RESEARCH PAPER

Cyberbullying of children in India: constitutional foundations, legislative gaps, and a layered protective architecture

Sneha Bhatt[1*], Dr. Vinod Kumar[2]
[1*]Research Scholar, Amity Law School, Amity University Rajasthan | Email: snehabhatt1998@gmail.com | ORCID: 0009-0006-5726-8165 (Corresponding Author)
[2]Associate Professor, Amity Law School, Amity University Rajasthan | Email: vkumar@amity.edu | ORCID: 0000-0001-5367-8681

Abstract:
Cyberbullying of minors constitutes a structurally distinct form of harm that defies the spatial and temporal limits of conventional bullying. India, with over 600 million internet users and a rapidly digitising youth demographic, lacks a coherent, child-specific legislative response to digital harassment. This article makes three original contributions: (i) it establishes a constitutionally grounded conception of cyberbullying harm anchored in *Justice K.S. Puttaswamy v. Union of India* (2017) and Article 21; (ii) it performs a systematic doctrinal analysis of the existing Indian statutory framework, identifying specific interpretive failures in the application of the Bharatiya Nyaya Sanhita (BNS) 2023, the Information Technology Act 2000, and POCSO 2012 to cyberbullying fact patterns; and (iii) it proposes a theoretically grounded, institutionally realisable three-tier protective architecture that addresses platform accountability, legislative reform, and restorative victim remedies. The study employs a doctrinal comparative legal methodology. Primary sources - statutes, constitutional provisions, and Indian and foreign judicial decisions - are analysed using the standard tools of legal interpretation. Comparative jurisdictions (EU, UK, Australia, South Korea) were selected on the basis of functional analogues to the Indian regulatory problem, assessed against three criteria: constitutional compatibility, institutional transferability, and empirical effectiveness. Psychological literature is surveyed to establish the harm threshold relevant to constitutional analysis. Indian law is symptomatically inadequate. The BNS 2023, IT Act 2000, and POCSO 2012 collectively fail to provide a coherent definitional, institutional, or remedial response to cyberbullying. The constitutional framework under Articles 14, 19, and 21 - as expanded in *Puttaswamy* - provides an underutilised but legally defensible foundation for child-specific online protection legislation. Comparative models, particularly the UK Online Safety Act 2023 and the EU Digital Services Act 2022, offer transposable elements, subject to identified constitutional constraints. A dedicated Child Online Safety Act for India is constitutionally justifiable, institutionally feasible, and normatively required. Platform impunity, the absence of victim-accessible civil remedies, and the failure to locate cyberbullying within the constitutional guarantee of dignitary rights are the three structural failures most urgently requiring correction.

Keywords: *cyberbullying; children; right to privacy; right to dignity; Puttaswamy; IT Act 2000; BNS 2023; POCSO; platform liability; Digital Services Act; comparative child protection law; doctrinal legal research*
How to cite this article: Bhatt S, Kumar V. Cyberbullying of children in India: constitutional foundations, legislative gaps, and a layered protective architecture. Int J Drug Deliv Technol. 2026;16(55s): 241-251. DOI: 10.25258/ijddt.16.55s.27

1. Introduction: the problem and its misdiagnosis

The literature on bullying has, for three decades, been organised around a set of assumptions that the digital environment has rendered obsolete. Olweus's foundational definition - intentional, repeated harmful behaviour carried out by an individual or group against a victim who cannot easily defend themselves - was developed in the context of the Norwegian school system in the 1970s and 1980s.[1] It encodes spatial and institutional assumptions: bullying occurs in bounded settings, during bounded hours, between identifiable actors, and ends when the child leaves the school gate. None of these assumptions survives the architecture of the contemporary internet.

The child who is targeted online in 2025 does not escape harassment at 3 p.m. The torment follows her into her bedroom, vibrates in her pocket at 2 a.m., and - because digital content is permanent, replicable, and addressable to unlimited audiences - may persist long after the immediate relationship that generated it has ended. This is not bullying in a new medium. It is a qualitatively different form of harm that requires a qualitatively different legal response.[2]

India's legislative response has not kept pace with this analytical recognition. The regulatory framework governing digital harassment of children remains a patchwork of provisions drafted for other purposes: cybercrime against adults (IT Act 2000), sexual offences against children (POCSO 2012), and generalised criminal intimidation (BNS 2023). No provision defines cyberbullying. No institution has primary responsibility for responding to it. No civil remedy exists for its victims. The result is a protection gap that is not merely administrative but constitutional: children possess, under Article 21 as interpreted in *Justice K.S. Puttaswamy v. Union of India*,[3] a fundamental right to privacy and dignity that the state is obligated to protect - and is

systematically failing to protect - against private digital harassment.

This article makes three original contributions to the existing literature. First, it grounds the legal analysis of cyberbullying in the constitutional framework established by *Puttaswamy*, an anchor that the existing Indian scholarship on cyberbullying has not systematically developed. Second, it performs a section-level doctrinal analysis of the BNS 2023, IT Act 2000, and POCSO 2012, identifying specific interpretive barriers to their application to cyberbullying fact patterns and assessing whether purposive construction can overcome them. Third, it proposes a three-tier protective architecture - constitutional, legislative, and institutional - that is evaluated against the criteria of constitutional justifiability, institutional feasibility, and empirical effectiveness.

The paper proceeds as follows. Part II declares the methodology. Part III establishes the definitional and typological framework. Part IV surveys the psychological evidence on harm, with particular attention to the constitutional harm threshold. Part V analyses the Indian legal framework in detail. Part VI examines comparative models. Part VII develops the protective architecture. Part VIII concludes.

2. Methodology

This study employs a doctrinal comparative legal methodology. Doctrinal analysis - the systematic examination of legal rules through the interpretation of primary sources including statutes, constitutional provisions, and judicial decisions - is the appropriate methodology for a study whose central research questions are: (a) whether existing Indian law adequately addresses cyberbullying, and (b) what legislative and institutional reforms are constitutionally permissible and normatively required.[4] The method is not descriptive; it is evaluative. The doctrinal analysis is conducted against a normative standard derived from the constitutional guarantee of dignitary rights under Article 21 and the international obligations under the UN Convention on the Rights of the Child (UNCRC), to which India is a party.[5]

The comparative analysis surveys four jurisdictions: the European Union (Digital Services Act 2022), the United Kingdom (Online Safety Act 2023), Australia (Online Safety Act 2021), and South Korea (Act on Promotion of Information and Communications Network, as amended). These jurisdictions were selected against three criteria. First, *functional analogy*: each jurisdiction has grappled with the same regulatory problem of platform accountability for child-directed digital harm and has produced a legislative response. Second, *constitutional compatibility*: each jurisdiction's constitutional framework was assessed for its analogical relevance to the Indian guarantee of fundamental rights, particularly with respect to the permissible scope of expression restrictions and platform obligations. Third, *empirical evidence*: jurisdictions whose legislative reforms have generated evaluative evidence - however preliminary - were preferred over those whose legislation is too recent to assess.[6]

Psychological literature is surveyed in Part IV not as a primary source of legal doctrine but as evidence relevant to the constitutional question of harm severity: whether cyberbullying causes harm of a nature and degree that engages the state's positive obligation under Article 21 to protect the right to life and dignity.

The study does not employ empirical socio-legal methods (surveys, interviews, or content analysis), and its findings are accordingly limited to legal analysis. The absence of reliable India-specific empirical data on cyberbullying prevalence - a gap noted below - is itself a finding relevant to the reform proposals in Part VII.

3. Definition and typological framework

3.1 The definitional contest

No scholarly consensus exists on the definition of cyberbullying. The most widely cited definition - Tokunaga's (2010) synthesis - requires intentionality, repetition, and a power imbalance.[7] This definition has been subjected to sustained criticism on two grounds that are directly legally relevant.

The first is the repetition requirement. Vandebosch and Van Cleemput (2008) argued that the repetition requirement, which reflects the iterative nature of physical bullying, is ill-adapted to the digital environment, where a single act - posting a morphed intimate image, creating a fake social media profile - can cause harm that replicates itself through the viral sharing behaviour of third parties without any further action by the perpetrator.[8] Menesini and Nocentini (2009) proposed replacing repetition with *publicness* as the relevant criterion, arguing that the reachability of an unlimited audience is the distinctive amplifying feature of digital harm.[9] This article adopts a hybrid position: repetition remains relevant as an indicative factor for less severe acts, but single-incident conduct causing severe or irreversible harm - particularly involving non-consensual intimate imagery or CSAM - should fall within the definition regardless of repetition.

The second is the power imbalance requirement. Traditionally understood as physical size, social status, or group membership, power imbalance in digital contexts is better understood as *information asymmetry*: the perpetrator possesses compromising information, images, or access that the victim cannot easily neutralise. The anonymity available to online perpetrators exacerbates this asymmetry by denying

victims the ability to identify, report, or counter their harassers.[10]

For the purposes of this article, cyberbullying is defined as: *intentional conduct carried out through electronic means that causes or is reasonably likely to cause psychological, reputational, or dignitary harm to a minor, where the perpetrator has a structural advantage over the victim arising from anonymity, information control, social influence, or technical access.* This definition removes the repetition requirement as a threshold element while retaining it as an aggravating factor, and reframes power imbalance in terms appropriate to digital environments.

3.2 Typological taxonomy

Type	Operational definition	Legal characterisation (Indian law)
Harassment	Repeated offensive, threatening, or distressing messages directed at a victim	BNS s. 351 (criminal intimidation); IT Act s. 66A (struck down); potential IPC analogue under BNS s. 352
Denigration	Posting false, damaging, or humiliating information about a victim	BNS s. 356 (defamation); IT Act s. 66C if impersonation involved
Impersonation	Creating fake profiles or accounts to damage a victim's reputation	IT Act s. 66D (cheating by impersonation); BNS s. 318
Outing and trickery	Sharing confidential personal information without consent	Privacy violation under Art. 21 post-Puttaswamy; no specific statutory provision
Exclusion	Deliberate social ostracisation through digital means	No statutory coverage; potential psychological harm trigger
Cyberstalking	Persistent surveillance, monitoring, or threatening communication	BNS s. 78 (stalking); IT Act s. 66A (struck down); gap in electronic surveillance context
Non-consensual intimate imagery (NCII)	Distributing or threatening to distribute intimate images without consent	POCSO ss. 13–15 if victim is minor; IT Act s. 67; BNS s. 77
Sextortion	Coercing a minor to produce or share sexual content under threat	POCSO s. 11(iv); IPC s. 383 (extortion) now BNS s. 308; overlap provisions

Table 1. Cyberbullying typology adapted from Willard (2007) with Indian legal characterisation by the author. Struck-down provisions noted for historical context only.

4. Psychological harm and the constitutional harm threshold

4.1 The clinical evidence

The clinical literature on cyberbullying's psychological consequences is now substantial enough to treat its core findings as established. A meta-analysis by Kowalski et al. (2014), synthesising 131 studies, found that cyberbullying victimisation was significantly associated with depression, anxiety, low self-esteem, somatic symptoms, and academic disengagement, with effect sizes generally exceeding those reported for traditional bullying.[11] Hinduja and Patchin (2010), in a study of 1,963 adolescents aged 10–18, found that cyberbullying victims were approximately 1.9 times more likely to have attempted suicide than non-victims - a finding since replicated across multiple national contexts, though with varying effect sizes.[12]

A critical neurological dimension is provided by Eisenberger et al. (2003), whose neuroimaging research demonstrated that social exclusion activates the same anterior cingulate cortex regions implicated in the experience of physical pain.[13] The legal relevance of this finding is considerable: it challenges the implicit assumption in tort and criminal law that psychological harm is categorically less severe than physical harm, an assumption that undermines the legal response to cyberbullying across multiple jurisdictions.

Three features of digital harm amplify these psychological effects beyond the levels recorded for conventional bullying. First, the absence of temporal and spatial sanctuary - the victim cannot leave the bullying environment - produces chronic hypervigilance associated with persistent cortisol elevation and sleep disruption.[14] Second, the publicness of digital harm amplifies shame through the mechanism of anticipated audience: the victim experiences humiliation not merely in the presence of actual witnesses but in the presence of a

potentially unlimited imagined audience, a phenomenological experience that significantly prolongs psychological recovery.[15] Third, the permanence of digital content means that humiliating material may resurface unpredictably, extending psychological harm across years rather than the bounded duration of a school year.[16]

4.2 Constitutional relevance: the harm threshold under Article 21

The constitutional significance of this evidence lies in its bearing on the state's positive obligation under Article 21. The Supreme Court in *Puttaswamy* held, unanimously across all six opinions, that the right to privacy is a fundamental right under Article 21 and encompasses, within its ambit, "the right to protect one's dignity, to develop one's personality, and to make choices about one's life."[17] Chandrachud J. (as he then was), writing for himself and two others, articulated a conception of privacy that expressly includes protection from non-consensual public exposure of personal information - a description that encompasses denigration, impersonation, outing, and NCII with precision.[18]

The state's positive obligation to protect fundamental rights against private actors - recognised by the Supreme Court in *Vishaka v. State of Rajasthan*[19] and subsequently consolidated - means that the failure to legislate against cyberbullying is not merely a policy choice but a potential constitutional dereliction. Where the state is aware of a systematic pattern of private conduct that violates the fundamental rights of a class of persons - here, children subjected to digital harassment - and fails to provide an adequate legal remedy, it violates its positive constitutional duty.[20]

Importantly, this constitutional analysis also defines the outer limits of cyberbullying legislation. Any statutory definition that criminalises online speech must satisfy the requirements of Article 19(2), which permits restrictions on freedom of expression only on specified grounds (sovereignty, security, public order, decency, morality, defamation, and contempt of court) and only to the extent "reasonable." The Supreme Court's invalidation of Section 66A of the IT Act in *Shreya Singhal* on grounds of vagueness and overbreadth[21] establishes a high constitutional bar for cyberbullying legislation: definitions must be precise, restrictions proportionate, and penal consequences calibrated to harm. The proposed model in Part VII is designed with these constraints in mind.

5. The Indian legal framework: a section-level analysis

5.1 The Bharatiya Nyaya Sanhita, 2023

The BNS 2023 replaced the Indian Penal Code, 1860 and contains several provisions with potential application to cyberbullying. However, each encounters interpretive or structural barriers that limit its utility as a child protection instrument.

Section 351 (criminal intimidation) criminalises threatening a person with injury to person, reputation, or property with intent to cause alarm. Its application to cyberbullying harassment requires that individual messages constitute "threats" - a standard not easily met by non-threatening but deeply distressing content such as repeated humiliation, denigration, or social exclusion. Moreover, Section 351 is not child-specific; it applies the same standard to adults, and its penalty structure does not reflect the heightened vulnerability of minor victims.

Section 78 (stalking) covers electronic communication that "fosters personal interaction" against a victim's expressed wishes. Cyberstalking of minors falls within this provision. However, proviso (i) to Section 78 provides that conduct is not stalking if carried out by the state "for the purpose of preventing or detecting crime" - a proviso irrelevant to cyberbullying but indicative of the provision's primary intended application. No aggravated stalking provision for minor victims exists.

Section 77 (voyeurism) covers capturing or disseminating images of a woman engaged in a private act without consent. It is gender-restricted (applies only to women) and limited to acts of a sexual nature, leaving non-sexual NCII, denigration through morphed non-sexual images, and harassment of male minors entirely outside its scope.

The structural gap across these provisions is consistent: they address discrete criminal acts without recognising cyberbullying as a pattern of conduct with cumulative harm. Indian criminal law has no equivalent of the UK's "course of conduct" framework under the Protection from Harassment Act 1997, which allows cumulative low-intensity harassment to be prosecuted as a single offence.[22]

5.2 The Information Technology Act, 2000

The IT Act's primary contribution to child online protection is Section 67B, which criminalises publishing or transmitting material depicting children in sexually explicit acts in electronic form. This provision - among the strongest child-specific provisions in Indian cyberlaw - is nonetheless limited to CSAM and does not extend to non-sexual cyberbullying.

Section 66C (identity theft) and Section 66D (cheating by impersonation) are applicable to impersonation-type cyberbullying but require proof of fraudulent or dishonest intent, a mens rea threshold that may be difficult to establish in peer-group impersonation cases where the perpetrator's primary motive is reputational damage rather than financial gain.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("IT Rules 2021") impose due diligence obligations on social media intermediaries, including grievance redressal mechanisms and content removal obligations. Rule 4(4) requires significant social media intermediaries to deploy technology-based measures to identify CSAM. However, the IT Rules 2021 contain no child-specific cyberbullying provisions, no mandatory response timelines for child-targeted harassment complaints distinct from general content, and no mechanism for schools or child welfare institutions to interface with platform takedown systems. The grievance redressal framework is reactive, complaint-driven, and premised on the capacity of the victim or their guardian to navigate a formal complaints process - a premise that systematically disadvantages minor victims.

5.3 The Protection of Children from Sexual Offences Act, 2012

POCSO 2012 provides the most targeted child protection framework in Indian law, but its scope is confined to sexual offences. Three provisions have potential application to cyberbullying in its most severe digital-sexual manifestations.

Section 11(iv) defines "sexual harassment" of a child to include showing pornography to a child. The provision does not explicitly address the coercive solicitation of sexual content from a child - the defining feature of sextortion - and the courts have not yet authoritatively resolved whether Section 11(iv) can be so construed. The Bombay High Court's decision in *Libnus v. State of Maharashtra* (2021)[23] - in which the Court controversially held that pressing a minor's breasts without direct skin contact did not constitute "sexual assault" - illustrates the interpretive conservatism that can limit POCSO's reach when applied to fact patterns at the margins of its express provisions.

Sections 13 and 14 criminalise using a child for pornographic purposes and storing CSAM respectively. These provisions are applicable to NCII cases involving minors and represent the strongest existing legal tools against digital sexual exploitation. Their limitation is substantive rather than interpretive: they address sexual content and do not engage with the broader spectrum of cyberbullying harm.

The cumulative picture from this section-level analysis is of a fragmented framework with significant gaps: no definition of cyberbullying, no child-specific harassment provision, no mandatory institutional response mechanism, no civil remedy, and no platform accountability regime specific to child-directed harassment.

5.4 Judicial responses: the landscape of decided cases

Indian courts have engaged with cyberbullying-adjacent fact patterns in a small but growing body of decisions. In *Kalandi Charan Lenka v. State of Odisha* (2017),[24] the Orissa High Court granted bail in a case involving the creation of a fake Facebook profile of a woman with obscene content - a fact pattern directly analogous to denigration-type cyberbullying. The Court's reasoning, however, proceeded entirely under Section 67 of the IT Act and Section 509 IPC (now BNS s. 79) - word, gesture or act intended to insult the modesty of a woman - without developing any child-specific doctrinal framework.

The Delhi High Court in *Jasleen Kaur v. State (NCT of Delhi)* (2018)[25] addressed online harassment of a woman through fabricated social media posts, again proceeding under general IT Act provisions. No Indian High Court or the Supreme Court has, to this author's knowledge, delivered a judgment specifically addressing cyberbullying of a minor as a distinct category of harm requiring doctrinal development. This evidentiary gap - the absence of child-specific cyberbullying jurisprudence - is itself analytically significant: it confirms that the current statutory framework does not provide a pathway through which courts can develop protective doctrine for minor victims.

6. Comparative legal models: functional analysis and transposability

6.1 European Union: Digital Services Act, 2022

The DSA represents the most structurally ambitious regulatory response to platform harms to date. Articles 34 and 35 impose obligations on Very Large Online Platforms (VLOPs) to conduct annual systemic risk assessments covering "actual or foreseeable negative effects... on the exercise of fundamental rights" and to implement proportionate risk-mitigation measures.[26] For child safety specifically, Article 28 prohibits targeting advertising to minors based on profiling, and Article 35(1)(k) requires VLOPs to implement measures protecting minors from "content that may impair their physical or mental development."

The DSA's structural contribution to the comparative analysis is its conceptual shift from reactive content moderation (remove harmful content upon complaint) to proactive risk governance (identify and mitigate systemic conditions that produce harmful content). This shift is constitutionally compatible with the Indian framework: the Supreme Court's proportionality doctrine, as developed in *Modern Dental College v. State of Madhya Pradesh* (2016),[27] requires that regulatory obligations be proportionate to the harm addressed - a standard that proactive risk governance, calibrated to platform scale, can satisfy.

6.2 United Kingdom: Online Safety Act, 2023

The UK Online Safety Act 2023 (OSA) is the most directly transposable comparative model for India, for three reasons. First, it operates within a common law constitutional tradition with structural similarities to Indian fundamental rights jurisprudence. Second, it imposes child-specific "safety duties" on in-scope services that require platforms to conduct children's risk assessments and implement measures to protect children from "priority harms" - a list that expressly includes cyberbullying and harassment.[28] Third, it creates Ofcom as the designated regulator with enforcement powers including significant financial penalties (up to £18 million or 10% of global annual turnover, whichever is higher).

The OSA's "duty of care" framework - imposing a proactive obligation on platforms to protect users rather than merely to respond to complaints - is analytically compatible with the positive obligation doctrine under Article 21 and provides a model for how Indian legislation could impose constitutionally grounded duties on private platforms. However, the OSA's regulatory architecture assumes a developed administrative state with the institutional capacity to implement sector-specific technology regulation - a capacity India is developing through the Data Protection Board established under the Digital Personal Data Protection Act, 2023, but has not yet operationalised at the required scale.[29]

6.3 Australia: Online Safety Act, 2021

Australia's OSA 2021 establishes the eSafety Commissioner with powers to issue removal notices for harmful online content, including cyberbullying material targeting Australians under 18. The Basic Online Safety Expectations (BOSE) regime requires platforms to "take reasonable steps" to ensure their services are not used for cyberbullying of children - a standard-of-care approach that explicitly imposes child safety obligations on platforms as a condition of operating in the Australian market.

An evaluation of the eSafety Commissioner's operations by the Australian Communications and Media Authority (2022) found a 91% compliance rate with removal notices for cyber-abuse material and a median removal time of 48 hours, suggesting that the institutional model is operationally effective.[30] The Commissioner model is transferable to India with modifications: rather than a standalone Commissioner, India could integrate child online safety functions into the Data Protection Board, leveraging existing institutional infrastructure while avoiding the cost and delay of creating a new body.

6.4 South Korea

South Korea's school-based cyberbullying prevention framework - established under the Act on the Prevention of and Countermeasures against Violence in Schools, as amended in 2023 - is the most developed school-institutional response model in the comparative set. It requires all schools to constitute a dedicated committee for bullying prevention and response, mandates reporting by teachers, and establishes a structured mediation process before criminal referral. Importantly, it treats cyberbullying as a school governance issue as well as a criminal matter, an approach with significant advantages for minor victims who may not wish to pursue criminal prosecution against known peers.[31]

6.5 Transposability assessment

Element	Source jurisdiction	Constitutional compatibility (India)	Institutional feasibility	Evidence of effectiveness
Proactive risk assessment duty on platforms	EU (DSA Art. 34)	High - proportionality doctrine supports	Medium - requires regulatory capacity	Preliminary positive (DSA enforcement ongoing)
Child-specific "duty of care" on platforms	UK (OSA 2023)	High - Art. 21 positive obligation supports	Medium - depends on DPDP Board operationalisation	Too early (OSA commenced 2024)
Removal notice power with mandatory timelines	Australia (OSA 2021)	High - reasonable restriction on Art. 19(1)(a) justified	High - can be integrated into existing grievance mechanism	Strong (91% compliance rate)
School-level committee and structured mediation	South Korea	N/A - non-regulatory measure	High - RTE Act amendment pathway available	Moderate evidence (cross-cultural validity requires assessment)

Table 2. Transposability assessment of comparative models. Author's original assessment.

7. Towards a layered protective architecture

The protective architecture proposed here is organised across three tiers: constitutional, legislative, and institutional. Each tier is evaluated against the criteria of constitutional justifiability, institutional feasibility, and normative adequacy. The architecture is explicitly not a transplant of any single foreign model but a synthesis designed for the Indian constitutional and institutional context.

7.1 Tier one: constitutional consolidation

The first tier does not require legislation. It requires the Supreme Court - or a High Court developing doctrine in an appropriate case - to authoritatively hold that cyberbullying of a minor engages the state's positive obligation under Article 21 read with the rights of the child under Article 39(f) and India's obligations under Articles 3, 16, and 19 of the UNCRC. Such a holding would produce three consequences.

First, it would establish that the failure to legislate against cyberbullying is constitutionally cognisable, providing the doctrinal foundation for public interest litigation directed at legislative reform. Second, it would create a constitutional cause of action under which minor victims could seek writs of mandamus directing state governments to implement existing statutory protections, particularly the IT Rules 2021 grievance mechanisms, with greater diligence. Third, it would impose a constitutional standard of proportionality against which future cyberbullying legislation is evaluated - constraining both under-protection (legislative inaction) and over-protection (overbroad criminalisation of online expression).

7.2 Tier two: legislative reform

A dedicated Child Online Protection Act (COPA) for India should contain the following core elements, each evaluated for constitutional validity.

Definition clause. The Act should adopt the definition proposed in Part III.1 of this article, which removes the repetition threshold for severe single-incident conduct while retaining repetition as an aggravating factor. This formulation avoids the vagueness that led to the invalidation of Section 66A in *Shreya Singhal* by anchoring the definition in objective harm indicators - "psychological, reputational, or dignitary harm" - rather than the subjective "grossly offensive" or "menacing" standards that the Court found constitutionally problematic.[32]

Platform accountability provisions. Platforms with more than five million registered users in India should be required to: (i) conduct annual child safety risk assessments and publish the results; (ii) designate a Child Safety Officer with operational authority over content moderation decisions affecting minors; (iii) implement an expedited 24-hour removal pathway for cyberbullying content targeting minors, distinct from the general content grievance mechanism; and (iv) provide structured reporting interfaces accessible to designated school counsellors and child welfare institutions. The constitutionality of these obligations under Article 19(1)(g) (right to carry on trade) is supportable: the Supreme Court in *Modern Dental College* held that regulations of professional activity satisfy the reasonable restrictions test under Article 19(6) where they pursue a legitimate public purpose and are proportionate.[33] Child online safety unambiguously satisfies the legitimate purpose criterion.

Civil remedy mechanism. The most significant innovation proposed is a civil protection order remedy for cyberbullying victims. The mechanism would allow a minor victim (through a parent, guardian, or school authority) to apply to a Judicial Magistrate for an emergency cyberbullying protection order (ECPO) directing: (i) immediate content removal; (ii) contact prohibition; and (iii) identity disclosure by the platform of an anonymous perpetrator, subject to a proportionality assessment. The ECPO mechanism addresses a structural failure in the current framework: the criminal justice pathway, premised on prosecution and punishment, is ill-suited to peer-group cyberbullying where the victim often knows the perpetrator and does not seek criminalisation but does need immediate practical relief. The civil remedy, drawing on the model of domestic violence protection orders under the Protection of Women from Domestic Violence Act, 2005,[34] provides a proportionate, victim-centred, and constitutionally grounded alternative.

The constitutionality of requiring platforms to disclose the identity of anonymous perpetrators requires particular attention. The right to anonymous online speech is an aspect of the right to privacy under Article 21 post-*Puttaswamy*. Compelled identity disclosure is therefore a restriction on a fundamental right and must satisfy the three-part test - legality, legitimate aim, and proportionality - established in *Puttaswamy* itself. The proposed mechanism satisfies this test: the disclosure obligation is created by statute (legality), pursues the protection of a child's fundamental rights (legitimate aim), and is conditioned on a judicial proportionality assessment (proportionality), ensuring that disclosure does not occur as a matter of course but only where necessary to prevent or remedy serious harm.

Mandatory reporting and data obligations. COPA should require state governments to publish annual child cybersafety reports, disaggregated by state, age, gender, and type of harm. This provision addresses a critical evidential gap: the absence of reliable India-specific data on cyberbullying

prevalence, which currently forces Indian scholarship to rely on global statistics whose transferability to the Indian context is unverified. Without a mandatory data collection regime, the evidence base for future legislative reform will remain inadequate.

7.3 Tier three: institutional and school-based framework

Legislative reform without institutional implementation is symbolic. The third tier of the proposed architecture addresses the institutional machinery through which COPA's provisions would be operationalised.

Child Online Safety Authority (COSA). Rather than creating a new standalone regulator - which would entail significant cost, delay, and capacity risk - the proposed model integrates child online safety functions into the Data Protection Board (DPB) established under the Digital Personal Data Protection Act, 2023, through a dedicated Child Online Safety Division with a ringfenced budget and a specialist Child Safety Commissioner. This model leverages existing institutional infrastructure, regulatory expertise, and statutory mandate while creating the specialist capacity that child online safety requires.

School-level mandatory framework. The Right to Education Act, 2009 should be amended to require all recognised schools to adopt a Cyber Safety Policy (CSP) containing: (a) a definition of cyberbullying aligned with COPA; (b) mandatory reporting obligations for teachers and school counsellors; (c) a first-response protocol for cyber incidents; and (d) an annual digital literacy programme meeting standards published by NCTE. The RTE amendment pathway is constitutionally straightforward - Article 21A confers legislative competence on Parliament to make education compulsory and free, and the Court in *Society for Unaided Private Schools of Rajasthan v. Union of India* (2012)[35] confirmed the broad reach of this competence over private as well as government schools.

Cross-cultural validity of school interventions. The existing evidence base for school-based cyberbullying interventions requires careful evaluation. The KiVa programme (Finland), frequently cited in this literature, has demonstrated effectiveness in Nordic educational contexts.[36] However, subsequent evaluations in non-Nordic contexts have produced mixed results. Nocentini and Menesini (2016) found that KiVa's effectiveness in Italian schools was significantly lower than in Finnish schools, attributing the difference to variations in peer group dynamics and teacher authority structures.[37] The proposed school framework therefore does not mandate a specific programme but requires schools to adopt evidence-based interventions meeting minimum criteria - peer mentoring components, bystander activation training, and digital literacy education - allowing contextually adapted implementation.

8. Conclusion

This article has argued three things. First, that cyberbullying of children is constitutionally cognisable as a violation of the right to privacy and dignity under Article 21 as expanded in *Puttaswamy*, and that the state's failure to provide an adequate legislative response is not merely a policy failure but a constitutional one. Second, that the existing Indian legal framework - the BNS 2023, the IT Act 2000, and POCSO 2012 - fails at the definitional, institutional, and remedial levels, and that this failure cannot be corrected through purposive construction alone. Third, that a constitutionally grounded, institutionally feasible protective architecture is available, drawing on and adapting elements from comparative models in the EU, UK, Australia, and South Korea, integrated through a proposed Child Online Protection Act and an amended RTE framework.

The most significant original contribution of this article is the civil remedy mechanism - the Emergency Cyberbullying Protection Order - which addresses the structural mismatch between the criminal justice framework and the practical needs of child victims who require immediate, practical relief rather than prosecution. This mechanism, grounded in the positive obligation doctrine under Article 21 and calibrated to satisfy the *Puttaswamy* proportionality test, represents a novel contribution to the Indian child protection law literature that the existing scholarship has not developed.

Three limitations of this study should be acknowledged. The doctrinal methodology cannot substitute for empirical data on cyberbullying prevalence in India, which does not exist in a reliable form. The comparative analysis is limited to jurisdictions whose legislative responses are sufficiently developed to generate evaluative evidence; the effectiveness evidence for the UK Online Safety Act 2023 remains preliminary. And the proposed COPA framework requires detailed legislative drafting that goes beyond the scope of a journal article. Each of these limitations points to a distinct research agenda: empirical socio-legal survey work on Indian cyberbullying prevalence; longitudinal evaluation of the UK OSA framework; and detailed legislative design work for COPA.

For the child who goes to sleep dreading what her phone will show in the morning, these are not academic limitations. They are reminders that scholarship in this field has a practical obligation - not merely to describe the problem, but to advance,

with rigour and precision, the legal architecture capable of addressing it.**Footnotes**

1. Olweus, D. (1993). *Bullying at school: what we know and what we can do*. Blackwell, pp. 9–10. The definition was developed through surveys in Norwegian and Swedish schools between 1970 and 1983.
2. Kowalski, R.M., Limber, S.P., & Agatston, P.W. (2012). *Cyberbullying: bullying in the digital age* (2nd ed.). Wiley-Blackwell, pp. 1–8.
3. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (nine-judge bench).
4. On doctrinal methodology in law, see Hutchinson, T. (2015). The doctrinal method: incorporating interdisciplinary methods in reforming the law. *Tilburg Law Review*, 20(2), 130–163.
5. Convention on the Rights of the Child, GA Res. 44/25 (1989), ratified by India, December 1992. Articles 3(1) (best interests), 16 (privacy), and 19 (protection from violence) are most directly engaged.
6. The comparative methodology draws on Zweigert, K. & Kötz, H. (1998). *Introduction to comparative law* (3rd ed., trans. Weir, T.). Oxford University Press, chapter 3 (functional method).
7. Tokunaga, R.S. (2010). Following you home from school: a critical review and synthesis of research on cyberbullying victimisation. *Computers in Human Behavior*, 26(3), 277–287. https://doi.org/10.1016/j.chb.2009.11.014
8. Vandebosch, H., & Van Cleemput, K. (2008). Defining cyberbullying: a qualitative research into the perceptions of youngsters. *CyberPsychology & Behavior*, 11(4), 499–503. https://doi.org/10.1089/cpb.2007.0042
9. Menesini, E., & Nocentini, A. (2009). Cyberbullying definition and measurement: some critical considerations. *Journal of Psychology*, 217(4), 230–232. https://doi.org/10.1027/0044-3409.217.4.230
10. Citron, D.K. (2014). *Hate crimes in cyberspace*. Harvard University Press, pp. 10–14.
11. Kowalski, R.M., Giumetti, G.W., Schroeder, A.N., & Lattanner, M.R. (2014). Bullying in the digital age: a critical review and meta-analysis of cyberbullying research among youth. *Psychological Bulletin*, 140(4), 1073–1137. https://doi.org/10.1037/a0035618
12. Hinduja, S., & Patchin, J.W. (2010). Bullying, cyberbullying, and suicide. *Archives of Suicide Research*, 14(3), 206–221. https://doi.org/10.1080/13811118.2010.494133. Effect size variation is documented in Gini, G., & Espelage, D.L. (2014). *Child Development*, 85(3), 1035–1040.
13. Eisenberger, N.I., Lieberman, M.D., & Williams, K.D. (2003). Does rejection hurt? An fMRI study of social exclusion. *Science*, 302(5643), 290–292. https://doi.org/10.1126/science.1089134
14. Nixon, C.L. (2014). Current perspectives: the impact of cyberbullying on adolescent health. *Adolescent Health, Medicine and Therapeutics*, 5, 143–158. https://doi.org/10.2147/AHMT.S36456
15. Suler, J. (2004). The online disinhibition effect. *CyberPsychology & Behavior*, 7(3), 321–326. https://doi.org/10.1089/1094931041291295
16. Gillespie, A.A. (2019). *Cybercrime: key issues and debates* (2nd ed.). Routledge, pp. 178–182.
17. *Puttaswamy*, (2017) 10 SCC 1, para. 3 of the concurring opinion of Chandrachud J. (as he then was). All six opinions of the nine-judge bench agreed that privacy is a fundamental right under Art. 21.
18. *Ibid*., paras. 168–175 (Chandrachud J.).
19. *Vishaka v. State of Rajasthan*, (1997) 6 SCC 241, para. 7. The Court held that the state's obligation under Art. 21 extends to protecting fundamental rights from violation by private actors in certain contexts.
20. For the positive obligation doctrine in Indian constitutional law, see Bhatia, G. (2016). *Offend, shock or disturb: free speech under the Indian Constitution*. Oxford University Press, pp. 45–52.
21. *Shreya Singhal v. Union of India*, (2015) 5 SCC 1, paras. 91–96. The Court held that s. 66A IT Act was unconstitutional for failing to define "grossly offensive" or "menacing" with sufficient precision.
22. Protection from Harassment Act 1997 (UK), s. 1(1). A "course of conduct" requires at least two incidents under s. 7(3).
23. *Libnus v. State of Maharashtra*, (2021) Crl. App. No. 165/2020 (Bom. HC). The decision generated substantial academic criticism: see Dasgupta, S. (2021). Skin-to-skin contact and POCSO: a doctrinal

analysis. *Indian Law Review*, 5(3), 302–315.
24. *Kalandi Charan Lenka v. State of Odisha*, (2017) 1 OLR (Cri) 213 (Ori. HC).
25. *Jasleen Kaur v. State (NCT of Delhi)*, (2018) Bail Appl. No. 2814/2017 (Del. HC).
26. Regulation (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), OJ L 277/1, Arts. 34–35.
27. *Modern Dental College and Research Centre v. State of Madhya Pradesh*, (2016) 7 SCC 353, paras. 46–51 (five-judge bench adopting proportionality as a standard of review under Art. 19).
28. Online Safety Act 2023 (UK), ss. 5–10 (illegal content duties), ss. 11–26 (safety duties for services likely to be accessed by children).
29. Digital Personal Data Protection Act, 2023, s. 18 (establishment of the Data Protection Board of India).
30. eSafety Commissioner (2022). *Annual report 2021–22*. Commonwealth of Australia, p. 34 (reporting compliance statistics for basic online safety expectations and removal notices).
31. Act on the Prevention of and Countermeasures against Violence in Schools (South Korea), as amended 2023, Arts. 12–14 (school violence response committees).
32. *Shreya Singhal*, (2015) 5 SCC 1, paras. 91–96.
33. *Modern Dental College*, (2016) 7 SCC 353, paras. 48–50.
34. Protection of Women from Domestic Violence Act, 2005, ss. 18–23 (protection orders, residence orders, and interim relief).
35. *Society for Unaided Private Schools of Rajasthan v. Union of India*, (2012) 6 SCC 1, para. 37 (confirming the reach of Art. 21A obligations over private unaided schools).
36. Kärnä, A., Voeten, M., Little, T.D., Poskiparta, E., Kaljonen, A., & Salmivalli, C. (2011). A large-scale evaluation of the KiVa anti-bullying program: grades 4–6. *Child Development*, 82(1), 311–330. https://doi.org/10.1111/j.1467-8624.2010.01557.x
37. Nocentini, A., & Menesini, E. (2016). KiVa anti-bullying program in Italy: evidence of effectiveness in a randomized control trial. *Prevention Science*, 17(8), 1012–1023. https://doi.org/10.1007/s11121-016-0690-z

38. References

1. Bhatia, G. (2016). *Offend, shock or disturb: free speech under the Indian Constitution*. Oxford University Press.
2. Citron, D.K. (2014). *Hate crimes in cyberspace*. Harvard University Press.
3. Eisenberger, N.I., Lieberman, M.D., & Williams, K.D. (2003). Does rejection hurt? An fMRI study of social exclusion. *Science*, 302(5643), 290–292. https://doi.org/10.1126/science.1089134
4. eSafety Commissioner. (2022). *Annual report 2021–22*. Commonwealth of Australia.
5. Gillespie, A.A. (2019). *Cybercrime: key issues and debates* (2nd ed.). Routledge.
6. Hinduja, S., & Patchin, J.W. (2010). Bullying, cyberbullying, and suicide. *Archives of Suicide Research*, 14(3), 206–221. https://doi.org/10.1080/13811118.2010.494133
7. Hutchinson, T. (2015). The doctrinal method: incorporating interdisciplinary methods in reforming the law. *Tilburg Law Review*, 20(2), 130–163.
8. Kärnä, A., Voeten, M., Little, T.D., Poskiparta, E., Kaljonen, A., & Salmivalli, C. (2011). A large-scale evaluation of the KiVa anti-bullying program: grades 4–6. *Child Development*, 82(1), 311–330. https://doi.org/10.1111/j.1467-8624.2010.01557.x
9. Kowalski, R.M., Giumetti, G.W., Schroeder, A.N., & Lattanner, M.R. (2014). Bullying in the digital age: a critical review and meta-analysis of cyberbullying research among youth. *Psychological Bulletin*, 140(4), 1073–1137. https://doi.org/10.1037/a0035618
10. Kowalski, R.M., Limber, S.P., & Agatston, P.W. (2012). *Cyberbullying: bullying in the digital age* (2nd ed.). Wiley-Blackwell.
11. Menesini, E., & Nocentini, A. (2009). Cyberbullying definition and measurement: some critical considerations. *Journal of Psychology*, 217(4), 230–232. https://doi.org/10.1027/0044-3409.217.4.230
12. Nixon, C.L. (2014). Current perspectives: the impact of cyberbullying on adolescent health. *Adolescent Health, Medicine and Therapeutics*, 5, 143–158. https://doi.org/10.2147/AHMT.S36456

13. Nocentini, A., & Menesini, E. (2016). KiVa anti-bullying program in Italy: evidence of effectiveness in a randomized control trial. *Prevention Science*, 17(8), 1012–1023. https://doi.org/10.1007/s11121-016-0690-z
14. Olweus, D. (1993). *Bullying at school: what we know and what we can do*. Blackwell.
15. Suler, J. (2004). The online disinhibition effect. *CyberPsychology & Behavior*, 7(3), 321–326. https://doi.org/10.1089/1094931041291295
16. Tokunaga, R.S. (2010). Following you home from school: a critical review and synthesis of research on cyberbullying victimisation. *Computers in Human Behavior*, 26(3), 277–287. https://doi.org/10.1016/j.chb.2009.11.014
17. Vandebosch, H., & Van Cleemput, K. (2008). Defining cyberbullying: a qualitative research into the perceptions of youngsters. *CyberPsychology & Behavior*, 11(4), 499–503. https://doi.org/10.1089/cpb.2007.0042
18. Willard, N.E. (2007). *Cyberbullying and cyberthreats: responding to the challenge of online social aggression, threats, and distress*. Research Press.
19. Zweigert, K., & Kötz, H. (1998). *Introduction to comparative law* (3rd ed., trans. Weir, T.). Oxford University Press.

Cases cited

1. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (SC, nine-judge bench).
2. *Shreya Singhal v. Union of India*, (2015) 5 SCC 1 (SC, two-judge bench).
3. *Modern Dental College and Research Centre v. State of Madhya Pradesh*, (2016) 7 SCC 353 (SC, five-judge bench).
4. *Vishaka v. State of Rajasthan*, (1997) 6 SCC 241 (SC).
5. *Society for Unaided Private Schools of Rajasthan v. Union of India*, (2012) 6 SCC 1 (SC).
6. *Kalandi Charan Lenka v. State of Odisha*, (2017) 1 OLR (Cri) 213 (Ori. HC).
7. *Jasleen Kaur v. State (NCT of Delhi)*, (2018) Bail Appl. No. 2814/2017 (Del. HC).
8. *Libnus v. State of Maharashtra*, (2021) Crl. App. No. 165/2020 (Bom. HC).

Legislation cited

1. Bharatiya Nyaya Sanhita, 2023 (India), ss. 77–78, 308, 351–352, 356.
2. Convention on the Rights of the Child, GA Res. 44/25, 20 November 1989.
3. Digital Personal Data Protection Act, 2023 (India), s. 18.
4. Information Technology Act, 2000 (India), ss. 66C, 66D, 67, 67B.
5. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (India), Rule 4.
6. Online Safety Act 2021 (Cth) (Australia).
7. Online Safety Act 2023 (UK), ss. 5–26.
8. Protection of Children from Sexual Offences Act, 2012 (India), ss. 11, 13–15.
9. Protection of Women from Domestic Violence Act, 2005 (India), ss. 18–23.
10. Regulation (EU) 2022/2065 (Digital Services Act), OJ L 277/1, Arts. 28, 34–35.
11. Right of Children to Free and Compulsory Education Act, 2009 (India).