In cases where the child is unable to settle instalment payments on a smartphone, the resulting domestic dispute can have catastrophic consequences. In Khavdya Dongar, Chhatrapati Sambhajinagar, 18-year-old Kunal Chandwade climbed on a cliff in August 2026 after parents and siblings got into an altercation over pending payments on an iPhone. Following a three-hour-long police and family intervention, Kunal lost his footing and fell off the cliff. Parents and his elder sister also lost their lives after trying to pull Kunal back.[6]

[5] V Narayan, 'Mumbai boy 1st Indian victim of 'Blue Whale' dare? Cops probe' *The Times of India* (20 September 2017) <https://timesofindia.indiatimes.com/city/mumbai/boys-suicide-turns-focus-on-the-blue-whale/articleshow/59853004.cms> accessed 206October 2026

[6] Mohammed Akhef, 'Family discord, not iPhone demand, behind Khavdya Dongar tragedy that led to three deaths: Police' *The Times of India* (23 August 2026) <https://timesofindia.indiatimes.com/city/aurangabad/family-discord-not-iphone-demand-behind-khavdya-dongar-tragedy-that-led-to-three-deaths-police/articleshow/133443953.cms> accessed 06 October 2026

The research and clinical data on early, unmoderated smartphone exposure make it clear that this issue is an intergenerational child welfare and public health crisis, not a family affair. Though Articles 19 and 21 afford protection of access to information, privacy, and personal autonomy, children cannot be said to have legal capacity to give informed consent or refuse algorithmically driven predation any more than they can opt out of puberty. Therefore, the State has a responsibility under the doctrine of parens patriae to act as a guardian for minor children and take whatever measures are necessary to protect them from predatory and coercive technology.

INDIAN LEGAL FRAMEWORK: APPLICABILITY, STATUTORY DEFICIENCIES, AND THE PAPER'S DISTINCT DEPARTURE

While the Indian statutory framework has some scattered protections across constitutional, criminal, intermediate, and privacy domains, its approach to child safety is a fragmented, reactive one. This paper does not look to reinvent these foundational doctrines; it uses their constitutional and statutory anchors but departs decisively from their operational limitations. The analysis below establishes how each current statute applies, where it fundamentally breaks down in the mobile-first child-browsing context, and how this paper's proposed framework bridges that divide.

Constitutional Mandate (Articles 21, 15(3), 39, and 19): Under Article 21, the Supreme Court has gradually interpreted personal liberty to include the right to a healthy, dignified childhood. Articles 15(3), 39(e), and 39(f) impose an affirmative duty on the State to shield children from moral abandonment and exploitation.[7] Crucially, Article 19(2) allows 'reasonable restrictions' on free speech in the interests of decency and morality, providing the legal foothold to regulate adult content. Traditional jurisprudence treats speech restrictions as content-level bans or post-publication censorship. The state's role is not considered different from the right of an adult to access speech; the difference between the right of an adult to access speech and the duty to protect minors from receiving age-inappropriate speech is not recognised.

[7] Constitution of India 1950, arts 15(3), 39(e)–(f)

The proposal does not advocate a wholesale censorship of adult content, but argues that age-verification, Article 19(2) as a manner-of-access restriction, not a content restriction, is entirely valid.

Criminal and Harm Frameworks (POCSO Act, 2012 & JJ Act, 2015): Sections 13-15 of the POCSO Act criminalise Child Sexual Abuse Material (CSAM), storage, and transmission;[8] Sections 19 and 21 mandate reporting of abuse; Section 23 guarantees strict victim anonymity. In parallel, Section 2(14) of the Juvenile Justice Act, 2015 classifies exposed or vulnerable minors as children in need of care and protection, not delinquents.[9] POCSO and the JJ Act are strictly post-facto, penal frameworks. They apply only when a sexual crime or exposure has materialised; they provide no technical mechanism to prevent a minor from casually encountering adult pornography or non-CSAM explicit pop-ups on a shared mobile phone.

The proposal transforms the protective welfare mandate of POCSO and the JJ Act from post-facto punishment into an ex-ante technological shield. Rather than punish parties after a child suffers psychological or moral harm, the paper engineers a digital barrier directly on the handheld device to ensure exposure cannot happen silently in the first place.

Cyber Governance and Intermediary Immunity (IT Act, 2000 & IT Rules, 2021): Sections 67, 67A, and 67B of the IT Act penalise the transmission of obscene, sexually explicit, and child-abusive electronic records.[10] Section 79 provides intermediaries with conditional 'safe-harbour' immunity,[11] while Rule 3 and Rule 4(4) of the IT Rules, 2021 mandate automated filtering tools for CSAM and prompt takedowns. The entire regime is predicated on reactive notice-and-takedown. Platforms evade liability for serving unsolicited explicit pop-ups or algorithmic recommendations by claiming intermediary immunity until a formal grievance is lodged. Rule 4(4) allows almost all proactive monitoring of mainstream pornography and graphic adult ads to auto-play to unidentified child users.

The proposed model re-interprets Section 79 compliance by conditioning safe-harbour status on algorithmic and session-level due diligence. Intermediaries lose immunity if they deliver

[8] Protection of Children from Sexual Offences Act 2012, ss 13–15
[9] Juvenile Justice (Care and Protection of Children) Act 2015, s 2(14)
[10] Information Technology Act 2000, ss 67, 67A and 67B
[11] *Ibid* s 79

explicit pop-ups, autoplay feeds, or unsolicited adult advertisements to an unauthenticated session or a profile running under a child lock.

Personal Data and Consent Framework (DPDP Act, 2023): Section 9 of the DPDP Act, 2023 prohibits behavioural tracking, targeted advertising, and data processing detrimental to minors, mandating verifiable parental consent prior to processing a child's personal data. This is the most acute statutory loophole in Indian law today. Section 9 applies solely upon data fiduciaries processing personal data. If an unauthenticated child picks up a parent's phone, opens a mobile browser without signing in, and streams open-access adult video or triggers programmatic pop-ups, Section 9 remains legally silent since no personal profile or account is being formally registered.

This proposal exploits the rule-making powers under Section 40 of the DPDP Act and Section 87 of the IT Act to turn data-processing consent into a device and session-level content gate, ensuring protection attaches to the physical viewing session, closing the fatal gap left by unauthenticated browsing.

COMPARATIVE STUDY OF GLOBAL LEGAL FRAMEWORKS

The global discourse on safeguarding minors online has produced divergent regulatory models, ranging from hard platform-level prohibitions to supply-chain device mandates. An evaluation of the statutory mechanisms across these jurisdictions reveals the friction between state intervention, parental autonomy, and informational privacy. Drawing inspiration from these successful legislative models of other nations provides a crucial precedent, highlighting the imperative for India to integrate similar robust, comprehensive frameworks tailored to its own socio- legal context in order to effectively safeguard minors within the digital sphere.

France –

Device-Level Parental Control by Default: France enacted Law No. 2022-300 of 2 March 2022 (Loi visant à renforcer le contrôle parental sur les moyens d'accès à internet), which amended the Code des postes et des communications électroniques (CPCE) by inserting some articles. Rather than burdening end-users or downstream online platforms with the compliance obligation, the statute intervenes upstream at the point of manufacture and distribution: All internet-capable terminal devices (smartphones, tablets, personal

computers) sold in France must feature an accessible, comprehensible parental control mechanism integrated directly into the operating system. Hardware manufacturers and OS vendors must prompt the user to activate this feature during the first configuration/first boot, free of charge.

The personal data of minors generated or collected through the activation of this mechanism cannot be used for commercial profiling, behavioural marketing, or direct advertising, a guarantee that persists even after the child reaches adulthood. Empowered market surveillance bodies can levy administrative fines, restrict non-compliant devices, or issue compulsory product recalls.[12]

Australia –

- Hard Minimum-Age Prohibition Under the Online Safety Amendment (Social Media Minimum Age) Act 2024 (amending the Online Safety Act 2021), Australia's chosen regulatory approach is that of a strict exclusion.
- Mandates that providers of age-restricted social media platforms must take 'reasonable steps' to prevent Australian children under sixteen years of age from holding accounts, carrying civil penalties of up to 30,000 penalty units.
- Unlike consent-based regimes, the Australian model creates a blanket age floor without any parental exception.
- Platforms are strictly prohibited from using age- assurance data for any secondary purpose and must destroy identity verification records once age determination is complete.[13]

European Union –

Data Protection and Algorithmic Design: The European framework regulates minors' digital exposure through two principal instruments:

- Establishes a default digital age of consent of 16 years for Information Society Services (ISS) offered directly to a child. For minors below this threshold (which individual

[12] Loi n° 2022-300 du 2 mars 2022 visant à renforcer le contrôle parental sur les moyens d'accès à internet (France)
[13] Online Safety Amendment (Social Media Minimum Age) Act 2024 (Australia)

Member States may lower to no less than 13), processing is lawful only with verifiable authorisation from the holder of parental responsibility.

- Imposes specific platform-safety duties, including a statutory prohibition against serving targeted advertising based on profiling when the platform is reasonably certain that the recipient is a minor.

United Kingdom –

Platform Duty of Care: The Online Safety Act 2023 establishes statutory duties of care overseen by Ofcom. It requires regulated user-to-user services to conduct children's risk assessments and deploy proportionate systems, specifically including highly effective age verification or age estimation, to prevent children of any age from encountering 'primary priority content' (such as CSAM, suicide, self-harm, and eating disorder encouragement).[14]

China –

- Centralised, Device-Integrated 'Minor Mode': The Cyberspace Administration of China (CAC) issued administrative provisions mandating a unified, three-sided 'Minor Mode' involving hardware terminal vendors, operating system developers, and application publishers.
- Imposes age-bracketed screen limits (e.g., 40 minutes for under-8s, up to 2 hours for 16-17-year-olds) and an automated system shutdown between 10:00 PM and 6:00 AM.
- Operates via centralised real-name registration tied directly to state citizen identification records, establishing a rigid control apparatus.[15]

South Korea –

From State Curfews to Parental Agency: South Korea's regulatory evolution offers a cautionary tale of legislative overreach:

- Banned minors under sixteen from playing online games between midnight and 6:00 AM. In December 2021, the National Assembly repealed this provision after empirical

[14] Online Safety Act 2023 (UK), s 137, sch 13
[15] *Regulations on the Protection of Minors Online 2024* (Cyberspace Administration of China 2024)

evidence showed minimal improvements in youth sleep patterns and widespread circumvention.

- Replaced the state-imposed curfew with a selective mechanism, obliging gaming companies to restrict access hours only upon the affirmative request of a parent or guardian, thereby returning primacy to the family unit.[16]

THE INDIAN REGULATORY LACUNA AND DOCTRINAL GAPS

India's domestic regime provides robust post-facto penal remedies but lacks an ex-ante content-access gating architecture: The primary statutory gap exists within Section 9 of the DPDP Act, 2023. While Section 9(1) commands that a Data Fiduciary obtain verifiable parental consent before processing a child's data, and Section 9(2)-(3) prohibit behavioural tracking and targeted advertising, its protective perimeter is legally confined to data processing. If a minor accesses an open video platform, unauthenticated websites, or receives algorithmically driven pop-ups without creating an account or submitting identifying credentials, Section 9 remains legally disengaged. Downstream intermediaries retain Section 79 safe-harbour immunity as long as they reactively take down notified content, leaving children vulnerable to the exact involuntary pop-up exposure.

PROPOSED SOLUTION: THE ENHANCED MULTI-LAYERED CHILD PROTECTION FRAMEWORK

To comprehensively address the child online safety problem without waiting for primary legislative overhaul, this model operates entirely via delegated rule-making powers under Section 40 of the Digital Personal Data Protection (DPDP) Act, 2023 and Section 87 of the Information Technology (IT) Act, 2000. It fills the gap between hardware controls, account-level authentication, and platform accountability across seven integrated layers.[17]

Layer 1: Mandatory Guardian Identity Verification (Sovereign e-KYC Gating): A rule notified under the DPDP Act Section 40 and the IT Act Section 87 mandates that any device, operating system, or digital platform accessible in India must require proof of majority (adult status) via verified government identity credentials before unrestricted or adult content tiers

[16] Youth Protection Act 1997 (South Korea), article 26; Game Industry Promotion Act 2006(South Korea), art 12(3)
[17] Digital Personal Data Protection Act 2023, s 9(1)–(3)

can be unlocked. Authentication relies on decentralised, sovereign identity systems (such as DigiLocker-based verification or official e-KYC protocols). This verification uses zero-knowledge cryptographic proofs (ZKPs). The platform receives an authenticated cryptographic confirmation that the supervising user is a verified adult, while neither the platform nor the state logs the individual's browsing telemetry or retains raw identity documents.

Layer 2: Dynamic Per-Session OTP Authorisation for Child Access: To resolve the widespread practical scenario where children access the internet using pre-logged-in adult accounts or shared family devices, the framework mandates dynamic One-Time Password (OTP) authorisation. Every time a secondary user or child launches a browser session, opens an unauthenticated content stream, or switches user profiles on a parent's device, an automated OTP is dispatched to the guardian's verified mobile number or email. Access to unrestricted web viewing remains locked until this OTP is affirmatively entered. This eliminates bypasses via incognito tabs, cookie clearing, or background browser sessions, ensuring that adult oversight is active for every distinct browsing session.

Layer 3: Statutory Parental-Verification Lock (Default-on Child Mode): Operating systems (Android, iOS, Windows, macOS) and browser engines must implement a default-on, tamper-resistant 'Child Mode' for all unauthenticated or newly configured environments. This converts the DPDP Act's Section 9 requirement, which currently applies only when personal data is processed, into an enforceable, ex-ante content-access gate. Open-web content and video feeds are restricted by default, preventing unauthenticated minors from encountering mature content even if no user account or tracking profile exists.

Layer 4: Mandatory Device-Level Age Gating at Point of Sale (POS): Following the upstream regulatory model established in France (Law No. 2022-300), the Bureau of Indian Standards (BIS) and the Ministry of Electronics and Information Technology (MeitY) issue standards requiring all connected terminal hardware sold in India to ship with activated, certified parental-control modules. Retailers, original equipment manufacturers (OEMs), and importers are legally prohibited from disabling these protections before retail distribution.

This shifts compliance onto commercial entities rather than policing individual domestic households.[18]

Layer 5: Enhanced Intermediary Algorithmic Due Diligence: Rule 4(4) of the IT Rules, 2021 is amended to require proactive algorithmic filtering of Child Sexual Abuse Material (CSAM) from recommendation feeds, autoplay suggestions, and programmatic pop-up advertisements. Platforms serving unsolicited explicit advertising, adult recommendations, or intrusive pop-ups to 'Child Mode' accounts or sessions shall automatically forfeit safe harbours under Section 79 of the IT Act, becoming civilly and criminally liable for algorithmic negligence.

Layer 6: Compulsory Digital Literacy and Education Resilience: The Right of Children to Free and Compulsory Education (RTE) Act, 2009's statutory curriculum guidelines for central and state education boards are amended to explicitly require media literacy, digital resilience, and online safety education appropriate to children's age and cognitive maturity. If algorithmic protections fail, children can recognise dark patterns, stop, exit, and report harmful content to parents or trusted adults without fear or stigma.

Layer 7: Institutional Oversight and Expedited Grievance Resolution: NCPCR and DPBI are designated as joint supervisory agencies responsible for monitoring the implementation of the Ordinance. A fast-track mechanism (modelled on the IT Rules, 2021's CSAM takedown provisions) will investigate parental complaints about circumvention, non-compliant OEM configurations, or unauthorised pop-up deliveries. Violative platforms will face steep fines and enforcement action.

CONCLUSION

India's digital revolution has impacted childhood in ways that its laws have failed to grapple with. While it promised to be an enabler in the discreet domain of parenting and online schooling, it has allowed recommendation algorithms to replace parental guidance. The discussion in this paper demonstrates that the problem is not that our Constitution's

[18] 'About NCPCR' (*National Commission for Protection of Child Rights*) <http://www.ncpcr.gov.in/public/about-ncpcr> accessed 06 October 2026; Adv Prashant Mali, 'Data Protection Board of India: Powers, Procedures & Adjudication' (*DPDPA*, 01 February 2026) <https://www.dpdpa.com/blogs/data_protection_board_india_dpbi_powers_procedures.html> accessed 06 October 2026

fundamental rights framework fails to account for children. It is that our statutes deal only with ex-post governance.

Statutes such as the POCSO Act 2012 and the Juvenile Justice Act 2015 provide for relief only in the wake of an offence or trauma. Section 79 of the Information Technology Act, 2000 offers a passive notice and takedown remedy, letting explicit content autoplay into children's screens without any ex-ante obligation on the part of the intermediaries. Even Section 9 of the new DPDP Act, 2023, which seeks to govern children's data privacy, contains no provision for the ordinary scenario in which an unauthenticated child browses through a family phone accessing open web content.

The lessons from other jurisdictions demonstrate that neither outright prohibitions on platforms nor reactive punitive measures suffice to keep children safe online. Rather, France's model of making parental locks a part of the operating system at the level of manufacture offers a useful benchmark.

The multi-tiered model suggested by this paper, which utilises the policy levers available to India through the IT Act and DPDP Act, fits within the framework of our own Constitution's obligation of parens patriae. By relying on delegated legislation, India can move beyond mere ex-post governance and create ex-ante shields for children. A combination of mandating default child-friendly modes of sale at the point of purchase, deploying Zero Knowledge proofs through DigiLocker for age of majority verification, requiring authorisations for shared-device usage and removing safe harbour immunity for platforms that continue to promote inappropriate content for children can be supplemented through a digital literacy curriculum and joint oversight by the NCPCR and the DPBI. This would move India towards the prevention paradigm in children's data protection without undermining the right to privacy or freedom of speech and expression. Putting children first in our digital revolution need not entail censorship or surveillance. It merely requires that our laws recognise their right to a dignified upbringing in the online sphere too.