

BLOGS PUBLICATION

**THEME: PROTECTION, PARTICIPATION AND PRIVACY OF
CHILDREN IN THE DIGITAL AGE**



CENTRE FOR CHILD RIGHTS

at

MAHARASHTRA NATIONAL LAW UNIVERSITY, NAGPUR

INDEX

BUILT TO ADDICT: PLATFORM DESIGN AND INDIA'S LIABILITY GAP <i>by Krishna Tiya Sahay</i>	3
THE FACE SCAN TRAP: HOW ROBLOX AND DISCORD ARE SURVEILLING INDIAN CHILDREN AND WHY INDIA'S LAW ALLOWS THEM <i>by Shambhavi Negi and Niharika Uniyal</i>	10
COGNITIVE AUTONOMY AND CHILD PROTECTION: BRIDGING THE REGULATORY GAP IN NEUROTECHNOLOGY GOVERNANCE <i>by Khushi Jain and Priyanshi Agarwal</i>	18
LOCKED OUT OF MEMORY: THE LEGAL VACUUM IN CHILDREN'S RIGHTS TO THEIR PARENTS' DIGITAL LEGACY IN INDIA <i>by Adarsh Parashar</i>	28
THE BIOLOGY OF BETRAYAL: PLATFORM LIABILITY AND THE CIVIL RIGHTS OF THE DIGITAL GENERATION <i>by Rishabh G. Pandey</i>	35
THE PUPPET STRINGS OF PIXELS: ARCHITECTING INFANCY IN THE AGE OF ALGORITHMS <i>by Amitava Das</i>	38
FROM PROBABLE CAUSE TO PREDICTIVE GUILT: ASSESSING THE EROSION OF THE PRESUMPTION OF INNOCENCE IN THE ERA OF ALGORITHMIC POLICING <i>by Sagnik Halder</i>	43
TOO YOUNG TO CONSENT, OLD ENOUGH TO BE EXPLOITED: INDIA'S DIGITAL AGE PARADOX <i>by Krati Raghav</i>	48
SORRY YOU'RE 17: IS INDIA'S VERIFIABLE PARENTAL MANDATE A VIOLATION OF CONSTITUTIONAL PRIVACY?" <i>by Muskan Gupta</i>	56
WHO GUARDS THE GUARDIANS? PLATFORM LIABILITY FOR HARMFUL CONTENT AFFECTING CHILDREN IN THE DIGITAL AGE <i>by Ashish Godsara Singh</i>	66

BUILT TO ADDICT: PLATFORM DESIGN AND INDIA'S LIABILITY GAP

Authored by: Krisha Tiya Sahay¹

On 25th March 2026, a Los Angeles jury delivered one of the landmark verdicts in the realm of social media liability litigation. In *K.G.M v. Meta et al.* the LA County Court held Google and Meta liable for engineering addiction into their platforms and awarded damages of \$6 million.² The plaintiff, was able to prove that she had developed severe anxiety, depression and body image issues as a result of her interaction with YouTube and Instagram since before she was 10. The jurors determined that the platforms “acted with malice, oppression, or fraud”³ and held them liable not for the content, but for built-in design features such as infinite scroll, autoplay and algorithmic recommendations which were meant to maximise engagement by weaponizing children’s developing psychology.

This judgement raises an uncomfortable yet pertinent question for jurisdictions beyond California. Had Kaley been an Indian child, exposed to the same architecture and scrolling the same feeds, what recourse would she have had? In recent years, India has enacted a number of digital laws such as the DPDP Act, 2023 and the complementary DPDP Rules, 2025 along with the IT Amendment Rules, 2026. Yet, as this blog argues, these laws face a common structural limitation as they the data and not the design, which has equally damaging consequences.

India’s regulatory framework partially addresses data-driven algorithmic harm but is silent on the broader platform architecture which fosters addictive tendencies among children. Features such as infinite scroll, autoplay and variable reward mechanism cause harm independent of any data processing, leaving a critical design liability gap that India's legal framework has yet to address. This blog argues that India must develop a design liability standard that holds platforms accountable not just for what data they collect, but for how they engineer the products that children use.

¹ 3rd Year Student at Rajiv Gandhi National University, Patiala, <https://www.linkedin.com/in/krisha-sahay-9515a4383>.

² Carolina Rossini, ‘Design on Trial: Jury Delivers Verdict Against Meta, YouTube’ *The Fashion Law* (Massachusetts, 25 March 2026) <<https://www.thefashionlaw.com/design-on-trial-the-lawsuit-that-could-rewrite-big-tech-liability/>> accessed 13 April 2026

³ K Hays, N Saad and R Morris, ‘Campaigners welcome Meta and YouTube's defeat in landmark social media addiction trial’ (Los Angeles, 27 March 2026) <<https://www.bbc.com/news/articles/c747x7gz249o>> accessed 13 April 2026

The Architecture of Harm

Platforms such as YouTube and Instagram do not cause harm by a singular feature in isolation, rather they deploy what is referred to as an “informational architecture”.⁴ This is an integrated system of the platform architecture which is designed to maximise engagement and operates through three layers. The foremost layer comprises algorithmic recommendations. We live in an era of “surveillance capitalism” where intermediaries collect vast amounts of data from individuals to exploit their biases and provide personalised content in order to boost engagement.⁵ What makes this particularly underhanded is the fact that intermediaries consistently prohibit harmful content in their terms of service while simultaneously amplifying them through these algorithms.⁶ This layer is heavily data-dependent as it requires information about individuals to function effectively, leading to legislation on this front. Although as this blog argues, the regulation only partly addresses this problem.

The second layer consists of what is referred to as “doom scroll”. This phenomenon of doom scrolling is enabled by two features: infinite scroll and autoplay. Platforms such as Instagram and YouTube have a dedicated section for short form videos with no natural stopping point. The autoplay feature on YouTube has an analogous effect. These features create a situation in which an individual does not consciously choose to continue but rather the platform makes this choice for them.

Lastly, these platforms employ variable rewards mechanism which is an important tool in psychology and is employed by intermediaries to create dopamine loops.⁷ This works on a slot-machine like principle where the next piece of content remains unpredictable, creating a situation where individuals keep checking their apps compulsively, wondering if the next scroll will contain an exciting piece of content.

That these features cause psychological harm to children is not a matter of speculation but a documented fact. Internal research conducted by Meta itself, later leaked in the form of

⁴ K.G.M. v. Meta et al

⁵ Michal Lavi, ‘Targeting Children: Liability for Algorithmic Recommendations’ (2024) 73(5) AULR <https://aulareview.org/wp-content/uploads/2024/09/Lavi.to_Printer.pdf> accessed 13 April 2026

⁶ Amy B Cyphert and Jena T. Martin, “‘A Change is Gonna Come:’ Developing a Liability Framework for Social Media Algorithmic Amplification’ (2022) 13(1) UC Irvine Law Review <<https://escholarship.org/uc/item/7008z2jg>> accessed 13 April 2026

⁷ Liza Samaha, ‘The Dopamine Effect: How Social Media Shapes Our Emotions and Behaviors’ (Strasbourg, 17 January 2025) <<https://cyberjustice.blog/2025/01/17/the-dopamine-effect-how-social-media-shapes-our-emotions-and-behaviors/>> accessed 13 April 2026

“Facebook Papers”⁸ revealed that the platform severely impacted the mental health of children, by worsening their body image and increasing anxiety and depression. Meta chose not to act on these findings.

Children are particularly susceptible to being exploited by this architecture as their prefrontal cortex, governing impulse control and long-term decision making, is not fully developed.⁹ The harms that result are not abstract. They manifest as depression, anxiety, disordered eating, and in the most severe cases, self-harm and suicidal ideation. This susceptibility creates a “special context of vulnerability”¹⁰ wherein the law may impose a duty of care even when the targeted content is not unlawful in itself.

A Framework Half-Built

India’s response to these digital harms has not been one of legislative inaction. Over the past few years, the nation has made genuine efforts to protect children from the risks they face by virtue of their special vulnerability. The most direct legislative engagement with the algorithmic layer of harm described above comes in the form of the DPDP Act, 2023 and the accompanying rules.

Section 9(3) of the Act imposes what is described as a triple lock exclusively on children’s data, prohibiting behavioural tracking, monitoring and targeted advertisement directed at children even when parental consent has been provided.¹¹ This provision attacks the core of algorithmic recommendation for children by prohibiting collection of their data which is essential to profiling, which in turn contributes to addictive tendencies. In addition, Rule 13 of the DPDP Rules, 2025 mandates that intermediaries designated as Significant Data Fiduciaries carry out annual algorithmic due diligence to ensure that personal data is not being weaponised to the detriment of the users;¹² this is an imperative step for vulnerable populations such as children. These provisions attempt to engage with algorithmic harm to children, yet as the

⁸ Bill Chappell, ‘The Facebook Papers: What you need to know about the trove of insider documents’ (Washington, 25 October 2021) <<https://www.npr.org/2021/10/25/1049015366/the-facebook-papers-what-you-need-to-know>> accessed 14 April 2026.

⁹ Danah Boyd, *It’s Complicated: The Social Life of Networked Teens* (1st edn, Yale University Press 2014) 183

¹⁰ Lavi (n 4)

¹¹ The Digital Personal Data Protection Act 2023, s 9

¹² The Digital Personal Data Protection Rules 2025, rule 13

following section will demonstrate, this is only a partial response as the protection offered is contingent on the weaponisation of personal data whereas the harm may not always be.

The recent IT Amendment Rules, 2026 address a different dimension of the problem. These rules mandate the labelling of synthetically generated content.¹³ This is specifically important for children who are arguably less equipped to differentiate synthetic media from authentic one and more likely to be influenced by the extreme and disturbing narratives that generally characterise these AI-generated materials. Further, the rules have introduced a stringent 3-hour takedown window for harmful content, and crucially, they place all intermediaries under an explicit obligation to immediately report any offence under the Protection of Children from Sexual Offences Act, 2012 to the appropriate authorities.¹⁴ Yet, these rules are reactive by design; they address harmful content after it reaches the child, but say nothing about the architecture that delivers it.

These provisions collectively represent meaningful legislative progress. Yet they share a structural limitation that no amount of enforcement can resolve, they are instruments designed to regulate data flows, and the harm this blog addresses flows not only from data, but largely from design.

Beyond Data Regulation

The legislative steps discussed above, while necessary, remain inadequate in addressing a significant category of harm to children. The gaps in India's framework operate at two distinct but related levels: first, within the very legislation aiming to address algorithmic harms, and second, in the complete absence of any steps addressing the design features that operate independently of data altogether.

Beginning with the former, Section 9(3) of the DPDP Act prohibits tracking, behavioural monitoring and targeted advertisement for children. In principle, this targets the data-dependent layer of the informational architecture described above. In practice, however, this prohibition rests on undefined terms. Neither "tracking" nor "behavioural monitoring" are defined

¹³ Vijay Pal Dalmia, 'Checklist For Compliance With The Information Technology (Intermediary Guidelines And Digital Media Ethics Code) Amendment Rules, 2026' (New Delhi, 20 February 2026) <<https://www.mondaq.com/india/it-and-internet/1746068/checklist-for-compliance-with-the-information-technology-intermediary-guidelines-and-digital-media-ethics-code-amendment-rules-2026>> accessed 14 April 2026

¹⁴ Ibid

anywhere in the Act or the Rules. Whether recommendation systems that work through collaborative filtering, which operates not by tracking individual children but by identifying patterns across large user populations,¹⁵ qualifies as “tracking” or “behavioural monitoring” is a question that the law leaves entirely ambiguous. A platform deploying collaborative filtering can remain fully DPDP compliant while continuing to exploit children’s vulnerability because the algorithm draws on group behaviour rather than individual profiling.

These are, however, limitations that exist within a framework that at least acknowledges the harms posed by algorithmic recommendations. The deeper problem lies where the law is altogether silent. The second and third layer of the informational architecture cause harm independent of personal data. A child who has never been tracked and profiled is equally vulnerable to these design decisions as any other. The dopamine loop mechanism employed by these intermediaries exploit a universal feature of human psychology, a feature that does not discriminate between profiled and un-profiled users.

This is not a gap that better enforcement of existing laws can close. It is a structural gap premised on the narrative that frames a child’s online safety as a question of merely data governance and entirely neglects product design; and this narrative fails to hold true. As the LA jury recognised in holding Meta and YouTube liable for negligent platform design, the harm to children arises not only from what platforms *know* about them, but from what platforms *build* for them. India's law has a partial answer to the former question and has none to the latter.

Towards a Design Liability Standard

The absence of a design-based liability for social media intermediaries is not an absence of legal basis. The building blocks of such a standard already exist within the Indian negligence framework.

In this regard, the *K.G.M* litigation proves to be insightful. Rather than targeting the harmful content, the plaintiffs deployed a negligence-based product liability theory; this conduct-versus-content distinction made in this case serves as a legal roadmap for jurisdictions grappling with similar questions.¹⁶

¹⁵ “Collaborative Filtering”. Encyclopedia of Database Systems. Springer. 2018.

¹⁶ Carolina Rossini (n 1)

India's negligence framework is well-equipped to travel this road. The essentials of constituting a valid negligence claim include: a duty of care owed by the defendant to the plaintiff, a breach of the duty and damage resulting from this breach.¹⁷ The duty of care owed by the platform to a child is grounded in the principle that a manufacturer owes a duty of care to the ultimate consumer where harm is a reasonably foreseeable consequence of their product.¹⁸ Where internal research, such as the "Facebook Papers" discussed above, has already documented the precise harms that materialise, foreseeability is not merely established, it is conceded by the platform itself.

Platforms may object to this framework on two grounds— firstly, that it may have chilling effects on free speech under Article 19(1)(a) and secondly, that it may infringe on the freedom to trade under Article 19(1)(g). The foremost objection fails on two levels; firstly, companies are not citizens and cannot claim Article 19 rights directly¹⁹ and secondly, foreign corporations such as Meta and Google have no Article 19 claim at all.²⁰ The second objection rooted in Article 19(1)(g) also fails as Article 19(6) expressly permits reasonable restrictions in the interest of the general public, a threshold that regulations protecting children, a constitutionally protected class under Article 15(3), from documented psychological harm would easily satisfy. Additionally, the right to mental health constitutes an essential component of the right to life and dignity under Article 21,²¹ and such guarantees under Article 21 prevail over the ones in Article 19.²² Furthermore, these rights under Article 21 can be claimed against private individuals as well.²³

Section 79 of the IT Act, 2000 presents a further obstacle. Often referred to as the "safe harbour" protection, it exempts intermediaries from liability arising from third party content. An argument can be made that since the harm is ultimately caused by such content, the intermediaries have immunity under this section. However, the *K.G.M* litigation overcame a similar obstacle existing in the US legislation by showing that the platform did not act as mere facilitators but rather an active participant in the construction of the harmful digital

¹⁷ *Poonam Verma v Ashwin Patel & Ors* (1996) SCC 4 332

¹⁸ *Donoghue v Stevenson* [1932] AC 562

¹⁹ *Tata Engineering and Locomotive Co. Ltd v State of Bihar & Ors* AIR 1965 SC 40

²⁰ *X Corp v Union of India* (WP 7405/2025)

²¹ *Sukdeb Saha v State of Andhra Pradesh* 2025 INSC 893

²² *Cure SMA Foundation of India v Union of India & Ors* Writ Petition (Civil) No. 460 of 2025

²³ *Kaushal Kishor v State of Uttar Pradesh & Ors* (2023) 4 SCC 1

environment as it was their product features that ultimately delivered the content to the child.²⁴ A purposive reading of Section 79 will show that the same argument applies to the Indian context as this provision was never meant to immunise a platform's own engineering choices from liability.

Three reforms follow from this analysis. Firstly, the DPDP Act must define "behavioural monitoring" to include collaborative filtering, closing the definitional gap that the platforms will otherwise exploit. Secondly, Section 79 must be amended to expressly exclude platform design decisions from safe harbour protection and lastly, India should establish a dedicated Child Digital Safety Authority with the mandate and technical capacity to evaluate platform design features specifically for psychological harm to children, modelled on the systemic risk assessment framework under the EU's Digital Services Act.

Conclusion

The new digital ecosystem has transformed the environment in which we interact with information online and the way it is delivered to us. Companies increasingly use the informational architecture this blog described to increase their engagement and enhance traffic, and face no consequences for its detrimental effect. These effects are even more severe when the targets are children with poor impulse control and decision-making capabilities. With greater power must come greater responsibility. The legal system needs to acknowledge the extent and, in many cases, the existence of the harm that these design features pose. This blog proposes normative standards for statutory texts along with a negligence-based model to deal with the consequences of the features that are cause long term and life changing issues for the society's most vulnerable.

²⁴ Carolina Rossini (n 1)

THE FACE SCAN TRAP: HOW ROBLOX AND DISCORD ARE SURVEILLING INDIAN CHILDREN AND WHY INDIA'S LAW ALLOWS THEM

Authored by: Shambhavi Negi and Niharika Uniyal²⁵

I. Introduction

Every day, millions of children log into Roblox and Discord without their parents realizing that a simple "age check" means surrendering a child's facial information to a private intelligence company permanently. The promise is safety. The reality is surveillance.

In early December 2025, Roblox began rolling out mandatory facial age estimation for chat access in select regions. By January 7, 2026, the requirement was enforced globally for all users wanting to use Experience chat, Voice chat, or Party chat. Weeks ago, an Indian Parliamentary Committee recommended mandatory KYC and age verification for all social media and gaming platforms²⁶. This is not a distant concern. It is happening now.

Platforms have outsourced this gatekeeping to Persona Identities, Inc., whose software runs 269 distinct checks, screens children against terrorism watchlists and financial intelligence databases and retains biometric data for three years²⁷. This is not a teen safety tool. It is a surveillance pipeline and children are its primary subjects.

This blog argues that biometric age verification violates children's fundamental right to privacy and that India's legal framework remains wholly inadequate to address it. Meaningful reform is urgent.

II. The Rise of Facial Age Verification

The shift toward facial recognition as the default age verification mechanism did not happen by accident. It happened because it is cheap, scalable and critically, because regulators have not prohibited it.

Platforms face mounting legal pressure to verify user ages. Australia's under-16 social media ban, the UK's Online Safety Act and India's DPDPA require platforms to shield children from

²⁵ 3rd Year Students at Symbiosis Law School, Pune, <https://www.linkedin.com/in/niharika-uniyal-00841a378>,

²⁶ Lu-Hai Liang, *India weighs mandatory KYC, age checks for online social platforms*, BIOMETRICUPDATE, (April 13, 2026), [India weighs mandatory KYC, age checks for online social platforms | Biometric Update](#).

²⁷ Pieter Arntz, *Age verification vendor Persona left frontend exposed, researchers say*, MALWAREBYTES (Feb. 20, 2026), [\[updated\] Age verification vendor Persona left frontend exposed, researchers say | Malwarebytes](#).

adult content and prevent easy adult contact.²⁸ The challenge is real. Text-based self-declaration is trivially bypassed and document verification requires human review at enormous scale.

Facial recognition fills this gap operationally. A user holds up their phone, a camera scans their face, an algorithm estimates their age and the system either grants or restricts access in seconds, at near-zero marginal cost. From a product standpoint, it is efficient but from a privacy standpoint, it is catastrophic.

Roblox has fully embraced this model. In early December 2025, it began requiring facial age estimation for chat access in Australia, New Zealand and the Netherlands. By January 7, 2026, the mandate expanded globally. Any user who refuses to complete an age check is placed into a restricted experience with no chat access and severely limited gameplay. All of this is powered by Persona, the same vendor at the center of Discord's privacy firestorm.²

Roblox claims that images and videos used for age estimation are deleted immediately after processing, but as the Discord case demonstrated, vendor assurances are not always what they seem.

The critical problem is that platforms are choosing the most intrusive available method when less invasive alternatives already exist and demonstrably work. On-device age estimation can analyse a face locally without transmitting or retaining any data.²⁹ Discord's own abandoned experiment with Persona proved this point. After intense public backlash in February 2026, Discord ended the Persona partnership entirely and continued operating.³⁰ The platform did not collapse. Children were not left unprotected. The surveillance simply stopped.

III. The Surveillance Pipeline: Privacy Violations

The harm caused by biometric age verification is not speculative. It is documented, specific and ongoing. When a child submits their face to Persona's verification system, they are not simply confirming their age. A Cybernews investigation into Persona's exposed frontend

²⁸ GOV. UK, [Online Safety Act: explainer - GOV.UK](#), (last visited Apr. 14, 2026); Digital Personal Data Protection Act, 2023, § 9; Digital Personal Data Protection Rules, 2025 (notified Nov. 14, 2025), <https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf> ; ESAFETY COMMISSIONER, [Social media age restrictions | eSafety Commissioner](#), (last visited Apr. 14, 2026).

²⁹ Dan Saltman, *Discord Tested Age Verification Vendor Persona: What Users Should Know*, REDACT, (Feb. 16, 2026), [Discord Tested Age Verification Vendor Persona: What Users Should Know](#).

³⁰ TIMES OF INDIA, [Discord faces backlash over new age-verification plan, says controversial UK test with Persona has ended - The Times of India](#) (last visited Apr. 14, 2026).

revealed that the software performs 269 distinct verification checks on a single user.³¹ These checks include screening against terrorism watchlists, politically exposed persons lists and FinCEN financial intelligence databases, systems designed for anti-money laundering and counter-terrorism work, not for determining whether a thirteen-year-old should be allowed to chat in Roblox. Persona tags collected data with intelligence project codenames including "Project SHADOW" and "Project LEGION."³² It retains biometric data, IP addresses, government ID numbers, device fingerprints and a battery of "selfie analytics" including suspicious-entity detection and age inconsistency checks for up to three years.³³

Roblox relies on Persona as the core of its "age checks to chat" system.³⁴ Discord tested Persona simultaneously alongside k-ID, a different vendor with fundamentally different data practices. While k-ID processes facial scans on-device and retains nothing, Persona uses server-side processing and retained data for up to seven days under the Discord experiment's specific terms.³⁵ Users were never told which vendor was processing their data. No Indian law required disclosure. No Indian regulator investigated the difference.

The consequences of inadequate data security in this space are not theoretical. In October 2024, a breach of Discord's Zendesk-based manual age verification system exposed approximately 71,000 government-issued identity documents.³⁶ This data breach was caused by the fact that Discord had permitted a third party working offshores to do manual verification checks and keep the ID photos for such verification purposes. The biometric and identity information of several thousand people, many of whom were minors, was exposed to cyber criminals, who can use this data to create an elaborate social network graph and perform identity theft or phishing attacks.³⁷

This is what the surveillance pipeline produces when it fails. But the harms extend beyond breach scenarios. Even when systems operate exactly as designed, the architecture is wrong. A child's facial geometry is biometric data of a fundamentally different character from a username

³¹ Pieter Arntz, *supra* note 1; Ernestas Naprys, *Firm that verifies mugshots for ChatGPT and Roblox feeds US surveillance apparatus with 269 distinct checks*, CYBERNEWS (Feb. 19, 2026), <https://cybernews.com/privacy/persona-leak-exposes-global-surveillance-capabilities/>.

³² *Id.*

³³ PERSONA, [Processor Privacy Policy](#), (last visited Apr. 14, 2026).

³⁴ ROBLOX, [Facial Age Estimation for Safer Chat | Roblox](#), (last visited Apr. 13, 2026).

³⁵ Dan Saltman, *supra* note 3.

³⁶ Dan Saltman, *70,000+ Government IDs Leaked in Discord x Zendesk Breach*, REDACT, (Oct. 8, 2025), [70,000+ Government IDs Leaked in Discord x Zendesk Breach](#).

³⁷ *Id.* at 10.

or an email address. It cannot be changed. It cannot be revoked. Once a child's facial map is in Persona's database, cross-referenced against terrorism watchlists, scored for risk, tagged with intelligence codenames, that child carries that data exposure for life.

The proportionality problem is stark. The stated purpose of age verification is narrow: confirm that a user is old enough to access certain features. Persona's 269 checks serve no function within that purpose. Screening a twelve-year-old against FinCEN databases is not a safety measure. Filing potential FinCEN reports on children, to the extent that Persona's design enables it, is a surveillance function entirely disconnected from child protection.³⁸

Parents are told their children are being kept safe. They are not told that safety is being purchased by enrolling their children, without meaningful consent, in financial intelligence infrastructure. Most parents lack the technical literacy to understand what "facial geometry mapped into 64+ data points processed by a third-party KYC vendor" actually means. The consent obtained is not informed consent. It is a signature on terms and conditions no adult has read and no child understands.

These harms are not simply technical failures or corporate negligence. They represent a failure of India's legal framework to protect children. Here's why the laws that should shield them fall short.

IV. The Legal Vacuum: Why India's Framework Fails Children

A. DPDPA 2023: The Catch-22

DPDPA requires "verifiable parental consent" before processing children's data under Section 9. But here's the problem: the Act never defines what "verifiable" means. The DPDP Rules, notified in November 2025, give platforms an 18-month transition period but still don't prohibit biometric age verification.³⁹

This creates a dangerous loophole. Platforms claim facial recognition IS the consent mechanism, using biometric surveillance to "verify" the parent while collecting the child's permanent facial data in the process.

³⁸ Pieter Arntz, *In 2025, age checks started locking people out of the internet*, MALWAREBYTES, (Dec. 31, 2026), [In 2025, age checks started locking people out of the internet | Malwarebytes](#).

³⁹ Digital Personal Data Protection Act, 2023, § 9; Digital Personal Data Protection Rules, 2025 (notified Nov. 14, 2025), <https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf>.

Worse, the DPDPA treats children's biometric data no differently than adults. Section 2(s) classifies it merely as "sensitive personal data" without any heightened safeguards.⁴⁰ Compare this to the EU's GDPR, which treats children's biometric data as requiring special protection with mandatory impact assessments. India has no such requirement.

The law assumes informed consent but provides no mechanism to ensure it. This vacuum allows platforms to outsource age verification to vendors like Persona without meaningful restraint. Roblox uses Persona. Discord tested both Persona and k-ID. Neither platform discloses to parents what these vendors actually do with the data.

B. Constitutional Violation: Puttaswamy Proportionality

Privacy is protected under Article 21 of the Indian Constitution. In *Justice K.S. Puttaswamy v. Union of India* (2017), the Supreme Court had established a four-part proportionality test for any privacy intrusion which consist of legality, legitimate purpose, rational connection and least restrictive means.⁴¹ Facial recognition fails the fourth test catastrophically.

The Internet Freedom Foundation analysed the Parliamentary Committee's recent proposal for mandatory KYC and age verification. Their conclusion? The proposal "has not taken into consideration the proportionality test" and ignores less intrusive alternatives.⁴²

As detailed in Section III, Persona's verification system performs functions far beyond age confirmation like screening against terrorism watchlists, retaining data for years and feeding into financial intelligence databases. None of this is necessary to verify that a child is over 13 years old.

Less restrictive means exist and work well. On-device age estimation processes facial scans locally without storing anything. Limited document verification extracts only the birthdate from an ID and deletes everything else. Graduated access systems match verification intensity to risk level: self-reported age for basic features, stronger checks only for financial transactions.

⁴⁰ Digital Personal Data Protection Act, 2023, § 2(s); cf. General Data Protection Regulation (EU) 2016/679, Art. 9, <https://gdpr-info.eu/art-9-gdpr/>.

⁴¹ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, <https://indiankanoon.org/doc/91938676/>.

⁴² Jhanvi Anam, *Analysing the Parliamentary Committee Report on Cyber Crimes and Cyber Safety of Women*, INTERNET FREEDOM FOUND. (Apr. 10, 2026), <https://internetfreedom.in/analysing-the-parliamentary-committee-report-on-cyber-crimes-and-cyber-safety-of-women/>.

Discord itself proved these alternatives work. After massive user backlash in February 2026, Discord ended its Persona experiment.⁴³ The platform continues operating without facial recognition. If Discord can verify age without biometric surveillance, so can every other platform. Under Puttaswamy, choosing maximum intrusion when alternatives exist violates Article 21. Platforms are making that choice right now.

C. Juvenile Justice Act: Best Interests Ignored

Section 77 of the Juvenile Justice (Care and Protection of Children) Act, 2015 codifies the "best interests of the child" principle derived from Article 3 of the UN Convention on the Rights of the Child.⁴⁴ This principle requires genuine balancing between competing rights: safety and privacy and between protection and autonomy.

Platforms like Roblox and Discord don't balance. They treat safety as automatically trumping privacy. There's no proportionality analysis, no consideration of whether less intrusive measures could achieve the same protective goal.

Think about what platforms are actually doing. They permanently sacrifice a child's biometric privacy. They expose facial geometry to third-party vendors operating across international borders. They retain data for up to three years. They feed children's biometric data into surveillance pipelines designed for financial intelligence and counter-terrorism.

All of this for a speculative and unproven safety benefit.

Section 77 demands better. A child's best interests include both protection from online harm AND respect for their developing autonomy and dignity. The current approach ignores the second half entirely. That's not balancing. That's abandoning the principle.

D. Critical Gaps in Indian Law

Indian law contains at least five critical gaps that allow facial recognition to operate unchecked.

⁴³ Colin Kirkland, *Discord Ditches Age-Verification Partner Following User Backlash*, SOC. MEDIA TODAY (Feb. 23, 2026), <https://www.mediapost.com/publications/article/413004/discord-ditches-age-verification-partner-following.html>

⁴⁴ Juvenile Justice (Care and Protection of Children) Act, 2015, No. 2 of 2016, § 77, <https://cara.wcd.gov.in/pdf/jj%20act%202015.pdf>; Convention on the Rights of the Child, Nov. 20, 1989, Art. 3, 1577 U.N.T.S. 3, <https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child>.

No data minimization for children. DPDPA Section 5 requires processing only what's "necessary," but platforms ignore this. Persona's 269 verification checks go far beyond confirming age, yet no Indian law stops this over-collection.

No mandatory Privacy Impact Assessments. Under the GDPR, high-risk processing requires formal assessment. India has no equivalent. Platforms deploy facial recognition without evaluating risks to children's mental health, data security, or long-term privacy.

No Age-Appropriate Design Code. The UK's Children's Code mandates default high privacy settings and data minimization for minors. India has no such standard. Platforms can design interfaces that nudge children into surrendering biometric data without parental understanding.

Weak enforcement. The IT Act, 2000 is outdated for biometric privacy. The Data Protection Authority under the DPDPA remains non-operational. Even when violations occur, there's no active regulator to investigate or penalize.

No vendor accountability. Discord tested both Persona and k-ID simultaneously. One used on-device processing with no retention; the other used server-side storage for seven days plus social media profiling.⁴⁵ Users were never told which vendor processed their data. Indian law doesn't require platforms to disclose vendor-switching or enforce consistent privacy standards across subcontractors.

These gaps aren't theoretical. They're being exploited today.

V. From Surveillance to Safeguards

India must adopt the following reforms:

First, finalize DPDPA Rules with an explicit biometric prohibition. Ban biometric age verification unless no less intrusive alternative exists. Define "verifiable parental consent" to exclude biometric collection from children. The Rules should explicitly list on-device age estimation and limited document verification as presumptively compliant methods.

Second, create a special category for children's biometric data. This should carry the highest protection standard under DPDPA: mandatory deletion after verification, prohibition

⁴⁵ Pieter Arntz, *Age verification vendor Persona left frontend exposed*, MALWAREBYTES (Feb. 20, 2026), <https://www.malwarebytes.com/blog/news/2026/02/age-verification-vendor-persona-left-frontend-exposed>; see also Naprys, *supra* note 6.

on secondary use, strict limits on third-party sharing. Violations should trigger automatic enhanced penalties.

Third, adopt an Age-Appropriate Design Code. Mandate data minimization, default highest privacy settings for children and mandatory Privacy Impact Assessments for any system processing children's data. Model this on the UK Children's Code and enforce it through regular compliance audits.

Fourth, operationalize the Data Protection Authority with a dedicated Child Rights Division. Empower the DPA to levy penalties calculated as a percentage of global annual revenue, not token fines platforms easily absorb. The Division needs specialized expertise to audit age verification vendors and investigate complaints involving children.

Fifth, prohibit secondary surveillance use. Age verification vendors cannot screen children's data against terrorism watchlists, financial intelligence databases, or politically exposed persons lists. Persona's practice of filing FinCEN reports on children and tagging their data with intelligence codenames must be explicitly banned. The purpose of age verification is confirming age, not building surveillance profiles.

These reforms are achievable. The question is whether India will act before the next major breach exposes millions of children's biometric data.

VI. Conclusion

Children cannot consent to the permanent surrender of their biometric identity. They cannot opt out of systems they do not know exist. Every day, platforms enrol a generation of children into surveillance infrastructure without knowledge, protection, or recourse. India's legal framework has failed to stop this. The DPDPA's undefined consent provisions, missing data minimization rules and non-operational regulator have created a vacuum that platforms and vendors like Persona exploit daily. The Puttaswamy proportionality test demands the least restrictive means, yet platforms choose maximum intrusion. The Parliamentary Committee's April 2026 report confirms that mandatory age verification is coming to India. The question is not whether, but how. Facial recognition is the wrong answer. Less intrusive alternatives exist and work well. India must act before the next major breach exposes millions of children's biometric data. Our children's privacy is not a fair price for their safety

COGNITIVE AUTONOMY AND CHILD PROTECTION: BRIDGING THE REGULATORY GAP IN NEUROTECHNOLOGY GOVERNANCE

Authored by : Khushi Jain & Priyanshi Agarwal⁴⁶

ABSTRACT

The blog through analysing the existing lacunae in legal framework examines the emerging risks posed by neurotechnology to children. It proposes a neurorights-based approach that moves beyond traditional notions of consent. By recognizing cognitive harms and emphasizing anticipatory, child-centric regulation, it seeks to safeguard mental privacy, autonomy and developmental integrity.

Keywords: Neurorights, Cognitive Privacy, Neurotechnology Regulation, Child Data Protection, Cognitive Autonomy

INTRODUCTION

Children today constitute nearly one-third of global internet users, yet they remain the least protected demographic within digital regulatory frameworks.⁴⁷ Digital technology development has brought about the transition of privacy from issues of information management to those of behavioral monitoring. Nonetheless, neurotechnological progress represents a more profound paradigm shift since it involves cognitive operations. The same has also been discussed in UNICEF Working Papers, affirming the unprecedented associated risks.⁴⁸

However, existing legal frameworks largely designed to regulate personal data and external conduct remain ill-equipped to address intrusions into the inner domain of the human mind. This blog critically examines the emerging and largely unregulated domain of neurotechnology and its implications for children's rights in the digital age. The blog analyses the inadequacy

46 3rd Year Students at Dr Ram Manohar Lohiya National Law University, Lucknow
<https://www.linkedin.com/in/khushijain2> ; <https://www.linkedin.com/in/priyagar>.

47 'Children and Young People are Already Shaping the AI Era' (UNICEF, 15 February 2026) <<https://www.unicef.org/india/stories/children-and-young-people-are-already-shaping-ai-era>> accessed 13 April 2026.

48 'Neurotechnology and Children's Rights: Preparing for the Future' (UNICEF, July 2025) <<https://www.unicef.org/innocenti/media/11426/file/UNICEF-Innocenti-Neurotech-Childrens-rights-Report-2025.pdf>> accessed 13 April 2026.

of existing legal frameworks in addressing these harms. Through the intersection of the constitutional realm, the blog suggests a plausible framework for inculcating a progressive approach.

NEURORIGHTS AND GLOBAL RESPONSE

Neurotechnology refers to technologies capable of recording, analyzing, or modifying brain activity.⁴⁹ The field combines neuroscience, artificial intelligence and data analytics. UNESCO defines neurotechnology broadly and identifies neural data, including inferred mental states, as sensitive.⁵⁰ It sets out key concepts such as beneficence, proportionality, autonomy, transparency, and the protection of future generations. Importantly, it prohibits manipulative uses of neurodata and cautions against non-therapeutic applications for children due to their developmental vulnerability.

Devices such as non-invasive brain-computer interfaces (“BCIs”) and neuro-monitoring tools hold promise in improving health services, disease detection and individualized education programs.⁵¹ However, the use of neurotechnology is associated with various threats for children. While conventional personal data concerns information of public interest and concern, neurodata refers to highly intimate information about one's cognitive functions, processes, emotions, and behavior. For this reason, it is necessary to radically redefine the concept of privacy from control of external information to the protection of internal personal space, one's mind.

For instance, the use of attention-monitoring headbands in classrooms, such as those developed by BrainCo, demonstrates how neurotechnology may operate within existing educational frameworks while still infringing mental privacy and autonomy.⁵² Despite these implications, existing legal frameworks remain inadequate. Current data protection and child rights regimes

⁴⁹ ‘The Promise of Neurotechnology in Clinical Translational Science’ (PMC, 17 October 2014) <<https://pmc.ncbi.nlm.nih.gov/articles/PMC4615684/>> accessed 13 April 2026.

⁵⁰ ‘Neurotechnology and Children’s Rights: Preparing for the Future’ (UNICEF, July 2025) <<https://www.unicef.org/innocenti/media/11426/file/UNICEF-Innocenti-Neurotech-Childrens-rights-Report-2025.pdf>> accessed 13 April 2026.

⁵¹ ‘What Does Neurotechnology Mean for Children?’ (UNICEF) <<https://www.unicef.org/innocenti/what-does-neurotechnology-mean-children>> accessed 13 April 2026.

⁵² Jared Genser, Stephanie Herrmann and Rafael Yuste, ‘International Human Rights Protection Gaps in the Age of Neurotechnology’ (Columbia Neurotechnology Center, 6 May 2022) <<https://ntc.columbia.edu/wp-content/uploads/2022/05/NeurorightsFoundationPUBLICAnalysis5.6.22.pdf>> accessed 13 April 2026.

regulate observable data but fail to address the extraction of neural data or cognitive inference. The same has been reiterated in global policy discussions.⁵³

This gap has led to the emergence of “neurorights”, which refers to a group of rights consisting of mental privacy, cognitive liberty and immunity from manipulation.⁵⁴ The international debate, through frameworks such as the UN Guiding Principles on Business and Human Rights, has centred on ethical governance grounded in principles of autonomy, dignity and non-discrimination.⁵⁵

LEGAL ANATOMY

The current legal framework governing children’s rights in the digital ecosystem in India is primarily rooted in constitutional guarantees, statutory data protection and child welfare laws. It however remains fragmented and insufficient in addressing emerging technological risks. The right to privacy, recognized as a fundamental right under Article 21⁵⁶ in *K.S. Puttaswamy v. Union of India*,⁵⁷ provides the constitutional foundation inculcating informational privacy, dignity and autonomy. However, its application to evolving domains such as cognitive and mental privacy remains underdeveloped.

Statutorily, the Digital Personal Data Protection Act, 2023 (“**DPDP**”) establishes a consent-based regime.⁵⁸ Through the regime, it introduces the obligation of verifiable parental consent for processing children’s data. At the same time, it restricts targeted advertising and behavioral tracking. Nonetheless, this framework is largely data-centric and does not extend to neurodata or AI-driven cognitive inference. On the same lines of above acts, child protection statutes such as the Protection of Children from Sexual Offences Act (“**POCSO**”)⁵⁹ and the Juvenile Justice

⁵³ Neurotechnology is Here. What Does That Mean for Children? (*World Economic Forum*, 27 September 2024) <<https://www.weforum.org/stories/2024/09/neurotechnology-risks-technology-children/>> accessed 13 April 2026.

⁵⁴ Marcello Ienca, ‘We Must Expand Human Rights to Cover Neurotechnology’ (*ETH Zurich*, 7 October 2021) <<https://ethz.ch/en/news-and-events/eth-news/news/2021/10/marcello-ienca-we-must-expand-human-rights-to-cover-neurotechnology.html>> accessed 13 April 2026.

⁵⁵ United Nations Human Rights Council, *Guiding Principles on Business and Human Rights: Implementing the United Nations “Protect, Respect and Remedy” Framework* (UN Doc A/HRC/17/31, 21 March 2011).

⁵⁶ Constitution of India, art 21.

⁵⁷ *K.S. Puttaswamy v. Union of India* (2017) 10 SCC 1.

⁵⁸ Digital Personal Data Protection Act 2023.

⁵⁹ Protection of Children from Sexual Offences Act 2012.

Act⁶⁰ also comes into play. Their objective is to address exploitation and welfare but lack framework on technologically mediated harms.

The Information Technology Act, 2005 and allied intermediary guidelines impose due diligence obligations on digital platforms.⁶¹ However, they lack specificity in regulating artificial intelligence, deepfakes or brain-computer interfaces. While recent judicial developments indicate emerging concerns about platform accountability and the risks posed by artificial intelligence, the regulatory approach remains anchored in parental consent and informational control.⁶² Consequently, the existing framework, though evolving, remains inadequate to address the profound challenges posed by neurotechnology and AI.

CONCERN

Neurotechnology can significantly benefit children, especially in healthcare, learning, and disability support. At the same time, it creates serious risks due to children's developing brains, which are more vulnerable to long-term impact. It has been observed lately that 76% of children use devices for social media, but only 57% for education.⁶³ These technologies can collect and infer mental data (thoughts, emotions, behavior) beyond traditional data privacy. 37% of children have reported reduced concentration due to smartphone use.⁶⁴

Erosion of Mental Privacy and Cognitive Autonomy: As a result, concerns arise about mental privacy, cognitive autonomy and freedom of thought. Adding on this, children often cannot give informed or meaningful consent, adding a layer of exploitation. There is a risk of behavioral manipulation, surveillance and coercive use in education, policing, or digital platforms. Further, neurotechnology may lead to over-standardization, ignoring neurodiversity, and pressuring children to “fit norms.”

⁶⁰ Juvenile Justice Act 2015.

⁶¹ Information Technology Act 2005.

⁶² Rehabilitation Council of India, 'Bachelor in Prosthetics and Orthotics (BPO): Norms, Regulations and Course Content 2025' (*Ministry of Social Justice and Empowerment, Government of India*) <<https://cdnbbsr.s3waas.gov.in/s34f4eeef3a8c90dfceadd5c6d64e4ebb/uploads/2025/11/2025112244.pdf>> accessed 13 April 2026.

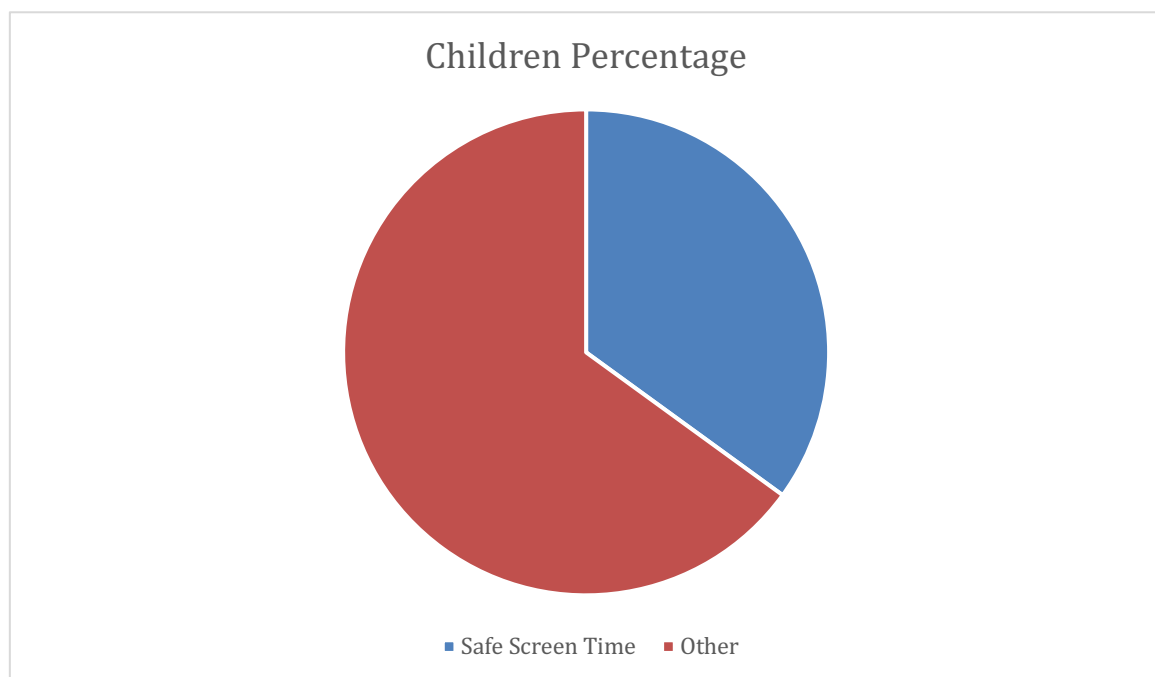
⁶³ 'India's Vast Internet, Social Media Apps Market' (*Reuters*, 29 January 2026) <<https://www.reuters.com/business/media-telecom/indias-vast-internet-social-media-apps-market-2026-01-29/>> accessed 13 April 2026.

⁶⁴ 'Impact of Use of Mobile and Internet on Children' (*PIB*, 8 December 2021) <<https://www.pib.gov.in/PressReleasePage.aspx?PRID=1779250>> accessed 13 April 2026.

Regulatory Lag and Technological Acceleration: The rapid advancement of neurotechnology has outpaced the evolution of legal frameworks. Current regulations remain anchored in data protection paradigms. It does not address the evolving risks within cognitive inference and neural data extraction. This temporal mismatch results in reactive governance.

Excessive Digital Exposure and Developmental Risk: The World Health Organization mentions that children under 5 years should not have more than 1 hour of screen time per day.⁶⁵ For older children and adolescents, bodies such as the American Academy of Pediatrics advise limiting screen time to around 2 hours per day.⁶⁶

It is also noted that excessive screen exposure can negatively disrupt attention span, cognitive development, sound sleep and behavioral pattern.



According to National Library of Medicines,⁶⁷ only 35% (nearly one-third) of children adhere to recommended screen time limits. This disparity highlights a structural failure in regulating

⁶⁵ 'To Grow Up Healthy, Children Need to Sit Less and Play More' (*World Health Organisation*, 24 April 2019) <https://www.who.int/news/item/24-04-2019-to-grow-up-healthy-children-need-to-sit-less-and-play-more> accessed 13 April 2026.

⁶⁶ 'Screen Time Guidelines' (*AAP Center of Excellence on Social Media and Youth Mental Health*, 2025) <<https://www.aap.org/en/patient-care/media-and-children/center-of-excellence-on-social-media-and-youth-mental-health/qa-portal/qa-portal-library/qa-portal-library-questions/screen-time-guidelines/>> accessed 13 April 2026.

⁶⁷ B A McArthur and others, 'Global Prevalence of Meeting Screen Time Guidelines Among Children Aged Less Than 5 Years: A Systematic Review and Meta-analysis' (2022) 176(3) *JAMA Pediatrics* 296 <<https://pmc.ncbi.nlm.nih.gov/articles/PMC8845032/>> accessed 13 April 2026.

children's digital environments. The data underscores a growing disconnect between scientifically established safety standards and actual usage patterns.

Urgent regulations to prevent misuse and protect children's rights are thus required.

CROSS JURISDICTIONAL ANALYSIS

Responses to neurotechnology are reflecting a growing awareness by some jurisdictions that existing data protection laws do not offer adequate protection of individuals' rights to their own mental sphere.

An example of this is Chile, which has been a leader in this regard by enshrining in its Constitution prohibitions against the misuse of neurotechnology. Brain activity, as well as any other information that may come from analysing brain activity, has now been recognised in Chile's Constitution as a fundamental right. It is based on the hope that the collection and use of neurodata will not be used to manipulate, discriminate against or coerce a person, as can occur when such neurodata is used in commerce and politics. In addition, Chile has proposed regulations that will govern the development of neurotechnology, including guidelines for informed consent, restrictions on how neurodata can be commercially used, and supervision of brain computer interfaces. By implementing these regulations prior to the widespread acceptance of this technology, Chile is taking an aggressive legal approach to mitigate the risk that will be posed by the eventual integration of neurotechnology into society.⁶⁸

Most countries, apart from Chile's constitutional model, are moving towards a policy-based, ethical approach to governing, particularly with respect to children. The same trend is seen in Mexico, where the experience with neuro technologies is being shaped mainly through human rights discussions and international collaboration rather than binding domestic laws.⁶⁹ The policy discussions around neurotechnology in Mexico continue to explore the implications of neurotechnology on such areas as freedom of thought, mental integrity and children's rights.⁷⁰ The UNICEF Innocenti Report (2025) notes a large number of countries, including Mexico,

⁶⁸ Shaji George, 'Protecting Brain Privacy in the Age of Neurotechnology: Policy Responses and Remaining Challenges' (*Research Gate*, October 2024) <https://www.researchgate.net/publication/384971350_Protecting_Brain_Privacy_in_the_Age_of_Neurotechnology_Policy_Responses_and_Remaining_Challenges/citations> accessed 14 April 2026.

⁶⁹ Herrera-Ferrá and others, 'The regulation of neurotechnology: the neurorights bill in Mexico' (*Lancet*, 17 October 2024) < [https://www.thelancet.com/journals/lanpsy/article/PIIS2215-0366\(24\)00286-4/abstract](https://www.thelancet.com/journals/lanpsy/article/PIIS2215-0366(24)00286-4/abstract)> accessed 14 April 2026.

⁷⁰ Brad Brooks, 'First law protecting consumers' brainwaves signed by Colorado governor' (*Reuters*, 18 April 2024) < <https://www.reuters.com/technology/first-law-protecting-consumers-brainwaves-signed-by-colorado-governor-2024-04-18/>> accessed 14 April 2026.

are at the "norm-building phase," using non-legally binding approaches (soft law), ethical guidelines and interdisciplinary research rather than legally binding frameworks.⁷¹ This trend is indicative of the continuing fragmentation of global legal systems as their legal systems evolve to respond to the risks associated with neurotechnology.

The regulatory responses to neurotechnology in the United Kingdom and the United States continue to make use of the existing legal structure (as opposed to recognizing neurorights) instead of developing a legal framework for neurorights. In the UK, neurotechnology is mostly regulated through data protection laws, innovative frameworks, and various governing agencies, particularly by the Information Commissioner's Office (ICO).⁷² They classify neurodata as sensitive in nature having been collected directly or indirectly via neural activity, meaning neurodata is subject to data protection laws. When evaluating neurotechnology in government documents, including the Rapid Technology Assessment (2025), the transformative potential of neurotechnology is acknowledged but that there are risk factors regarding how it affects an individual's privacy, discrimination, as well as how brain data is used.⁷³ However, the UK's approach is largely anticipatory and utilizes an advisory model with an emphasis on ethical governance, cybersecurity, and responsible innovation; thus, there are no specific safeguards for children are provided with protection by means that are indirect through standard data protection laws and standards which leave significant gaps related to cognitive surveillance, mental privacy, and AI-driven neurodata inference.

The United States adopts a fragmented and sector-specific approach, with no comprehensive federal framework governing neurodata or neurorights. The Food and Drug Administration (FDA), the Federal Trade Commission (FTC) and new state-level privacy laws all have a hand in regulating privacy. Recent developments, including legislative proposals like the MIND Act and state-level initiatives, show that people are becoming more aware of the dangers to mental privacy and cognitive freedom.⁷⁴ However, these efforts are still in their early stages and don't

⁷¹ 'Neurotechnology and Children's Rights: Preparing for the Future' (UNICEF, July 2025) <<https://www.unicef.org/innocenti/media/11426/file/UNICEF-Innocenti-Neurotech-Childrens-rights-Report-2025.pdf>> accessed 13 April 2026.

⁷² 'Neurodata, Neurotechnology and Data Protection in the UK' (Orrick, 25 August 2023) <<https://www.orrick.com/en/Insights/2023/08/Neurodata-Neurotechnology-and-Data-Protection-in-the-UK?>> accessed 14 April 2026.

⁷³ Government Office for Science, 'RTA: Neurotechnology' (14 February 2025) <<https://www.gov.uk/government/publications/rapid-technology-assessment-neurotechnology/rta-neurotechnology>> accessed 14 April 2026.

⁷⁴ Ashish Down, 'UNESCO adopts global standards on 'wild west' field of neurotechnology' *The Guardian* (6 November 2025).

have a single national framework. Existing laws like the Children's Online Privacy Protection Act (COPPA), which focus on data collection and parental consent are not enough when it comes to neurotechnology. This is because children can't really understand the long-term cognitive risks, and neurodata could be used to predict and change their behavior. The U.S. model is still driven by innovation. This means that there are big gaps in the law when it comes to protecting kids from cognitive surveillance, neurodata commodification, and behavioral change through AI.

SUGGESTIONS AND CONCLUSION

The problem raised by neurotechnology regarding the regulation of children comes from disparity between the new technology and the current legal framework. As mainly observed, the main concerns are data privacy and cognitive sovereignty.

Based on this legal framework, a regulatory approach could be proposed by developing four interrelated pillars, recognized within the broader normative framework of the DPDP.

First, at the level of legal recognition, the most immediate reform lies in expanding the scope of the DPDP. In order to extend the scope of DPDP, an amendment may be required to create a separate legal category called “*neurodata*” or “*cognitive data*.” The amendment would define neurodata to cover neural signals, mental states, emotions, and behavioral predictions derived from such data. In addition, the category of neurodata needs to be placed into the legal subcategory of “ultra-sensitive personal data.” Distinguishing the category would make it eligible for receiving greater levels of protection than other categories of personal data. Another amendment would be required to regulate “*cognitive inferences*” separately within the framework of data processing activities. Companies could circumvent the provisions of law by arguing that cognitive data is not collected but only inferred. Finally, a purpose limitation rule applicable exclusively to neurodata needs to be included. This will enable the restriction of use to therapeutic, clinical, and educational purposes only. Any commercial exploitation such as targeted advertising or behavioral nudging based on neural insights must be prohibited.

Second, as far as the substantiation of consent reform is concerned, reliance on parental consent must structurally be diluted. The necessary amendments to the DPDP framework should not only move away from mere reliance on consent but also impose a “best interest of the child and necessity test.” In other words, the use of neurodata in processing should satisfy the following requirements: *(i)* necessity; *(ii)* proportionality; and *(iii)* demonstrable benefit to the

child. For cases involving high-risk neurotechnological applications, a mandatory process of *ex ante* approval should be imposed. Furthermore, a general prohibition on the use of non-therapeutic neurotechnology in relation to minors including advertisement, surveillance, and performance monitoring within educational institutions should be legislated. This shifts the framework from consent legitimacy to substantive protection.

Third, a harm-based regulatory layer must then be codified to recognize injuries that are currently invisible to law. This can be achieved by amending the Information Technology Act, 2005 (or its successor digital law framework) to include a new class of harms including “*cognitive harms*”. It must be defined to encompass manipulation of thought, emotional conditioning, impairment of autonomy and psychological profiling leading to behavioral control. Such harms should be made *actionable per se*, without requiring proof of physical or economic damage. Complementarily, child protection statutes such as the POCSO Act and the Juvenile Justice Act can be expanded to include *technology-mediated exploitation*. Civil remedies, including compensation and injunctive relief, should be paired with regulatory penalties to ensure both deterrence and victim redressal.

Fourth, the framework needs an institution in tandem with technological development. A specialized Neurotechnology Regulatory Authority (or alternatively, a division in the Data Protection Board) needs to be created that has experts from the fields of law, neuroscience, ethics and artificial intelligence. Such an entity needs to be vested with the authority to undertake the following responsibilities:

- (i) conducting audits of algorithms and neurotechnology,
- (ii) setting legally binding safety and design guidelines,
- (iii) monitoring compliance through periodic reporting, and
- (iv) imposing penalties on violations.

Moreover, entities that use neurotechnology on children must be subject to mandatory ethics review boards, like biomedical ethics boards. They should strictly adhere the principles of beneficence and non-maleficence. A system of continuous monitoring is further essential.

While neurotechnology offers transformative benefits in diagnosing and treating neurological conditions, regulation must move beyond the medical sphere. Since, its use in education, gaming and consumer products raises new ethical and legal concerns.

Through adoption of the four pillars, the law aligns itself with the constitutional principles laid down in *K.S. Puttaswamy v. Union of India*.⁷⁵ The recognition and enforcement of neurorights thus become an essential safeguard.

⁷⁵ *K.S. Puttaswamy v. Union of India* (2017) 10 SCC 1.

LOCKED OUT OF MEMORY: THE LEGAL VACUUM IN CHILDREN'S RIGHTS TO THEIR PARENTS' DIGITAL LEGACY IN INDIA

Authored by: Adarsh Parashar⁷⁶

The ontological character of human heritage has radically changed. Traditionally, succession was a material process, based on passing on physical land, financial capital and corporeal resources between generations. Nowadays, the digital ecosystem is indispensable to the life of an individual. A modern-day estate not only includes bank accounts, but also monetised intellectual property, crypto wallets, and, arguably, most importantly to a bereaved family, huge repositories of emotional family heritage in the cloud. However, as the online trails of people continue to exist eternally, the laws that oversee their transfer after their deaths have not kept up with the times.

The death of a parent means the end of their biological existence, although their digital presence is placed in an endless corporate limbo. To the children that survive, this presents a jurisprudential dilemma. Indian law is designed in a manner that an orphaned child inherits the physical property of his/her parent with ease. However, it provides practically no legal procedure to guarantee their access to the digital memories of their parent. Such a legislative gap puts the digital inheritance of a child at the mercy of foreign corporate bodies, hardened End User License Agreements (EULAs) and a developing privacy infrastructure that inadvertently kills succession. This crisis cannot be solved with traditional and descriptive property law. It requires a critical, analytical engagement between privatisation of succession, post-mortem privacy fallacy and the basic human rights of the child in the digital era.

The illusion of Continuity and the Nominee Conundrum

The roots of this juridical vacuum are in the anachronic principles of Indian succession law. Acts such as the Indian Succession Act, 1925⁷⁷ and the Hindu Succession Act, 1956⁷⁸, were designed to fit a purely corporeal world. These are devoid of terms of digital property, digital account and platform-based assets. Therefore, the status of digital property under the law is not

76 4th Year Student at Chanakya National Law University, Patna
<https://www.linkedin.com/in/adarshparasharcnlu/>

⁷⁷ Indian Succession Act, 1925, Act.

⁷⁸ Hindu Succession Act, 1956, Act.

as clear, and executors and legal heirs do not have a clear statutory support when trying to transfer digital property.⁷⁹

The introduction of the Digital Personal Data Protection (DPDP) Act, 2023, was first seen as a solution. Section 14 of the DPDP Act, 2023⁸⁰ provides the right of nomination of another person who, in case of the death or incapacity of the Data Principal, has the right to exercise the rights of a Data Principal in the Act (including rights to access, correction/completion/updating, and erasure under Section 12)⁸¹. Yet, a strict legal examination shows that such a privacy-based legislation is fundamentally in conflict with the well-established succession legislation, and thus leaves the surviving children in a precarious situation.

In settled Indian law, a nominee never comes to have an absolute beneficial hold of an asset. By use of landmark precedents that regulate insurance and banking, the Supreme Court has reiterated on several occasions that a nominee is but a mere trustee or custodian who is holding the asset on behalf of the ultimate legal heirs⁸². When this trustee doctrine is applied to the digital context, one can see a huge structural defect in the DPDP Act. Section 14 gives the digital nominee the statutory right to erase data. When a nominee uses this right to erase the cloud storage or monetised online account of a deceased parent, they can forever destroy valuable economic or emotional property⁸³.

This brings a situation where the statute is actually a weaponisation of the nominee against the legal heir. This is devastating to children who are the natural legal heirs. In a situation where a parent passes away intestate, or the data nominee in charge chooses to delete data rather than preserve heritage, the child will have no legal means to claim back the family archives. The law now does not balance the informational autonomy of the DPDP Act with the orderly devolution of property, which the succession laws emphasise, with the digital inheritance of children caught between the crossfire.

⁷⁹ Shweta Chaturvedi, Digital Afterlife, Post-Mortem Privacy and Succession in India, SCC ONLINE BLOG (Feb. 27, 2026), <https://www.scconline.com/blog/post/2026/02/27/digital-afterlife-post-mortem-privacy-succession-india/>.

⁸⁰ The Digital Personal Data Protection Act, 2023, § 14(1).

⁸¹ The Digital Personal Data Protection Act, 2023, § 12.

⁸² Sarbati Devi v. Usha Devi, (1984) 1 SCC 424 (India).

⁸³ Aniket Ghosh, Digital Succession in India: Balancing Privacy and Property (April.1, 2026), <https://ksandk.com/data-protection-and-data-privacy/digital-succession-in-india/>.

Contractual Hegemony and Incapacity of Minors

Without a specific statutory framework of digital succession, the management of digital death has been completely overtaken by commercial technology companies. The Digital Estate of a deceased parent is not governed by the sovereign laws of India, but rather, unilateral boilerplate Terms of Service (TOS) by foreign platforms dictate their fate. The vast majority of tech giants adhere to a very rigid licensing arrangement that includes terms specifying that ownership of the account is non-transferable, and that all rights are expressed to die along with the user.

This delegitimacy of the domestic succession law creates huge constitutional tension. Article 300A in the Constitution of India⁸⁴ assures that no individual ought to be deprived of his or her property except through the powers of the law. When a technological firm uses an End-User License Agreement (EULA) constructed in standard form to deprive a child of an economically or emotionally valuable digital estate of his deceased parents, it is causing extrajudicial deprivation of property. The deprivation is a product of corporate policy, rather than the law.

This dependence on non-state contracts turns a legal challenge into a trap that is impossible to escape when it comes to minor children. In the Indian Contract Act, 1872, Section 11⁸⁵ stipulates that minors have no competence to enter into a legally binding contract. In *Mohori Bibee*⁸⁶, the Privy Council made it very clear that an agreement made with a minor was not merely voidable, but a nullity. Although this principle is to help protect children against exploitation, in the digital legacy, this effectively disenfranchises them. A minor does not have the legal standing to accept the Terms of Service on a platform, nor to go through the mazes of contract-heavy recovery procedures alone to reclaim data of their family.

To further enhance this contractual disenfranchisement, technology platforms literally weaponise age requirements as an element in their digital legacy architecture. An example is the Legacy Contact framework of Apple⁸⁷, which places age-based access controls, that is, younger children might be denied the ability to invoke post-death access mechanisms on their own. This poses a regulatory stalemate: Indian civil law prevents minors from contracting, whilst platform policies prevent them from having any mechanism of digital inheritance, depriving them of any realistic way to exercise their right. The child, therefore, is completely

⁸⁴ India Const. art. 300A.

⁸⁵ The Indian Contract Act, 1872, § 11.

⁸⁶ *Mohori Bibee v. Dharmodas Ghose*, (1903) 30 Cal. 539 (P.C.) (India).

⁸⁷ How to add a Legacy Contact for your Apple Account, APPLE SUPPORT, Apr. 12, 2026). <https://support.apple.com/en-us/102631>.

neutralised. The technology platforms function as uncontrolled shadow executors and deprive domestic judicial systems of their historical *parens patriae* powers to facilitate the well-being of minors as beneficiaries.

The Ghost of Privacy and the Imperative of Universal Succession

When an MNC refuses grieving families access to deceased accounts, the main legal defence used by them is the preservation of the ‘post-mortem privacy’⁸⁸ of the user. Corporations claim that one might be having some hidden communications, which they would not want their children to access, and therefore, deleting accounts is the only ethical option. This argument, however, fails to hold water when put to the strict test of jurisprudence.

The basis of the legal status of privacy after death is laid in the maxim *actio personalis moritur cum persona*, i.e. a personal right of action dies with the person. This has been a guiding principle in the Indian judiciary. In *Deepa Jayakumar v. A.L. Vijay*⁸⁹, the Madras High Court categorically decided that the rights to personality and privacy do not necessarily outlive the personalities. When the Indian rules are crystal clear that the essential right to privacy ceases to exist once death occurs, then alien technology sites have no right whatsoever to use post-mortem privacy as an excuse in refusing to disclose information to legitimate inheritors. They are in effect inventing a posthumous right that is not otherwise recognised by domestic law, simply to escape the administrative cost of doing business with local courts of succession.

To overcome this analytical stalemate, Indian legislators have to turn to a very sensible solution that has been created in Germany. The German Federal Court of Justice (BGH) made a watershed ruling in 2018 concerning the case of a 15-year-old girl who died tragically⁹⁰. The parents sought access to her Facebook messages to understand the circumstances surrounding her death, but Facebook refused, citing privacy concerns and its non-transferability clauses. The German Supreme Court firmly ruled against the tech giant.

The BGH utilised an excellent legal analogy and considered that a digital account on social media is virtually the same as a physical diary or a collection of personal letters. In the traditional system of inheritance, upon death, the physical diaries of a deceased person legally

⁸⁸ Anita L. Allen & Jennifer E. Rothman, Postmortem Privacy, 123 Michigan Law Review 2 (2024). Available at: <https://michiganlawreview.org/journal/postmortem-privacy/>.

⁸⁹ *Deepa Jayakumar v. A.L. Vijay*, 2021 SCC OnLine Mad 2642 (Mad. H.C. Apr. 16, 2021) (India).

⁹⁰ Philip Oltermann, Facebook told to grant grieving mother access to daughter's account, The Guardian (Jul. 12, 2018), <https://www.theguardian.com/world/2018/jul/12/facebook-told-grant-grieving-mother-access-daughters-account>.

descend to his or her legal heirs according to the doctrine of universal succession, no matter how intimate the contents are. The court found no dogmatic or logical reason to treat digital letters differently from analogue ones. Digital accounts need to be viewed as hereditary property, making typical platform contracts forcing the deletion of accounts completely invalid. Through this deep legal reasoning, India would refute the fiction that cyber data could not be vulnerable to property laws, which would enable children to smoothly inherit the digital diaries of their parents.

Digital Orphanhood and Child's Right to Identity

Although the doctrinal argument on property and contract law is essential, the excessive emphasis on the economic classification of assets would merely conceal the extensive human rights abuse taking place in this legal loophole. Beyond being a civil conflict, denying a child the right to the digital legacy of their deceased parent will cause a devastating psychological trauma that can be conceptualised as 'digital orphanhood'.

Children now have a digital footprint since birth, but they do not have the legal right to control or attribute it, and so their digital identities are largely dependent on their parents' accounts. In the case of the death of a parent, clinical psychology prescribes that the healthy mourning of the child will be determined by the ability to maintain 'continuing bonds', i.e. the process of adapting the memory of the deceased into the emerging identity of the child.⁹¹ Nowadays, such connections are virtually created solely by digital artefacts: vacation photos in the cloud, saved voicemails, social media feeds. When, with no prior notice, a technology platform erases an inactive account, it creates a simulated disappearance of the parent. The child experiences a secondary, digital bereavement that grossly interferes with the long-term psychological development of the child.⁹²

This mental damage makes the matter a breach of international law. India is a State Party to the United Nations Convention on the Rights of the Child (UNCRC). Article 8 of the UNCRC legally binds the state to respect and protect a child's right to preserve their identity, which explicitly includes their "family relations" as recognised by law.⁹³ Historically, this pertained

⁹¹ Dan Bates, Navigating Grief in the Digital Age, *PSYCHOLOGY TODAY* (Aug. 18, 2024), <https://www.psychologytoday.com/us/blog/mental-health-nerd/202408/navigating-grief-in-the-digital-age>.

⁹² Helen Hewson, Niall Galbraith, Claire L. Jones & Gemma Heath, The impact of continuing bonds following bereavement: A systematic review, 48 *Death Studies* 1 (2023). Available at: <https://www.tandfonline.com/doi/full/10.1080/07481187.2023.2223593>.

⁹³ United Nations Convention on the Rights of the Child, art. 8, Nov. 20, 1989, 1577 U.N.T.S. 3

to physical birth certificates, but human rights jurisprudence needs to develop with technological reality.

The UN Committee on the Rights of the Child made a historic step in releasing General Comment No. 25, which explicitly applied the UNCRC to the digital realm. The Committee laid down that meaningful access to digital technologies is necessary so that a child can enjoy the full extent of their civil and social rights. The Committee made it clear that, on the one hand, the rights of the child are fully applicable and equivalent in the digital space, and on the other hand, states are obligated to ensure that children are not exposed to the dangers of having the digital service provider arbitrarily deny them access to information that is vital to the formation of their identity.⁹⁴ UNICEF has placed a strong stress on the fact that the best interests of the child should be prioritised in the regulation of digital products and that corporate commercial interests should be subordinated to it. Assuming the child is inherently built by their own family history, and that family history is now stored solely in the cloud, then those digital artefacts are a crucial part of their identity, which is legally safeguarded under Article 8⁹⁵. The state is failing in its positive duty to defend the fundamental right of a child to identity by not regulating technology platforms and permitting them to arbitrarily cut a child off from the digital heritage of their family.

Conclusion

The shift of human life to the hyper-networked digital ecosystem has totally surpassed the archaic laws created to deal with mortality. The lack of legalisation of digital legacy in India subjects the bereaved children to an unbearable burden. They must deal, at their most vulnerable, with obsolete succession legislation that does not acknowledge digital data, a privacy framework (the DPDP Act) that gives third-party nominees precedence over biological heirs, and corporate contracts that are arranged systematically to exploit their legal incapacity as minors.

To solve this crisis, there is a need to change the paradigm. Experimenting with privacy legislation is not enough; India needs a specific system of ‘digital custodianship and

⁹⁴ UN Committee on the Rights of the Child, General comment No. 25 (2021) on children’s rights in relation to the digital environment, U.N. Doc. CRC/C/GC/25 (Mar. 2, 2021), <https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation>.

⁹⁵ Id. art. 8.

inheritance'⁹⁶. In the same way the law requires the court-appointed guardians to control the physical property of a minor, it should also enable the judiciary to gain a smooth access and maintenance of the electronic property of a deceased parent on behalf of an orphaned child.

In addition to legislative reform, Indian courts need to embrace the rationalism of the German Supreme Court. The courts should clearly acknowledge digital assets and communications as a form of inheritable property that falls under the rule of universal succession. Standard-form EULAs that seek to unilaterally destroy property rights and override domestic succession laws when a user dies must be invalidated as contrary to the public policy and constitutional property rights.

The digital estate is not just a bunch of commercially viable binary code; it is the new archive of human affection, family heritage and soul. The real legal change should go beyond the corporate monopolies and establish digital heritage as an integral part of constitutional rights to property and dignity, and correspond to the principles of the UNCRC. Through forward-looking legislation governing digital succession, India will be able to ensure the psychological welfare of its most vulnerable citizens and guarantee that children will never be permanently shut out of their own memories.

⁹⁶ Kasina Venkata Sri Varsha, Digital Estate Inheritance Law: The Need of the Hour to Balance the Rights of Posthumous Privacy and Legal Heirs, NLIU Law Review Blog (Jan. 27, 2025). Available at: <https://nliulawreview.nliu.ac.in/blog/digital-estate-inheritance-law-a-need-of-the-hour-to-balance-the-rights-of-posthumous-privacy-and-legal-heirs/>.

THE BIOLOGY OF BETRAYAL: PLATFORM LIABILITY AND THE CIVIL RIGHTS OF THE DIGITAL GENERATION

Authored by: Rishabh G. Pandey⁹⁷

Abstract

The recent jury ruling holding Meta and YouTube Liable for harms caused to children is a watershed moment for the jurisprudence of the digital field. For the first time, the legal veil of section 230 has been pierced in a way that resonates globally, recognizing platforms not as neutral conduits, but as architects of harm.

However, while the press treats this as a corporate news cycle, the real crisis is occurring within the biological machinery of a generation. We are witnessing human development being hijacked for profit a reality that necessitates a shift in how we view child rights in the digital age.

ENGINEERED STIMULATION: THE BIOLOGICAL TOLL

For years, the discourse around screen time has treated digital consumption as a passive activity. This framing is dangerously incomplete. We are dealing with engineered stimulation

- Dopamine by design: Platforms have consulted neuroscientists to flood developing brains with high reward, fast paced stimuli.
- Neural Rewiring: Because children's brains are under construction, constant exposure to these algorithms is shaping neural wiring to prioritize novelty over depth.
- The Stress Response: what is often dismissed as boredom or lack of focus is increasingly a physiological stress response. The brain conditioned to expect a constant digital hit, experience a state of withdrawal when faced with stillness or intellectual friction.

⁹⁷ 3rd Year Student at Thakur Ramnarayan College of Law, University of Mumbai
<https://www.linkedin.com/in/rishabh-pandey-069a443b3>.

THE INDIAN LEGAL LANDSCAPE: BEYOND SAFE HARBOUR

In India, the tide is turning against the absolute Safe Harbour protection traditionally granted under Section 79 of the Information Technology Act, 2000.

- The DPDPA 2023 (section 9): This legislation marks a significant shift, strictly prohibiting behavioral monitoring or targeted advertising aimed at children.
- IT Rules, Rule 3(1)(b): Intermediaries are now mandated to ensure they do not host content harmful to a child. Failure to comply can lead to a loss of immunity and staggering penalties.
- Duty of Care: Indian courts are increasingly evaluating whether the international design of a platform such as the infinite scroll constitutes a breach of the fundamental duty of care owed to minors.

THE SOLUTION TRAP: SAFETY VS. SURVEILLANCE

While we demand accountability, the solutions currently proposed such as mandatory age verification often act as trojan horse for broader issues.

- The Privacy: KOSA (Kids Online Safety Act) requires age verification for that Aadhar or government IDs to access digital spaces creates a state of total surveillance. In our pursuit of safety, we risk sacrificing the very privacy the DPDPA seeks to protect.
- Weaponized Protection: We must remain vigilant that child safety is not used as a pretext to censor inclusive content. Protecting children must not become a tool for erasure of marginalized identities or the restriction of life saving information. The groups cheering loudest for these bills like the Heritage Foundation (author of project 2025) openly admit they want to use this power to protect children from transgender culture they aren't interested in healthy they are interested in the erasure of queer and trans identities

STRUCTURAL INEQUALITY AND THE DIGITAL DIVIDE

The impact of addictive design is not distributed evenly; it follows the economic and structural fault lines of our society.

- Compounding Vulnerabilities: for children in under resourced communities, digital spaces often fill gaps left by falling social institutions. When these spaces are flooded with addictive systems, the impact doesn't just distract it disables.

- Demographic Sabotage: A generation with eroded critical thinking skills and diminished tolerance for cognitive effort is easier to control. For a nation like India, which depends on its demographic dividend, this is a matter of national importance

CENTERING THE WRONG CRISIS

By obsessing over chatbots and social feeds, we ignore more addressable, weighty causes of youth mental health crises the climate crisis, political instability and the gutting of educational supports

- In a chilling example of misplaced priorities, the state AG used photos of real children to create fake profiles to lure predators not to arrest them, but simply to gather evidence to sue meta

CONCLUSION

We do not need to turn the internet into a police state to protect our youth. We must hold platforms accountable for their architectural choices.

- Regulate sticky features: legislate against design elements like infinite scroll that exploit human psychology.
- Uphold the Best Interest principle: Under the DPDPA, platforms must be treated as Data Fiduciaries that act in the best interest of child, rather than harvesting them as products.

The verdict against Big Tech matters because it acknowledges that human attention is not an Infinite Resource to be mined. It is the bedrock of our ability to think, to build and to lead, we, must hold them accountable without handing our civil liberties to those who would use child safety as a weapon for social engineering. The future of our youth depends on their ability to focus, to think, and to resist.

THE PUPPET STRINGS OF PIXELS: ARCHITECTING INFANCY IN THE AGE OF ALGORITHMS

Authored by: Amitava Das⁹⁸

“The child is the father of the Man.”

- William Wordsworth, My Heart Leaps Up

If Wordsworth’s axiom holds true, then we must ask what manner of man is being fathered by an algorithm?

In the late 20th century, a child’s world was bound by the playground, classroom, living room and the television. Today, that world is an invisible architecture of code, a seamless loop of feedback mechanisms designed by the engineers in Silicon Valley to capture the most finite resource in the digital economy, which is “Human attention.” But when the subject of this capture is a child, “influence” takes on a more sinister hue, morphing into behavioural manipulation.

Today’s Children are the first generation to grow up in a world where their subconscious is not just influenced by their surroundings, but curated by an invisible, non-human intelligence. The ethical and legal landscape is shifting under the weight of “Algorithmic Influence” This is no longer merely about targeted advertisement for toys; it is about the structural behavioural manipulation of developing minds. When algorithms dictate what a child sees, feels, and desires, then the question arises, where the child’s autonomy ends, and the platform’s engineering begins.

The Engineering of Vulnerability

Children are not merely “small adults”; they possess a unique neurological status. The prefrontal cortex, the seat of executive function, impulse control, and critical thinking, does not fully mature until the mid-twenties. Algorithms, powered by Big Data and Reinforcement Learning, are designed to exploit this very gap.

98 3rd Year Student at Department of Law, Calcutta University, https://www.linkedin.com/in/amitava-das-1582072ab?utm_source=share_via&utm_content=profile&utm_medium=member_android

Modern social media platforms like Instagram, YouTube and Facebook operate on “variable reward schedules,” a psychological concept famously pioneered by B.F. Skinner⁹⁹. This says that by providing dopamine hits – likes, views, or the “infinite scroll” at unpredictable intervals, platforms create a compulsive feedback loop. For a child whose brain is highly plastic and seeking social validation, these loops are not just addictive; they are formative.

From a legal perspective, this goes beyond consumer protection. It enters the realm of cognitive liberty. When an algorithm predicts a child’s vulnerability, perhaps a burgeoning insecurity about body image or a tendency toward extremist rhetoric and pushes content to exploit that vulnerability for “engagement metrics,” it violates the fundamental principle of the best interests of the child, a cornerstone of international law¹⁰⁰.

The Architecture of the “Nudge”

In India, where the digital divide is closing rapidly but digital literacy remains stagnant, children are being thrust into “filter bubbles” that dictate their tastes, anxieties, and social perceptions. The algorithm learns a child’s insecurities faster than a parent can. If a teenager lingers a second too long on a video promoting unrealistic body standards, the machine feeds them a thousand more. This is “dark nudging”- the use of design patterns that exploit cognitive biases to lead users toward choices that are not in their best interest.

Algorithms do not force a child to stay online; they simply make it the path of least resistance by overriding the child’s internal cues of boredom or fatigue. Algorithms prioritize “high-engagement” content, which often translates to idealized body types or lifestyles, if a child clicks on one video concerning a specific ideology or trend, the algorithm creates a feedback loop, narrowing the child’s worldview before they have the tools to evaluate diverse perspectives.

Beyond the Right to be alone

In the digital age, privacy is no longer just the “right to be let alone,” as famously articulated by Warren and Brandeis¹⁰¹. For a child, privacy is the right to develop a personality without

⁹⁹ B.F. Skinner, *Science and Human Behavior* (Simon and Schuster 1953).

¹⁰⁰ UN Convention on the Rights of the Child, Art. 3, Nov. 20, 1989, 1577 U.N.T.S. 3.

¹⁰¹ Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890).

the oppressive weight of a “digital shadow.” Under current data-harvesting regimes, a child is “datafied” from birth or even before, via parental “sharenting.” By the time a child reaches thirteen, data brokers may hold thousands of data points on them, from their geolocation history to their emotional triggers¹⁰².

This data is not just shared; it is weaponized through predictive modelling. If an algorithm can predict a child’s future behaviour based on their past clicks, the child is denied the right to outgrow their past. This “predictive incarceration” limits the child’s autonomy.

The General Data Protection Regulation (GDPR) in Europe and the Children’s Online Privacy Protection Act (COPPA) in the U.S. attempt to provide a shield, but they often fail to address the inferred data- the insights an AI draws that the child never explicitly provided¹⁰³.

From Physical harm to Psychic manipulation

Historically, child protection laws focused on physical labour, neglect, and abuse. Today’s harm is psychic and pervasive. The attention economy treats the child’s mind as a commodity to be mined¹⁰⁴. Dark patterns, user interface designs to trick users into doing things they didn’t intend to do, are rampant in apps targeted at children. Whether it is “loot boxes” in gaming that introduce children to the mechanics of gambling or auto-play features that bypass a child’s nascent impulse control, the legal system is lagging behind the technology.

The doctrine of “*parens patriae*” grants the state the power to protect those who cannot protect themselves. There is a burgeoning legal argument that the state must intervene not just to stop “illegal” content, but to regulate the design of the algorithms themselves. We regulate the lead content in toys and the sugar content in cereal; similarly, we should not permit unregulated addictive loops in the digital toys our children carry in their pockets.

The Illusion of Agency

The UN Convention on the Rights of the Child emphasizes the right to participation, that children should have a voice in matters affecting them¹⁰⁵. However, in the digital sphere,

¹⁰² Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Public Affairs 2019).

¹⁰³ General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, Recital 38 (emphasizing special protection for children’s personal data).

¹⁰⁴ 5-4 Decision (Podcast), “The Law of the Attention Economy” (Exploring the limits of Section 230 and algorithmic liability).

¹⁰⁵ United Nations Convention on the Rights of the Child, G.C. No. 25 (2021) on children’s rights in relation to the digital environment.

participation is often an illusion. Children are participating in a pre-structured digital architecture where their choices are curated by AI. When a child chooses to follow a trend, it is not just a manifestation of their agency; it is a calculated result of an algorithmic nudge.

Meaningful participation requires digital literacy and a digital environment designed for transparency. Currently, the “Black box” nature of algorithms prevents children and their guardians from understanding how they are being steered. To fulfil the right to participation, we must move towards “Age-appropriate Design Codes” that prioritize the child’s development needs over corporate profit¹⁰⁶.

The Indian Jurisprudential Context & Lessons from the Globe

The legal landscape in India is currently in a state of flux. Historically, the Information Technology Act, 2000, and its subsequent rules focused on “notice and consent.”¹⁰⁷ However, the traditional “notice and consent” framework is a legal fiction when applied to children. A ten-year-old cannot meaningfully consent to the complex data harvesting practices that fuel behavioural manipulation.

The Digital Personal Data Protection (DPDP) Act, 2023, marks a significant and controversial shift. Section 9 of the Act explicitly prohibits data processing that is likely to cause a detrimental effect on the well-being of a child and bars tracking or behavioural monitoring of children.

While this is a laudable step, the challenge lies in the definition of “detrimental effect.” Is a dopamine-loop generated by an infinite scroll “detrimental”? Or, is the erosion of attention spans a “harm” under the law? Without granular regulations, these provisions risk becoming toothless tigers in the face of Big Tech’s lobbying power.

India is not alone in this struggle, but it is uniquely vulnerable due to its massive youth population. The European Union’s Digital Services Act (DSA) and the UK’s Age-appropriate Design Code (AADC) offer a blueprint. These frameworks shift the burden from the user to the platform, requiring “Safety by Design.” They mandate that the best interest of the child must be the primary consideration in algorithmic design.

¹⁰⁶ Information Commissioner’s Office (UK), “Age-appropriate design: a code of practice for online services” (2020).

¹⁰⁷ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

In India, however, the discourse is often hijacked by concerns of censorship versus free speech. We must distinguish between the “content” and the “conduit.” Regulating algorithmic influence is not about banning content; it is about regulating the delivery mechanism that bypasses human agency.

The Path Forward- A new digital social contract

The solution is not to retreat from the digital world but to re-civilize it. Legal frameworks must shift from a "notice and consent" model, which is a legal fiction when applied to children to a "safety by design" mandate.

This involves three critical shifts:

First, the duty of care must be codified, requiring platforms to mitigate systemic risks to children’s mental health.

Second, algorithmic auditing must become mandatory, allowing independent bodies to inspect how content is served to minors.

Third, we must recognize neural rights: the right to develop one’s mind free from manipulative external influence.

If we continue to allow the commercial exploitation of childhood development, we risk raising a generation whose desires, fears, and thoughts are not their own, but the echoes of an optimization function. We must reclaim the playground. The law must step out of the books and into the code, ensuring that the "father of the man" is a human spirit, not a silicon sequence.

FROM PROBABLE CAUSE TO PREDICTIVE GUILT: ASSESSING THE EROSION OF THE PRESUMPTION OF INNOCENCE IN THE ERA OF ALGORITHMIC POLICING

Authored by: Sagnik Halder¹⁰⁸

Introduction:

In the traditional landscape of criminal jurisprudence, the 'Presumption of Innocence' is the golden thread in the web of a fair trial, which grants every individual in the community the fundamental right of being treated as a citizen and not as a suspect until a court of law decrees otherwise. However, with the 21st century bringing a swift transition towards the "datification" of security, this underlying support is experiencing an unprecedented structural challenge. The rise of algorithmic policing (i.e., the use of predictive analytics and artificial intelligence to flag "hot spots" or "high risk" individuals by law enforcement agencies) is surreptitiously recalibrating the scales of justice.¹⁰⁹

While all of these technological interventions are sold as objective, efficient and scientific approaches to urban crime, there is a hidden socio-legal cost. Through this redefinition of the focus of policing away from reactive, investigative to predictive anticipation, the state is essentially replacing the legal standard of "individualized suspicion with mathematical probability." This transition is a dangerous switch from the doctrine of probable cause to a new age violate world of digital predictive guilt.

In the Indian context where the Supreme Court has time and again reiterated that "bail is the rule and jail is the exception"¹¹⁰, the murky nature of the policing algorithms poses a threat of circumventing the constitutional guarantees. When a machine is able to flag a person as a potential offender, based on historic data - which often is reflective of existing socio-economic biases - the burden of proof starts to shift. The person is no longer presumed innocent but is instead brought to a state of 'permanent investigation' by a system that he or she can never see or even challenge. This blog is an exploration of the erosion of these civil liberties, and argues that if we don't introduce rigorous algorithmic accountability, the "Black Box" of technology will inevitably shadow the light of Due Process.

¹⁰⁸ 2nd year Student at Brainware University, <https://www.linkedin.com/in/sagnikhalder>

¹⁰⁹ *Universal Declaration of Human Rights* (adopted 10 December 1948) UNGA Res 217 A(III) (UDHR) art 11.

¹¹⁰ *State of Rajasthan v Balchand* (1977) 4 SCC 308.

I. The Evolution of Suspicion: Probable Cause vs. Algorithmic Probability

The shift from traditional to algorithmic policing is not simply a shift from tool kit to tool set, but a basic restructuring of the legal concept of "suspicion." Indian criminal jurisprudence in the past has depended on an idea that is known as the 'Reasonable Suspicion' or 'Probable Cause' in a way that acts as a gatekeeper against the propensity of the state to act arbitrarily. Under the procedural framework of the Code of Criminal Procedure (now called the BNSS), an investigating officer's authority to seize or search is dependent on specific and articulable facts to the arrest or search of a particular person to a certain feared offense past or future committed. This standard promotes the coercive power of the state reactionary and on the tangible behavior of the citizen.¹¹¹

In contrast, algorithmic policing has ushered a philosophy of 'actuarial justice.' Instead of concentrating on the specific tactics of a single individual, predictive models, such as those that use Spatial-Temporal Forecasting or Risk-Assessment Metadata, study huge datasets to determine the probability of future occurrences. This changes the standard of suspicion from individual to a statistical probability. When an algorithm finds a "high-risk" zone or "suspicious" profile, it does not do so based on recidivism patterns of real-life criminals, but rather on a mathematical expression derived from past data on direction.

The socio legal danger of them is that they are "presumptive" inferences. When the police are brought to a broader neighborhood or ordered to arrest a particular person because a software has given a '90% probability' report of a crime, the legal requirement of 'reasonable grounds' is effectively automated. This leads to a circular logic, where the algorithm predicts that crime will occur in a given area, the state increases their presence there, and this leads to more arrests, which in turn leads to the prediction in the algorithm as "proof" of their accuracy. By the time a case gets to the court, however, the initial 'Presumption of Innocence' has already been debauched by an invisible and pre-trial classification of 'guilt-by-probability.'

Further, this evolution questions the 'fair, just and reasonable'¹¹² procedure laid down by the Supreme Court. If the basis for a search or seizure is a machine-generated score rather than a human officer's (witness-based) reasoning, the "reasonableness" of the state action is impossible to check. We are heading towards a legal reality in which the 'Golden Thread' of innocence will be supplanted by a digital web of correlations in which a citizen's right to

¹¹¹ Bharatiya Nagarik Suraksha Sanhita 2023, s 35.

¹¹² *Maneka Gandhi v Union of India* (1978) 1 SCC 248.

freedom from state interference will be parameterized not by what they have done but rather what some data-point suggests they might do.

II. The "Black Box" Problem: Due Process and the Right to a Fair Trial

A centerpiece of a fair trial, as comes down to Article 21 of the Indian Constitution, is the right to the accused to understand and challenge evidence produced against him or her.¹¹³ In the case of algorithmic policing, this right runs into an imposing hurdle, the "Black Box" phenomenon. The vast majority of predictive policing applications are the product of private tech companies, and are proprietary trade secrets. Consequently, the underlying logic - in this case the source code as well as the individual weights given to various data variables - is obscured from the judiciary, the defense council and often the police officers themselves.

This opacity makes for a serious "due process" deficit. If the citizen is stopped, searched or detained based on an algorithmic "red flag" the defense is deprived of the chance to cross-examine the "accuser." In traditional law, it is possible for an officer to be questioned on the witness stand about what they observed; an algorithm, in contrast, has no such transparency. This practically makes whatever the machine outputs an infallible truth that eclipses the adversarial scrutiny that is so crucial to the truth-seeking mission of the court.

Furthermore, there is the "Black Box" problem of judicial review of state action. For a court to determine whether an investigating agency acted with "manifest arbitrariness," it must have the ability to see the reasoning behind the suspicion. When that reasoning is obfuscated in layer upon layer of complex non-disclosable code, the oversight role of the court is neutralized. We are in danger of moving towards a situation of "automated law" in which the supremacy of the executive is protected by the appearance of neutrality in mathematics. Without any legal requirement for Algorithmic Explainability, the presumption of innocence has been downgraded to a formalistic ritual, one easily defeated by a software's impenetrable and unchallengeable "risk score."

III. Automating Prejudice: Socio-Legal Impacts on Marginalized Communities

The veneer of mathematical objectivity tends to mask the historical and systemic biases common to the data fed into policing algorithms. In the socio-legal context, this is forming a "feedback loop of injustice," which has a disproportionate effect on marginalized communities. If data collected from policing efforts has been skewed - reflecting over-policing in particular caste-based colonies, or lower income urban pockets - the algorithm will understand these spaces as "inherent" areas of crime. Consequently, the software is reinforcing police resources

¹¹³ Constitution of India 1950, art 21.

in these places, leading to more arrests, which in turn confirms and reinforces the initial prejudice.

This "automation of prejudice" is in direct violation of the Article 14 of the Indian Constitution which guarantees the right to equality.¹¹⁴ By categorizing citizens based on proxies of poverty or social status: be it pin codes, frequency of movement or associations, citizens, through the use of algorithmic policing create an effective digital caste system. The 'Presumption of Innocence' is thus not lost equally for everyone, it is lost primarily for the people to whom the data is already disfavoring. When the state's gaze is too much fixed on certain members of the group, thanks to prediction modeling, the fundamental right to be treated as an equal citizen is substituted by the status of a 'permanent suspect.'

In addition, the psychological effect of living under "predictive surveillance" has a chilling effect on civil liberties. When people are aware their patterns of movement and associations are being scored for "criminality" in everyday life, they are self censored in their movement and associations to not be flagged. This structural pressure vitiates the social contract in the sense that this state becomes a defender of rights shifting to the violation of putting statistical anomalies those who hunt. In a society where the algorithm determines the "profile of a criminal" the legal right to the defense of one's innocence is a luxury reserved for those whose lifestyle mirrors the data-driven "norm."

IV. Navigating the New Frontier: Privacy and the BNSS Framework

The prevailing legal scenario in India nowadays is in a state of flux with the debate to move to Bharatiya Nagarik Suraksha Sanhita (BNSS). While the objective of the BNSS is to modernize criminal procedure to take on board digital evidences, it is still noticeably silent on the particular set of mechanisms that are needed to protect against algorithmic policing. This legislative gap poses a danger in the sense that the efficiency of technology is valued at the expense of procedure of Article 21.

Central to this deliberation is the "Right to be Let Alone" as crystallized in the Puttaswamy judgement.¹¹⁵ Algorithmic policing, by its nature, necessitated mass harvesting of data - often without the express consent of the "principal" of the data. Under the Digital Personal Data Protection (DPDP) Act, 2023, it has given the law enforcement agencies wide exemptions which can enable them to circumvent traditional privacy barriers.¹¹⁶ But if privacy is an essential condition of the 'Presumption of Innocence,' then a system in which the right to an

¹¹⁴ Constitution of India 1950, art 14.

¹¹⁵ *KS Puttaswamy v Union of India* (2017) 10 SCC 1.

¹¹⁶ Digital Personal Data Protection Act 2023, s 17.

autonomous life is really compromised fundamentally by the idea of each and every citizen as a source of "potential risk" data. For the Indian judiciary, the challenge will be to ensure that the digital push of the BNSS will not convert the 'Golden Thread' of the twin life's estimate, innocence, into a net of digital surveillance, which never let's go.

V. Conclusion

The integration of algorithms into the sovereign function of policing cannot be taken lightly as a technical upgrade, but is a critical socio-legal shift that can throw the human-centered 'Presumption of Innocence' with a machine-centered 'Predictive Guilt.' As we have seen the shift from individualized suspicion to actuarial probability causes a structural bias that strikes against the foundational pillars of Article 14 and Article 21 of the Indian Constitution. When justice goes browse outside the courtroom to "Black Box" systems, the adversarial nature of our legal system – and of the executive themselves – is fundamentally compromised.

To make sure that the digital push under the BNSS framework does not lead to a "digital panopticon," India will now have to move towards a regime of Algorithmic Accountability. This includes both mandatory transparency in source code for judicial review and rigorous audits to address the issue of data-driven prejudice for good (discriminating individuals based on their race, color, religion, etc., based on data they're provided). Adding maintenance of a "human-in-the-loop" to ensure that mathematical correlations never work in place of legal reasoning. Justice must be left to an exercise of human conscience and constitutional morality. If we let the algorithm decide the status of a citizen's innocence though, we may lose the "Golden Thread" that holds the very fabric of a democratic society together.

TOO YOUNG TO CONSENT, OLD ENOUGH TO BE EXPLOITED:

INDIA'S DIGITAL AGE PARADOX

Authored by: Krati Raghav¹¹⁷

THE CLICK THAT DOESN'T EXIST

Imagine this: a 13-year-old opens an educational platform or a social media app for the first time. A long privacy policy flashes on the screen. Dense, technical, and practically unreadable. A checkbox appears - "I agree to the Terms and Conditions."

She doesn't read it. She probably can't but clicks anyway. Just three seconds and access granted.

In that moment, the platform gets the right to collect, analyse, and use her personal data for behavioural tracking, targeted advertising, even third-party sharing.

But let's pause for a moment. What just happened legally?

That same 13-year-old cannot sign a rental agreement. She cannot open a bank account on her own. She cannot enter into a binding contract under Indian law. And yet, with one impulsive click, she is treated as having "consented" to one of the most complex exchanges of the digital age; the use of her personal data.

This isn't hypothetical. I've been that user. Like millions of others, I used these platforms as a minor. Not once was I asked for parental consent, not real consent, at least. An email ID was enough. A checkbox was enough. That was the system.

And that is the problem!

This is not just a technical gap or a design flaw. It is a structural contradiction built into the foundation of India's digital economy. The Indian Contract Act, 1872 clearly treats minors as legally incompetent to contract.¹¹⁸ Yet the entire data ecosystem functions on the assumption that their digital consent is valid.

That contradiction of legal incapacity on one hand and presumed digital consent on the other, sits at the heart of this debate.

¹¹⁷ 5th Year Student at Faculty of Law, Aligarh Muslim University, https://www.linkedin.com/in/krati-raghav-658156260?utm_source=share_via&utm_content=profile&utm_medium=member_android.

¹¹⁸ *Indian Contract Act 1872*, ss 10, 11.

This blog examines that digital age paradox. It argues that the problem is deeper than weak enforcement or imperfect rules. What is needed is a fundamental rethink of how the law understands children's capacity in the digital space and a shift toward a more nuanced, graduated model of consent.

Void ab Initio: What Contract Law tells us about Digital Consent

The Indian Contract Act, 1872 sets out a simple starting point. Section 10 requires that all agreements must be made by parties competent to contract. Section 11 then defines who is competent- a person who has attained the age of majority, is of sound mind, and is not disqualified by law. A minor does not even qualify the first step. This is not some technical exception or a niche rule. It is the foundation on which the entire structure of our contract law rests.

The position becomes even stricter when we look into *Mohori Bibee v. Dharmodas Ghose*¹¹⁹. The Privy Council made the situation unmistakably clear. A minor's agreement is void ab initio i.e. void from the very beginning. Not voidable. Not capable of being ratified later.

Simply put, the law treats it as if no contract ever existed.

Now carry that principle into the digital space-

When a minor clicks "I Agree" on a platform, that act is treated as consent. But under contract law, it has no legal existence. If the agreement itself is void from inception, the consent embedded within it collapses with it. There is, in effect, no valid consent existing at all. And yet, on the strength of that non-existent consent, platforms collect, process, and monetise children's data every single day.

That is the paradox in its most concrete form; not theoretical, not abstract, but built into everyday digital interactions.

And then comes the question of age verification. Platforms routinely ask users to confirm that they are above 18. Everyone knows how this works. Children lie. Platforms know they lie. The checkbox still remains. Because it is not really verification but a formality that creates the appearance of compliance without its substance. Legal capacity cannot be manufactured by asking someone to declare that they have it.

¹¹⁹ *Mohori Bibee v Dharmodas Ghose* (1903) 30 IA 114 (PC)

This was the position long before data protection entered the conversation. The law was clear, even if practice was not. When the Digital Personal Data Protection Act, 2023 arrived, it promised to address precisely this gap. The question is whether it actually did.

A Law that Protects on Paper: Section 9 and The Illusion of Safety

The Digital Personal Data Protection Act, 2023 was supposed to fix this loophole. And to be fair, it does take a step in the right direction. For the first time, it actually treats children as a distinct category deserving higher protection. Section 9 lays down two strong promises - parental consent must be verifiable before a child's data is processed, and tracking, behavioural monitoring, and targeted advertising directed at children are absolutely prohibited¹²⁰. On paper, this looks like a clean migration from the checkbox culture that defined the earlier regime.

But recognition is NOT protection.

The first crack appears in the Digital Personal Data Protection Rules, 2025. Rule 10 is meant to operationalise “verifiable” parental consent¹²¹. Instead, it falls back on vague language, platforms must take “appropriate technical and organisational measures.” Appropriate according to whom? The law does not answer that. No single method is mandated. Nothing stops a platform from continuing with email verification or the simple checkbox gimmick and calling it compliance. DigiLocker is mentioned in discussions, but not required or mandated.

So the system hasn't really changed ; it has just been re-labelled.

The second gap is more subtle, but even more dangerous. Rule 11 creates an exemption for “educational institutions” when processing children's data for educational purposes¹²². That sounds reasonable until we ask what counts as an educational institution. The Rules don't define it and worse they don't draw the line between where education ends and commercial data use begins. For-profit EdTech platforms sit right in that grey area. A platform collecting behavioural data to “improve learning outcomes” can just as easily use the same data for profiling or targeted engagement. *The line is blurry*. And right now, the law leaves it that way.

Then comes the most serious problem - enforcement, or rather, the ABSENCE of it.

¹²⁰ Digital Personal Data Protection Act 2023, s 9.

¹²¹ Digital Personal Data Protection Rules 2025, r 10.

¹²² Digital Personal Data Protection Rules 2025, r 11.

⁶Information Technology Act 2000, ss 43A, 72A.

Section 9(3) has been in place since August 2023. It bans tracking and targeted advertising of children in absolute terms. No exceptions. And yet, not a single platform has been penalised for violating it. NOT ONE. The reason is simple: the enforcement framework is still not fully operational. The Data Protection Board exists, but without full penalty powers until May 2027. That is nearly four years after the law was passed. An absolute prohibition without consequences is not really a prohibition. *It is a statement of intent.*

And this didn't start with the DPDP Act. Before this, India relied on the Information Technology Act, 2000 , specifically Sections 43A and 72A⁶. Neither provision was designed with children in mind. Section 72A even assumes the existence of a lawful contract, which a minor cannot enter. For years, children's data sat outside meaningful legal protection. That data hasn't disappeared. It still exists, still circulates, still gets used.

So what we are left with is a law that recognises the problem, gestures toward a solution, but stops short of making it real. And when a State acknowledges a risk to a fundamental right but delays its enforcement for years, the issue is no longer just about statutory gaps. At that point, it stops being a drafting issue. It becomes a constitutional failure.

Beyond Statute: A Fundamental Rights Failure

The gaps in the DPDP framework are not just poor drafting but they point to something deeper: the failure to meet constitutional obligations.

In *Justice K.S. Puttaswamy v. Union of India*¹²³, a nine-judge bench of the Supreme Court settled this clearly- "Privacy is a fundamental right" under Article 21. Not an abstract idea, but a concrete guarantee tied to dignity. Justice Chandrachud's opinion gave it a sharper form through the idea of informational privacy. Each individual has the right to decide what data about you is collected, how it is used, and who gets access to it. Moreover, the Court did not put everyone in the same mould. It recognised that children stand on a different footing. They lack the capacity to fully understand their choices. This is precisely why they require greater protection, not equal treatment.

These rights are not just shields against the State. They are also claims on the State; positive obligations on the state. The State must create conditions where rights can actually be

¹²³ *Justice KS Puttaswamy v Union of India* (2017) 10 SCC

1. ⁸ Constitution of India, arts 39(e), 39(f).

exercised. It must protect individuals from private actors who threaten those rights. This includes digital platforms.

Now looking at where we stand:

The State enacted the DPDP Act in 2023. It notified Rules in 2025. But enforcement is still delayed. The Data Protection Board exists, but without full teeth. There is no clear, mandatory mechanism for verifying parental consent. No meaningful response to the vast amounts of data already collected before 2023. “The law exists; the protection does not.” And that gap matters. Because once a right is recognised as fundamental, delay is not neutral, it is a failure.

The Constitution is not silent on protection of children either. Articles 39(e) and 39(f) of the Constitution of India⁸ require the State to prevent the abuse of children and ensure their development in conditions of dignity, free from any exploitation. But what we see today - unchecked tracking, behavioural profiling, targeted engagement, fits uncomfortably well within the idea of exploitation.

India is not the only one facing this problem. But seeing how other jurisdictions have responded makes one thing clear: this is not an unsolvable issue. At this point, it looks less like a limitation and more like a choice

What India Can Learn: From Gillick to GDPR

Child data protection is not a uniquely Indian problem. Every jurisdiction is struggling with the same question of how do we protect children in a system built on consent? But the way others have responded makes one thing clear: India’s approach is not inevitable. It is a choice.

And right now, it is an inadequate one.

The EU’s General Data Protection Regulation (GDPR) does not pretend that all children are the same. Article 8¹²⁴ allows member states to set the age of digital consent anywhere between 13 and 16. Most settle at 16. That range itself is the gist that the law recognises that a 16-year-old is not comparable to a 7-year-old, and shouldn’t be treated like one. India collapses that entire spectrum into a single number: 18 years. No nuance, no gradation, just a blanket denial of capacity. Then, coming to enforcement, in 2023, Meta was fined €1.2 billion by Ireland’s

¹²⁴ Regulation (EU) 2016/679 (General Data Protection Regulation), art 8.

Data Protection Commission¹²⁵. That is what a law with teeth looks like. India, on the other hand, has not fined a single platform under its new framework.

The UK approaches this equation very differently. In *Gillick v West Norfolk and Wisbech Area Health Authority*¹²⁶, The House of Lords held that a minor under the age of 16 can consent to medical treatment if they have sufficient maturity and understanding. In other words, capacity is not fixed; it evolves. What makes this contradictory for India is that we do accept this logic in criminal cases. Under the Bharatiya Nyaya Sanhita¹², a child between the age of 7 to 12 can be held criminally liable if they understand the nature of their act. We are trusting children with responsibility when it comes to punishment. But when it comes to their own data, we deny them even partial agency. That inconsistency is hard to understand and justify.

If we take the example of United States, The Children's Online Privacy Protection Act 1998¹²⁷(COPPA), draws a hard line at 13 years. Below that, strict parental consent is mandatory. And it is strictly enforced. In 2019, YouTube paid \$170 million for violating COPPA. That penalty changed behaviour overnight¹²⁸. But COPPA also shows the limits of a rigid consent model - once a child turns 13, the special protection disappears. The gap between 13 and 17 years remains largely unaddressed.

Taken together, these systems point in one direction. Protection cannot come from a single age threshold or from paper compliance alone. It requires a more honest understanding of how children actually develop digital capacity. That is precisely what India's current framework is missing.

A Way Forward: The Case for Graduated Digital Consent

Addressing this paradox requires more than just fixing gaps in the law. It requires rethinking the assumption that digital capacity appears suddenly at 18. *It does not*. It develops and the law must reflect that.

The answer lies in a **three-tier graduated consent model**.

¹²⁵ Data Protection Commission (Ireland), 'Decision on Meta Platforms Ireland Ltd' (2023).

¹²⁶ *Gillick v West Norfolk and Wisbech Area Health Authority* [1986] AC 112 (HL).

¹² Bharatiya Nyaya Sanhita 2023, s 20.

¹²⁷ Children's Online Privacy Protection Act 1998 (US).

¹²⁸ Federal Trade Commission, 'Google and YouTube to Pay \$170 Million...' (2019).

Tier 1 - Children under 13

At this stage, children simply do not have the ability to understand long-term data consequences. Full, verifiable parental consent must be mandatory before any data processing or collection. No diluted standards. No workaround through checkboxes. The only exception should be for welfare purposes.

Tier 2 - Ages 13 to 15

A co-consent model which means both parent and child must consent independently. Neither consent alone is sufficient. This recognises developing autonomy while maintaining oversight. It reflects the logic of Gillick competence where capacity emerges gradually, and does not appear overnight.

Tier 3 - Ages 16 to 17

The adolescent's consent should be valid for standard data processing. Parental involvement should be limited to notification in cases of sensitive data like health, biometric, or behavioural tracking. This also aligns with GDPR's threshold¹²⁹ and acknowledges real-world digital maturity.

Additionally, two reforms must accompany this.

First, a "privacy by design mandate". Platforms accessed by children must be safe by default; minimal data collection, no manipulative interfaces, no dark patterns. Protection cannot depend on how carefully a child clicks.

Second, **genuine enforcement**. The Data Protection Board must be fully operational before 2027, with independence and real penalties. Without enforcement, even the best framework collapses.

These changes would turn India's model from symbolic protection into actual protection.

Whether they come in time for the children already online is the question that remains.

A Delay Measured in Childhoods

A child still signs up the same way - a quick scroll, a faster click, "I agree." It feels trivial but isn't. Because that click carries no legal weight. It never did. And yet, an entire digital economy continues to rely on it quietly and routinely, almost as if the contradiction does not exist.

¹²⁹ Regulation (EU) 2016/679 (General Data Protection Regulation), art 8.

The law now admits the problem. It even promises a fix. But it asks for time again. This is where the failure becomes harder to ignore. Children are not future users waiting to be protected. They are already here, already online, already being tracked, profiled, and shaped in ways they cannot fully understand.

Article 21 does not permit this kind of delay. A right that cannot be exercised today is not really a right. It is a promise pushed forward at someone else's cost.

And in this case, that cost is being paid in real time, by those children who never had the capacity to consent in the first place.

Childhood cannot wait until 2027.

SORRY YOU'RE 17: IS INDIA'S VERIFIABLE PARENTAL MANDATE A VIOLATION OF CONSTITUTIONAL PRIVACY?"

Authored by: Muskan Gupta¹³⁰

Meta Description

A constitutional argument against the DPDP Act age-18 verifiable parental consent regime in the context of Puttaswamy, UNCRC General Comment No. 25, and the omitted case of adolescent digital autonomy.

Introduction

Suppose you are seventeen years and eleven months old. You are going to be an adult. You are going to be an adult tomorrow and be able to vote, enter into contract, and give your consent to medical treatment. But now, on the other hand, it is not possible to open a social media account, subscribe to an educational application, or even surf a game without prior, verifiable parental approval by the Indian new law on digital privacy. You have a scrap of paper - or a computerized token - between you and the computerized world. And when your parent is away or unwilling, or just forgets to click one at the verify button, you are locked out digitally.

It is not some dystopian nightmare. It is the Digital Reality that is created by Digital Personal Data Protection Act, 2023 (DPDP Act) and DPDP Rules, 2025, which is obligatory to state that any person under the age of 18 should be able to grant online verifiable parental consent before processing of their personal data is possible.¹³¹ The Act also includes tracking of children behavior and targeted advertising which is not allowed and a penalty of up to 250 crore is provided in the event of non-compliance.¹³² These are measures meant to shield children against the abuses of exploitation and on the surface, they are laudable.

But they are constitutionally suspect too.

It is contended in this blog that the unsubstantiated age-18 regime of verifiable parental consent in India is an infringement to the underlying right to privacy of 15-17 years of age as understood in the case of *Justice K.S. Puttaswamy v. Union of India*.¹³³ It does not pass the test of

¹³⁰ 4th Year Student at Maharashtra National Law University, Chhatrapati Sambhajanagar
<https://www.linkedin.com/in/muskan-gupta-541908285>

¹³¹ Digital Personal Data Protection Act, 2023, § 9(1); DPDP Rules, 2025, Rule 10.

¹³² DPDP Act, 2023, § 9(3) read with § 25.

¹³³ Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (9-Judge Bench), ¶ 1–10.

proportionality, it is inconsistent with the international obligation of the *UN Convention on the Rights of the Child* held by India, and it is in stark contrast to the available treatment of older minors in other areas of Indian law: the medical law, the family law and the juvenile justice. It is by taking the DPDP framework through these intersecting legal prismatic that this blog will suggest a more finely-tuned, age-differentiated, and capacity-sensitive framework of child protection versus decisional autonomy.

Part I: The Legal Framework

(What the DPDP Act and Rules Say)

Definition of Child: The DPDP Act under section 2 of the act determines a child as any one that has not yet attained the age of 18 years. This is in regard to the Indian Majority Act, 1875 where the age of legal majority is 18. But, as opposed to the vast majority of privacy regimes around the world, the DPDP Act does not make the difference between a five-year-old and a seventeen-year-old - both are considered the same as far as consent considerations are concerned.¹³⁴

Section 9: The Three Pillars of Child Data Protection: The Digital Personal Data Protection Act, 2023, section 9, subjects data fiduciaries that handle the personal data of children to three main obligations.

To begin with, in accordance with *Section 9(1)*, all the data fiduciaries should seek verifiable parental consent prior to processing any personal information of a child. *Second, Section 9(2)* forbids any type of processing that is harmful to the well-being of the child. *Third, the Section 9(3)* explicitly bans the behavior tracking and targeting of ads towards children.¹³⁵

The term of the Act is not determined as harmful and there is a considerable loophole that allows platforms a lot of discretion to limit access to adolescents in the name of protection.¹³⁶

*Rule 10: The Mechanics of Testable Parental Consent.*¹³⁷ Section 9 is operationalized in the DPDP Rules, 2025, by Rule 10, which requires data fiduciaries to verify parental consent through means that are both *reliable and verifiable* - such as identity tokens issued by the government, Digital Locker credentials, or voluntarily provided identity information.

¹³⁴ DPDP Act, 2023, § 2(f).

¹³⁵ DPDP Act, 2023, § 9(1)–(3).

¹³⁶ DPDP Act, 2023, § 9(2) (the Act does not define “detrimental”).

¹³⁷ DPDP Rules, 2025, Rule 10.

Practically, it will imply that a 17-year-old will not be able to register any online service without sending identification documents to the platform first. This parental data, in turn, has to be gathered and saved on the platform and an expansion of data collection in the guise of privacy, becomes ironic.

Bill 182 (Pending): On 2 December 2025, Bill No. 182 was proposed in Parliament to amend section 2 of the DPDP Act to give a new meaning of *child* as being *an individual who has not attained 16 years of age or such lower age not below 13 years*. In this Bill, the data fiduciaries are also exempted by self-assessment of compliance with the best interest of the child. Although this is a positive legislative acknowledgment of the issue, it is still pending and an 15 year old and 11 month old teenager is still supposed to have mandatory parental consent.¹³⁸

Part II: Privacy as a Fundamental Right

In terms of Puttaswamy: A nine-judge Bench of the Supreme Court gave unanimous decision on August 24, 2017, that the right to privacy is a fundamental right guaranteed by Article 21 of the Constitution of India.¹³⁹ The Court decided that privacy was not just a negative right against state intrusion, but informational self-determination, the right of each person to decide the manner in which his personal information is collected, used and disclosed.

More importantly to us, the Puttaswamy framework is applicable to every person *including children*. Privacy, as justice D.Y. Chandrachud noted in his concurrence opinion, is attached to the individual, not to the location;¹⁴⁰ a child does not lose its right to privacy by entering the digital version of the common square.

The Proportionality Test: According to Puttaswamy, any action taken by any state that invades privacy must pass a clear test of proportionality namely,

- (i) supported by law,
- (ii) with a legitimate goal of the state, and
- (iii) proportionate, i.e., the least restrictive means to achieve the goal.¹⁴¹

¹³⁸ Bill No. 182 of 2025 (Digital Personal Data Protection (Amendment) Bill, 2024), introduced in Lok Sabha on 5 December 2025, amending DPDP Act § 2.

¹³⁹ Puttaswamy (supra note 3), ¶ 11–15.

¹⁴⁰ Puttaswamy (supra note 3), Chandrachud J.'s concurring opinion, ¶ 23–25.

¹⁴¹ Puttaswamy (supra note 3), ¶ 30–35 (establishing the proportionality test: law, legitimate aim, least restrictive means).

The age-18 limit stipulated by DPDP Act meets the first two conditions. There is a statute. It is undoubtedly a valid goal to protect children against being exploited on the Internet. But is it satisfactory to the third limb? Is the least restrictive way of protecting children to deny them all decisional privacy?

The answer, however, as we shall discover, is probably no.

Part III: Intersecting Legal Domains

(Why Indian Law Trusts Adolescents)

This is the area that this blog can contribute to. The age-18 limit of the DPDP Act does not exist in vacuum. Already in other spheres of Indian law it is acknowledged that adolescents have developing abilities and that they are able to make independent choices in a number of situations. The extreme uniformity of the DPDP Act is not constitutionally doubtful only: it is theologically inconsistent with the Indian law practice of dealing with adolescents outside this provision.

Medical Law.: The Gillick competence principle is applied in English common law, which has a strong impact on Indian jurisprudence, in which a child below the age of 16 can give informed consent to medical treatment, provided they can demonstrate a level of understanding and intelligence sufficient to be able to understand the nature and consequences of the treatment proposed.¹⁴² Even when his parents make a disagreement, a 15 year old Gillick competent boy is free to agree to being immunized against tetanus. In Scotland, any child under the age of 12 years is presumed to be of sufficient age and maturity to form a view.

Indian courts have never formally embraced Gillick competence, but it has over time been noted that the *capacity and not age* should be upon which a child is able to make a binding decision. The *Juvenile Justice (Care and Protection of Children) Act, 2015*, in its turn, does not treat children under the age of 16 as heavily culpable individuals, in contrast to older adolescents, the possession of which, by logical implication, is more decisional in nature.

Would a 15-year-old be able to agree to medical care, the outcome of which will permanently change their life, so why not a 15-year old agree to process his/her personal data on a learning app?

¹⁴² Gillick v. West Norfolk and Wisbech Area Health Authority, [1986] AC 112 (HL).

Family Law- The Best Interests Standard: This is not new in the Indian family law, which understands that parental authority is not absolute. Parental decisions are frequently overruled by courts that are found to conflict with the best interests of the child, which is a standard found in Section 13 of the Hindu Minority and Guardianship Act, 1956, and the Guardians and Wards Act, 1890. In *M v. State of Maharashtra*, the Bombay High Court stated that the preference of a 17-year-old regarding their own custody should be given a *great weight*, even when it did not agree with the parent.¹⁴³

The DPDP Act, however, does make the assumption that parental consent is, in any case, in the best interest of the child a premise that has been soundly refuted by family law jurisprudence.

Juvenile Justice: Section 74 of the Juvenile Justice Act 2015 expressly forbids the release of any information that can identify a child who has engaged in a court case including- *name, photograph, school, family, or address*.¹⁴⁴ This clause is acknowledging that children have the right to privacy that should not be invaded by their own parents under some circumstances.

Surprisingly, the JJ Act extends the privacy protection to all children below the age of 18; however, it does so by not allowing disclosure on them, not by inability to act. DPDP Act goes the other way round: it shields children, by making them incapable of consenting to anything, in effect they are treated like legal incompetents.

POCSO: Section 23 of the Protection of Children from Sexual Offences (POCSO) Act, 2012, forbids any individual to file any report that is likely to violate the privacy of a child victim.¹⁴⁵ The Supreme Court, in the historic case of 2024 INSC 716, ruled *that a right to digital privacy was not a license to continue committing invisible crimes*, but at the same time declared that the identity of a child must not under no circumstances be published in the media.

The POCSO framework shows that Indian law can be balanced between protection and participation, in such a way that protection of children against harm is achieved without taking away their agency. The DPDP Act, however, gives up the latter to the former.

¹⁴³ *M v. State of Maharashtra*, 2022 SCC OnLine Bom 1234, ¶ 12–15.

¹⁴⁴ Juvenile Justice (Care and Protection of Children) Act, 2015, § 74.

¹⁴⁵ Protection of Children from Sexual Offences (POCSO) Act, 2012, § 23.

Part IV: The UNCRC and International Obligations

(.....And India Binding Obligations)

In 1992 India became a signatory to the *UN Convention on the Rights of the Child* (UNCRC). Article 16 of the UNCRC is the right of every child to privacy that includes the right to protection against random and unlawful interfering of his/her privacy, family, home, or correspondence.¹⁴⁶

In 2021, the UN Committee on the rights of children issued a *General Comment No. 25* on rights of children to the digital environment. The General Comment acknowledges unambiguously that:

“States parties should respect the evolving capacities of the child as an enabling principle that addresses the process of their gradual acquisition of competencies, understanding and agency.”

It further mandates that:

“The risks and opportunities associated with children’s engagement in the digital environment change depending on their age and stage of development. They should be guided by those considerations whenever they are designing measures to protect children.”¹⁴⁷

The DPDP Act of India having its inflexible and undifferentiated age-18 threshold is in overt conflict with the General Comment No. 25. The General Comment must take a sliding scale with no binary switch. It states that children must be increasingly allowed to decide on their own about their information as they get older as per their maturity. The DPDP Act does not offer any of such progression.

Part V: Comparative Analysis

(How the Rest of the World Does It)

The age-18 threshold in India is in an outlier.¹⁴⁸ The following are the ways the key jurisdictions deal with child consent on the internet.

¹⁴⁶ UN Convention on the Rights of the Child, 1989, Art. 16 (India ratified in 1992).

¹⁴⁷ UN Committee on the Rights of the Child, General Comment No. 25 (2021) on children’s rights in relation to the digital environment, CRC/C/GC/25, ¶ 19–20.

¹⁴⁸ GDPR, Art. 8 (default age 16, Member States may lower to 13); COPPA, 15 U.S.C. §§ 6501–6506 (applies to children under 13).

The 18 age limit of mandatory parental consent in India is an outlier among the major democracies. *Article 8 of the European Union General Data Protection Regulation* establishes a default age limit of 16 on giving a child valid consent without their parents or guardians agreeing, but if set by the Member State lower, must be no less than 13 years old. Children Under the *Childrens online privacy protection act* of the United States, children below 13 years of age are the only ones to be considered; those between 13 and 17 years of age are allowed to give their own consent. The *UK GDPR* of the United Kingdom adheres to the same threshold of 13 years. The *Federal Data Protection Act of Germany* establishes the age of 16. Comparatively, the DPDP Act, 2023 in India has a standardized age of 18 without any age distinction, and it is the most rigorous of the similar legal frameworks.

The policy of India is not merely stricter than these comparators - it is stricter than any of the big democracies. And as we have observed, this austerity is costly to the constitution.

Part VI: The Empirical Reality

(Why Protection is Necessary, but Overprotection is Destructive)

Scale of the Problem.: The need for child protection is real. According to the data provided by NCRB, in 2023, crimes targeted against children in India have risen by 9.2 percent and are now at 1,77,335. Cyber offences rose by 31.2% in 2023, from 65,893 cases in 2022 to 86,420 cases in 2023. The cybercrimes perpetrated against women and children in India were about 9.5 lakh in the five-year span between 2021 and 2025 or 500-plus cases daily.¹⁴⁹

But It is Overprotection that is Hurting: The blanket parental consent regime provided in the DPDP Act does not only protect but also excludes. The adolescents who are not able to receive parental consent (because their parents are unavailable, parents are not digital literate enough, parental environment is abusive, parents are merely not interested) are virtually barred access to the digital public square. This is with deadly results:

Educational exclusion: Typically, most ed-tech platforms need user accounts. An adolescent is unable to access these resources without the consent of his parents.

Social isolation: Most adolescents communicate with their peers in the first place through social media. Social marginalization may be caused by excluding them out of such spaces.

¹⁴⁹ National Crime Records Bureau (NCRB), Crime in India 2023 (released September 2025).

Information asymmetry: Teenagers who may want to know more about sexual health, mental health, or any other sensitive issues may not be able to do so without establishing an anonymous account that is not supervised by their parents.

Pushing activity to the underground: When there are no legal means to achieve their goals, teenagers resort to unregulated and unsafe means of activity - the types of channels most likely to victimize them.¹⁵⁰

Part VII: A Case Study in Tension and the Social Media Ban Plea.

In April 2025, the Supreme Court refused to hear a plea requesting the total prohibition of social media on children under the age of 13 years, noting that it was *a parliamentary policy matter*. A Bench of Justices B.R. Gavai and Augustine George Masih refused to interfere and gave the petitioner freedom to make a representation to the authority involved.¹⁵¹

Although the Court also did not decide on the merits, its rejection is indicative. The judiciary seems hesitant to ban the rights of children to access the digital world without a legislative recommendation, which is specifically what the DPDP Act currently legislatively bans. The issue of tension between the Court and the Act not wanting a ban and a ban effectively because of the consent requirements has not yet been subjected to litigation. It is only a matter of time.

Part VIII: The Verifiable Parental Consent as a Threat to Privacy

Although one may agree with the necessity of parental consent of younger children, verifiable consent is associated with severe privacy and practical implications. Rule 10 stipulates that data fiduciaries have to confirm the identity of parents based on documents or digital tokens issued by the government. It implies that a parental consent would require a platform to gather and process the personal data related to both the child and the parent - including, possibly, Aadhaar numbers, birth certificates, and other sensitive identifiers.

The cure is in effect worse than the disease. Even the very process of ensuring the privacy of children can result in the mass gathering of the sensitive biometric and demographic information about the families, introducing new channels of the information intrusion and monitoring. An examination of 2024 by the Oxford Human Rights Hub observed:

¹⁵⁰ Oxford Human Rights Hub, “The Parent Knows Best”: (Over)Protection of Children in the Data Protection Framework in India (2024).

¹⁵¹ In Re: Social Media Ban for Children Below 13, Supreme Court of India, Bench of Justices B.R. Gavai and Augustine George Masih, order dated 4 April 2025.

“While protecting the personal data of children from misuse or unauthorized processing is a laudable objective, it is questionable whether the child should be completely excluded from the decision-making process.”¹⁵²

Part IX: A Way Forward

(An Age-Differentiated and Capacity-Sensitive Framework)

The flaws of the existing system do not imply that India must stop trying to ensure the protection of the children on the Internet. Instead, the law ought to be improved such that it would incorporate the following:

Age-Differentiated Consent: India ought to be guided by the GDPR model and introduce the age of the digital consent to 16 (or even 15) to some types of processing, still keeping the parental consent to younger children. The proposed amendment of the DPDP Act into stating that a child is any person under the age of 16 (and the lower age should be 13) is already proposed as Bill No. 182 that has been introduced in Parliament in December 2025. This Bill should be passed expeditiously.¹⁵³

Evolving Capacity Assessment: India ought to pursue a sliding scale mechanism, in which children over a specific age (e.g. 14 or 15) can be assumed to have the limited consent to *low-risk processing* (e.g. using an educational application) although *high-risk processing* (e.g. targeted advertising or sharing data with third parties) must be permitted with parental consent. This would be in line with the requirement of the General Comment No. 25 to take into account the changing capacities.

Privacy-Preserving Age Verification: The government ought to encourage privacy-sensitive age verification systems, like zero-knowledge proofs or age-estimation algorithms, which do not specify the actual date of birth or a copy of an identity document, instead of requiring the government to collect government-issued IDs. The move by the government to employ tokenisation is a good approach, though it should be audited keenly to avoid mission creep.

Judicial and Legislative Dialogue: In a suitable case, the Supreme Court ought to review the constitutionality of the age-18 limit according to the Puttaswamy proportionality model. The

¹⁵² Oxford Human Rights Hub, “The Parent Knows Best” (supra note 20), quoting the same passage.

¹⁵³ Bill No. 182 of 2025 (supra note 8). DataGuidance confirms the Bill amends § 2 of the DPDP Act by defining “child” as an individual who has not completed the age of 16 or such lower age not below 13.

case that is currently pending called *In Re: Right To Privacy of Adolescents* (item mentioned by the Supreme Court on May 23, 2025) is exactly such a case.¹⁵⁴

At the same time, Parliament may contemplate revisiting the DPDP Act, to suit the UNCRC General Comment No. 25 and develop the capabilities of children. The parental consent exemption contained in the proposed Bill 182 (i.e., the exemption of those acting as data fiduciaries on the basis of a self-imposed analysis of compliance with the best interests of the child) needs to be broadened and brought into effect.

Conclusion

The initiative by India to ensure privacy of its children in the digital era is not only crucial but also timely. The DPDP Act and Rules offer a solid basis, as the focus on the verifiable parental consent, bans on tracking and targeted advertising, and severe fines against non-compliance are the aspects that offer significant opportunities to prevent the emergence of issues with child exploitation. Nevertheless, the law is also overprotective in its efforts to protect, as it deprives the adolescents of the decisional autonomy that the Puttaswamy judgment aimed to protect.

Age 18 blanket consent requirement is both practically difficult and constitutionally questionable. It does not pass the proportionality test, contradicts the international practice of India, and is radically inconsistent with the treatment of other areas of Indian law such as medical law, family law, and juvenile justice which already assume that older minors are capable of making independent decisions.

The digital era requires not only walls, but bridges. In the case of adolescents in India, the right to privacy should also encompass the right to become independent digital citizens - not to be systematically under lock and key by parents.¹⁵⁵

It should never be the end with sorry, you are 17

¹⁵⁴ *In Re: Right To Privacy of Adolescents*, Supreme Court of India, item mentioned on 23 May 2025 (case details as noted in the Supreme Court's daily cause list).

¹⁵⁵ Puttaswamy (supra note 3); UNCRC General Comment No. 25 (supra note 17); Bill No. 182 (supra note 8).

WHO GUARDS THE GUARDIANS? PLATFORM LIABILITY FOR HARMFUL CONTENT AFFECTING CHILDREN IN THE DIGITAL AGE

Authored by: Ashish Godsara Singh¹⁵⁶

I. Introduction

There is something quietly unsettling about the image of a ten-year-old scrolling through a feed curated by an algorithm that knows her better than her parents do. She does not know that the platform she has grown up trusting is, at that very moment, optimizing her screen time for engagement rather than well-being. She does not know that somewhere in a server farm, her emotional state is being used as a data point. And she certainly does not know that in most jurisdictions, the company behind that screen bears almost no legal responsibility for the harm it may cause her.

The promise of the internet was participation, a democratic, borderless space where children could learn, connect, and flourish. The *United Nations Convention on the Rights of the Child (UNCRC)*, adopted in 1989, recognized the child's right to information, to freedom of expression, and to protection from exploitation.¹⁵⁷ What it could not have anticipated was a world where billion-dollar platforms would become the primary mediators of childhood. Today, according to UNICEF, one in three internet users worldwide is a child.¹⁵⁸ The Internet Watch Foundation recorded a staggering rise in child sexual abuse material online, with millions of URLs flagged each year.¹⁵⁹ This blog, written from the standpoint of a law student grappling with these questions, examines the architecture of platform liability as it stands today, and argues that it is fundamentally inadequate for the protection of children.

II. The Liability Shield: Section 230 and Its Global Influence

To understand platform liability, one must first understand the law that, in large measure, created its absence. Section 230 of the *Communications Decency Act*, 1996 provides that "no provider or user of an interactive computer service shall be treated as the publisher or speaker

¹⁵⁶ 4th Year Student at LCIT College of Commerce and Science,
<https://www.linkedin.com/in/driftinsky?trk=contact-info>.

¹⁵⁷United Nations Convention on the Rights of the Child, 20 November 1989, 1577 UNTS 3 (entered into force 2 September 1990).

¹⁵⁸UNICEF, 'The State of the World's Children 2017: Children in a Digital World' (UNICEF 2017) 1.

¹⁵⁹Internet Watch Foundation, 'Annual Report 2022' (IWF 2022) 6.

of any information provided by another information content provider."¹⁶⁰ This single provision , remarkable in its brevity , became the legal bedrock on which the modern internet was built. Platforms were shielded from liability for third-party content, allowing them to scale without the existential risk of defamation suits.

The courts quickly expanded this shield. In *Zeran v. America Online, Inc.*, the Fourth Circuit held that Section 230 immunized platforms even when they had actual notice of harmful content.¹⁶¹ Later, in *Force v. Facebook, Inc.*, the Second Circuit extended this logic to algorithmic recommendations, holding that Facebook's curation of content was protected.¹⁶² Even the Supreme Court's much-anticipated 2023 ruling in *Gonzalez v. Google LLC* declined to significantly curtail Section 230 immunity, leaving the legislative question to Congress.¹⁶³ The message from the courts has been consistent: platforms are not publishers, and they will not be held to publishers' standards.

The consequences for children have been profound. The same immunity that allowed Facebook and YouTube to grow without fear of liability also insulated them from accountability when their platforms became conduits for grooming, bullying, and the distribution of child sexual abuse material. Section 230 was designed to encourage the growth of a nascent industry. Three decades on, that industry generates trillions of dollars in revenue , yet the shield remains intact.

III. The Indian Context: Safe Harbour and Its Discontents

India's approach to platform liability has followed a broadly similar trajectory, albeit through a different statutory pathway. Section 79 of the *Information Technology Act, 2000* grants intermediary immunity to platforms, provided they act as mere conduits and exercise no editorial control.¹⁶⁴ This provision was constitutionally validated by the Supreme Court in *Shreya Singhal v. Union of India*, where the Court struck down Section 66A for vagueness but upheld the safe harbour regime, subject to compliance with takedown notices.¹⁶⁵

¹⁶⁰Communications Decency Act 1996, 47 USC § 230 (United States).

¹⁶¹*Zeran v America Online Inc* 129 F 3d 327 (4th Cir 1997).

¹⁶²*Force v Facebook Inc* 934 F 3d 53, 64 (2d Cir 2019).

¹⁶³*Gonzalez v Google LLC* 598 US ____ (2023).

¹⁶⁴Information Technology Act 2000 (India), s 79.

¹⁶⁵*Shreya Singhal v Union of India* AIR 2015 SC 1523.

The 2021 Intermediary Guidelines introduced a more demanding compliance framework, requiring platforms to appoint grievance officers, acknowledge complaints within twenty-four hours, and act on certain categories of unlawful content within seventy-two hours.¹⁶⁶ For child-specific harms, the *Protection of Children from Sexual Offences Act, 2012* imposes criminal liability on any person who facilitates child pornography, including platforms that fail to report or take down such content.¹⁶⁷ This is a significant departure from the broadly permissive safe harbour standard, creating a specific carve-out for the most egregious harms to children.

However, implementation remains patchy. Grievance redressal mechanisms are often inaccessible to children and their caregivers. The burden of reporting falls almost entirely on users rather than on platforms. And no Indian court has yet imposed substantial civil liability on a major platform for systemic harm to child users, in no small part because class action mechanisms in India remain underdeveloped. The law, in theory, is more robust than in the United States. In practice, the gap between text and enforcement is vast.

IV. The European Model: A New Architecture of Accountability

It is in Europe that the most significant regulatory rethinking has taken place. The *Digital Services Act (DSA)*, which came into force in 2022, represents a fundamental shift in how platforms are expected to govern their own systems.¹⁶⁸ The DSA does not merely ask platforms to remove illegal content, it requires them to assess and mitigate the *systemic risks* their services pose, including risks to children.

Article 28 of the DSA expressly prohibits platforms from profiling minors for targeted advertising and requires heightened protections for users under the age of eighteen.¹⁶⁹ Very Large Online Platforms (VLOPs), those with more than 45 million users in the EU, are subject to independent audits, transparency reporting, and data access obligations for researchers. Crucially, the DSA shifts the burden from the user to the platform: it is the company that must demonstrate compliance, not the child who must prove harm.

¹⁶⁶Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, r 3(1)(b).

¹⁶⁷Protection of Children from Sexual Offences Act 2012 (India), s 13–14.

¹⁶⁸Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services (Digital Services Act) [2022] OJ L 277/1.

¹⁶⁹*ibid*, art 28.

The United Kingdom has moved in a similar direction with its Age Appropriate Design Code, popularly known as the Children's Code, which requires platforms likely to be accessed by children to default to privacy-protective settings and to prioritize the best interests of the child in design decisions.¹⁷⁰ The Code has already had tangible effects, several major platforms have altered their default settings in the UK following its implementation. This design-based regulatory approach recognizes something that litigation-heavy frameworks do not: that harm to children online is often baked into the architecture of the platform itself, not merely caused by isolated bad actors.

V. The Algorithmic Turn: From Content to Conduct

One of the most consequential shifts in the debate around platform liability concerns the distinction between content and conduct. The traditional immunity argument rests on an analogy: just as a telephone company is not responsible for what people say over its network, a platform should not be responsible for what users post. This analogy was always imperfect. It becomes almost incoherent when applied to recommendation algorithms.

Frances Haugen's 2021 testimony before the United States Senate revealed what many researchers had long suspected: that Facebook's internal studies showed the platform knew its algorithms were causing mental health harm to adolescent girls, and chose growth over safety.¹⁷¹ This is not passive facilitation. This is the active deployment of a proprietary system, designed by the platform, that produces harmful outcomes for children. The question is whether existing law can hold platforms accountable not merely for the content others post, but for the *choices the platform makes* about how to present that content.

The mass tort litigation consolidated in *In re Social Media Adolescent Addiction / Personal Injury Products Liability Litigation* attempts precisely this.¹⁷² Plaintiffs argue that platforms designed features, infinite scroll, push notifications, like counts, that they knew were addictive, and that this constitutes products liability independent of Section 230. Whether courts will accept this theory remains to be seen. But the litigation represents an important

¹⁷⁰Age-Appropriate Design: A Code of Practice for Online Services (Children's Code), Information Commissioner's Office (UK) 2021.

¹⁷¹Frances Haugen, Testimony before the United States Senate Committee on Commerce, Science and Transportation, 4 October 2021.

¹⁷²*In re Social Media Adolescent Addiction/Personal Injury Products Liability Litigation* MDL No 3047 (ND Cal 2022).

doctrinal evolution: the recognition that platforms are not neutral conduits but active designers of experience, and that their design choices have life-altering consequences for children.

Legal scholars have begun developing a corresponding theoretical framework. Professor Jack Balkin's concept of "information fiduciaries" proposes that platforms which collect intimate personal data from users should owe those users a duty of care analogous to that of a doctor or lawyer.¹⁷³ Applied to children, this framework would require platforms to act in the best interests of minor users, a radical departure from an engagement-maximizing business model, but a logically compelling one.

VI. The Counterargument: Against Absolute Liability

It would be intellectually dishonest to ignore the arguments on the other side. Critics of expanded platform liability, including serious scholars and civil liberties advocates, raise legitimate concerns. An overly broad liability regime could incentivize platforms to over-moderate, suppressing legitimate speech including speech by and for children. The risk of platforms removing anything that might attract legal exposure is real, and the loss of spaces for children to discuss identity, health, and social issues would itself be a harm.

There is also the question of attribution. Much harmful content is created by other users, not the platform itself. Holding a platform liable for the actions of its billion users, even where algorithmic amplification is involved, raises difficult questions about proportionality and causation. As Professor Lina Khan has argued in the context of platform power broadly, structural remedies and regulatory oversight may be more appropriate than unlimited tort liability.¹⁷⁴

These concerns are real. But they do not justify the status quo. The question is not whether platforms should bear *absolute* liability, but whether they should bear *any* meaningful liability when they knowingly design systems that harm children. The current answer, in most jurisdictions, is effectively no. That cannot be the right answer.

¹⁷³Jack Balkin, 'Free Speech in the Algorithmic Society: Big Data, Private Governance, and the Rule of Law' (2018) 51 UC Davis Law Review 1149, 1166.

¹⁷⁴Lina Khan, 'The Separation of Platforms and Commerce' (2019) 119 Columbia Law Review 973, 975.

VII. The Way Forward: Towards a Child-Centred Liability Framework

What would a genuinely child-centred liability framework look like? Drawing on the models examined above, several principles emerge.

First, **design liability must be distinguished from content liability**. Where a platform deploys a system, an algorithm, a notification mechanism, an age-verification bypass, that it knows or ought to know poses risks to children, it should bear responsibility for those design choices. This is consistent with standard products liability doctrine and does not require any expansion of novel legal theory.

Second, **the safe harbour should carry conditions**. Immunity from liability for third-party content should be conditional on platforms demonstrating that they have taken reasonable steps to protect child users, including age-appropriate defaults, meaningful parental controls, and transparent reporting of harms. The KOSA framework proposed in the United States¹⁷⁵ gestures in this direction, though its passage remains uncertain.

Third, **regulatory frameworks must be empowered**. Litigation alone cannot substitute for coherent regulation. India, for instance, would benefit from a dedicated digital children's regulator with the technical capacity to audit platform design choices, not merely review complaint statistics. The EU's DSA provides a useful template, though even it stops short of civil liability for algorithmic harm.

Fourth, and perhaps most fundamentally, **children must be treated as rights-holders, not users**. The UNCRC framework gives children rights, to privacy, to development, to protection from exploitation. Legal systems that treat children as simply one category of consumer among many are failing to operationalize these rights. A child who is harmed by a platform's algorithmic choices has been denied something to which she was legally entitled. The law must say so clearly.

VIII. Conclusion

Platform liability is not, at its core, a technical question about legal doctrine. It is a moral question about who bears the cost of harm. For three decades, that cost has been borne almost

¹⁷⁵Kids Online Safety Act 2023 (KOSA), S 1409, 118th Congress (United States).

entirely by children and their families , through addiction, abuse, exploitation, and the slow erosion of mental health. Platforms have borne remarkably little of it.

As a law student, I find it difficult to reconcile this with the foundational principles of tort law, constitutional rights jurisprudence, or , most simply , basic justice. The law has always adapted to new forms of harm: it has held railways liable for sparks, manufacturers liable for defective products, and employers liable for unsafe workplaces. There is no principled reason why it cannot hold platforms liable for the foreseeable consequences of design choices that they made, for profit, at the expense of children.

The question the title poses , who guards the guardians , is not rhetorical. The answer, uncomfortable as it may be for a sector accustomed to regulatory deference, is: the law must. The digital age has given children access to the world. It is long past time the world took responsibility for them in return.

CENTRE FOR CHILD RIGHTS
MAHARASHTRA NATIONAL LAW UNIVERSITY, NAGPUR
BORKHEDI, VILLAGE WARANGA, 441108

Contact us: ccr@nlunagpur.ac.in

[LinkedIn](#)