



In their Best Interests

A Review of the Legal Framework on Children's Digital Safety in India

This report is an independent, non-commissioned piece of work by the Vidhi Centre for Legal Policy, an independent think-tank doing legal research to help make better laws.

Published in September 2026

By the Vidhi Centre for Legal Policy

A-232 Ratan Lal Sahdev Marg, Defence Colony, New Delhi - 110024

Preferred citation: Supriya Shekher, Kahaan Mehta, Shehnaz Ahmed, Nirmalya Chaudhuri and Rudraksh Lakra, 'In Their Best Interests: A Review of the Legal Framework on Children's Digital Safety in India' (Vidhi Centre for Legal Policy, 2026)

Designed by: Nandita

© Vidhi Centre for Legal Policy

This work is licensed under Creative Commons Attribution

ShareAlike 2.5 India License.

About the Authors

Supriya Shekher is a Research Fellow in the Centre for Applied Law and Technology Research at the Vidhi Centre for Legal Policy.

Kahaan Mehta is a Senior Resident Fellow in the Centre for Applied Law and Technology Research at the Vidhi Centre for Legal Policy.

Shehnaz Ahmed is the Lead of the Centre for Applied Law and Technology Research at the Vidhi Centre for Legal Policy.

Nirmalya Chaudhuri was a Research Fellow in the Centre for Applied Law and Technology Research at the Vidhi Centre for Legal Policy.

Rudraksh Lakra was a Research Fellow in the Centre for Applied Law and Technology Research at the Vidhi Centre for Legal Policy.

Acknowledgements

The authors would also like to thank **Anushka Pandey** and **Evelina Dash**, Senior Resident Fellow and Project Fellow, respectively, at the Centre for Applied Law and Technology Research at Vidhi; and **Karishma Srivastava** and **Vrinda Pareek**, Former Senior Resident Fellows at Vidhi, for their research and contributions to this Report.

We thank **Ameen Jauhar**, Data Governance Lead, CABI, and **Sunetra Ravindran**, Lead, Vidhi Karnataka, for their valuable inputs as peer reviewers of this Report.

We would also like to thank the interns who worked with us at various stages of the research and writing of this Report: **Alekhya Sattigeri**, **Animesh Gupta**, **Antima Tiwari**, **Neha Tiwari**, **Pushpendra**, **Saad Misbah** and **Samrudh Shiolkar**.

Errors in this Report, if any, are solely those of the authors.

Abbreviation	Full Form / Meaning
AADC	Age-Appropriate Design Code
AI	Artificial Intelligence
AU	African Union
BNS	Bharatiya Nyaya Sanhita, 2023
CALPRA	Child and Adolescent Labour (Prohibition and Regulation) Act, 1986
CBDR	Common But Differentiated Responsibilities
CSEA	Child Sexual Exploitation and Abuse
CSEAM	Child Sexual Exploitation and Abuse Material
DPDP Act	Digital Personal Data Protection Act, 2023
EU	European Union
ICT	Information and Communication Technology
IoT	Internet of Things
IT Act	Information Technology Act, 2000
ITPA	Immoral Traffic (Prevention) Act, 1956
IT Rules	Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021
JJ Act	Juvenile Justice (Care and Protection of Children) Act, 2015
M1	Mode 1 - Criminalisation of the Identified Harm or certain aspects of it
M2	Mode 2 - Regulation of conduct by ecosystem stakeholders, including intermediaries and gatekeepers, through non-criminal measures
M3	Mode 3 - Incidental and interpretive inclusion
M4	Mode 4 - Rights-based protective framework
Misleading Ads Guidelines	Guidelines for Prevention of Misleading Advertisements and Endorsements for Misleading Advertisements, 2022 ("Misleading Ads Guidelines") under the Consumer Protection Act, 2019
NCPCR	National Commission for Protection of Child Rights
OECD	Organisation for Economic Co-operation and Development

Abbreviation	Full Form / Meaning
Ofcom	Office of Communications (United Kingdom)
POCSO	Protection of Children from Sexual Offences Act, 2012
PROG Act	Promotion and Regulation of Online Gaming Act, 2025
PROG Rules	Promotion and Regulation of Online Gaming Rules, 2026
Q-A	Quadrant A - Explicitly framed for digital touchpoints and explicitly applicable to children
Q-B	Quadrant B - Explicitly framed for digital touchpoints and incidentally applicable to children
Q-C	Quadrant C - Explicitly applicable to children and agnostic to digital touchpoints
Q-D	Quadrant D - Agnostic to digital touchpoints and incidentally applicable to children
SGI	Synthetically Generated Information
SSMI	Significant Social Media Intermediary
UNCRC	United Nations Convention on the Rights of the Child
UNICEF	United Nations Children's Fund
UNTS	United Nations Treaty Series

Table of Contents



Executive Summary

1

Introduction

2

Research Methodology

3

Children and Digital Technology: An Overview of Interaction Touchpoints

4

Harms and Touchpoints

5

Legal Analysis of Harms to Children Arising out of Digital Interactions

6

Global Experience

7

Principles to Inform Digital Safety Frameworks for Children

Executive Summary

This report analyzes Indian laws to assess how they cover emerging harms in digital spaces for children. Children in India, and across the world, are becoming digital natives. The digital world is not a demarcated space that they 'enter' and 'exist in', but rather a condition of their lives. Recent reportage has flagged serious concerns about the safety of children in digital spaces. This has triggered responses from across the three branches of government in India. By reviewing the Indian legal landscape, the report provides an important preface to the discourse around digital safety of children in India.

In order to provide a comprehensive assessment, the report first identifies the different touchpoints between children and digital technology, and the harms that are reported to arise in this context. The report organizes relevant information on this from across disciplines, so as to enable a meaningful assessment of how Indian laws respond to such harms.

The analysis of Indian laws follows from thirty-four provisions across ten statutes and their subordinate legislation, mapped against fourteen harms. While nine of such harms were found to be legally recognized to varying degrees, five were found to be fully outside the scope of prevailing Indian laws. Findings in this regard reveal a pattern around which Indian laws are organized, namely that legal coverage emerges to be dense particularly with respect to harms which involve a wrongful act by an identifiable actor. Child sexual exploitation and abuse, for instance, accounts for fifteen of the thirty-four provisions, and is engaged with through three modes: criminalisation, due-diligence of intermediaries, and general anti-trafficking law extended through interpretation.

...legal coverage emerges to be dense particularly with respect to harms which involve a wrongful act by an identifiable actor.

Some harms are covered principally through regulation of others. For instance, cyberbullying and online harassment are covered primarily through provisions on sexual harassment, voyeurism, and stalking, some of which are women-specific. Other harms are engaged through specific vectors. Obesity and body image concerns are addressed through advertising standards, dependence on digital devices through online money gaming regulation, etc. Therefore, even where a specific harm may arise from multiple touchpoints or a combination of them, the regulatory aspect appears to address them in a hyperspecific context, or not at all. The five harms which Indian laws presently do not cover are: sleep disturbances, impairment of eyesight, impairment of cognitive development, deterioration of pro-social behaviour, and the exploitation of children's labour in digital contexts. These harms are the result of cumulative exposure, and where the causal chain between the harm and the touchpoint is complex. Consistent with our findings with respect to covered harms, in the absence

of discrete identifiable actors or definite settings, the Indian legal landscape covers them indirectly, or not at all.

The analysis of prevailing and emerging harms in the digital environment to children was observed to possess certain features which present Indian laws

These harms are diffuse, embedded in how the digital environment ordinarily operates, and several outlast the interaction which may have produced them,

do not directly account for, or respond to. These harms are diffuse, embedded in how the digital environment ordinarily operates, and several outlast the interaction which may have produced them, impacting neurological, socio-behavioral, and developmental aspects of a child. It is also important to clarify some harms compound over time and bleed into one another, and therefore may not be mutually exclusive. The severity with which harms may impact children is also different,

and contingent on the child's specific circumstances, such as their age, gender, sexual minority status, self-esteem, degree of adult supervision etc.

Four systemic limitations emerge from this analysis. First, Indian laws relevant to the context of the report engage with harms after they have occurred, through different modes such as punishment or content removal. The 'due diligence' obligations under the Information Technology Act, 2000 ("IT Act") only apply in the context of digital spaces that qualify as 'intermediaries'. Second, Indian laws relevant and studied for the context of this report view children as a monolithic category of persons under the age of eighteen. This contradicts the findings of this report, which emphasizes that the law must account for the fact that children's capabilities, understanding, and autonomy develop over time. Third, with respect to age assurance as an emerging governance measure, the report observes that this is a binary compliance gate, rather than a design obligation calibrated between safety, privacy, and best interests. In their present form, such measures are process-neutral, do not require implementation proportionate to risk, and do not contain sufficient safeguards to protect children's varied interests and rights in the verification process. Fourth, prevailing provisions do not adequately capture the dynamics of sustained online harm, or the emergence of newer types of harm. Indian criminal law, for instance, continues to focus on whether specific content is obscene, or threatening, or fraudulent, rather than addressing scenarios where the harm operates through misuse of information or manipulation, such as in the case of grooming and doxxing. A patchwork of legal provisions come together to provide an *ex post* response to such harms.

Reforms in comparable jurisdictions have responded to similar systemic risks primarily through *ex ante* regulation of digital ecosystems. Three approaches emerged from a survey of laws in fourteen countries and instruments adopted by geo-political blocs. Each approach regulates a different 'object'. The first approach is of imposing 'duty-of-care' obligations to respond to systemic risks to harm in or from the technological environment. These are identified by a body established under law, by creating obligations on ecosystem participants, and requiring mitigation of foreseeable risks, which is verified through audits. The second approach is of 'age-appropriate design'. This approach treats childhood as a structured legal category, and regulates ecosystem players

based on different conditions of childhood in which they encounter the technology. The third approach is of categorical restrictions, which regulates the boundary between children and digital technology. Therefore, the question under this approach is whether the child should be admitted at all to a specific digital environment. The thresholds and locus of decisions on this vary across jurisdictions. International instruments are observed to carry a common set of principles, such as the best interests of the child, evolving capacities requiring differentiated treatment, safety-by-design, and proportionality to actual risk.

The report describes these approaches in order to expound on the range of regulatory methods adopted. These considerations are subject to domestic laws, socio-economic, and cultural settings, and therefore, the report does not suggest their wholesale import in the Indian context.

Synthesizing these findings with the Indian constitutional and legal order, the report closes with seven principles that may inform legislative, regulatory, policy and industry self-regulatory interventions towards digital safety of children:

- 1. Children are rights-bearers and active participants in digital spaces**
- 2. The child's best interests are paramount**
- 3. Intervention to ensure children's digital safety must be proportionate to risk.**
- 4. Measures must account for children's developmental realities.**
- 5. Safety-by-design is the baseline condition for all children-facing digital spaces.**
- 6. All stakeholders bear a common but differentiated responsibility for ensuring children's digital safety.**
- 7. Frameworks should be purposive, proactive, and adaptive.**

There are two features of the framework of these principles which must be borne in mind. First, these are envisaged to operate in parallel with criminal law, and not by supplanting it. Second, this framework does not propose that legislation is the default answer to respond to every harm that is identified. These principles are accompanied with an 'interpretation' guide, which can assist relevant stakeholders in evolving the principle to their specific context. The chapter also provides an 'implementation' guide to provide some signposts for what the manifestation of such principles may look like.

CHAPTER 1

Introduction

Introduction

The Indian constitutional order assigns a distinctive legal significance to childhood. It recognizes that the State and society must not only shield children from conditions that foreclose on their development, but also actively secure the conditions that make this development possible. Constitutional provisions on children which prohibit hazardous employment, introduce the directive to protect children against exploitation, and material and moral abandonment, the guarantee of free and compulsory education, and the mandate for early childhood care, reflect an understanding that a child is a developing subject of care, to be protected and provided for.

The legislative framework built on this constitutional foundation has operationalized these commitments through successive instruments, such as statutes governing the right to education, juvenile justice, and protection from sexual offences, legislation addressing child labour, child marriage, and pre-natal sex determination, and measures regulating adoption, guardianship, and early childhood welfare.

Across these statutes, certain principles recur. The best interest of the child constitutes a primary consideration in all decisions that affect them. Physical and emotional development are identifiable and explicit legal interests. The laws have therefore attempted to cultivate protection and enablement of children as structural and systemic responses, operating not only through individual remedy, but also through the construction of institutional safeguards.

These laws were drafted to mitigate distinct harms in specific actual or situational geographies. However, children today live in a world where the boundaries of such geographies have been blurred by digital technology.

The context in which these principles, safeguards and enablers were developed were identifiable and relational. Harms that these statutes were designed to address arose from specific actors operating in defined social contexts, such as the household, the school, the workplace, or a shelter. Protection and enablement therefore took the shape of shields installed as enforceable obligations between the child and the source of harm. Designated persons and institutions were responsible for maintaining their safety and promoting their growth.

In the current environment, children do not encounter digital technology as a separate domain which they enter occasionally. Schools assign homework through digital platforms, government welfare systems require digital 'passes' for access, and families use devices as tools for care, education, and entertainment from the earliest years of childhood. In many ways, children's use of digital technology is a condition for participation in contemporary social and personal life in significant ways.

The Annual Status of Education Report 2024 found that 89.1% of children aged 14–16 reported having a smartphone at home. Among children who reported being able to use a smartphone, 76% said they had used it for social-media-

related activities in the preceding week¹. A 2026 survey found that over a fifth of children between the ages of 11 and 18 accessed the internet through shared family devices². Recent legislative and regulatory developments signal a growing recognition that the conditions of childhood now extend into environments that existing frameworks were not designed to reach. The Digital Personal Data Protection Act, 2023 (“**DPDP Act**”) recognizes the child as an occupant of a digital environment requiring distinct protection from other participants within it. This operates at different levels: first by gatekeeping their entry, and second by regulating how their personal data is processed including prohibition on processing that has a detrimental effect on the well-being of children and targeted advertising. Amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (“**IT Rules 2021**”) have progressively recognized ‘intermediaries’ as a distinct actor-group which interact with children by expanding their obligations with respect to them. The Promotion and Regulation of Online Gaming Act, 2025 (“**PROG Act 2025**”) imposes a comprehensive prohibition on real money online games, arriving at the Union level after years of fragmented state-level responses to the harms that such platforms were seen to cause, including to children. Lawmakers, Union and State governments, and bodies created by them, technology companies, parents, and schools are all increasingly engaging, and are promoted to engage with how Digital India’s children must be situated in the constitutional and legal schema, and how the obligations of protection and enablement translate into this evolving context.

These legislative efforts represent the law’s attempt to address harms that do not arise in fixed geographies, that do not always originate from a singular identifiable actor, and that bear a more diffused and mediated relationship with children than harms which earlier frameworks tried to address. In navigating this terrain, each intervention has worked from harms it could identify and the remedies it could conceive. However, interactions with digital technologies may also trigger harms which themselves do not operate within categories or boundaries. Harms may also bleed into one another.

For example, a single interaction may simultaneously engage questions of autonomy, privacy, and psychological and physiological well-being. If regulatory responses address such harms as independent of each other, they may fail to meet the constitutional and legal aspirations for children.

This possible failure is further compounded by the fact that the digital environment has fundamentally morphed the role of technology companies, guardians and society and their relationship with children ‘on technology’. As these stakeholders navigate an unfamiliar territory, the law attempts to assign specific legal responsibilities to some actors, while others may continue to play an uncharted invisible role. Creating legal responses to structural harms

¹ ASER Centre, Annual Status of Education Report (Rural) 2024 (28 January 2025) 62 https://asercentre.org/wp-content/uploads/2022/12/ASER_2024_Final-Report_13_2_24-1.pdf accessed 5 August 2026.

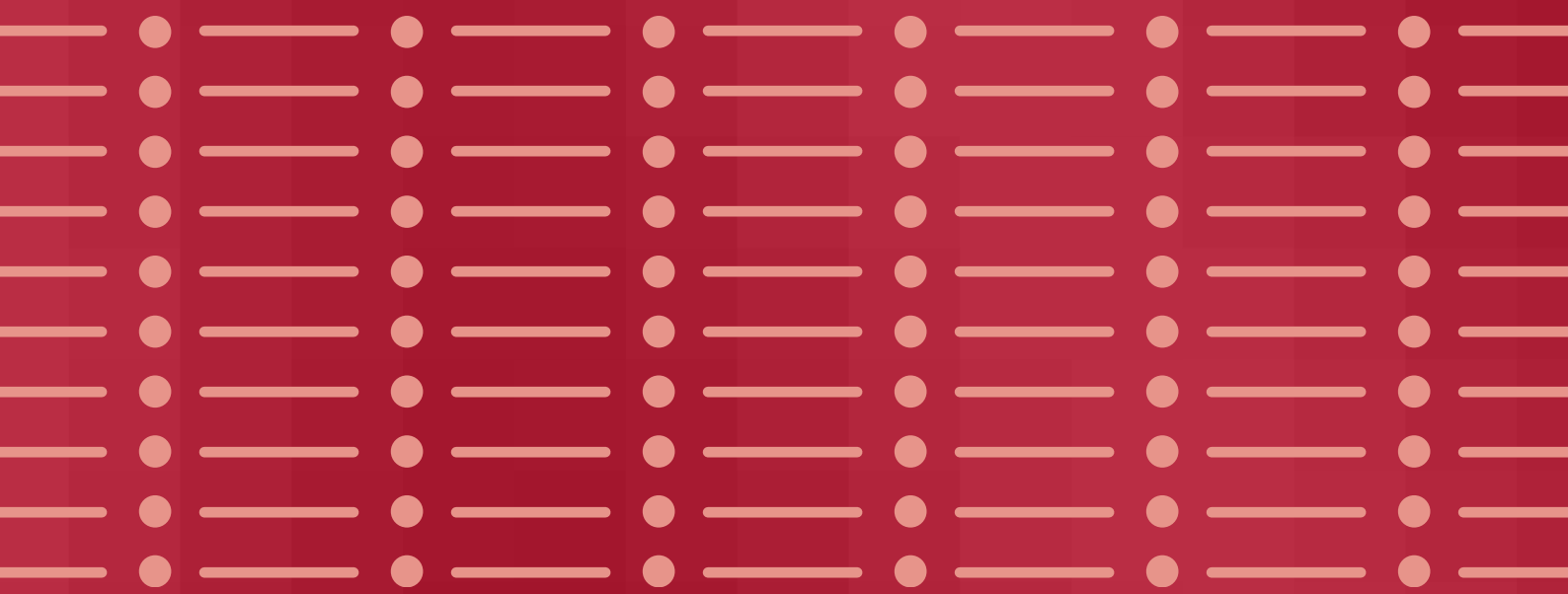
² Young Leaders for Active Citizenship, How Young Indians Navigate Digital Life: Findings from the Student Cyber Resilience Education and Empowerment Nationwide (SCREEN) Survey 2026 (British Asian Trust and BT Group, January 2026) <https://www.britishasiantrust.org/media/lgvn0rhx/screen-survey-2026.pdf> accessed 4 August 2026.

without accounting for such complexities of the digital ecosystem of children may relocate the problems, rather than resolving them.

A comprehensive, systematic mapping of the ways in which children interact with digital systems across the span of their childhood, the spectrum of harms those interactions may produce for different children, and the extent to which India's legal framework is equipped to address them as a whole will serve as a meaningful foundation for reform. Without that foundation, interventions will continue to address the symptoms of a problem without examining its structure or manifestations across contexts.

This report seeks to contribute to building that foundation. It is organized around five questions: how children interact with digital technology, what harms those interactions are reported to produce, how India's existing legal framework is addressing those harms, what regulatory approaches have been adopted by comparable jurisdictions, and what normative principles should inform stakeholder responses going forward.

It begins by mapping the landscape of interaction, that is, the touchpoints between children and digital technology. From that map, it identifies the spectrum of harms those interactions are reported to cause. It then examines India's legal framework against harms to children in the digital space, thereafter, assessing the presence and extent of legal coverage, thereby identifying where existing instruments may be falling short. A comparative analysis of regulatory approaches follows, drawing on the experience of legal systems that have confronted similar questions, before the report concludes with a principles-based framework to guide the full range of stakeholders, from legislators, regulators, platforms, parents, educators, and civil society, in responding to the studied harms.



CHAPTER 2

Research Methodology

Research Methodology

To achieve its objective of providing a comprehensive study of how India situates harms arising out of children's interaction with digital technology, the research for this report was structured around the five research questions set out in the Introduction.

Answering these questions requires movement across empirical, doctrinal, comparative, and normative methods. A methodology confined to any one of these would produce an incomplete account. The report accordingly draws on a combination of approaches, including a scoping review of interdisciplinary literature, doctrinal legal analysis, comparative legal analysis, and expert consultation.

The scoping review established the empirical and conceptual terrain of the different types of interactions and the harms reported to arise from them; the doctrinal legal analysis mapped India's laws against that terrain; the comparative legal analysis situated Indian law within a broader regulatory context and assisted in identifying gaps; and the expert consultations served both as a forum for surfacing contextual nuance and as a means of analytical validation across each stage. Together, these methods enable the report to move from a description of the problem to its diagnosis, to the development of a normative framework to address it.

Scoping Review of Secondary Literature

The identification of children's digital touchpoints and the harms associated with them is grounded in a scoping review of peer-reviewed literature drawn from multiple disciplines, including law, sociology, psychology, education, and medicine. As a distinct form of systematic review, the scoping review method is suited to the study of a broad and heterogeneous field and evidence and is not confined to the limited body of knowledge typically reflected in other research methodologies.

A scoping review research method is suitable on this subject. Children at the different developmental stages interact with heterogeneous technologies through touchpoints that vary by context, and actors who are multiple and dispersed. Research on the subject is correspondingly scattered across disciplines, each examining a particular harm in specific settings for particular groups. Reading this body of information together permits a systems-level view of the ecosystem.

The review conducted for the purpose of harm identification consists primarily of empirical studies, or doctrinal works grounded in empirical evidence. Theoretical and conceptual literature was considered where it provided frameworks that informed the classification or analysis of harms. The review

focuses on literature published between 2010 and 2025, reflecting the period during which social media platforms, algorithmic content delivery, and the broader digital ecosystem assumed the character related to the one they now have. Where it offered foundational or conceptual framing, material published before 2010 was also reviewed.

Certain analytical boundaries of this exercise should be stated to ensure a meaningful reading.

First, the harm identification exercise does not seek to establish a causal relationship between digital interactions and the identified harms beyond the findings of the literature itself. The identification, definition, and scope of the harms are strictly limited to those recognised by the authors of the secondary literature surveyed; this report does not constitute an independent empirical study.

Second, the harms identified have not been classified into mutually exclusive categories. This is a deliberate choice, intended to avoid replicating the gap in present research and regulatory thinking on this subject, since digital harms may overlap or occur simultaneously. The typology developed in this report attempts to reflect that complexity.

Third, it is important to acknowledge the absence of sufficient literature examining the direct causal relationships between specific touchpoints and harms across the varied contexts that constitute the lived experience of Indian children today. While this report provides a systematic overview of what the existing literature discloses, the absence of India-specific empirical research on the causal relationship between touchpoints and harms remains a gap that future dedicated studies will need to address.

Doctrinal Legal Analysis

The report undertakes a doctrinal and textual analysis of Indian laws to assess the extent to which the harms identified through the scoping review are recognised and addressed.

The analysis is structured around the distinct modes through which the law is observed to engage with this subject, developed in full in Chapter 5:

- direct prohibition and criminalisation of a harm, or of the conduct producing it;
- regulation of the conduct of ecosystem stakeholders through duties, standards, and obligations;
- incidental and interpretive inclusion of a harm within the scope of a broader provision not specifically designed to address it;
- the creation of rights-based protective frameworks tailored to children as a vulnerable population;

This doctrinal analysis assesses the presence and extent of legal coverage; it does not assess the normative appropriateness of that coverage. The report does not equate the existence of a legal response as the right response, nor does it speak to implementation quality, institutional readiness, or alignment with cross-sectoral consensus. Judicial interpretation of statutory provisions and executive practice are fast-evolving and have therefore been incorporated only where they have materially shaped the operative meaning of a provision. These are distinct inquiries whose dynamic character places them beyond the scope of a scoping review and doctrinal exercise, and they merit dedicated research from the relevant stakeholders.

Comparative Legal Analysis

Digital safety of children has emerged as a focal issue in several jurisdictions, which have adopted a range of response models.

The comparative analysis covers fourteen jurisdictions, drawn from across the five United Nations regional groups, so that the analysis reflects a diverse range of political, social, and legal contexts. The analysis examines both national legal frameworks and international and supranational instruments developed by bodies such as the United Nations, the European Union, the Organisation for Economic Co-operation and Development (“OECD”), and the African Union.

The comparative review is confined to enacted, legally binding legislative or regulatory frameworks. Proposed legislation (draft bills), including instruments under consultation, and non-binding guidance documents are excluded from this comparative review. Where authoritative English translations of foreign statutes were unavailable,

the analysis relied upon secondary literature, academic commentary, and other accessible interpretive sources. The comparative analysis reflects the state of law as of 15 May 2026.

Expert Consultations

The foregoing methods were supplemented by structured expert consultations convened virtually in 2025. Consultations were held with experts across the disciplines of law, medicine, and psychology, and with stakeholder groups working directly with children, including schools, technology companies, international bodies, and civil society organisations operating at the grassroots level. A larger group convening was also held to allow for a structured exchange of views across experiences, expertise, and disciplines.

The breadth of representation was intentional. Speaking to limited groups in silos, without allowing different disciplines to present their views on the identified issues, would have produced a fragmented understanding of both the problem and the responses it requires, the very condition that is symptomatic of the regulatory ecosystem today. This report has benefited from the full range of perspectives that bear on the issues it seeks to address.

The consultations were organised around the report's methodology and core research questions. Inputs were invited on the nature and range of children's interactions with digital technologies that is, the touchpoints, the contexts of use, and the factors that shape usage patterns across

different demographic and socio-economic groups. Stakeholders were also asked structured questions on the harms arising from those interactions, with particular attention to how a child's age, gender, and socio-economic circumstances affect their exposure and vulnerability. Participants further offered inputs on the adequacy of existing legal and policy measures, and on alternative, non-regulatory mitigation strategies relevant to specific contexts.

These discussions served functions that the scoping review and doctrinal analysis could not. On the question of digital touchpoints, they surfaced dimensions not fully captured in the Indian literature, including the role of digital public infrastructure systems, institutional surveillance technologies in educational settings, and the position of the State as both regulator and participant in children's digital environments. On harm identification, they informed decisions about classification and terminology, and surfaced social, physical, and psychological specificities that the literature lacks. The consultations also raised the question of children's own participation in research of this kind, which was identified as the subject of a much-needed future empirical study.

The findings from the consultations serve as a source of contextual grounding and as an instrument of methodological, analytical, and normative validation. Where consultation inputs bear significantly on the analysis or conclusions, this is noted in the relevant section of the report.

CHAPTER 3

Children and Digital Technology

**An Overview of Interaction
Touchpoints**

3

Children and Digital Technology: An Overview of Interaction Touchpoints

The digital environment children inhabit is constituted by a range of technologies and the interactions they make possible. This chapter maps the touchpoints through which children interact with digital technology. A touchpoint is any point at which a child and a digital technology come into contact, either through the child's own engagement, as in picking up a device or opening an application, or through exposure the child does not necessarily choose, as with the surveillance and identification systems that increasingly operate around them. The chapter organises these touchpoints into three categories: products, services, and content, before turning to the ecosystem of actors whose roles and responsibilities shape how children encounter them. It does not treat the touchpoints as inherently harmful. Instead, it identifies them structurally, so that the analysis of harms and of legal coverage that follows rests on an accurate account of the environment in which children and digital technology meet.

Three categories of touchpoints



Product



Service



Content

3.1 ‘Digital Touchpoints Not Just Online Touchpoints’

A foundational decision in this study is to describe children’s interactions in terms of the ‘digital’ environment rather than the ‘online’ one. The term ‘online’ and the vocabulary around it suggests that there is a bounded environment that children may connect to and disconnect from, or that there is an “offline” world lying outside the online world. Such a conception births false suppositions and can misguide how we understand harms and ways to mitigate them, leading to misguided policies with unwanted byproducts.

A child recorded by a classroom surveillance system, carrying an identity token, wearing a device that tracks health and movement or provides assistance, are instances of sustained digital interactions without the child ‘going online’ or ‘being online’. Rather than conceiving their interactions with technology as distinct events occurring multiple times over different periods of time, this report treats the technologically mediated world as a condition that children inhabit.

The instruments governing this field also hold the ‘digital’ world as the subject of discussion, rather than the ‘online’ world. The United Nations Convention on the Rights of the Child (“**UNCRC**”), in General Comment No. 25 (2021), defines the digital environment to encompass “information and communications technologies, including digital networks, content, services and applications, connected devices and environments, virtual and augmented reality, artificial intelligence, robotics, automated systems, algorithms and data analytics, biometrics and implant technology”³. The OECD, on revising its 2012 Recommendation on the Protection of Children Online, renamed it in 2021 the Recommendation on Children in the Digital Environment, discarding the online frame⁴. This report therefore examines children’s interactions

with digital technology in the broader sense, in line with the complexities noted by the United Nations Educational, Scientific and Cultural Organization, that while all digital technologies share the ability to process and communicate information in digital form, they differ widely in characteristics, roles, and applications⁵.

...this report treats the technologically mediated world as a condition that children inhabit.

3.2 Classification of touchpoints

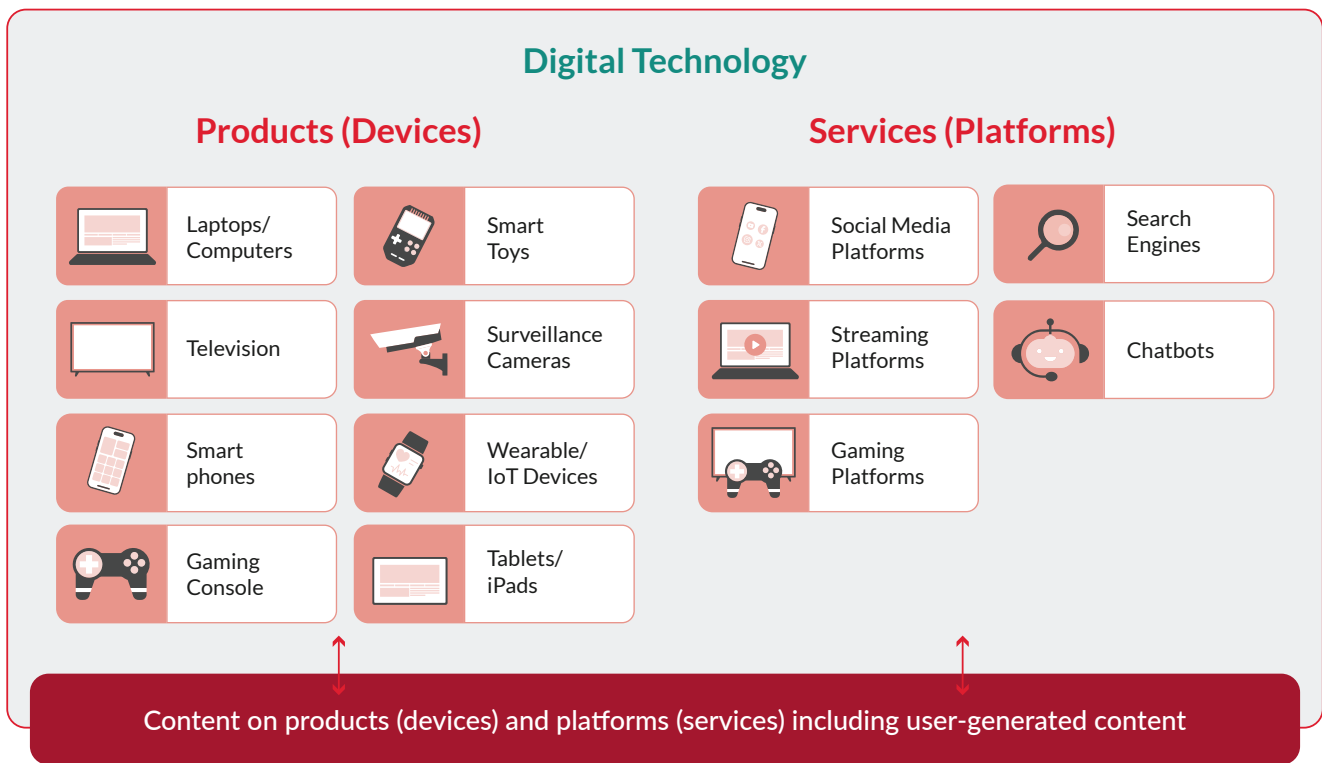
Children’s interactions with digital technology are mediated by many kinds of technology and many modes of engagement. The interdisciplinary literature which was studied examines these touchpoints across varied settings, context, actors, and socio-economic groups. However, that literature has studied them in isolation, with respect to a specific mode in a specific context, for a specific group. A child does not encounter touchpoints one at a time. They operate together, in different levels of continuity and context. It is the combination of these touchpoints that shapes a child’s overall experience of the digital environment. Examining them apart cannot capture the experience in a manner that is necessary to understand the ‘state of the system’.

To overcome this, the report organises the twelve touchpoints identified through the scoping review into three broad categories: products (devices), services (platforms), and content (whether user-generated or otherwise). Each category involves distinct actors and modes of interaction, but they are closely interconnected in practice, and a single interaction will often engage more than one at the same time. The figure below illustrates this structure.

³ UN Committee on the Rights of the Child, General Comment No 25 (2021) on Children’s Rights in Relation to the Digital Environment, UN Doc CRC/C/GC/25 (2 March 2021).

⁴ OECD, Recommendation of the Council on Children in the Digital Environment (OECD/LEGAL/0389, adopted 16 February 2012, amended 31 May 2021) <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0389> accessed 5 August 2026.

⁵ Carolina Castro-Grau and Magdalena Claro, The Role of Digital Technologies in 21st Century Learning (UNESCO International Institute for Educational Planning (IIEP) Buenos Aires Office for Latin America 2023) https://unesdoc.unesco.org/ark:/48223/pf0000386981_eng accessed 29 July 2026.



Infographic 1: Digital Touchpoints

Alt Text: Digital Technology, split into Products (Devices) — laptops/computers, smart toys, television, surveillance cameras, smartphones, wearable/IoT devices, gaming console, tablets/iPads — and Services (Platforms) — social media platforms, search engines, streaming platforms, chatbots, gaming platforms. Both connect to content on products and platforms.

3.2.1 Products (devices)

Devices are the physical tools through which children access and engage with digital technology. The review identified the following as the main devices through which children interact with digital technology: smartphones, laptops, tablets, televisions, gaming consoles, wearables, Internet of Things devices, and smart toys.

While some devices require active and conscious engagement, in the Indian context, it is found that such engagement may be layered with elements of domestic digital life, such as the high proportion of shared device usage noted above. The device is therefore not always a dedicated unsupervised point of access. Depending on the context, the device usage of a child may or may not be under the oversight of a responsible adult.

Other devices create interactions that may be passive. Wearables and Internet of Things devices collect and process data through sensors which do not require active engagement from the child. However, tracking movements, location, or physiological activity, and its usage, are background processes that the child may not be aware of, and that adults responsible for their welfare may not be monitoring. A 2026 survey found that over a fifth of parents of

The nature of the interaction created by the device varies across the type of device, the context of use, and the degree to which the child is an active or passive participant in the interaction.

children between the ages of 11 and 18 were largely unaware of their children's online activity⁶. Smart toys extend this model into play contexts by incorporating internet connectivity, voice interaction, and, in some cases, integration with the child's physical environment. As a result, they may continuously collect behavioural data without the child's awareness. Gaming consoles, while requiring active engagement, create networked social environments that extend well beyond the game itself. They incorporate real-time interaction with other users, diverse communication features, and in some cases financial transactions as well. This makes them sites of interaction whose full character is not always visible to those outside it.

Another relevant dimension is whether the interaction is chosen or mandated. Devices in educational settings, such as tablets, laptops and interactive boards incorporated into school infrastructure situate the child in digital interactions that they cannot opt out of. Expert consultations conducted for this report highlighted that institutional technologies, including surveillance cameras and biometric systems in schools represent touchpoints that are frequently overlooked in discussion of children's digital safety, despite involving significant data collection and the absence of meaningful consent mechanisms. Televisions, increasingly internet connected, occupy a similar context as a shared household device whose interactive dimensions may not always follow a conscious and informed decision regarding engagement.

3.2.2 Services (platforms)

Services are the systems and applications that operate on or through devices. These are designed environments which organize, mediate, and shape the nature of the child's interaction with digital technology. The scoping review identified the following as the primary services through which children interact with digital technology: social media platforms, streaming platforms, gaming platforms, search engines, and conversational tools

...the service itself is an actor in shaping what the child encounters, how long they remain engaged, and a determiner of subsequent actions.

including chatbots and large language models.

Services may not be passive conduits. Services are often designed for sustained engagement through algorithmic personalization, recommendation systems, or notification mechanisms. These are used to both analyse user behaviour and tailor interactions. This means that, in such cases, the service itself is an actor in shaping what the child encounters, how long they remain engaged, and a determiner of subsequent actions.

Social media platforms, including those primarily oriented towards short-form video content, image sharing, and text-based communication facilitate social interaction, self-expression, and content sharing among users. They are general-purpose platforms, not designed specifically for children, yet widely accessible by them. Several platforms are now creating separate interfaces as dedicated spaces for children, ensuring that they continue to engage with the platform albeit with different features. Their architecture is structured around user-generated content, social feedback mechanisms such as 'likes' and 'comments', and recommendation systems that surface content based on prior behaviour. The actors involved in a child's experience on social media may not only be the platform, but also users (both known and unknown) whose content, behaviour, and responses shape the child's interaction, including in ways that no single actor may control.

Streaming platforms provide access to audio-visual content organized through recommendation systems that continuously surface material based on viewing history and other algorithms. Unlike social media platforms, the service is not strictly

⁶ Young Leaders for Active Citizenship, How Young Indians Navigate Digital Life: Findings from the Student Cyber Resilience Education and Empowerment Nationwide (SCREEN) Survey 2026 (British Asian Trust and BT Group, January 2026) <https://www.britishasiantrust.org/media/1gvn0rhx/screen-survey-2026.pdf> accessed 4 August 2026.

centred around social exchange. Instead, the interaction is primarily one of consumption, in which the child interacts with content produced by others, rather than producing content themselves. However, the recommendation architecture means that the content a child encounters is not simply what they may have chosen, diffusing their control over it. In other words, it may be difficult to draw the distinction between the child's choice and the platform's curation during the interaction.

Gaming platforms create interactive environments around rules, objectives, and feedback mechanisms designed to sustain engagement. Many contemporary gaming platforms are networked, enabling real-time discussions with known and unknown users, which may be one-to-one, one-to-many, or many-to-many. Gaming platforms therefore assume the character of entertainment forums, social spaces, and in some instances, commercial marketplaces, with a corresponding range of actors and relationships. Unlike streaming platforms, the child participates more actively here, and their participation, choices, and behaviours are a part of that interaction, arguably diffusing control.

Search engines and conversational tools, including chatbots and large language models, function as interfaces through which children create or access information. These are index and retrieve environments based on user queries, rather than social settings or content consumption platforms. Search engines, in addition to retrieving content, surface it according to algorithms which, in most cases, are based on relevance, and in a commercial context, on paid placements as well. Conversational tools process natural language inputs and generate responses based on underlying computational models. Both categories present the child with outputs which, without appropriate information about the platforms, appear authoritative and personalized, but may be shaped by processes that are opaque to the child and the parents or guardians responsible for them. Expert consultations conducted for this report identified children's interactions with large language model applications as an emerging touchpoint which goes beyond responses to search queries and are observed to spill over into companionship and support.

3.2.3 Content

Content refers to the material that is accessed, created, or shared through devices and services. In *Infographic 1: Digital Touchpoints*, content is positioned below and flowing from both products and services, as an independent element of interaction, but not a discrete tool or environmental feature that exists free of other touchpoints.

Unlike devices and services, content may not have a single identifiable point of origin or control. User-generated content, which constitutes a significant proportion of material in contemporary digital environments, is produced by a wide and often anonymous range of actors, distributed through platform systems, and encountered by children in contexts which may be removed from the original act of creation. The absence of a single identifiable point of origin or control is a defining structural characteristic of digital content.

A related feature is that content, once created and shared, may persist and circulate across devices and platforms beyond the control of the child who produced or encountered it. Permanence and cross-platform mobility of content is another set of features of content which influence how the touchpoint is situated, particularly where they circulate even after the interaction has ended.

It is also important to note that children occupy a dual position in relation to content, that they may not occupy in relation to devices or services. They are consumers of material produced by others, and also producers of content. This dual position is a relevant feature of content as a touchpoint where questions of harm and safety are concerned. Content is also the category of touchpoint in which the child's developmental stage is most directly relevant. Children are at fundamentally different stages of cognitive, emotional and social development, which impact the implications of the content on the child depending on where they are in that spectrum.

Intersections and overlaps

While the classification into products, services, and content provides a structured framework for analysis, these categories do not operate independently in practice. A single

interaction may engage all three simultaneously, such as when a child is watching a video, they engage a device, a platform, and content on it all at once. The effects of any given interaction, and the harms that may arise from it, may be the combination of the features of all three. For understanding the harm, it is important to analyse how different elements interact.

Finally, it is important to highlight that digital technology is continuously evolving, and so are the touchpoints through which children engage with it. New devices, platforms, and forms of content continue to emerge, and AI is increasingly embedded in everyday applications that generate responses and adapt to user behaviour. At the same time, immersive technologies such as virtual and augmented reality, along with smart and connected devices, are making interactions more continuous and less visible. As a result, touchpoints are not fixed but constantly shifting, requiring ongoing review and adaptation to understand children's evolving interactions with technology.

...digital technology is continuously evolving, and so are the touchpoints through which children engage with it.

3.3 Touchpoint Ecosystems

The report seeks to identify the ecosystem within which digital touchpoints operate, situating children's interactions with technology within a broader network of influences and relationships. This enables a clearer understanding of how these interactions are shaped and where responsibilities may lie.

Within this ecosystem, a range of actors carry different roles and responsibilities that influence how children access and engage with digital technology. These roles are not fixed and often overlap, reflecting the complexity of digital environments.

In the case of devices, parents or guardians often act as gatekeepers. They provide access, set boundaries, and guide usage. Their role is shaped by awareness, resources, and social context. Children, as users, bring their own preferences and behaviours to these interactions.

Manufacturers and software developers design devices and applications. Their choices affect usability, safety features, and data practices. Internet service providers and telecom operators enable connectivity. Educational institutions influence usage by integrating digital tools into learning environments.

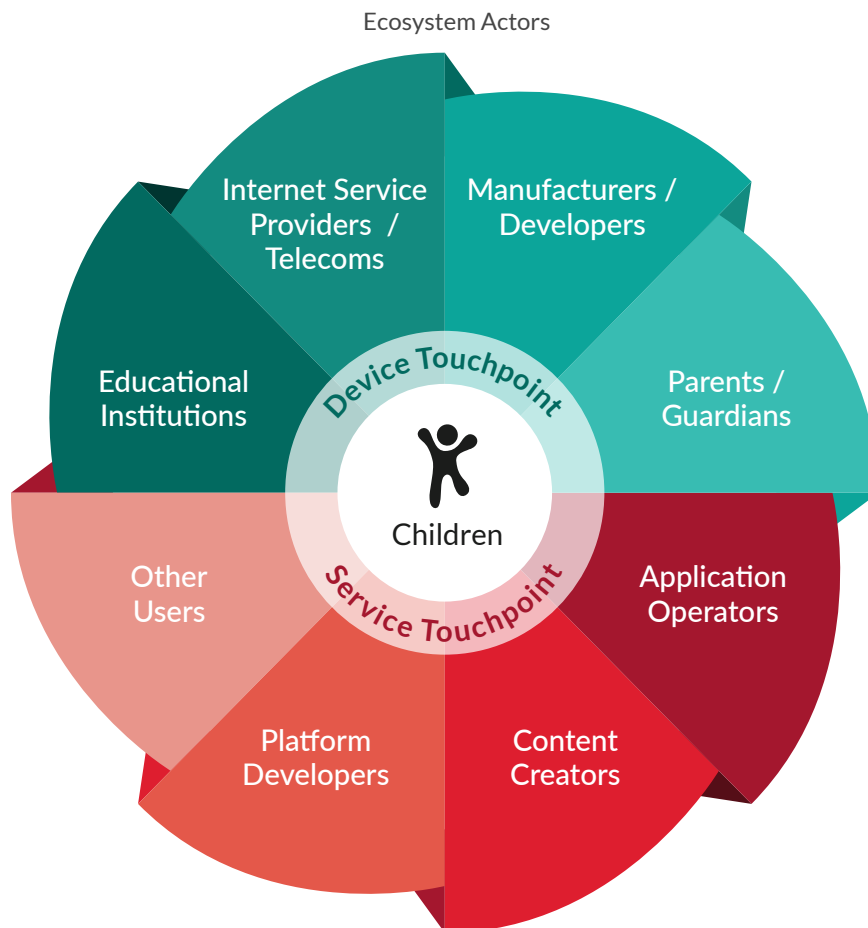
For services, additional actors are involved. Platform developers design systems of interaction. Application operators manage functionality. Content creators produce material that circulates on these platforms. Other users also contribute to content, especially in interactive environments.

Regulators provide the legal and policy framework within which these actors operate. However, the pace of technological change often creates gaps between regulation and practice.

The touchpoints and actors mapped in this chapter constitute the terrain within which children's digital lives unfold. Each touchpoint, in addition to representing an entry-point, also presents as an avenue for cultivating

children's safety, development, and rights in suitable contexts. The actors who populate this ecosystem each carry nuanced visibility and responsibility for what occurs within it. The following chapter locates and examines harms that existing literature has documented in children's interaction with technology across these touchpoints and actors.

Understanding the structure of interactions allows for the harm analysis in the following chapter to move beyond a catalogue of adverse outcomes, towards an understanding of the conditions under which those outcomes arise.



Infographic 2: The touchpoints and actors constitute the terrain within which children's digital lives unfold

Alt Text: Ecosystem Actors around Children at the centre, split into Device Touchpoint — Internet Service Providers/ Telecoms, Manufacturers/Developers, Parents/Guardians, Educational Institutions, and Service Touchpoint — Application Operators, Content Creators, Platform Developers, Other Users.



CHAPTER 4

Harms and Touchpoints

4

Harms and Touchpoints

The previous chapter mapped and analysed the various touchpoints that act as interfaces between children and the digital world. This chapter undertakes the subsequent inquiry of whether and what harms may arise from their interactions with such touchpoints. It reviews existing literature across the domains of medicine, law, psychology, and development studies, and builds on inputs gathered during stakeholder consultations, to identify whether harms may indeed arise in this context, and if so, what those harms are.

The chapter is divided into two sections. The first section derives a working definition of “harm” for the purposes of this report. The second section enumerates fourteen harms to children in their interactions with digital technology.

4.1 Definition of “Harm”

4.1.1 Methodology

The term “harm”, in the context of child protection, has not been defined as such in any Indian statute. This report, therefore, undertakes a first-order exercise of developing this definition for its purposes. It analyses the following sources for this purpose: (a) Indian statutes that either define “harm”, albeit in a different context, or refer to cognate concepts that are closely allied to the concept of “harm”; and (b) international or supranational treaties and legal texts, most notably, the UNCRC, to which India is a party.⁷

⁷ United Nations Convention on the Rights of the Child, 1989 (adopted 20 November 1989, entered into force 2 September 1990) 1577 UNTS 3.

4.1.2 Defining “Harm”

A definition of “harm” in this context should take into account not only how the term and other allied phrases have been used in existing legislations but also consider the broader values and interests that laws pertaining to children seek to promote and protect. To this end, the use, meaning, import and spirit of the term is gleaned from statutes related to safety of children presently in force in India.

The Protection of Children from Sexual Offences (“POCSO”) Act, 2012 identifies prevention and redressal of sexual abuse and exploitation of children as its primary goal. It notes that the “physical, emotional, intellectual and social development of the child” is a paramount value that the Act seeks to uphold⁸. Thus, the legislation views prevention of sexual exploitation not as an end in itself, but as a means to protect certain values essential for the dignified upbringing of a child.

The Juvenile Justice (Care and Protection of Children) Act, 2015 (“JJ Act”) defines a “child in need of care and protection” as a child, inter alia, having been subjected to exploitation, abuse and neglect⁹. The inclusion of ‘neglect’ to this list presupposes the notion that harm to a child, and the need for protection, may arise from both commission and omission of certain acts. The JJ Act also provides interpretive tools, including the principle of the ‘best interest of the child’, and ‘protection of the dignity and rights of the child’.¹⁰

In the context of personal data protection, the DPDP Act, prohibits data fiduciaries from processing personal data of a child that is “likely to cause any detrimental effect on the well-being of a child”.¹¹

Therefore, in addition to the protection of the safety, rights and interests of a child as mentioned above, the law imposes a duty to protect the “well-being” of a child.

The Consumer Protection Act, 2019, though not specifically pertaining to children’s safety, adopts an expansive definition of “harm” in relation to product liability.¹² In addition to physical injury, the definition of “harm” encompasses “mental agony or emotional distress attendant to personal injury”.¹³

The Protection of Women from Domestic Violence Act, 2005, extends protection to children from “physical”, “sexual”, “verbal”, “emotional” and “economic” abuse, thereby recognizing each of them as specific domains which deserve recognition and protection.¹⁴

Similar reflections are found in the UNCRC. The UNCRC provides useful guidance on the values and interests to be advanced to protect children. The Convention specifies that, “in all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration.”¹⁵ The drafting here is relevant in that it recognizes ‘interests’, and not ‘rights’ which require statutory recognition. The UNCRC mandates States to take measures in order to “protect the child from all forms of physical or mental violence, injury or abuse, neglect or negligent treatment, maltreatment or exploitation, including sexual abuse”.¹⁶ Further, the Convention mandates protection against “economic exploitation”,¹⁷ supporting the notion that harm to children can arise in the economic sphere as well.

⁸ Protection of Children from Sexual Offences Act, 2012, Statement of Objects and Reasons.

⁹ Juvenile Justice (Care and Protection of Children) Act, 2015, s 2(14)(iii).

¹⁰ *ibid* s 3.

¹¹ Digital Personal Data Protection Act, 2023, s 9(2).

¹² Consumer Protection Act, 2019, s 2(22).

¹³ *ibid*.

¹⁴ Protection of Women from Domestic Violence Act, 2005, s 3(a).

¹⁵ United Nations Convention on the Rights of the Child, 1989, art 3.

¹⁶ *ibid* art 19(1).

¹⁷ *ibid* art 32(1).

The foregoing analysis shows the range of values and interests that different statutes in India, as well as the UNCRC seeks to protect across different types of harms. Based on the same, and for the purposes of this report, the following broad-based definition of “harm” is adopted:

“Harm” refers to any effect that is detrimental to the physical, mental, emotional, developmental or sexual safety and well-being of a child, or has an adverse impact on the rights and interests of a child.

4.2 Identification of “Harm”

This chapter undertakes a scoping survey of secondary literature, and builds on inputs emerging from stakeholder consultations, to identify harms to children in digital spaces. Most of the studies surveyed are either empirical or experimental in nature or are doctrinal studies that make use of empirical evidence. The date range for such studies has been fixed between 2010 and 2025, reflecting the fact that notable technological strides in the digital sphere have largely taken place post-2010.

It may be noted that this exercise does not seek to draw any causation between the harms and the digital interaction where none exists in the underlying study examined or stakeholder input referred to. Further, the harms identified, their definitions and scope are strictly in relation to those identified or studied in secondary literature or gathered from stakeholder consultations.

4.2.1 Enumerating Harms

1. Sleep disturbances

In an empirical, questionnaire-based study conducted among school children between classes 8 and 10 in rural areas near Pune, a correlation was found between increased screen time and inadequate sleep, often by delaying sleep time.¹⁸ Approximately 83% of the surveyed school children exhibited excessive screen time, with mobile phones being the most commonly used device for screen exposure (used by 99% of the participants).¹⁹ Further, the Indian Academy of Paediatrics has identified emission of blue light from digital devices as a contributing factor to sleep disturbance.²⁰

2. Obesity and musculo-skeletal problems

In an empirical, questionnaire-based study conducted among 8 to 10 year old schoolchildren in Delhi, excessive screen time was found to be associated with physical inactivity and poor eating behaviour, which could increase the risk of children being overweight or obese.²¹ The Indian Academy of Paediatrics reports that excessive screen media use in children is linked to obesity, partly because associated sleep deprivation can alter hunger-regulating hormones such as ghrelin and leptin, increasing appetite and reducing satiety.²²

A scoping study examining the association between screen time and musculoskeletal pain in adolescents found a positive association between the two, noting that the thoracolumbar, back and cervical regions were the most frequent anatomical locations. Screen times greater than 4 hours were found to lead to musculoskeletal

¹⁸ R John, A Pokale, A Chutke and others, ‘Prevalence of excess screen time among secondary school children in rural India’ (2024) 64(4) Journal of Preventive Medicine and Hygiene 457, available at <https://pmc.ncbi.nlm.nih.gov/articles/PMC10876028/#sec1-1> accessed 10 October 2025.

¹⁹ R John, A Pokale, A Chutke and others, ‘Prevalence of excess screen time among secondary school children in rural India’ (2024) 64(4) Journal of Preventive Medicine and Hygiene 457, available at <https://pmc.ncbi.nlm.nih.gov/articles/PMC10876028/#sec1-1> accessed 10 October 2025.

²⁰ P. Gupta, D Shah, N Bedi and others, ‘Indian Academy of Paediatrics Guidelines on Screen Time and Digital Wellness in Infants, Children and Adolescents’ (2022), available at <https://www.indianpediatrics.net/mar2022/235.pdf> accessed 10 October 2025.

²¹ R Semar and N Bakshi, ‘Correlation of screen time with eating behaviour among school-going children aged 8 to 10 years in East Delhi, India’ (2023) Journal of Indian Association for Child and Adolescent Mental Health 1, available at <https://journals.sagepub.com/doi/full/10.1177/09731342221144877#bibr18-09731342221144877> accessed 10 October 2025.

²² P. Gupta, D Shah, N Bedi and others, ‘Indian Academy of Paediatrics Guidelines on Screen Time and Digital Wellness in Infants, Children and Adolescents’ (2022), available at <https://www.indianpediatrics.net/mar2022/235.pdf> accessed 10 October 2025.

pain, with intensity depending on the frequency of use of the screens, as well as on the simultaneous use of devices.²³ A systematic review examining a potential association between personal electronic device usage and musculoskeletal disorders in children aged 5-17 years, however, concluded that there is preliminary evidence to support the idea that factors such as duration spent on the device, type of device, and position adopted, may be associated with musculoskeletal pain in children and adolescents. That said, the study concluded that further research is needed to definitively identify the risk factors for musculoskeletal pain associated with personal electronic device usage in children and adolescents.²⁴

3. Impairment of eyesight due to digital device usage

A scoping survey of relevant literature between 2021 and 2023 found that early exposure (before the age of 1 or 2 years) to digital technologies was associated with eyesight-related issues.²⁵

4. Depression and suicidal ideation

A scoping review of literature on adolescent social media use noted that social media use has generally been correlated with depressive

symptoms, although some findings were inconsistent and the quality of evidence varied across studies.²⁶ Another qualitative study reviewing medical literature observed that problematic internet and smartphone use may be associated with depressive symptoms, loneliness and social isolation among adolescents.²⁷ Literature surveys have found that increased use of social media has been linked to self-harm behaviour, since adolescents often tend to emulate the self-injurious behaviour of others online.²⁸

5. Stress and anxiety

A study examining the impact of Information and Communication Technology (“ICT”) use on salivary cortisol patterns among 72 school children aged 10 and 13 found that children who had used ICT for an average of three hours on the preceding day showed a significantly reduced cortisol awakening response the next day. The study suggested that prolonged ICT use may be associated with stress-related changes in cortisol regulation.²⁹

Literature has also found a profound influence of social media on adolescent mental health, including anxiety.³⁰ Excessive social media use has been associated with increased loneliness, social comparison, and fear of missing out, all of which are

²³ Sérgio Soares da Silva and others, ‘Screen Time and Musculoskeletal Pain in Adolescents: A Systematic Review’ (2020) 10 International Journal of Development Research 35745, available at <https://www.journalijdr.com/screen-time-and-musculoskeletal-pain-adolescents-systematic-review> accessed 5 August 2026.

²⁴ A Clark and others, ‘The Relationship Between Usage of Personal Electronic Devices and Musculoskeletal Pain in Children and Adolescents: A Systematic Review’ (2024) 15 Association of Paediatric Chartered Physiotherapists Journal 28, available at <https://apcp.csp.org.uk/sites/default/files/journal/2024-12/JOURNAL%20A.Clark%20A%20Cooper-Ryan%20T%20Brown%20S%20Preece%20A%20Clarke-Cornwall.pdf> accessed 4 August 2026.

²⁵ S Selak, J Horvat and M Zmavc, ‘Problematic Digital Technology Use Measures in Children Aged 0-6 Years: A Scoping Review’ (2025) 12 JMIR Mental Health 1, available at <https://mental.jmir.org/2025/1/e59869/> accessed 10 October 2025.

²⁶ A M Khalaf, A L Alubied and others, ‘The Impact of Social Media on the Mental Health of Adolescents and Young Adults: A Systematic Review’ (2023) Cureus 1, available at https://assets.cureus.com/uploads/review_article/pdf/176889/20230904-18910-555yiy.pdf accessed 11 October 2025.

²⁷ K Krishnamurthy, A Bharatha and others, ‘Navigating the Digital Dilemma: Internet and Smartphone Addiction among Children and Adolescents’ (2025) Advances in Human Biology 53, available at https://journals.lww.com/adhb/fulltext/9900/navigating_the_digital_dilemma_internet_and.103.aspx accessed 11 October 2025.

²⁸ A M Memon, S G Sharma and others, ‘The role of online social networking on deliberate self-harm and suicidality in adolescents’ (2018) 60(4) Indian Journal of Psychiatry 384, available at https://journals.lww.com/indianjpsychiatry/fulltext/2018/60040/the_role_of_online_social_networking_on_deliberate.3.aspx accessed 11 October 2025.

²⁹ M Wallenius, A Hirvonen and others, ‘Salivary Cortisol in relation to the Use of Information and Communication Technology (ICT) in School-Aged Children’ (2010) 1(2) Psychology 88, available at <https://www.scirp.org/journal/paperinformation?paperid=2100> accessed 11 October 2025.

³⁰ T Masri-zada and others, ‘The Impact of Social Media & Technology on Child and Adolescent Mental Health’ (2025) 9 J Psychiatry Psychiatr Disord 111, available at <https://pmc.ncbi.nlm.nih.gov/articles/PMC12165459/> accessed 4 August 2026.

risk factors for developing or exacerbating anxiety in adolescents.³¹

A central factor contributing to these negative effects is social comparison. Female adolescents, particularly, may experience heightened stress from online bullying, cyberstalking, or social exclusion, all of which have been found to be linked to increased anxiety.³² Social media is also changing communication patterns among adolescents. A growing number of young people experience greater ease with text-based and digital messaging than with direct, face-to-face interaction. Consequently, in-person exchanges may provoke heightened anxiety, particularly for adolescents who already struggle with social anxiety.³³

6. Lowered self-esteem and body image issues

The Indian Academy of Paediatrics, in a review of literature on social media use among adolescents, noted that certain online behaviours and negative social comparisons on social media may be associated with low self-esteem, body image concerns, and other adverse psychological impacts in vulnerable adolescents.³⁴ This correlation is explained by citing a negative reinforcement mechanism; a lower number of “likes” or more negative comments on a post can lower one’s

own perception of oneself, further fuelled by comparisons on social media.³⁵ In a scoping review of literature published between 2008 and 2014, low self-esteem was identified as one of several factors associated with increased online risk behaviours among adolescents using social networking sites.³⁶ These studies highlight the complex relationship between digital use and how children perceive themselves, with online content often inviting or inducing harmful comparisons with a “perfect” yardstick, which may be entirely fictional or socially constructed.

7. Addiction to digital devices

A scoping study observed that overexposure to digital environments in very young children may contribute to the deregulation of serotonin and dopamine neurotransmitter pathways in the developing brain. The study noted that these effects have been associated with online activity abuse and internet addiction and are akin to those observed in severe substance abuse syndromes.³⁷ In a medical case study involving a 9-year-old child, it was observed that addictive screen time use may reduce social coping behaviours and involve craving patterns resembling substance dependence. The study also noted that digital media addictive behaviour may be associated with brain structural changes related to cognitive control and emotional

³¹ Cheng Huang, ‘Time Spent on Social Network Sites and Psychological Well-Being: A Meta-Analysis’ (2017) 20(6) *Cyberpsychology, Behaviour, and Social Networking* 346, available at <https://pubmed.ncbi.nlm.nih.gov/28622031/> accessed 4 August 2026.

³² Elizabeth M Seabrook, Margaret L Kern and Nikki S Rickard, ‘Social Networking Sites, Depression, and Anxiety: A Systematic Review’ (2016) 3(4) *JMIR Mental Health* e50 <https://pmc.ncbi.nlm.nih.gov/articles/PMC5143470/> accessed 5 August 2026.

³³ Jean M Twenge and W Keith Campbell, ‘Associations between screen time and lower psychological well-being among children and adolescents: Evidence from a population-based study’ (2018) 12 *Preventive Medicine Reports* 271 <https://pmc.ncbi.nlm.nih.gov/articles/PMC6214874/> accessed 5 August 2026; John A Naslund and others, ‘Social Media and Mental Health: Benefits, Risks, and Opportunities for Research and Practice’ (2020) 23(1) *JMIR e23244* <https://pmc.ncbi.nlm.nih.gov/articles/PMC7785056/> accessed 5 August 2026.

³⁴ P. Gupta, D Shah, N Bedi and others, ‘Indian Academy of Paediatrics Guidelines on Screen Time and Digital Wellness in Infants, Children and Adolescents’ (2022), available at <https://www.indianpediatrics.net/mar2022/235.pdf> accessed 10 October 2025.

³⁵ P. Gupta, D Shah, N Bedi and others, ‘Indian Academy of Paediatrics Guidelines on Screen Time and Digital Wellness in Infants, Children and Adolescents’ (2022), available at <https://www.indianpediatrics.net/mar2022/235.pdf> accessed 10 October 2025.

³⁶ Sonia Livingstone and Peter K Smith, ‘Annual Research Review: Harms experienced by child users of online and mobile technologies: the nature, prevalence and management of sexual and aggressive risks in the digital age’ (2014) 55(6) *Journal of Child Psychology and Psychiatry* 635, available at <https://acamh.onlinelibrary.wiley.com/doi/full/10.1111/jcpp.12197> accessed 11 October 2025.

³⁷ B Drespe-Langley, ‘Children’s Health in the Digital Age’ (2020) 17(9) *International Journal of Environmental Research and Public Health* 3240, available at <https://pubmed.ncbi.nlm.nih.gov/32384728/> accessed 11 October 2025.

regulation.³⁸

8. Impairment of cognitive development

A scoping review found that early exposure to digital screens before the age of 1 or 2 years was associated with poor cognitive development in some studies.³⁹ A broad based literature review spanning the years 2001 to 2024 observed that prolonged and excessive use of digital devices may contribute to cognitive overload, potentially affecting memory retention, learning processes, sustained attention, and deep focused thinking. The review further noted that prolonged exposure to screen-based multitasking may reduce the efficiency of neural circuits involved in concentration and attention. Overall, the review concluded that, while digital devices may offer numerous opportunities for cognitive enhancement, their use must be carefully managed to prevent adverse effects on, inter alia, children's cognitive development. It stated that further research is needed to fully understand the long-term impacts of digital device usage.⁴⁰

9. Cyberbullying and online harassment

A qualitative study by UNICEF noted that cyberbullying victimization is associated with lower psychological well-being and externalizing behaviours such as feeling angry or 'acting out'. Another finding was that more children are

bystanders of cyber-bullying than they are bullies or victims. It noted that perpetrators of cyber-bullying are more likely to also be victims. Online and offline perpetration and victimization are also highly correlated. Further, cyber-bullying victimization is associated with lower psychological well-being and externalizing behaviours.⁴¹ Literature also shows that these harms further fuel other harms to children. An empirical survey conducted among adolescents in Uttar Pradesh and Bihar found that victims of cyberbullying were at a higher risk of depressive symptoms and suicidal thoughts compared to adolescents who had not experienced cyberbullying victimisation.⁴²

10. Child sexual exploitation and abuse

Literature has noted the risk of sexual predators using the internet and social networks to groom young people for exploitation. The study further observed that young adolescents should be accompanied in their exploration of internet use, while older individuals should be educated about the associated online risks.⁴³ Another study observed that technological developments have increased the potential for the live streaming of child sexual abuse to proliferate, highlighting the role of digital technologies in facilitating such forms of harm.⁴⁴ Further, the susceptibility to harm is also not uniform when one takes into account the demographic characteristics and

³⁸ G Lissak, 'Adverse physiological and psychological effects of screen time on children and adolescents: Literature review and case study' (2018) 164 *Environmental Research* 149, available at <https://www.sciencedirect.com/science/article/abs/pii/S001393511830015X> accessed 11 October 2025.

³⁹ S Selak, J Horvat and M Zmavc, 'Problematic Digital Technology Use Measures in Children Aged 0-6 Years: A Scoping Review' (2025) 12 *JMIR Mental Health* 1, available at <https://mental.jmir.org/2025/1/e59869/> accessed 10 October 2025.

⁴⁰ V Javier Clement-Suarez, Ana I Beltran Velasco and others, 'Digital Device Usage and Childhood Cognitive Development: Exploring Effects on Cognitive Abilities' (2024) 11(11) *Children* 1299, available at <https://www.mdpi.com/2227-9067/11/11/1299> accessed 11 October 2025.

⁴¹ M Stoilova, S Livingstone and others, 'Investigating Risks and Opportunities for Children in a Digital World' (2021) Discussion Paper, available at <https://www.unicef.org/innocenti/media/5621/file/UNICEF-Investigating-Risks-Opportunities-Children-Digital-World-2021.pdf> accessed 12 October 2025.

⁴² C Maurya, T Muhammad and others, 'The effects of cyberbullying victimization on depression and suicidal ideation among adolescents and young adults: a three year cohort study from India' (2022) 22 *BMC Psychiatry* 1, available at <https://link.springer.com/article/10.1186/s12888-022-04238-x> accessed 12 October 2025.

⁴³ Pierre Andre Machaud and Caroline Free, 'Alice in Wonderland: Adolescents and Digital Technologies' (2016) *International Handbook on Adolescent Health and Development* 397, available at https://link.springer.com/chapter/10.1007/978-3-319-40743-2_20 accessed 12 October 2025.

⁴⁴ Larissa S Christensen, 'It's Like Poof and It's Gone: The Live-Streaming of Child Sexual Abuse' (2024) 28 *Sexuality and Culture* 1467, available at <https://link.springer.com/article/10.1007/s12119-023-10186-9> accessed 12 October 2025.

unique circumstances of each child. In a Swedish questionnaire-based study involving 3,432 high school students, sexual minority adolescents reported higher rates of sexual abuse, problematic offline sexual encounters with persons met online, and online harassment compared to heterosexual adolescents. The study further observed that victimised adolescents and sexual minority adolescents reported more psychiatric symptoms, lower self-esteem, and a weaker sense of coherence.⁴⁵ The effects of this harm are also gendered; a scoping survey observed that gender may shape children's online experiences, noting that some groups of girls are more vulnerable to social risks such as violence, gender discrimination, sexual harassment, and other harmful online experiences.⁴⁶

11. Breach of personal data and informational privacy

Digital interactions often impinge upon the right to privacy and the protection of personal data of children. A study published in *The Lancet* noted concerns regarding smart toys and digital platforms as potential sources of data extraction, including risks relating to security breaches and the commercial exploitation of children's personal information.⁴⁷ It has also been observed that digital parental control systems, which are commonly used by parents to monitor children's online activities, may compromise a child's privacy by revealing records of the child's online activity to parents.⁴⁸

Therefore, a measure meant to "protect" children may end up adversely impacting their rights and interests.

With respect to the right to privacy, the Indian Supreme Court has recognised various facets of privacy in addition to informational privacy, including bodily privacy (protecting the physical body from violation or restraint of movement), spatial privacy (concerning private spaces, like homes, where access by others can be restricted), and decisional privacy (the ability to make intimate personal choices, particularly those regarding sexual or procreative nature and relationships).⁴⁹ UNICEF has also recognised that children's right to privacy is multifaceted, and the physical, communications, informational and decisional aspects of children's privacy hold relevance in digital contexts as well.⁵⁰ That said, there is a dearth of empirical literature focused on such other facets of children's privacy in digital contexts, and is primarily focused on informational privacy. Therefore, the scope of this harm, for the purposes of this report, is limited to informational privacy of children in digital contexts.

12. Exploitation of children's labour in digital contexts

A qualitative study observed that 'sharenting', or the practice of parents sharing posts, images, and videos about their children on social media, may expose children to risks such as privacy violations, identity theft, cyberbullying, psychological harm,

⁴⁵ G Priebe and C G Svedin, 'Online or offline victimisation and psychological well-being: a comparison of sexual minority and heterosexual youth' (2012) 21(10) *European Child and Adolescent Psychiatry* 569, available at <https://portal.research.lu.se/en/publications/online-or-off-line-victimisation-and-psychological-well-being-a-c> accessed 12 October 2025.

⁴⁶ S Livingstone, A Nandi and others, 'Young adolescents and digital media: uses, risks and opportunities in low- and middle-income countries' (2017) LSE Research Online, available at https://eprints.lse.ac.uk/83753/1/Livingstone_Young_Adolescents_Digital_Media.pdf accessed 12 October 2025.

⁴⁷ I Kickbusch, D Piselli and others, 'The Lancet and Financial Times Commission on governing Health Futures 2030: Growing up in a Digital World' (2021) 398 *Lancet* 1727, available at <https://www.thelancet.com/action/showPdf?pii=S0140-6736%2821%2901824-9> accessed 12 October 2025.

⁴⁸ T Sangeetha, K Mythili and others, 'Age Based Content Controlling System using AI for Children' (2024) 10 *EAI Endorsed Transactions on Internet of Things* 1, available at <https://publications.eai.eu/index.php/IoT/article/view/5313/2945> accessed 12 October 2025.

⁴⁹ Justice KS Puttaswamy (Retd) v Union of India (2017) 10 SCC 1.

⁵⁰ UNICEF, *Children's Online Privacy and Freedom of Expression* (2018) 12. "Children's physical privacy is affected by technologies that track, monitor and broadcast children's live images, behaviour or locations. Children's communications privacy is threatened where their posts, chats, messages or calls are intercepted by governments or other actors, and children's informational privacy can be put at risk when children's personal data are collected, stored or processed. Children's decisional privacy may be affected by measures that restrict access to beneficial information, inhibiting children's ability to make independent decisions in line with their developing capacities."

and financial exploitation. The study further noted that child social media influencers may be vulnerable to financial exploitation because existing legal protections governing child earnings often do not apply to online content creation.⁵¹ Another qualitative study observed that companies and social media platforms may benefit from brand promotion through child influencers, while the compensation received by children for their labour may not always be fair.⁵²

13. Unhealthy relationship with money due to exposure to digital technologies

A literature review of 204 studies on the impact of digital money on children and young people's financial education noted that digital money increases impulsive spending, normalises financial risk-taking due to gamification, and fundamentally changes how children perceive and relate to money.⁵³ It was noted that as money becomes digital, it becomes more abstract and less tangible, thereby making it harder for children to grasp fundamental financial concepts compared to using physical cash.⁵⁴

Studies mapped in the same literature review also pointed towards a stable prevalence of gambling among children, with evidence of adolescents developing gambling disorders, influenced by various factors including low self-esteem and reduced parental supervision.⁵⁵

These concerns are not confined to real-money transactions. A survey examining adolescent involvement in simulated gambling activities, conducted across over 1,200 adolescents from seven secondary schools in Australia, found that a significant proportion of young people engage in a range of simulated gambling activities via internet gambling sites, social media, smartphone applications, and video games. Adolescents with a history of engagement in simulated gambling activities appeared to be at greater risk of endorsing indicators of pathological gambling.⁵⁶ Taken together, this body of evidence indicates that digital technologies may play a role in shaping children's financial attitudes, risk tolerance, and spending behaviours in ways that may have lasting consequences for their financial well-being.

14. Deterioration of pro-social behaviour and impairment of interpersonal development due to digital exposure

There is research to indicate that excessive digital media use is associated with a range of deteriorating social behaviours in children, including reduced empathy, weakened peer relationships, and an erosion of prosocial conduct. A cross-sectional study conducted across 400 school-going children aged 6–12 in Surat, India, found that behavioural difficulties, particularly hyperactivity, conduct problems, and peer difficulties, increased progressively with greater screen time exposure.⁵⁷

⁵¹ Charlotte Yates, 'Influencing "kidfluencing": Protecting Children by Limiting the Right to Profit from Sharenting' (2023) 25(4) *Vanderbilt Journal of Entertainment and Technology Law* 845, available at https://scholarship.law.vanderbilt.edu/cgi/viewcontent.cgi?params=/context/jetlaw/article/1607&path_info=Influencing_Kidfluencing_Protecting_Children_by_Limiting.pdf accessed 12 October 2025.

⁵² A Bakioglu, 'Digital Capitalism and Child Labour Exploitation on Youtube' (2024) 37(1) *Sociology Lens* 131, available at <https://onlinelibrary.wiley.com/doi/abs/10.1111/johs.12456> accessed 12 October 2025.

⁵³ Money and Pensions Service, 'The impact of digital money on children and young people' (2024, pg 4) <https://maps.org.uk/en/publications/research/2024/the-impact-of-digital-money-on-children-and-young-people> accessed 5 August 2026.

⁵⁴ *ibid* pg 24.

⁵⁵ *ibid* pg 12.

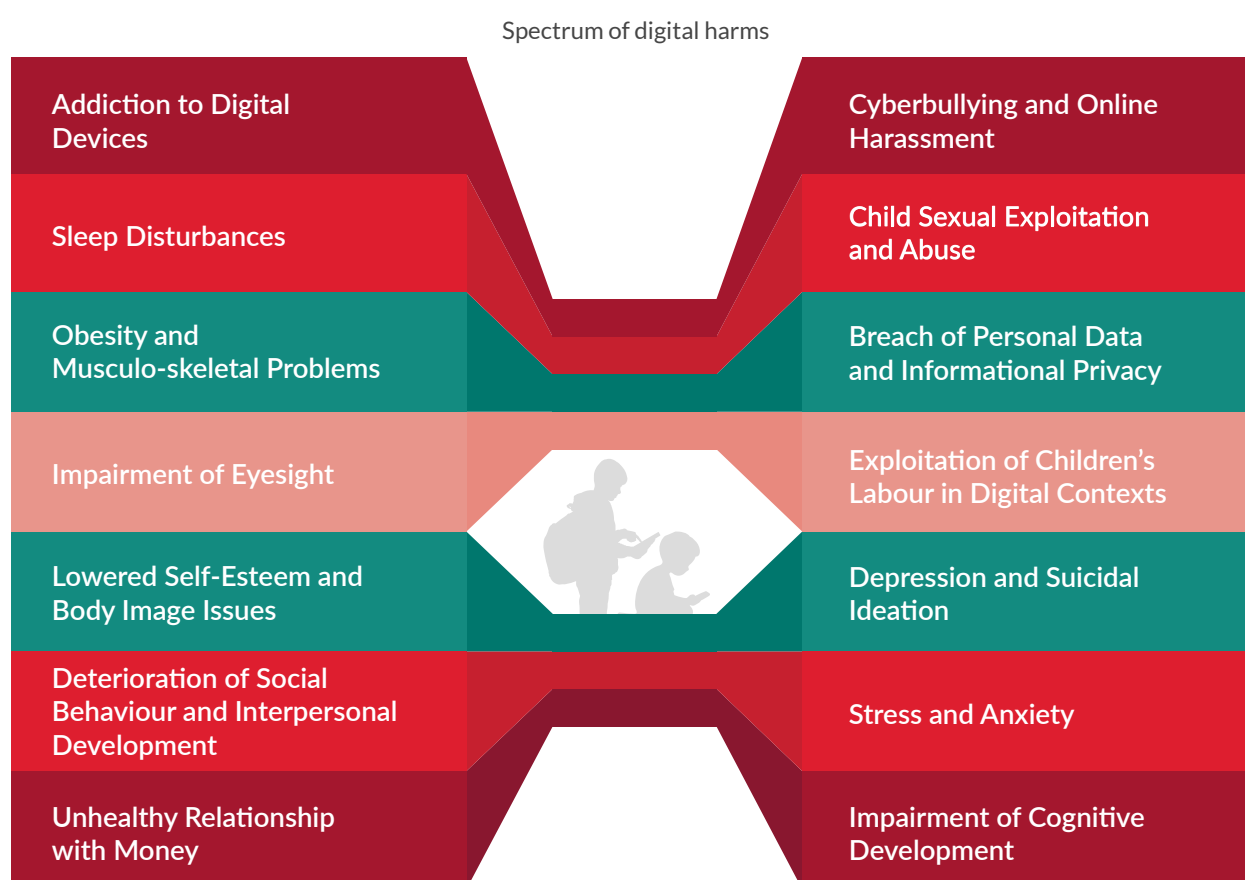
⁵⁶ Ofcom, 'Children's online spending and potential financial harm: Quantitative research' (2025) <https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/research-statistics-and-data/online-services-research/childrens-online-spending-and-potential-financial-harm-quantitative-research.pdf> accessed 5 August 2026.

⁵⁷ Prashant V Kariya, Rinam N Doshi and Amit S Jain, 'Screen Time Addiction and Its Association with Behavioral Problems among School-Aged Children: A Cross-Sectional Study' (2025) *Journal of Child and Adolescent Psychiatry and Mental Health Practice*, <https://www.jccpractice.com/article/screen-time-addiction-and-its-association-with-behavioral-problems-among-school-aged-children-a-cross-sectional-study-651/> accessed 5 August 2026.

A separate observational study of 100 children aged 3–7 in Andhra Pradesh reinforced these findings, demonstrating that children in the high screen time group scored lowest across all measured domains of social competence, including cooperation, responsibility, empathy, and self-control.⁵⁸

The evidence on aggression and internet-linked conduct is similarly concerning. A survey study of 1,148 high school students in Shanxi Province, China, found that the anonymity of online environments may reduce self-awareness and inhibitions, making aggressive responses

more likely, while exposure to violent games and inflammatory content further triggers hostile thoughts and behaviours. Notably, gender did not moderate this relationship, suggesting that the aggression-linked risks of internet addiction are distributed across boys and girls alike.⁵⁹



Infographic 3: The harms associated with children's digital technology use

Alt Text: Spectrum of digital harms: 14 harms including addiction, sleep disturbances, obesity, eyesight impairment, low self-esteem, social behaviour deterioration, cyberbullying, child sexual exploitation and abuse, privacy breach, child labour exploitation, depression, anxiety, and cognitive impairment

⁵⁸ Rajasekhar Reddy Munamala¹, Shaik Mohammad Rafi², Ramisetty M Uma Mahesh, 'Impact of screen time on social skills development in young children: An observational study' (2024) 6(3) International Journal of Academic Medicine and Pharmacy 739, available at https://academicmed.org/Uploads/Volume6Issue3/152.%20%5B3414.%20JAMP_PH%5D%20669-673.pdf accessed 5 August 2026.

⁵⁹ Yanyan Zhang and others, 'The relationship between internet addiction and aggressive behavior among adolescents during the COVID-19 pandemic: Anxiety as a mediator' (2022) 227 Acta Psychologica 103612, available at <https://doi.org/10.1016/j.actpsy.2022.103612> accessed 5 August 2026

Key Takeaways

When read together, some observations which can help understand harms to children better, especially when read alongside the ecosystem of touchpoints and actors are:

1

Several of the harms documented in this chapter are characterised by their diffusiveness. They are not produced by discrete acts of identifiable actors but are embedded in how the digital environment is designed and operates. Addiction, deterioration of self-esteem, financial harm, cognitive impairment, erosion of prosocial behaviour and data extraction, each arises from the ordinary functioning of the technology. Platform architecture designed for sustained engagement, recommendation systems that surface content based on prior behaviour, devices that collect data as background processes, make it difficult to assign responsibility straightforwardly to one single actor, even in specific contexts. This is distinct from harms such as cyberbullying, or child sexual exploitation and abuse, where a perpetrator makes a deliberate choice. However, even in those circumstances, given the diffusive nature of harms on interactions with digital technology, systemic features that fail to protect children against harms warrant examination. Legal frameworks that may assign obligation to a single duty-holder may reach the perpetrators but may fall short of covering the combination of conditions that made the harm possible.

2

Several harms outlast the interaction in which they arise. The literature on addiction documents structural changes in the regions of the brain governing cognitive control and emotional regulation. These persist in the body beyond the period of use. With respect to financial harms, changes to risk-taking behaviour and gambling activities produce harms that impact financial health and attitude. The relationship between online victimisation and offline harm was observed with cyberbullying, meaning that the harm and its impact cross out of the digital context into the child's life. The prosocial behaviour studies measure deterioration in social attributes that extend beyond prolonged screen use itself. Persistence of the impact of such harms appears across neurological, attitudinal, relational, and developmental areas, indicating that the interaction itself may not be the sole unit of the harm. Legal frameworks organized around discrete interactions, and their immediate consequences may therefore be insufficient to meaningfully protect and nurture children in the digital space.

3

A third feature that appears in specific harm progressions is 'compounding'. These are the harms which explicitly increase vulnerability to other harms. Cyberbullying victimization is found to be associated with depression and suicidal ideation. Depression is also associated with self-harm through emulation of self-injurious behaviour encountered online. Simulated gambling is explicitly associated with elevated risk of pathological gambling. For such instances, responses which address the harm at any single stage without considering the progression may be ill-suited.

4

In case of several harms, the nature and severity of the impact is influenced by characteristics specific to the child. Age, gender, sexual minority status, self-esteem, and degrees of parental supervision emerge as factors that determine different outcomes. Sexual minority adolescents report significantly higher rates of abuse. Female adolescents face heightened exposure to anxiety-producing harms. Low self-esteem and reduced parental supervision determine whether gambling exposure produces disorder. Harms, therefore, are also mediated by the child's specific conditions. Responses calibrated to the 'average child' may systematically fail those whose circumstances place them at a greater risk.

Together, these features describe a 'harm environment' whose structure does not resolve into discrete acts or impacts, identifiable actors who are uniquely responsible, or bounded interactions. To understand whether Indian law adequately responds to these features, a detailed review of the Indian legal systems' interventions with respect to children and digital technology is required.

CHAPTER 5

Legal Analysis of Harms to Children

Arising out of Digital Interactions

5

Legal Analysis of Harms to Children Arising out of Digital Interactions

The previous chapter identified fourteen harms which may be reasonably linked to interactions of children with digital technology (hereinafter “Identified Harms”). “Harm” was defined as:

“...any effect that is detrimental to the physical, mental, emotional, developmental or sexual safety and well-being of a child, or has an adverse impact on the rights and interests of a child.”⁶⁰

These harms were identified based on medical, psychological, sociological, and developmental literature, as well as stakeholder consultations, irrespective of whether and how the law recognises and engages with them. This chapter now undertakes the latter inquiry. The objective is to assess whether and to what extent the Identified Harms have entered the State's legal imagination.

Law, much like medicine, psychology, or sociology, engages with harm through its own institutional logic, which the chapter elaborates upon in Section 5.2.⁶¹ However, where medicine identifies harm primarily through its effects on

⁶⁰ See Chapter 4.

⁶¹ See Section 5.2.

the body and mind, the law constructs harm by defining conduct, assigning responsibility, establishing duties, and prescribing consequences. A harm need not be medically observable to be legally cognizable, and vice versa.

This chapter proceeds in four parts, articulating the rationale for adopting a legal lens to assess harm coverage, developing a theoretical framework of the distinct modes through which law engages with harms, and introducing a coverage assessment system to systematically assess the nature and extent of legal coverage of the Identified Harms. The chapter concludes with an analysis of findings to identify patterns, gaps and systemic deficiencies in the legal architecture.

5.2 How Law Engages with Harm: A Theoretical Framework

This section elaborates upon the distinct modes through which law engages with harm as a regulatory object. Understanding these modes is a prerequisite to assessing which harms have been captured by law in the context of digital safety of children, how they have been regulated, and which remains beyond law's reach. This framework is intended to contextualize the coverage assessment in Section 5.4 (hereinafter, the “**Integrated Quadrant-Mode Matrix**”). Notably, these modes are not mutually exclusive. The State may choose to respond to a single harm through multiple modes.

5.2.1 Criminalisation of certain conduct

The law names a category of conduct, declares it impermissible, and attaches penal consequences to those who engage in it. There is a defined wrongful act, a defined wrongdoer, and a defined consequence. This mode is deployed for harms that are severe to warrant the coercive force of criminal

law, capable of being defined with sufficient precision, and involving an identifiable wrongdoer with requisite intent or knowledge.

Example: Child sexual exploitation and abuse is criminalised through the POCSO Act⁶², and the Information Technology Act, 2000 (“IT Act”)⁶³.

In the *Integrated Quadrant-Mode Matrix* in Table 3, this mode is assigned to a particular provision of a law, if it criminalises an Identified Harm, or any constituent aspect(s) of it.

5.2.2 Regulation of conduct of ecosystem stakeholders, including intermediaries and gatekeepers, through non-criminal measures

Not all harms may lend themselves to the logic of criminalisation. They may not be caused or carried out by a single individual, or by a discrete wrongful act. In many instances, the law, instead of imposing criminal sanctions, imposes duties, standards, directions, and obligations on certain ecosystem stakeholders, including intermediaries and gatekeepers (especially in digital contexts), who may be best placed to prevent, detect, or mitigate the harm. Such regulation, may for instance, be suited to contexts where the harm is not attributable to a single wrong doer, but arises from systemic practices or operational choices.

Example: The DPDP Act requires data fiduciaries to obtain verifiable parental or guardian consent before processing the personal data of children.⁶⁴ The IT Rules 2021 impose proactive duties on intermediaries to identify, flag, and remove child sexual abuse material.⁶⁵ Regulation of fiduciaries, intermediaries or other gatekeepers recognizes that those who control the infrastructure or environment through which harm occurs are best positioned to prevent it.

In the *Integrated Quadrant-Mode Matrix* in Table 3, this mode is assigned to a particular provision of

⁶² Protection of Children from Sexual Offences Act 2012, chs II and III.

⁶³ Information Technology Act, 2000, s 67B.

⁶⁴ Digital Personal Data Protection Act 2023, s 9.

⁶⁵ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, r 4(4).

a law, if it imposes certain obligations, standards, duties, and/or directions on any concerned ecosystem entity with respect to an Identified Harm, or any aspect(s) of it.

5.2.3 Incidental and interpretive inclusion

A harm may also be regulated incidentally or through interpretation, not always attributable to a deliberate State choice. This mode typically applies to: (a) technologically manifested harms in the context of laws designed for offline contexts, or (b) harms which do not apply to children specifically by design, but may nonetheless cover children, as part of the wider population group, in their ambit.

Example: The coverage of technology-facilitated digital harms in cognate provisions of the Bharatiya Nyaya Sanhita, 2023 (BNS)⁶⁶ not drafted for digital contexts, or applicable only to women, and therefore incidentally covering female children, exemplify this mode.

In the *Integrated Quadrant-Mode Matrix in Table 3*, a provision of law is assigned this mode where it does not directly address an Identified Harm, but may be interpreted to do so, based on a textual reading. This arises in three situations: first, where the provision does not explicitly contemplate a technologically-mediated context but is capable of being extended to one by interpretation; second, where the provision applies to the general population without recognising children as a distinct category requiring specialised protection, but may nonetheless apply to children as part of that broader population; and third, where the provision applies to children only incidentally, as members of a wider group (for instance, female children falling within a provision directed at women generally).

5.2.4 Protective frameworks

Law creates a comprehensive protective framework for vulnerable populations, establishing institutional infrastructure, procedural safeguards, rights-based mechanisms tailored to specific vulnerabilities. This mode is suitable to contexts

where the vulnerable group requires not merely protection from a specific harm, but a holistic framework recognising their distinct status. It is relevant for harms where isolated prohibitions or duties would not suffice and protection requires specialised institutions, procedures, rehabilitation mechanisms, etc.

Example: The JJ Act articulates guiding principles (including best interest of the child), creates specialised bodies (such as Juvenile Justice Board, Child Welfare Committee, etc), establishes procedural safeguards and provides for rehabilitation and reintegration.

In the *Integrated Quadrant-Mode Matrix in Table 3*, a provision of law is assigned this mode where it creates a comprehensive protection framework for children as a vulnerable population, in context of an Identified Harm, or any aspect(s) of it.

5.2.5 Harms beyond legal regulation

Beyond the foregoing spectrum of legal and regulatory engagement, lie certain harms which remain outside the legal apparatus. These are harms for which no legal provision, however general or stretched, provides coverage. They are harms that the State has not yet conceptualised as subjects of legal regulation at all. Such an approach may be a conscious choice as the State views such harms to be better addressed through non-legal interventions (such as education, advocacy, etc.) or may also be a deferral pending empirical evidence necessitating legal intervention. In some cases, it may also be a regulatory oversight.

Such harms are typically gradual in onset or may result from prolonged exposure to a certain act or omission, making it challenging to identify discrete conduct, clear causal links or appropriate points of regulation. As will be evident from Section 5.4, harms such as inadequate sleep, eyesight impairment, and cognitive development may fall in this category.

⁶⁶ Bharatiya Nyaya Sanhita, 2023 (BNS), s 96, s 98 and s 99.

5.3. Quadrant Classification Methodology

This section describes the methodology for assessing the legal coverage of Identified Harms. The preceding sections outlined how law can engage with harm through different modes. However, assessing legal coverage requires a systematic classification mechanism that captures not only the modes through which law engages with the Identified Harms, but also the contexts they contemplate. Two contextual dimensions are particularly relevant. First, whether the law recognises children’s distinct vulnerabilities, requiring differentiated protection. Second, whether the law contemplates digitally mediated harm, recognizing that digital touchpoints create distinct risks and require tailored responses. This section develops an Integrated Quadrant-Mode Matrix that operates along these two contextual dimensions combined with the different modes in which law engages with the Identified Harms.

5.3.1. Scope and limitations

The analysis below is subject to the following:

1. The framework assesses coverage, and not adequacy. It examines whether legal provisions exist that recognise the Identified Harms, not whether these provisions are normatively appropriate, sufficient to further children’s interests, adequately implemented, or aligned with global best practices.
2. The analysis is confined to the text of existing laws, and does not extend to interpretive variability, including how courts or authorities have applied or may apply these provisions in practice.
3. The Integrated Quadrant-Mode Matrix operates on a non-hierarchical basis. Placement in one quadrant over another carries no qualitative conclusions as to the relative superiority or adequacy of any regulatory response.

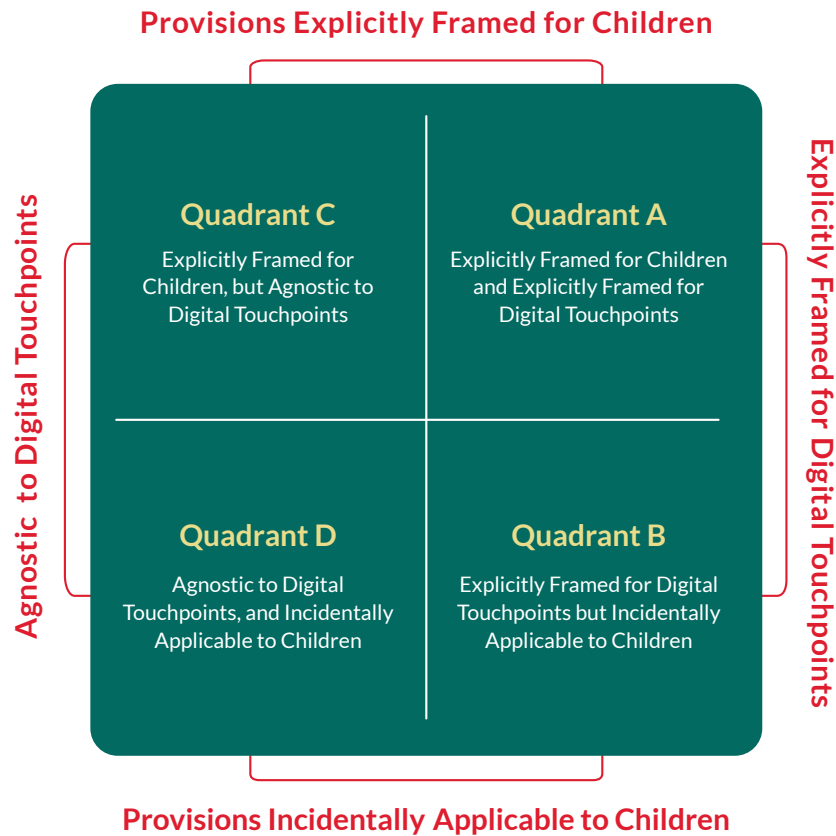
5.3.2 Overview of the approach for mapping legal coverage of harms to children in digital spaces

Each Identified Harm has been evaluated for its legislative coverage, examining whether and to what extent the harm is addressed in any existing statute, subordinate legislation, or regulation.

As discussed, the Identified Harms are not mutually exclusive. For the classification purpose, legal provisions are mapped to the harms that they directly address. For instance, a law criminalising cyberbullying is mapped against the Identified Harm of cyberbullying, though preventing cyberbullying may reduce depression as a downstream effect. This approach prioritises clarity and avoids double counting.

5.3.3 The Quadrant Classification Framework

The coverage of each harm is classified using a structured two-axes quadrant system.



Infographic 4: The Four Quadrants

Alt Text: Quadrant grid: horizontal axis runs from agnostic to explicitly framed for digital touchpoints; vertical axis runs from incidentally to explicitly framed for children. Quadrant A: explicit on both axes. Quadrant B: explicit touchpoints, incidental to children. Quadrant C: agnostic on both axes. Quadrant D: agnostic touchpoints, explicit to children.

Axis 1 (Horizontal): Provisions Explicitly Framed for Digital Touchpoints versus Provisions Agnostic to Digital Touchpoints

The horizontal axis distinguishes between provisions based on their relationship to digital touchpoints:

- **Provisions Explicitly Framed for Digital Touchpoints:** Provisions explicitly framed for digital, online, or electronic contexts, specifically contemplating mediation through digital touchpoints, and drafted with digital platforms, services, or interactions in mind.
- **Provisions Agnostic to Digital Touchpoints:** General provisions that may apply to digital touchpoints but are not explicitly framed for them, drafted without specific reference to digital technology, but may be interpreted or extended to cover digitally mediated harms.

Axis 2 (Vertical): Provisions Explicitly Framed for Children versus Provisions Incidentally Applicable to Children

The vertical axis distinguishes between provisions based on whether they recognize children as requiring special or otherwise differentiated protection:

- **Provisions Explicitly Framed for Children:** Provisions explicitly recognizing children as a distinct category requiring special, heightened, or differentiated protection, reflecting an understanding that children's vulnerabilities, developmental stages, or rights warrant tailored legal responses.
- **Provisions Incidentally Applicable to Children:** Provisions not applicable to children specifically, singling them out for special treatment or recognition, but applicable to them only incidentally, as part of a wider population group.

5.3.3.1 Explaining the four quadrants

Quadrant A: Explicitly Framed for Children and Explicitly Framed for Digital Touchpoints

Quadrant A provisions exhibit the following characteristics:

- they are specific to the digital, online, or electronic context, demonstrating legislative recognition that digital touchpoints mediate or create distinct forms of harm; and
- they recognize children as a distinct category requiring heightened or otherwise differentiated protection.

Quadrant A provisions represent instances where the legislature has directly addressed an Identified Harm, or any constitutive aspect(s) of it, with tailored legal provisions.

Example: Section 9 of DPDP Act requires data fiduciaries to obtain verifiable parental consent before processing children's personal data and prohibits tracking, behavioural monitoring or targeted advertising at children.

Quadrant B: Explicitly Framed for Digital Touchpoints but Incidentally Applicable to Children

Quadrant B provisions exhibit the following characteristics:

- they are framed specifically for digital, online, or electronic contexts, reflecting legislative awareness of harms mediated by digital touchpoints; and
- they apply to children only incidentally, as part of a wider population group.

Quadrant B provisions address an Identified Harm, or any constitutive aspect(s) of it, but do not differentiate between adults and children.

Example: Section 78 of BNS criminalises stalking a woman using electronic means addressing a harm mediated through a digital touchpoint, without distinguishing between women and minor girls. Section 2(35) of BNS defines a woman "as a female human being of any age".

Quadrant C: Provisions Explicitly Framed for Children, but Agnostic to Digital Touchpoints

Quadrant C provisions exhibit the following characteristics:

- they specifically recognise children as a distinct category, reflecting legislative recognition of children's special vulnerabilities;
- they are not explicitly framed for digital, online, or electronic contexts, having been drafted either before the digital age or without specific contemplation of harm mediation through digital touchpoints; and
- they may nevertheless apply to digital harms through broad drafting, or reasonable interpretation.

Quadrant C provisions reflect a legislative commitment to child protection, but one that predates or does not explicitly account for the digital environment.

Example: Sections 96, 98 and 99 of BNS criminalise the procurement, sale and purchase of children for illicit intercourse or immoral purposes do not refer to digital touchpoints, but may potentially be interpreted to cover online procurement or trafficking.

Quadrant D: Provisions Agnostic to Digital Touchpoints, and Incidentally Applicable to Children

Quadrant D provisions exhibit the following characteristics:

- they may only incidentally apply to children, as part of a wider population group;
- they are not specific to digital, online, or electronic contexts, being general legal norms applicable across various contexts; and
- they may be interpreted to tangentially cover an Identified Harm, or any constitutive aspect(s) of it.

Example: Section 72 of BNS prohibits printing or publication of information identifying victims of specified sexual offences, applicable to all victims regardless of age and not specific to digital

publication, but potentially interpretable to cover online publication or dissemination.

5.3.3.2 Harms beyond legal coverage and outside the quadrant

Beyond the four quadrants lies a fifth category of Identified Harms for which no legal provision provides coverage. These are harms that the State has not recognised as subjects of legal recognition. The distinction between Quadrant D and non-coverage lies in interpretative reach. An Identified Harm falls in Quadrant D if existing general provisions can reasonably be interpreted to apply, even if not designed for that purpose. An Identified Harm falls outside the quadrants entirely when the harm's nature, structure or causation lies beyond the scope of existing laws.

5.3.4 Integrating the Quadrant Classification Framework with Modes of Engagement

The modes of legal engagement (section 5.2) and quadrant classification (section 5.3) serve distinct but complementary analytical purposes. Together they provide comprehensive understanding of legal coverage along three dimensions.

- Quadrants reveal whom the law addresses (whether child specifically or only incidentally as part of a wider population group), what contexts it contemplates (mediated by digital touchpoints or agnostic to them)
- Modes reveal how law regulates (through criminalisation, regulation of the conduct of ecosystem stakeholders, interpretation or a protective framework)
- Combined analysis reveals the architecture of legal coverage - whether an Identified Harm receives a targeted or incidental coverage.

This section applies the Integrated Quadrant-Mode Matrix to each of the Identified Harms. Each of the harms have been assessed for legal coverage across Indian statutes and subordinate legislation. The findings are presented in tabular format. For each provision, the table identifies - (a) the relevant legal provision; (b) whether the provision is explicitly framed for digital touchpoints (c) whether the provision is explicitly framed for children (d) quadrant classification; (e) which mode(s) of legal engagement it employs; and (f) brief description of how the provision engages with the Identified Harm.

5.4 Coverage Assessment

Quadrant Legend

Quadrant	Description	Tech-Specific?	Child-Specific?
Q-A	Explicitly Framed for Digital Touchpoints + Explicitly Applicable to Children	✓	✓
Q-B	Explicitly Framed for Digital Touchpoints + Incidentally Applicable to Children	✓	✗
Q-C	Explicitly Applicable to Children + Agnostic to Digital Touchpoints	✗	✓
Q-D	Agnostic to Digital Touchpoints + Incidentally Applicable to Children	✗	✗
—	No Applicable Legal Instrument	—	—

Table 1: Quadrant Legend

Modes of Legal Engagement

M1	Criminalisation of the Identified Harm or certain aspect(s) of it.
M2	Regulation of conduct exhibited by ecosystem stakeholders, including intermediaries and gatekeepers, through non-criminal measures
M3	Incidental and interpretive inclusion
M4	Rights-based protective framework

Table 2: Models of Legal Engagement

How to read the Integrated Quadrant-Mode Matrix

1. The Identified Harms are not uni-dimensional. As evident from Chapter 4, an Identified Harm may include one or more distinct aspects / dimensions. In the table below, a provision mapped against a particular Identified Harm need not address all such aspects / dimensions; inclusion in the table requires that it speaks to at least one. This has been done to ensure analytical comprehensiveness.

Example: The Identified Harm of unhealthy relationship with money due to digital exposure covers within its ambit aspects such as impulsive spending, financial risk-taking, distorted perceptions of money, and the development of gambling-like disorders through simulated gaming. The PROG Act 2025, in prohibiting offering, aiding, abetting, inducing or otherwise indulging or engaging in the offering of online money games and online money gaming services, cited financial harms, particularly to young children, and the risk of irresponsible financial behaviour in youth. It therefore engages with only one specific dimension of this Identified Harm, not its full scope.

2. A single law may engage with an Identified Harm through more than one mode. For instance, the IT Act read with the IT Rules 2021 criminalises certain conduct (M1: publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form) and imposes conduct regulations on intermediaries through non-criminal measures (M2: certain due diligence requirements). However, when assigning a mode of engagement to a specific provision, only that provision and directly connected provisions are considered, not the parent law as a whole.

This is because the analysis in the table below proceeds provision by provision rather than law by law, on the premise that a single Identified Harm may be addressed by multiple laws through multiple specific provisions. For the same reason, the analysis is not limited to laws specifically designed for children's protection; a law of general application may address a relevant harm and may do so through more than one mode.

Table 3: Integrated Quadrant-Mode Matrix⁶⁷

Harms		Legal Provision	Explicitly Framed for Digital Touchpoints (Y/N)	Explicitly Framed for Children (Y/N)	Mode(s)	Relevant Quadrant	Explanation
1	Obesity and Musculo-Skeletal Problems due to digital device usage	1.1 Misleading Ads, Guideline 8	✓	✓	M2	A	Prohibits advertisements from condoning or encouraging practices detrimental to children's physical health. Junk food advertisements are prohibited during children's programmes and on channels exclusively for children
2	Depression and Suicidal Ideation	2.1 IT Rules 2021, Appendix	✓	✓	M2	A	Content Classification (U, U/A 7+, U/A 13+, U/A 16+, A) & Restrictions - 'A'-rated content to be rendered inaccessible to children; access control mechanisms to be made available for U/A 13+ or higher rated content.
3	Stress and Anxiety	3.1 Mental Healthcare Act 2017	✗	✓	M4	C	Establishes a rights-based framework for persons with mental illness. Stipulates the procedure for admission of a minor in a manner that their best interests are taken into account; prohibits electro-convulsive therapy for minors.
4	Lowered Self Esteem and Body Image Issues due to online exposure	4.1 Misleading Ads Guidelines, G8	✓	✓	M2	A	Prohibits such advertisements targeted towards children which may develop a negative body image in them

⁶⁷ **Note:** Rule 3(1)(b)(iii) of the IT Rules 2021, places a due diligence obligation on intermediaries to not disseminate content that is 'harmful to children'. The Rules further define "harm" as any effect which is detrimental to a user or child. The text of the provision read with the definition provides little clarity as to what actually qualifies as harmful. Given this ambiguity, it is not possible to determine which of the harms listed below fall within the scope of this provision, and it has therefore been excluded from the table.

Harms		Legal Provision	Explicitly Framed for Digital Touchpoints (Y/N)	Explicitly Framed for Children (Y/N)	Mode(s)	Relevant Quadrant	Explanation
5	Addiction to Digital Devices	5.1 PROGA, 2025 – Statement of Objects & s. 4-6 ⁶⁸	✓	✓	M1	A	Recognises addiction to online gaming platforms as causing social, psychological, and public health harms 'particularly among young individuals.' Mandates the Central Government to promote age-appropriate, safe social gaming content; prohibits online money games and online money gaming services; and advertisements related to online money games.
		5.2 PROG Rules, 2026 - Rule 12	✓	✓	M1	A	It provides that no online game of an online game service provider shall be registered except where the Central Government requires an online game of an online game service provider or a category of online games to be registered, having due regard to, inter alia, risk of harm to users, including children.
6	Cyberbullying and Online Harassment	6.1 BNS 2023, s. 75	✗	✗	M3	D	Criminalises sexual harassment of women. ⁶⁹ The coverage is incidental and interpretive since: (a) it does not explicitly contemplate sexual harassment in the digital context, and (b) only derivatively applies to female children as women, to the exclusion of children who are male, or outside the binary.
		6.2 POCSO, s. 11	✓	✓	M1	A	Criminalises sexual harassment of children.

⁶⁸ Note: The PROGA seeks to address the harms of: (a) addiction to digital devices, and (b) unhealthy relationship with money due to exposure to digital technologies (Harm 10) by prohibiting offering, aiding, abetting, inducing or otherwise indulging or engaging in the offering of online money games and online money gaming services. The approach is classified based on the legal mechanism through which the prohibition is enforced, rather than the prohibition itself. As the prohibition is enforced through the criminalisation of the prohibited conduct, it is classified under Mode M1.

⁶⁹ The law defines a “woman” as a female human being of any age.’ See Bharatiya Nyaya Sanhita 2023, s 2(35).

Harms		Legal Provision	Explicitly Framed for Digital Touchpoints (Y/N)	Explicitly Framed for Children (Y/N)	Mode(s)	Relevant Quadrant	Explanation
6	Cyberbullying and Online Harassment	6.3 BNS 2023, s. 77	✓	✗	M3	B	Criminalises voyeurism against women, including using electronic devices. The coverage is incidental, since it only covers female children derivatively as women, to the exclusion of children who are male, or outside the binary.
		6.4 BNS 2023, s. 78	✓	✗	M3	B	Criminalises stalking a woman, including using electronic means. The coverage is incidental, since it only covers female children derivatively as women, to the exclusion of children who are male, or outside the binary.
		6.5 BNS 2023, s. 351	✗	✗	M3	D	Criminalises, threatening another by any means, inter alia, with any injury to his person, reputation or property, with intent to, cause alarm to that person, or to cause that person to do any act which he is not legally bound to do, or to omit to do any act which that person is legally entitled to do, as the means of avoiding the execution of such threat. The coverage is only interpretive and incidental, since it may cover threat-based cyberbullying, especially involving reputational threats, but it is not a cyberbullying provision by design.
		6.6 BNS 2023, s. 356	✗	✗	M3	D	Criminalises making or publishing in any manner, any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm the reputation of such a person. This may incidentally cover instances of cyberbullying where defamatory content is posted or shared online against a victim.

Harms		Legal Provision	Explicitly Framed for Digital Touchpoints (Y/N)	Explicitly Framed for Children (Y/N)	Mode(s)	Relevant Quadrant	Explanation
7	Child Sexual Exploitation and Abuse	7.1 Immoral Traffic (Prevention) Act 1956, (ITPA) s. 5	✗	✗	M3	D	Criminalizes procuring, inducing, or transporting any person for prostitution; enhanced punishment if the person is a minor (under 18), or a child (under 16). The coverage is interpretive, since it may be interpreted to apply to procurement or inducement of children for prostitution through digital means.
		7.2 IT Act 2000, s. 67B	✓	✓	M1	A	Criminalises publishing or transmitting of material depicting children in sexually explicit acts, etc., in electronic form
		7.3 IT Rules 2021, Rule 4(2)	✓	✓	M2	A	First originator traceability requirement for SSMLs providing messaging services.
		7.4 IT Rules 2021, Rule 4(4)	✓	✓	M2	A	Obligation on SSMLs to proactively identify and remove information depicting child sexual abuse or conduct.
		7.5 IT Rules 2021, Rule 3(1)(cb)	✓	✗	M2	B	Obligation to take appropriate and expeditious action against unlawful Synthetically Generated Information ("SGI").
		7.6 IT Rules 2021, Rule 3(1)(d)	✓	✗	M2	B	Notice and takedown obligation on intermediaries upon receiving actual knowledge.

Harms		Legal Provision	Explicitly Framed for Digital Touchpoints (Y/N)	Explicitly Framed for Children (Y/N)	Mode(s)	Relevant Quadrant	Explanation
7	Child Sexual Exploitation and Abuse	7.7 IT Rules 2021, Rule 3(2)(b)	✓	✗	M2	B	Obligation to remove or disable access to certain content (showing an individual in full or partial nudity, depicting such individual in any sexual act or conduct, or in the nature of impersonation in electronic form including artificially morphed images).
		7.8 IT Rules 2021, Rule 3(3)	✓	✗	M2	B	Due diligence in relation to SGI.
		7.9 IT Rules 2021, Rule 4(1A)	✓	✗	M2	B	Enhanced ex-ante obligations for SSMLs in relation to SGI.
		7.10 POCSO Act 2012, ss. 11(iii)–11(vi)	✓	✓	M1	A	Criminalises sexual harassment of children, including through electronic means.
		7.11 POCSO Act 2012, s. 13	✓	✓	M1	A	Criminalises use of children for pornographic purposes in any form of media.
		7.12 POCSO Act 2012, s. 15	✓	✓	M1	A	Criminalises the storage or possession of pornographic material in any form involving a child.

Harms		Legal Provision	Explicitly Framed for Digital Touchpoints (Y/N)	Explicitly Framed for Children (Y/N)	Mode(s)	Relevant Quadrant	Explanation
7	Child Sexual Exploitation and Abuse	7.13 BNS 2023, s. 96	✗	✓	M3	C	Criminalises procurement of a child for illicit intercourse. The coverage is interpretive, since it may be interpreted to apply to procurement of children for illicit intercourse through digital means.
		7.14 BNS 2023, s 98	✗	✓	M3	C	Criminalises selling a child with intent or knowledge that the child will be used for prostitution, illicit intercourse, or any unlawful and immoral purpose. The coverage is interpretive, since it may be interpreted to apply to selling a child for prostitution through digital means.
		7.15 BNS 2023, s 99	✗	✓	M3	C	Criminalises buying, hiring, or otherwise obtaining possession of a child with intent or knowledge that the child will be used for prostitution, illicit intercourse, or any unlawful and immoral purpose. The coverage is interpretive, since it may be interpreted to apply to buying a child for prostitution through digital means.
8	Breach of Personal Data and Informational Privacy	8.1 JJ Act 2015, s. 74	✓	✓	M1, M4	A	Prohibits the disclosure of the identity of a child in conflict with the law, or a child in need of care and attention, in the media.
		8.2 BNS 2023, s. 72	✗	✗	M3	D	Prohibits the printing or publication of any information that may identify a victim of specified sexual offences under BNS. The coverage is incidental, since it only derivatively includes female children as women.

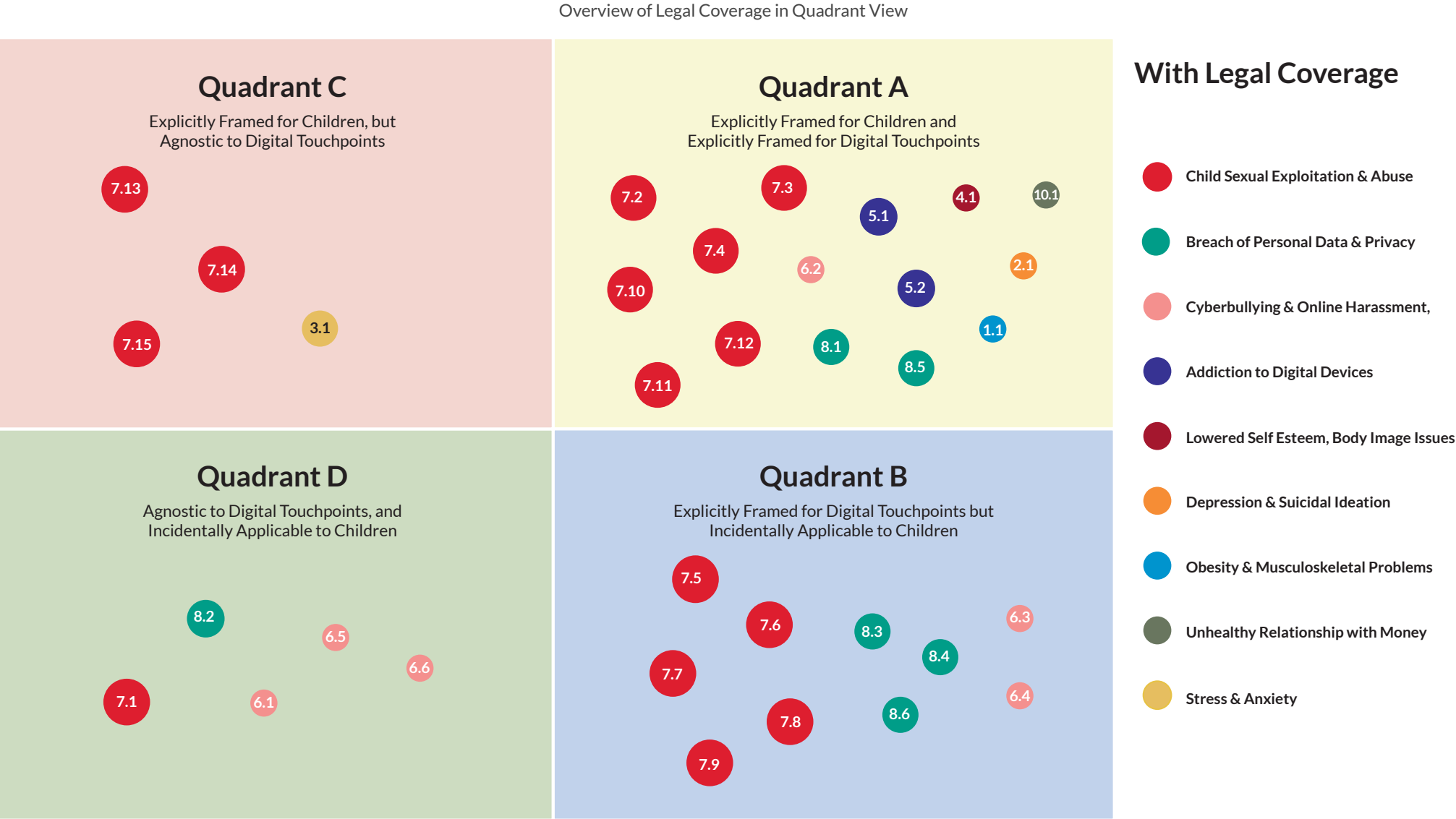
Harms		Legal Provision	Explicitly Framed for Digital Touchpoints (Y/N)	Explicitly Framed for Children (Y/N)	Mode(s)	Relevant Quadrant	Explanation
8	Breach of Personal Data and Informational Privacy	8.3 BNS 2023, s. 77	✓	✗	M3	B	Criminalises voyeurism against a woman, including using electronic means. Since capturing and/or disseminating the image of a woman engaging in a private act are both criminalised, informational privacy is affected as the woman loses control over personal information about herself engaging in a private act without her consent. Dissemination further exposes that information to third parties without her knowledge or approval. The coverage is incidental, since it only derivatively protects female children as women.
		8.4 BNS 2023, s. 78	✓	✗	M3	B	Criminalises stalking a woman, including monitoring the use of the internet, e-mail or any other form of electronic communication by a woman. Since the monitoring of a woman's electronic communications constitutes the covert collection of her personal information, it may be construed as a crime against her informational privacy as well. The coverage is incidental, since it only derivatively protects female children as women.
		8.5 DPDP Act 2023, s. 9	✓	✓	M2	A	Requires data fiduciaries to obtain verifiable parental or guardian consent before processing a child's personal data. Further prohibits data fiduciaries from tracking or behaviourally monitoring children and from targeting advertising at children.

Harms		Legal Provision	Explicitly Framed for Digital Touchpoints (Y/N)	Explicitly Framed for Children (Y/N)	Mode(s)	Relevant Quadrant	Explanation
8	Breach of Personal Data and Informational Privacy	8.6 Aadhaar Act, 2016, s. 28	✓	✗	M1, M2	B	Duty to ensure security and confidentiality of identity information, including biometric information, and authentication records; imposition of civil penalty, and /or imprisonment and/or fine for disclosure of such information.
9	Exploitation of Children's Labour in Digital Contexts	-	-	-	-	-	CALPRA 1986 prohibits the employment of children under 14, subject to exceptions for family enterprises and children working as artists in audio-visual entertainment. Adolescents (14–18) are prohibited only from hazardous occupations. Further, the NCPCR has issued non-binding guidelines, recommending safeguards for children/adolescents creating content for social media platforms by parent/guardian/family⁷⁰, as well as content created by production houses for social media platforms or short video platforms involving children/adolescents for economic gains⁷¹. However, this table does not assign regulatory coverage to this harm because CALPRA does not expressly recognise child influencers as 'artists', and the NCPCR Guidelines are non-binding.

⁷⁰ Note: Safeguards include ensuring that: (a) the child's education is not affected while carrying out such work, (b) the child is afforded adequate rest, and (c) the child is not made to act in a manner that is inappropriate to the child or that may distress him or put her in embarrassing situations. National Commission for Protection of Child Rights, Guidelines for Child and Adolescent Participation in the Entertainment Industry or Any Commercial Entertainment Activity (2023), r 3 and r 4.

⁷¹ Note: Safeguards include ensuring that: (a) the child's education is not affected while carrying out such work, (b) the child is afforded adequate rest, and (c) the child is not made to act in a manner that is inappropriate to the child or that may distress him or put her in embarrassing situations. National Commission for Protection of Child Rights, Guidelines for Child and Adolescent Participation in the Entertainment Industry or Any Commercial Entertainment Activity (2023), r 3 and r 4.

Harms		Legal Provision	Explicitly Framed for Digital Touchpoints (Y/N)	Explicitly Framed for Children (Y/N)	Mode(s)	Relevant Quadrant	Explanation
10	Unhealthy Relationship with Money due to Exposure to Digital Technologies	10.1 PROGA 2025	✓	✓	M1	A	Recognises addiction to online gaming platforms as causing, inter alia, financial harms 'particularly among young individuals.'
11	Sleep Disturbances	-	-	-	-	-	-
12	Impairment of Eyesight due to Digital Device Usage	-	-	-	-	-	-
13	Impairment of Cognitive Development	-	-	-	-	-	-
14	Deterioration of pro-social behaviour and impairment of interpersonal development due to digital exposure	-	-	-	-	-	-



Infographic 5: Harms to Children in Digital Space - Quadrant View

Alt Text: Quadrant view of legal coverage: 34 provisions plotted by harm category across Quadrants A–D, colour-coded per legend.

5.5 Analysis and Conclusion

The Integrated Quadrant-Mode Matrix reveals distinct patterns in how Indian law engages with the Identified Harms to children. While some harms have attracted significant regulatory scrutiny, others receive only incidental coverage and some fall entirely outside the legal framework. This section analyses these patterns in three parts - (i) a quantitative overview of provision distribution across the four quadrants; (ii) qualitative observation on which harms have received attention, how they have been regulated, and what choices reveal about State regulatory priorities; and (iii) systemic gaps emerging from this mapping exercise.

5.5.1 Quantitative Overview

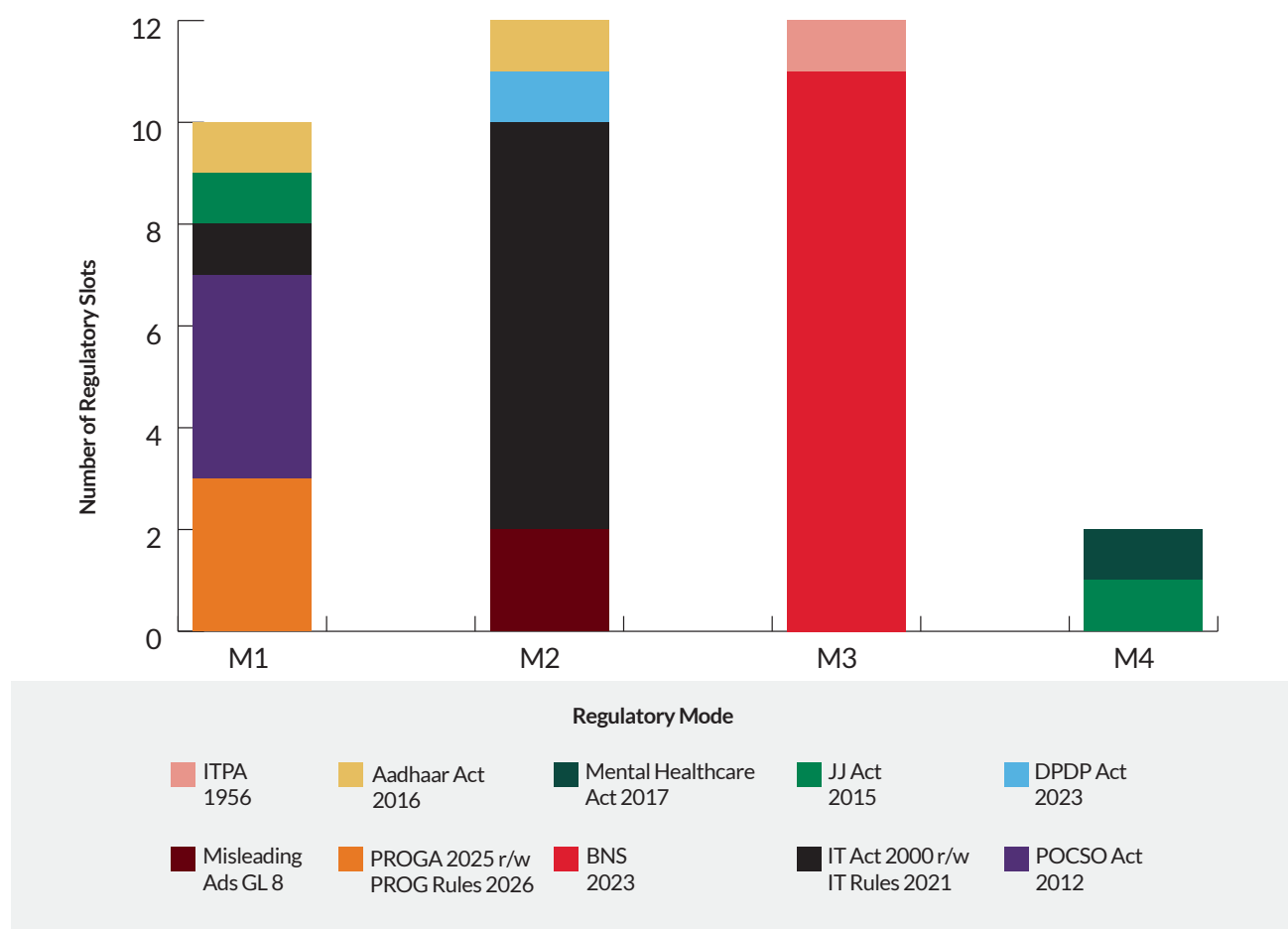
The coverage exercise identified 34 legal provisions across 10 statutes and their subordinate legislation, mapped against 14 categories of Identified Harms.

1. Out of 14 Identified Harms, 9 harms have received some form of legal recognition. However, the remaining 5 harms (~35%) (sleep disturbances, impairment of eyesight due to digital device usage, impairment of cognitive development, deterioration of pro-social behaviour and impairment of interpersonal development due to digital exposure, and exploitation of children’s labour in digital contexts) have no applicable legal instrument.
2. The distribution of the 34 legal provisions across quadrants is as follows:

Quadrant	Description	Number of Provisions (%)
Q-A	Explicitly Framed for Digital Touchpoints + Explicitly Applicable to Children	15 (44.1%)
Q-B	Explicitly Framed for Digital Touchpoints + Incidentally Applicable to Children	10 (29.4%)
Q-C	Explicitly Applicable to Children + Agnostic to Digital Touchpoints	4 (11.8%)
Q-D	Agnostic to Digital Touchpoints + Incidentally Applicable to Children	5 (14.7%)

Table 4: Quantitative Overview of Harms to Children in Digital Space

3. The analysis of the mode of legal engagement reveals the following distribution.



Graph 1: Distribution by Mode of Legal Engagement

Alt Text: Stacked bar chart of regulatory slots by mode: M1 totals 10, M2 totals 12, M3 totals 12, M4 totals 2, broken down by statute per the legend.

4. Key Observations

4.1 Quadrant Distribution

- **Quadrant A dominance:** The highest legal coverage is concentrated in Quadrant A (Explicitly Framed for Digital Touchpoints + Explicitly Applicable to Children), with the majority of these provisions concerning Child Sexual Exploitation and Abuse (CSEA). This suggests that where the State has deliberately engaged with digital harms to children, it has done so through tailored, provisions explicitly framed for digital touchpoints, and explicitly applicable for children.
- **Quadrant C sparsity:** Quadrant C (Agnostic to Digital Touchpoints + Explicitly Applicable to Children) has the least coverage (4), indicating minimal reliance on general law to address the Identified Harms to children.

4.2 Mode Distribution

- **Mode 2 and 3 dominance:** Mode 2 (Regulation of conduct exhibited by ecosystem stakeholders) and 3 (Incidental and interpretive coverage) emerge as the dominant mode of legal engagement with the Identified Harms. In case for Mode 2, this is due to several provisions in the IT Rules 2021, primarily concerned with due diligence obligations to retain intermediary safe harbour, majorly focused on checking the hosting and dissemination of Child Sexual Exploitation and Abuse Material (CSEAM).

In case of Mode 3, this is primarily due to various provisions of the BNS, which have not been drafted explicitly for children and/or digital touchpoints, but may be interpreted to incidentally cover Identified Harms to children.

- **Mode 4 sparsity:** The least number of provisions have been assigned Mode 4 (Protective, Rights-based framework). It is only the JJ Act which makes an effort towards constructing a principles-informed, rights-based protective framework for children in conflict with the law, and children in need of care and attention, complemented by an institutional mechanism for the same. The Mental Healthcare Act is also characterised by such engagement, albeit for a sub-set of children (those needing mental healthcare support) receiving incidental coverage within a wider population group (people needing mental healthcare support).

Absence of legal recognition: The complete absence of any legal instrument for ~35% of the Identified Harms signals that while the law is robust for physical and sexual harms in digital contexts, it does not recognise harms that are diffuse, gradual or developmental in nature.

5.5.2 Qualitative Observations

1. The harm of child sexual exploitation and abuse has attracted the most amount of regulatory attention

This harm has received layered regulatory treatment across 15 provisions, spanning 4 legal instruments (IT Act, 2000 read with the IT Rules 2021, ITPA 1956, POCSO 2012 and BNS 2023) and employing 3 modes (M1, M2, and M3). This includes direct criminalisation of CSEA under the IT Act and POCSO Act, proactive due-diligence obligations upon intermediaries, including significant social media intermediaries under the IT Rules, 2021, and interpretative expansion of general anti-trafficking laws.

This density of coverage, representing 15 provisions out of total 34 provisions (~46%) may be attributed to the severity and seriousness of this particular harm, that it lends to multiple regulatory approaches. It also bears mentioning that this harm lends itself well to the logic of criminalisation, in as much as it entails a discrete wrongful act, an identifiable wrongdoer, and a definable category of prohibited conduct. Further, it also requires regulation of a digital touchpoint, namely intermediaries, through which CSEAM is distributed, published and transmitted.

2. Informational privacy harms to children have begun receiving regulatory attention

Privacy related harms are addressed across four provisions spanning three laws. The most explicit recognition of this harm is through the DPDP Act, which imposes categorical obligations on data fiduciaries in respect of children's data and prohibits behavioural monitoring and targeted advertising directed at children. This has been a result of a broader judicial effort to read in a fundamental right to privacy for all within India's constitutional scheme.

3. Legal engagement with the harm of cyberbullying and online harassment is fragmented, addressing only certain aspect(s) of the harm, primarily for female children

This harm primarily receives coverage through BNS provisions on sexual harassment, voyeurism, and stalking, and the POCSO provision on sexual harassment; all these provisions criminalise certain prohibited conducts (Mode 1). The BNS provisions are women-specific and do not differentiate between adult women and minor girls. A girl-child is protected only derivatively, as a woman, and not specifically as a child. Male children, gender-nonconforming children, and children who do not identify within the binary are entirely outside the protective ambit of these provisions. Both BNS and POCSO provisions are only applicable to sexual contexts, leaving the non-sexual dimensions of cyberbullying and online harassment unaddressed. Application of the BNS provision on criminal intimidation to cyberbullying is, at best, a strained interpretation limited to instances that cross the threshold of reputational harm arising from threat-based conduct. Literature referenced in Chapter 4 demonstrates the severity and egregious nature of this harm, as well as its tendency to further cause other harms, such as anxiety and depression. Government policy literature has itself recognised cyberbullying as a harm encountered by children in digital spaces⁷². Therefore, the lack of a more layered and multi-modal legal and regulatory engagement with cyberbullying and online harassment, that is cognisant of their full scope beyond sexual or threat-based contexts, merits attention.

4. Certain harms, even if represented in the Integrated Quadrant-Mode Matrix, have only received sparse coverage in very limited contexts

Identified Harms like obesity and musculoskeletal problems, lowered self-esteem and body image issues and addiction to digital devices appear in Quadrant A, but the coverage is narrow in scope and confined to particular vectors of harm. For instance, obesity and musculoskeletal problems are

⁷² The National Commission for Protection of Children, in its guidelines titled 'Being Safe Online', identifies cyberbullying as an online risk affecting children. Further, the Ministry of Home Affairs' Handbook for Adolescents / Students on Cyber Safety identifies cyberbullying as an online threat faced by children, recognises its physical, psychological, and emotional consequences, and outlines preventative / cautionary measures for children. National Commission for Protection of Child Rights, 'Being Safe Online' (NCPCR 2017) https://www.ncpcr.gov.in/uploads/16613370496305fdd946c31_being-safe-online.pdf accessed 4 August 2026.

addressed only incidentally in the specific context of advertising standards prohibiting content detrimental to children's physical health. Lowered self-esteem and body image issues are similarly engaged with only through the lens of misleading advertisements. Stress and anxiety find coverage only in the general, non-child-specific framework of the Mental Healthcare Act, 2017. Addiction to digital devices has received legal and regulatory attention only in the context of online gaming; the law has linked this Identified Harm only to a singular manifestation through the digital touchpoint (service) of online gaming. However, as is evident from Chapter 4, the harm may occur through other touchpoints as well (the internet, and general digital device usage leading to excessive screen exposure).

5. Certain harms lie outside the universe of legal coverage altogether

Inadequate sleep, impairment of eyesight, deterioration of pro-social behaviour, impairment of cognitive development, exploitation of children's labour in digital contexts, attracts no applicable legal instrument at any level. These harms, with the exception of the last, may be read as sharing certain common characteristics. First, the onset of such harms, such as sleep deprivation and cognitive impact is gradual. Second, their impact is not always immediately visible, like harms such as CSEA or cyber bullying or harassment. Third, establishing the chain of causation between the specific digital interaction and the harm is complex. Fourth, these harms are not attributable to discrete wrongful acts or specific wrongdoers and are structurally produced through cumulative exposure.

The inability of laws to address such harms exposes the limitations of the existing modes of legal engagement. Mode 1 (criminalisation) requires defined acts and identifiable perpetrators, which as explained earlier is not possible in these cases. Mode 2 (regulation of conduct of ecosystem stakeholders) form of engagement has been limited to either content related liability under the IT Rules, 2021 or consumer protection issues. It has so far not been employed to explore questions relating to the design of digital touchpoints that are critical in the context of such harms. Mode 3 (interpretative inclusion) does not apply here in light of the absence of any specific general legal provision keeping such harms in mind. Similarly, mode 4 (protective frameworks) is also absent since there is no protective architecture for children's digital well-being in India.

5.5.3 Systemic Limits in Legal Coverage and Approaches

The preceding analysis has mapped the existence and distribution of legal provisions addressing the Identified Harms. While that exercise was confined to assessing coverage rather than adequacy, it also reveals certain systemic limits in how law addresses child safety in digital contexts. These limits do not concern individual legal provisions or laws discussed earlier, but the law's fundamental orientation and conceptual boundaries. This section identifies four such limits.

1. Law addresses harm after occurrence, not through preventive design

The first gap concerns when harm becomes legally cognizable. Currently, the law addresses harm to children primarily after it occurs through punishment, content removal or compensation, and not through preventive measures that kick in prior to the harm occurring. Criminal laws like the POCSO Act, IT Act and BNS define prohibited conduct, establish culpability and provide for punishment of perpetrators, after harm has occurred. While such criminal laws remain indispensable for egregious violations, they were not designed to regulate the conditions under which children encounter or navigate digital spaces. The intermediary liability framework shaped by section 79, IT Act, read with IT Rules 2021, treats child safety as a compliance condition for claiming safe harbour immunity, rather than a fundamental principle informing the legal design. The DPDP Act marks a more deliberate engagement with children as a distinct category of data principals with enhanced protection. While protection of children's privacy is a meaningful protection under the DPDP Act, the law does not engage with the broader experience of a child navigating the digital space, the design features that structure that experience, or the risks that may flow from them.

Across these instruments, core product and service design decisions (including recommendation algorithms and engagement mechanisms) shaping the user's digital experience acquire legal relevance (if at all) once a legally recognised harm has occurred. Law has not yet imagined that the conditions under which children encounter digital touchpoints might themselves require regulation. The structural asymmetry between the capacity of large platforms to engineer behavioural outcomes through design and a child's developmental capacity to contextualise or resist such engineering remains outside legal imagination. No existing provision requires digital touchpoints to be designed in a manner that child safety considerations are embedded into design choices or even assess foreseeable risks emanating from such decisions.

A purely reactive framework operates on the assumption that harm can be identified, attributed and remediated after it has occurred. However, the scale of potential exposure, the vulnerability of those impacted, and the irreversibility of certain developmental consequences requires a reassessment of a purely reactive approach.

2. Law does not recognise children as requiring age-appropriate protection in digital spaces

The second limit concerns how law conceptualises children as subjects requiring protection. Law does not recognise children as requiring age-appropriate protection calibrated to development stages, treating childhood as a monolithic category.

The UNCRC establishes two foundational principles - best interest of the child⁷³ and the principle of evolving capacities, which recognises that children are a heterogeneous group and that their abilities, needs, and levels of autonomy

⁷³ Convention on the Rights of the Child (adopted 20 November 1989, entered into force 2 September 1990) 1577 UNTS 3, art 3(1).

change as they grow.⁷⁴ Law and policy must be responsive to these changes, so that children's rights are respected in ways that correspond to their capacities at different stages of life. UNCRC General Comment No. 25 applies these principles specifically to digital ecosystems, recommending age-appropriate measures informed by multidisciplinary research. The age-appropriate approach seeks to prevent harm at its source and empower children through design responsive to developmental stages. It has increasingly become a central element of best comparative practice.

Indian law does not meaningfully operationalise these principles. The state relies heavily on criminal law to address digital harms affecting children. Criminal law, by its nature, addresses serious and specific acts or omissions committed with a specific mental intention. However, many harmful digital practices may not meet the threshold for criminalisation, even when their effects on children are significant and cumulative. Harms such as sustained cyberbullying, algorithmic exposure to harmful content, or manipulative platform design are real and measurable, but may accrue gradually across multiple interactions and digital touchpoints rather than flowing from a single identifiable act by an identifiable perpetrator. Establishing the causal chain required by criminal law in such cases is a formidable task, and in many cases, many harmful practices may not meet these thresholds. Further, not every harm warrants it to be treated as an offence.

The IT Rules, 2021 impose obligations on intermediaries vis-à-vis unlawful and harmful content, including CSEAM, but do not require intermediaries to implement specific age-appropriate child safety measures, as seen in many countries discussed earlier. This absence is traceable to the objective of the rules, which is to provide a safe harbour to intermediaries rather than to create a safer digital space for children. These rules therefore govern intermediary conduct without acknowledging that children interact with such platforms differently from adults, are exposed to different risks and require correspondingly different protections built into this digital touchpoint. The DPDP Act takes a step towards requiring verifiable consent of parents before processing personal data of children. However, even this provision does not reflect the developmental nuance that principles of evolving capacities and best interest envisage. This limitation is, in part, explicable given that it is linked to the legal age for the capacity to contract. However, DPDP Act also does not envisage age-appropriate safety standards. While the JJ Act reflects a child-centred philosophy, including recognising the best interest of the child as a guiding principle, it has no application to platform design obligations or the risks that children encounter in a digital context.

Consequently, platforms operating in one of the largest markets for child users bear no system-level design duties in respect of their safety and well-being. Law does not recognise that a six-year-old, twelve-year-old and a seventeen-year-old encounter a digital touchpoint with fundamentally different protections.

⁷⁴ *ibid* art 5.

3. Law does not recognise age assurance to be proportionate to the risks and rights-respecting

The third limit concerns how law conceptualises age assurance, which is a critical component when it comes to child safety in digital spaces. DPDP Act requires data fiduciaries to obtain verifiable parental consent before processing personal data of a child.⁷⁵ To do this, data fiduciaries must exercise due diligence and use appropriate technical and organisational measures to verify that the individual identifying herself as the parent is an adult.⁷⁶ However, the law does not establish what constitutes appropriate age assurance methods, does not require risk proportionate implementation, and does not mandate safeguards to protect children's rights in the verification process itself.

It appears that law treats age assurance as a binary compliance requirement which involves verification, failing which data cannot be processed. It does not recognise age assurance itself as a design obligation requiring calibration between safety, privacy and best interest of the child.

Mechanisms that rely heavily on parental consent often rest on the assumption that parents have the digital literacy, awareness, and technical capacity to act in their child's best interests.⁷⁷ In many households, especially where digital literacy is low or where children are the primary users of digital services, parental consent may be neither informed nor meaningful. For instance, a 2023 study found that only 30% of children, 35% of parents, and 26% of educators are aware of digital safety, and only 3% of parents in India use techniques to mediate safe digital experiences for their children.⁷⁸ Further, hard verification mechanisms based on documentary evidence, such as government IDs, may create barriers to access and also raise concerns about intrusive data collection, and practical burdens on both families and service providers.⁷⁹ A narrow focus on parental consent may shift responsibility from digital touchpoints to parents, reducing incentives for service providers to adopt safety-by-design or invest in age-appropriate digital environments. Age assurance or verification continue to remain a compliance gate in India rather than a design obligation requiring proportionate, rights - respecting and evidence-based implementation.

4. Gaps in criminal law coverage of emerging harms

The fourth limit concerns which harms the law fails to expressly recognise. Criminal provisions under the POCSO Act, IT Act and BNS do not

⁷⁵ Digital Personal Data Protection Act 2023, s 9(1).

⁷⁶ Digital Personal Data Protection Rules, 2025, r 10(1).

⁷⁷ *ibid.*

⁷⁸ Citizen Digital Foundation, With Alice, Down the Rabbit Hole: Webinar on Online Child Safety in India with CSOs, Parents, and Policymakers (Report, 14 June 2024) https://b58a3240-b788-4b8e-b1ed-39f5ca507ffa.filesusr.com/ugd/d2759d_ca7984fe036945188217ac55a516c1bc.pdf accessed 4 August 2026.

⁷⁹ Sidharth Deb and others, Navigating Children's Privacy and Parental Consent Under the DPDP Act 2023 (The Quantum Hub and Young Leaders for Active Citizenship 2023) <<https://thequantumhub.com/wp-content/uploads/2023/11/TQH-YLAC-Childrens-Privacy-under-DPDP-Act-2023.pdf>> accessed 4 August 2026.

adequately capture the dynamics of sustained online abuse or the emergence of new forms of harm. Criminal law continues to focus on whether content is obscene, threatening or fraudulent, failing to address harms that operate through manipulation or misuse of information, sometimes divorced from sexual conduct.

Child grooming exemplifies this limit. Grooming entails a deliberate process through which an adult forms a relationship with a child with the intent of sexual exploitation.⁸⁰ This may take the form of gradually gaining trust, desensitising the child to sexual conversations, manipulating them into sharing explicit content or arranging offline meetings for abuse. Such conduct is often designed to avoid detection. Parents or guardians may remain unaware unless they actively monitor the child's online activity. Section 67B(c) of the IT Act criminalises the act of cultivating, enticing, or inducing a child into an online relationship for sexually explicit purposes or in a manner that would offend a reasonable adult.⁸¹ Similarly, Section 11(vi) of the POCSO Act addresses cyber-grooming by defining sexual harassment of a child carried out with sexual intent, including for pornographic purposes or for sexual gratification.⁸² However, neither the IT Act nor the POCSO Act adequately addresses situations in which children are solicited online and subsequently lured into in-person meetings.⁸³ This legislative gap diverges from the approaches adopted in the United Kingdom, Scotland, Norway, and Canada.⁸⁴ Further, under the POCSO Act and the IT Act, only grooming carried out for the purpose of sexual exploitation is criminalized. In contrast, the regulatory frameworks in the United Kingdom, Scotland, and the United States define grooming far more broadly.⁸⁵ Requiring proof of sexual purpose at the relationship's inception, inadequately reflects the incremental and manipulative nature of grooming, which frequently commences with innocuous communication that only gradually escalates towards exploitation. Further, under section 67B(c) of the IT Act, the conduct must occur in a manner that would offend a reasonable adult. This introduces an inappropriate standard that fails to account for children's developmental vulnerability. The result is a gap between the psychology of grooming and the criminal law's capacity to intervene before harm escalates.

Another emerging concern that remains unregulated is doxing, the disclosure

⁸⁰ Interagency Working Group, Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (ECPAT International 2011) <https://ecpat.org/wp-content/uploads/2021/05/Terminology-involveguidelines-396922-EN-1.pdf> accessed 4 August 2026.

⁸¹ Information Technology Act, 2000, s 67B(c).

⁸² Protection of Children from Sexual Offences (POCSO) Act, 2012, s 11(vi).

⁸³ Daniel Manoj and others, Behind the screens: Understanding the gaps in India's fight against online child sexual abuse and exploitation April 2025 <https://doi.org/10.1016/j.chipro.2024.100088> accessed 4 August 2026.

⁸⁴ United Kingdom Sexual Offences Act, 2003 s 15; United Kingdom Serious Crime Act 2015, s 67; Scotland, Protection of Children and Prevention of Sexual Offences Act 2005, s 1; New Zealand, Crimes Amendment Act, 2005, s 131B; Norwegian Penal Code 2005, s 306; Canadian Criminal Code 1985, s 172.1; Title 18 of the United States Code § 2422b, 2001.

⁸⁵ UK Sexual Offences Act, 2003 s 15; Scotland, Protection of Children and Prevention of Sexual Offences Act 2005, s 1; Section 172.1; Title 18 of the United States Code § 2422b, 2001.

of personal information online to target, intimidate, or harm someone.⁸⁶ Victims must rely on a patchwork of provisions under the IT Act and the BNS, none of which adequately captures the distinctive nature of this harm.⁸⁷ Various provisions dealing with the sharing of content primarily focus on content that is obscene, sexual or involves intimate imagery. Further, breaches of privacy and confidentiality under Section 72, and data theft under Section 43 read with Section 66, are treated primarily as economic offences rather than as social or gendered harms.⁸⁸ The DPDP Act does not impose any criminal sanctions for non-compliance.

Further, the proliferation of deepfake technology and other forms of synthetic media introduces substantial regulatory challenges. The legislative uncertainty centres on interpretive ambiguity regarding whether existing provisions encompass purely synthetic content.

⁸⁶ Saurojit Barua, Understanding Doxing & Its Impact, April 2024 <https://www.mondaq.com/india/privacy-protection/1450880/understanding-doxing-its-impact?ref=static.internetfreedom.in>. accessed 4 August 2026.

⁸⁷ Anita Gurumurthy, Amrita Vasudevan and Nandini Chami, 'Examining Technology-mediated Violence against Women through a Feminist Framework: Towards appropriate legal-institutional responses in India' (SSRN Scholarly Paper ID 3876187, 2018) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3876187 accessed 4 August 2026. ; Internet Freedom Foundation, 'Why Doxxing Remains a Legal Grey Area: Navigating the Legal Uncertainty of Online Exposure' (Internet Freedom Foundation, 2025) <<https://internetfreedom.in/why-doxing-remains-a-legal-grey-area-navigating-the-legal-uncertainty-of-online-exposure/>> accessed 4 August 2026.

⁸⁸ *ibid.*

CHAPTER 6

Global Experience



Global Experience

The preceding chapter examined the engagement of Indian laws with Identified Harms. In that process, the Chapter also identified certain systemic limitations with the existing legal approach. The Integrated Quadrant-Mode Matrix revealed that India's approach operates primarily through criminal law provisions and the intermediary liability framework linked with safe harbour provisions under the IT Act read with IT Rules, 2021. The existing legal approach indicated that the legal response is oriented towards harm redressal or deterrence rather than harm prevention. Even when the law adopts a conduct regulation approach through regulation of ecosystem participants like IT Act, IT Rules, 2021 and DPDP Act, it treats children as a homogeneous category across the age spectrum.

Given these observations, this chapter explores instruments adopted by international and regional organisations and laws across countries that have recognised preventive design obligations and age-appropriate measures. This chapter focuses on such measures because they represent regulatory approaches structurally different from India's current architecture. They provide useful comparative information for understanding other modes through which the law engages with digital safety issues relating to children. This chapter does not evaluate the relative merits of different approaches, nor does it seek to suggest that the measures observed are necessarily optimal for all contexts.

The chapter proceeds in two parts. First, it examines international conventions relating to children's rights to identify normative principles that guide global discourse on child safety in digital spaces. Second, it discusses national legal frameworks in select countries that have adopted preventive regulatory approaches.⁶⁸

⁶⁸ **Note:** Three clarifications are necessary. First, jurisdictions contemplating or in the process of enacting legislation have not been included. Second, non-binding guidance or advisory materials have been excluded, as they do not yet constitute legally enforceable obligations. Third, where authoritative English translations of relevant statutes were unavailable, the analysis relies on secondary literature.

6.2 International Normative Framework

International legal instruments addressing children's rights in digital environments have evolved considerably over the past decade, with notable developments in how they conceptualise state and private sector obligations. This section focuses on instruments adopted by the United Nations ("UN"), the European Union ("EU"), the Organisation for Economic Co-operation and Development ("OECD"), and the African Union ("AU").

6.2.1. United Nations

The United Nations Convention on the Rights of the Child ("CRC")⁹⁰ is a legally binding international treaty that recognises the civil, political, economic, social, and cultural rights of children. Its application in the digital environment has been elaborated through General Comment No. 25 issued by the Committee on the Rights of the Child ("**General Comment No. 25**").⁹¹ General Comment No. 25 applying UNCRC requires countries to ensure that "best interests of every child is a primary consideration" in all actions regarding "*provision, regulation, design, management and use of digital environment*."⁹² It expressly addresses private sector conduct stating that countries must ensure that "digital service providers" actively engage with children, apply appropriate safeguards and consider their views for developing products and services.⁹³ Notably, it also recognises privacy by design and

safety by design as important considerations to respond to different forms of harms or risks children face in the digital environment.⁹⁴ The comment also recognises children's "evolving capacities" requiring that measures to protect children in digital environments are age-appropriate and informed by up-to-date multidisciplinary research.

6.2.2. Organisation for Economic Cooperation and Development

The OECD adopted the Recommendations on Children in Digital Environment⁹⁵ in 2021, accompanied by Guidelines for Digital Service Providers.⁹⁶ The recommendations also recognised best interest of the child and age appropriateness as guiding principles to ensure a safe and beneficial digital environment.⁹⁷ The guidelines emphasise that in designing and delivering services for children, "digital service providers" must take a precautionary approach and adopt a safety-by-design approach to address risks. The recommendations also highlight the need for interventions that are proportionate to the risks and based on evidence.⁹⁸

6.2.3. African Union

The African Charter on the Rights and Welfare of the Child, read with Resolution No. 17/2022 of the African Committee of Experts on the Rights and Welfare of the Child, adopts a rights-based approach to children's protection in digital environments. The framework recognises the best interests of the child, non-discrimination, child participation, and

⁹⁰ Convention on the Rights of the Child (adopted 20 November 1989, entered into force 2 September 1990) 1577 UNTS 3.

⁹¹ UN Committee on the Rights of the Child, General Comment No 25 (2021) on children's rights in relation to the digital environment (2 March 2021) UN Doc CRC/C/GC/25.

⁹² *ibid* para 15.

⁹³ *ibid* para 17.

⁹⁴ *ibid* para 77, 88, 110, and 116.

⁹⁵ OECD, Recommendation of the Council on Children in the Digital Environment (OECD/LEGAL/0389, 2021) <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0389> accessed 4 August 2026.

⁹⁶ OECD, Recommendation of the Council on Children in the Digital Environment (OECD/LEGAL/0389, 2021) Annex: Guidelines for Digital Service Providers <https://legalinstruments.oecd.org/public/doc/272/272.en.pdf> accessed 4 August 2026.

⁹⁷ *ibid* Recs 1(a), 4.

⁹⁸ *ibid* rec 3.

freedom of expression⁹⁹, while emphasising the responsibility of States¹⁰⁰ and private-sector actors to protect children online through regulatory measures, industry standards, and platform accountability¹⁰¹. It also promotes measures to prevent and address online harms, including child sexual abuse material, through coordinated child-protection systems and cross-border cooperation.¹⁰²

6.2.4. European Union

The Guidelines on Children's Data Protection in an Education Setting (2021), adopted under the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981), emphasise the best interests of the child, evolving capacities, the right to be heard, and non-discrimination, particularly in relation to vulnerable children¹⁰³. The guidelines require children's data to be processed in accordance with core data-protection principles, including lawfulness, fairness, necessity, proportionality, transparency, and data minimisation¹⁰⁴. They further promote privacy and data protection by design, appropriate safeguards, and impact assessments to identify and mitigate risks to children's rights.¹⁰⁵

Key Observations

Several common principles emerge across these instruments. First, they articulate the best interest of the child as a primary consideration for any intervention in the digital space, whether it is laws or policies or the digital services itself. Second, they recognise children's evolving capacities, requiring differentiated approaches that account for developmental stages, rather than treating all children uniformly. Third, some instruments envisage a precautionary approach or a safety-by-design approach, which is in line with preventive approaches. Fourth, they emphasise proportionality, calling for measures to be calibrated to actual risk rather than blanket restrictions. Finally, they impose obligations not only on state parties, but also indirectly on the private sector or digital service providers, whose design choices often shape children's digital experience.

⁹⁹ African Charter on the Rights and Welfare of the Child (adopted 11 July 1990, entered into force 29 November 1999) OAU Doc CAB/LEG/24.9/49, arts 3–5, 7.

¹⁰⁰ African Committee of Experts on the Rights and Welfare of the Child, Resolution No 17/2022 of the ACERWC Working Group on Children's Rights and Business on the Protection and Promotion of Children's Rights in the Digital Sphere in Africa (2022).

¹⁰¹ *ibid.*

¹⁰² *ibid.*

¹⁰³ Council of Europe Committee of Convention 108, Guidelines on Children's Data Protection in an Education Setting (2021) T-PD (2020)07rev, [5.1].

¹⁰⁴ *ibid* [4.1].

¹⁰⁵ *ibid* [4.1].

These international instruments or frameworks establish the normative frameworks that some jurisdictions have begun to operationalise through binding national legislation.

6.3. Laws in Select Countries | Key Approaches

Laws in select countries addressing children's digital safety through preventive mechanisms can be organised around three regulatory approaches, discussed below. This section examines each of these approaches, identifies the jurisdictions in which it is operative, and concludes with comparative analysis.

The jurisdictions examined in this section were selected on the basis of three criteria, which apply in sequence. First, the report's broader comparative scope as set out in the methodology chapter covers fourteen jurisdictions distributed across the five United Nations regional groups, with the intent to ensure an analysis that reflects diverse legal, social, and political contexts. From within that set, this section examines those jurisdictions that have enacted binding legislative or regulatory instruments specifically directed at children's digital safety or digital safety with children as an identified constituency. The cut-off date for this examination is 15 May 2026. Proposed legislation, draft bills under consultation, and non-binding guidance are excluded here. Second, among the jurisdiction that meets the first criterion, this section only focuses on instruments with a view to understand and categorize regulatory approaches, instead of a jurisdiction-by-jurisdiction checklist. This approach ensures that the chapter does not strain to identify specific provisions (such as regulating for a specific harm, or in a specific context) which may not be suited to the Indian context, or for which adequate empirical information is not available.

6.3.1. Duty of Care and Systemic Risk Regulation

This approach imposes ex-ante structural duties on entities that provide services, including to children. These duties typically include identification, assessment, and mitigation of foreseeable risks arising from the operation of their services. They are attached to the service itself, following a mechanism of identification including through thresholds and risk assessments. Proportionate mitigation measures are prescribed, with a transparency requirement typically involving audit submissions that would permit a regulator to evaluate the adequacy of the measures undertaken. These duties are not contingent on the occurrence of a specific harm or the receipt of a complaint.

The cleanest instances of these approaches can be seen in the United Kingdom, the European Union, and Australia. The United Kingdom's Online Safety Act 2023 imposes structured duties on providers of user-to-user services and search services to respond to illegal content and content harmful to children. Each duty is operationalized through risk assessments and proportionate mitigation measures, with Office of Communications ("OfCom") as the enforcing regulatory authority.¹⁰⁶ OfCom's Protection of Children Codes¹⁰⁷ are in force as of May 2026, requiring covered services to identify and mitigate risks to children specifically through age assurance measures where appropriate, content moderation systems that are calibrated to child users, and design changes addressing algorithmic amplification of content harmful to children. The child-safety

¹⁰⁶ Online Safety Act 2023, c 50, s 2–3 (United Kingdom).

¹⁰⁷ Ofcom, Protection of Children Code of Practice for User-to-User Services (2025) [https://assets.publishing.service.gov.uk/media/680a04f7532adcaab3a2718/FINAL - Protection of Children Code of Practice for user-to-user services_2025_Parli AC.pdf](https://assets.publishing.service.gov.uk/media/680a04f7532adcaab3a2718/FINAL_-_Protection_of_Children_Code_of_Practice_for_user-to-user_services_2025_Parli_AC.pdf) accessed 4 August 2026.

duty is a freestanding statutory duty rather than a sub-category of a general user-safety duty. The European Union's Digital Services Act¹⁰⁸ organizes its corresponding duties around the concept of system risks which explicitly include risks to minors. Platforms that fall within the regulatory coverage must annually assess systemic risks, implement identifiable mitigation measures, and submit independent audit reports.¹⁰⁹ The European Commission's enforcement powers operate alongside those of the national Digital Service Coordinators.¹¹⁰

Australia's Online Safety Act establishes Basic Online Safety Expectations as a statement of what service providers are expected to follow,¹¹¹ paired with industry codes that become binding upon registration with the eSafety Commissioner.¹¹² Content from which children should be protected is grouped into categories of escalating severity,¹¹³ with platform responses ranging from proactive detection and removal of the most serious illegal content¹¹⁴ to access restrictions and age-assurance measures for content that is lawful for adults but inappropriate for children.¹¹⁵ The eSafety Commissioner consolidates regulatory¹¹⁶, investigatory¹¹⁷, and complaint-handling functions within a single body¹¹⁸, which gives the Australian framework its distinctive institutional depth within this approach.

The primary regulatory object under this approach is platform conduct, with an anticipatory regulatory posture. Platform conduct is treated as a system in operation enabling regulation of system features

such as recommendation dynamics, algorithmic amplification, virality and aggregation of design choices, both individually and together. Grounding the application of the regimes in user thresholds, reach and category of services, allows regulators to address harms that arise from the operation of services as a whole. Since compliance with these measures is grounded in transparency through self-assessments and third-party/independent audits, the effectiveness of this approach is tied directly to the regulator's institutional capacity to parse through system-level evidence.

6.3.2. Age-Appropriate Models

This approach treats childhood as the variable around which platform obligations are organized. Rather than imposing duties in terms of risks to users generally, with children treated as a sub-category of users, it establishes obligations that are specific to children. The unit of regulation here is the child's encounter with the service, and whether it is calibrated as per the child's developmental stage. It therefore accounts for the gradients of capacities, vulnerabilities, and protections which vary as per the child, required to be recognized by platforms and operationalized in design.

This approach is seen as adopted by the United Kingdom's Age-Appropriate Design Code 2020 ("AADC"), California's Age-Appropriate Design Code Act, and Brazil's Estatuto Digital da Criança e do Adolescente.

The UK's AADC sets out fifteen standards that any online service should assess if their service is likely

¹⁰⁸ Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L277/1, art 28.

¹⁰⁹ *ibid* arts 33-35, and 37.

¹¹⁰ *ibid* art 57.

¹¹¹ Online Safety Act 2021 (Cth) s 44, 45 and 46 (Australia).

¹¹² *ibid* ss 140 and 143.

¹¹³ *ibid* ss 6, 106 and 107.

¹¹⁴ *ibid* ss 46, 109 and 110.

¹¹⁵ *ibid* ss 46, 63D, 108, and 119.

¹¹⁶ *ibid* s 27.

¹¹⁷ *ibid* ss 31, 34, 37, 42, and Part 14.

¹¹⁸ *ibid* ss 30, 32, 36, and 38-40.

to be accessed by children.¹¹⁹ These include the best interests of the child as a primary consideration in design¹²⁰, the age-appropriate application of standards by reference to specified developmental bands¹²¹, data minimisation¹²², default high-privacy settings¹²³, restrictions on profiling¹²⁴, transparency in language that children can understand¹²⁵, and the limitation of detrimental use of children's data¹²⁶. The Code is enforced through the data protection apparatus, which gives the Information Commissioner's Office investigatory and penal powers under the United Kingdom General Data Protection Regulation and Data Protection Act.¹²⁷ The Code does not turn on platform size or user threshold. Instead, it applies to any service likely to be accessed by children¹²⁸, which gives it a regulatory reach that is conceptually broader than scale-gated frameworks even where its enforcement intensity is necessarily concentrated.

Brazil's Estatuto Digital da Criança e do Adolescente, enacted in September 2025, incorporates age-appropriate design within a broader children's digital rights framework.¹²⁹ The

statute imposes duties on platforms providing services to children and adolescents,¹³⁰ including duties to consider the child's developmental stage in the design of the service,¹³¹ to implement age-appropriate safety measures,¹³² to apply higher protections by default,¹³³ and to align service design with the principles of the Estatuto da Criança e do Adolescente, the country's foundational children's rights statute.¹³⁴

Australia's age-appropriate-design obligations are anchored within the Online Safety (Basic Online Safety Expectations) Determination 2022.¹³⁵ The determination introduced additional expectations applicable to services likely to be accessed by children, requiring providers to take reasonable steps to ensure the best interests of the child are a primary consideration in the design and operation of the service.¹³⁶ These expectations are operationalised through three identifiable design features. First, the Determination requires that accounts identified as belonging to child users be configured with the most restrictive default settings available on the service.¹³⁷ Second, the

¹¹⁹ Information Commissioner's Office, Age-Appropriate Design Code: A Code of Practice for Online Services Likely to be Accessed by Children (2020) <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/> accessed 11 August 2026.

¹²⁰ *ibid* standard 1 (Best interests of the child).

¹²¹ *ibid* standard 2 (Age-appropriate application).

¹²² *ibid* standard 3 (Transparency).

¹²³ *ibid* standard 4 (Detrimental use of data).

¹²⁴ *ibid* standard 6 (Default settings).

¹²⁵ *ibid* standard 7 (Data minimisation).

¹²⁶ *ibid* Standard 11 (Profiling).

¹²⁷ Data Protection Act 2018, ss 142–154.

¹²⁸ *ibid* s 123(1).

¹²⁹ Lei 15.211 de 17 de setembro de 2025 (Estatuto Digital da Criança e do Adolescente) ['Digital Statute for Children and Adolescents'] (Brazil).

¹³⁰ Lei 15.211 de 17 de setembro de 2025 (Estatuto Digital da Criança e do Adolescente) (Brazil) art 5.

¹³¹ *ibid* arts 3, and 4(III) and 7.

¹³² *ibid* arts 8 and 10.

¹³³ *ibid* arts 7(1), 8(IV) and 17(4).

¹³⁴ *ibid* art 3.

¹³⁵ Online Safety (Basic Online Safety Expectations) Amendment Determination 2024 (Cth).

¹³⁶ *ibid* s 6(2A).

¹³⁷ *ibid* s 6.

Determination requires services to take design measures that reduce the exposure of child users to harmful content, including controls over what content is surfaced to child accounts,¹³⁸ design constraints on recommender systems, and classification of content categories that child accounts should not encounter through ordinary use of the service.¹³⁹ Third, the Determination requires that reporting and complaint mechanisms be accessible, age-appropriate, and operable by the child without adult mediation.¹⁴⁰ The Determination is administered by the eSafety Commissioner, whose remit extends across Australia's online safety regime more broadly. The Australian framework is therefore hybrid, with age-appropriate-design obligations operating alongside the duty-of-care architecture examined in the previous section, and the same regulator engaging both.

This approach locates the regulatory subject differently than in the previous approach. Whereas the duty-of-care approach examined in the previous section treats the platform as a system in operation and engages with its outputs, this approach treats childhood as a developmentally structured legal category and engages with the conditions under which platforms encounter that category of users. The United Kingdom's Code identifies five developmental bands and assigns differentiated design implications to each, producing a conception of childhood that is internally structured and granular; the platform must therefore cater its design to a spectrum rather than to a single child. Brazil draws on the principles of its foundational children's rights statute to supply the developmental content, which means the design obligation is interpretively connected to a broader corpus of rights and protections that the platform must read alongside the statute itself. Australia frames the obligation

through expectations calibrated according to developmental stages but does not specify bands in the manner of the United Kingdom Code, leaving the developmental gradient to be operationalised through the regulator's guidance and through the platform's own assessment of its child user-base. These are not three implementations of the same design obligation; they are three different working conceptions of what the design obligation is responsive to. The reach of the obligation, the latitude available to the platform, and the question the regulator must answer when assessing compliance all shift across them.

6.3.3. Restrictive Approach

This approach addresses the digital safety of children by restricting their access to specific digital services or categories of use within them. The regulatory approach is not to require the service to be designed differently for child users, nor to require the platform to assess and mitigate risks arising from its operation. The unit of regulation, therefore, is the boundary between the child and the services, and the regulatory question which is asked is whether the child should be admitted to the service at all, and if so, on what terms.

Australia's Online Safety Amendment (Social Media Minimum Age) Act 2024¹⁴¹, France's Loi visant à instaurer une majorité numérique 2023¹⁴², and the regime introduced through Florida's HB 3 in 2024¹⁴³ are notable examples of this approach. Each operationalizes access restriction through different mechanisms such as platform prohibition, parental authorization, or a combination of both. It is notable that the age threshold in each of these jurisdictions, based on which access is determined, is different.

Australian law prohibits specified social media platforms from allowing children under the

¹³⁸ *ibid* s 8B.

¹³⁹ *ibid* ss 12(1), and 11.

¹⁴⁰ *ibid* ss 13-14.

¹⁴¹ Online Safety Amendment (Social Media Minimum Age) Act 2024 (Cth).

¹⁴² Loi n° 2023-566 du 7 juillet 2023 visant à instaurer une majorité numérique et à lutter contre la haine en ligne (Digital Majority and Anti-Online Hate Act) (France).

¹⁴³ Florida House Bill CS/CS/HB 3 (2024) Online Protections for Minors, Chapter 2024-146.

age of sixteen from holding accounts.¹⁴⁴ The obligation is assigned to platforms, who must take reasonable steps to prevent persons under the age of sixteen from creating or maintaining accounts.¹⁴⁵ The Minister may, on the advice of the eSafety Commissioner, extend or exclude particular services from that scope by legislative rules.¹⁴⁶ ¹⁴⁷ The designation process, provided in the legislation, turns on whether the sole or significant purpose of the service is to enable online social interaction between users.¹⁴⁸ The French legislation takes a different approach, wherein the statute prohibits social network operators from allowing children under 15 to register for accounts unless authorization has been given by a holder of a parental authority.¹⁴⁹ The platform must use a technical solution conforming to a framework issued by the regulator and the data protection authority to verify the age of the user and confirm parental authorisation.¹⁵⁰ Therefore, while the French framework does not exclude children under 15 year old from social networks outright, it conditions access on verifiable parental consent. Here, the locus of decision is the parent, and the platform's obligation is limited to ensuring that parental consent is registered before an account is created.

Florida's approach combines the Australian and French orientation. The HB 3 (2024) prohibits social media platforms from allowing children under 14 to create or maintain accounts and requires platforms to terminate existing accounts identified as belonging to them.¹⁵¹ For children between the ages of 14 and 16, parental consent is required for account creation.¹⁵²

Each of the three frameworks above operates

on the same regulatory structure but distributes responsibility and decision-making authority across different actors within the digital ecosystem. In the Australian framework, the decision lies with the platform layered under a categorical statutory prohibition for some services, therefore removing parental control from the decision-making process. As mentioned previously, the relevant age thresholds also differ across jurisdictions, with Australia setting the threshold at under 16 years, France at under 15 years, and Florida at under 14 years. Given the severity of the restriction, each threshold must be read as a substantive choice about the age at which the regulatory approach shifts from exclusion to participation, and which actor in the digital ecosystem is responsible for enforcement. Unlike other approaches, this approach does not engage with questions of platform design and features, nor does it regulate content generated by other users on the platforms.

¹⁴⁴ Online Safety Act 2021 (Cth), s 5.

¹⁴⁵ *ibid* ss 63D and 63E(4).

¹⁴⁶ *ibid* ss 63C(1)(b), 4, (5)(a), (6)(b), and (7)(a).

¹⁴⁷ *ibid* ss 63C(1)(b), (4), and 5(a).

¹⁴⁸ *ibid* s 63C(1)(a)(i).

¹⁴⁹ Loi n° 2023-566 (n 142) art 4.

¹⁵⁰ *ibid*.

¹⁵¹ Florida House Bill CS/CS/HB 3 (2024) Online Protections for Minors, Chapter 2024-146, §§ 501.1736(2)(a), 501.1736(2)(b)(1).

¹⁵² *ibid* s 501.1736(3)(a).

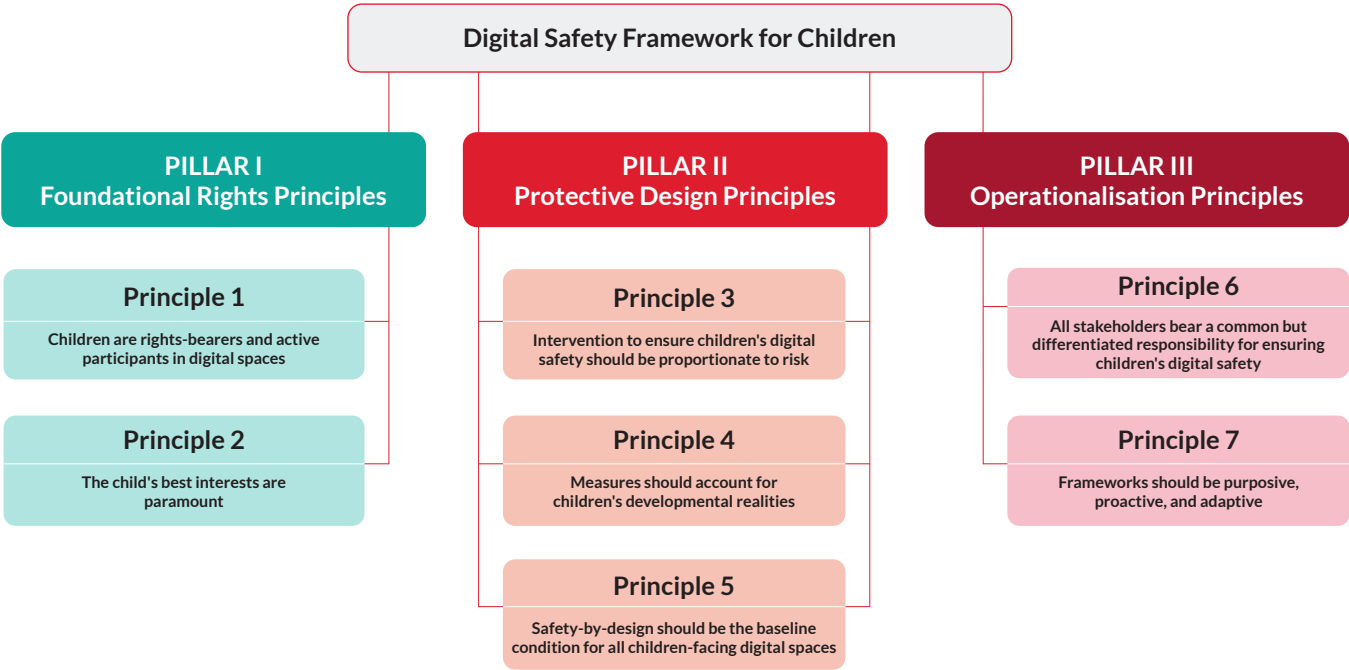
CHAPTER 7

Principles to Inform Digital Safety Frameworks for Children



Principles to Inform Digital Safety Frameworks for Children

The foregoing chapters of this report have identified certain harms that children may encounter in digital spaces, mapped legal responses to those harms and gaps in the same, and the approaches adopted by certain jurisdictions and international institutions in addressing children's digital safety. Drawing on that analysis, this chapter now sets out a broad normative framework of principles that may inform legislative, regulatory, policy and industry self-regulatory interventions towards digital safety of children. This framework is organised around seven principles, which are grouped into three pillars reflecting their distinct but interrelated aspects of child protection in digital environments



Infographic 6: Digital Safety Framework for Children

Alt text: Hierarchy diagram: Digital Safety Framework for Children, organised into three pillars: Foundational Rights Principles, Protective Design Principles, and Operationalisation Principles, comprising seven principles in total.

Pillar I (Principles 1 and 2), establishes the foundational rights framework within which all subsequent principles are to be understood. These principles affirm children’s legally recognised rights as active participants in digital spaces, and that their best interests must be the primary consideration in all decisions that shape their digital lives.

Pillar II (Principles 3, 4 and 5) set the guardrails concerning interventions to ensure children’s digital safety. These principles require that protective measures for children must be proportionate to risk, account for the developmental realities of childhood rather than treating children as a homogenous category and require safety-by-design obligations on those who build and govern digital spaces.

Pillar III (Principles 6 and 7) addresses questions of implementation and framework design. These principles concern how the normative commitments established in the preceding pillars may be operationalised through clearly distributed accountability across all relevant stakeholders, and frameworks that are purposive, proactive and adaptive in the face of a rapidly evolving technological landscape.

These principles represent foundational commitments essential to digital safety of children. While each principle targets a distinct objective, they function as an integrated set of mutually reinforcing obligations. This framework is intended to operate in parallel with a robust criminal law. For the most severe harms encountered by children in digital spaces, criminal liability is warranted, for purposes such as deterrence and vindication of the victim’s rights. The principles set out below speak to a broader ecosystem of children’s digital safety, primarily oriented towards preventive, structural, and systems-level interventions that complement criminal law apparatus.

Principle 1: Children are rights-bearers and active participants in digital spaces

Children are active participants in digital environments, which are important avenues for the exercise of their legally recognised rights. Any framework governing digital safety must recognise and uphold such rights, rather than being rooted exclusively in protectionist instincts.



Interpretation

“important avenues for the exercise of their legally recognised rights”

Digital environments are increasingly becoming integral to several aspects of children's lives. As recognised by the UN General Assembly, they are not merely spaces for recreation or social interaction but increasingly the terrain on which education, access to government services, commerce, and civic participation are conducted.¹⁵³ Thus, digital spaces afford new opportunities to children for the realisation of their rights, and they should be able to enjoy the benefits of technological progress.

“must recognise and uphold such rights”

Children enjoy a full range of legally recognised rights enshrined in domestic laws, as well as international instruments. This includes the right to equality and non-discrimination, freedom of expression, association and peaceful assembly, education, life and liberty in their broadest sense, which in itself includes the right to privacy, and protection from exploitation.¹⁵⁴ These rights do not diminish upon a child's entry into digital spaces; they apply with equal force therein.

A digital safety framework must recognise and uphold such rights as the operative baseline from which all measures geared towards children's digital safety proceed.

“rather than being rooted exclusively in protectionist instincts”

Children are a vulnerable population, owing to which they require specialised legal protection.¹⁵⁵ However, safety measures must function as enablers for realisation of their legally recognised rights, rather than a trade-off to be pursued at the expense of such rights.

Consider, for instance, recent legislative measures in certain jurisdictions imposing categorical restrictions or outright bans on children's access to social media platforms.¹⁵⁶ Such measures are typically advanced on protective grounds. However, blanket restrictions of this nature must be carefully evaluated and informed by an understanding of children's rights in digital spaces. Such measures risk curtailing children's rights to expression, association, access to information, and participation in public life in digital spheres, thereby necessitating sufficient proportionality requirements (see [Principle 3](#) for a discussion on what constitutes proportionality).



Implementation

- 1. Recognising children's rights as the foundation:** Digital safety frameworks for children must explicitly recognise children's legally recognised rights as foundational rather than aspirational. Safety objectives must be framed as furthering, rather than displacing, these rights.
- 2. Rights-compatibility assessments for restrictive measures:** Measures that may restrict children's access to digital spaces or otherwise limit the exercise of their rights therein, could be subject to ex ante assessment encompassing - (a) the impact of the proposed measure across the full range of affected rights, (b) consideration of less restrictive alternatives, and (c) transparent documentation of the

¹⁵³ United Nations General Assembly Res 78/187 (19 December 2023) UN Doc A/RES/78/187.

¹⁵⁴ Constitution of India, arts 14, 15(1), 15(3), 19(1)(a)-(c), 21, 21A, 23 and 24.

¹⁵⁵ Convention on the Rights of the Child (adopted 20 November 1989, entered into force 2 September 1990) 1577 UNTS 3.

¹⁵⁶ Online Safety Amendment (Social Media Minimum Age) Act 2024 (Australia); Indonesian Ministry of Communication and Digital, Regulation of the Minister of Communication and Digital No 9 of 2026 concerning Child Protection in the Digital Space.

reasoning in a manner open to scrutiny and review.

3. **Institutionalised mechanisms for participatory governance:** Children must be recognised as stakeholders in the design, implementation, and review of frameworks that govern their digital lives. Institutional mechanisms must facilitate meaningful child participation in safety design frameworks, ensuring that protective measures reflect lived experiences.

Principle 2: The child's best interests are paramount

The principle of 'best interests of a child' predates the advent of digital technology¹⁵⁷, and has been understood to operate simultaneously as a substantive right, a principle of interpretation, and a rule of procedure across legal frameworks.¹⁵⁸ An expansive understanding of this principle is required, one that extends beyond protection from harm alone, to encompass the realisation of the full range of legally recognised rights available to a child. In practice, this principle requires an individualised and context-specific assessment, calibrated to the unique circumstances of the child or relevant group of children.

Interpretation

"operate simultaneously as a substantive right, principle of interpretation, and a rule of procedure"

As a substantive right, this principle operates as a demonstrable requirement imposed upon any decision-maker whose actions have a bearing on the interests of a child, requiring evidence that children's interests were genuinely assessed and accorded appropriate weight in the particular instance.

As an interpretive principle, it requires that if a provision is susceptible to more than one reasonable interpretation, the interpretation that

more effectively serves the child's best interests must be preferred.

Lastly, as a rule of procedure, it may be understood as giving effect to the 'demonstrability' component of the substantive right aspect. It may be ensured through measures such as the transparent reasoning underlying relevant decisions, clear articulation of the weight accorded to children's interests, and where appropriate, processes that are open to scrutiny and review.

"expansive understanding of this principle"

While protecting children from harm, such as exposure to harmful content, online exploitation, or privacy violations is vital to child safety, the best interest principle demands a broader application. As elucidated in Principle 1, children are rights-holders, and any framework attendant to their best interests should be expansive enough not just to protect them, but to enable the adequate realisation of the full range of their rights.

Current laws addressing children's digital safety in India demonstrates structural limitations in this regard. Existing frameworks centre predominantly on sexual harm, organised around two objectives: the prosecution of perpetrators, and the regulation of intermediaries within the framework of safe harbour. Such an approach unaccompanied by any proactive frameworks does not put the child as the focal point; rather, the approach is primarily oriented towards and designed around the conduct of other actors. A framework genuinely oriented toward the best interests of the child requires elements beyond the two listed above, entailing the treatment of the child's interests (protective and enabling alike) as the organising principle.

For instance, this reorientation of child safety frameworks may entail the imposition of a duty of care on digital platforms, particularly those whose reach, scale and technical capacity position them as having a significant influence on children's digital environment. This represents a departure from safe harbour frameworks, which are primarily

¹⁵⁷ UNGA, 'Declaration of the Rights of the Child' Res 1386 (XIV) (20 November 1959) UN Doc A/4354; UN Commission on Human Rights, 'Report of the Working Group on a Draft Convention on the Rights of the Child' (2 March 1989) UN Doc E/CN.4/1989/48.

¹⁵⁸ UN Committee on the Rights of the Child, 'General Comment No 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration' (29 May 2013) UN Doc CRC/C/GC/14.

concerned with legal immunity for platforms with respect to content. In contrast, a duty of care is affirmative in character, and requires platforms to take active steps to identify, assess, and mitigate risks to children arising from the design, operation, and content of their services.¹⁵⁹ It does not require absolute protection from harm, but only that sufficient care has been taken.¹⁶⁰ The rationale is that design choices in underlying digital environments are not neutral and the costs of the resulting harms should be borne by those responsible for those choices rather than externalised onto children and society.¹⁶¹ For platforms whose design choices affect children at scale, such a duty should be proportionate to both their reach and their capacity.

[Principle 7](#) discusses the contours of such a proactive approach in further detail.

“individualised and context-specific assessment”

Just as children are not a homogenous group, this principle is also not a fixed or uniform standard. The application of this principle requires a case-by-case determination for individual decisions and with regard to the particular circumstances of the relevant group of children for collective decisions. Relevant contextual considerations may include, but are not limited to, a child's social location (across the axes of caste, gender, sex, ethnicity, culture, geographical location, disability status, citizenship status), economic status, age, maturity, cognitive and emotional development, family / community circumstances, as well as prior experience of harm or vulnerability.¹⁶²

Implementation

1. **Child rights impact assessments:** Actors whose actions are likely to have outsized impact on the interests of children, and possess requisite institutional capacity may consider Child Rights Impact Assessment prior to implementation.¹⁶³ Such an assessment could encompass identification of the population of children affected, evaluation of the potential impact across the range of children's interests, consideration of alternatives, and documentation in a manner that permits meaningful transparency.
2. **Meaningfully engaging with children's own views:** There is a need to consider establishing structured, accessible, and inclusive mechanisms for consulting children, including those from marginalised or vulnerable groups who may face additional barriers to participation, in the design and review of frameworks that affect them.
3. **Transparent reasoning:** Where decisions significantly affecting children are made, the decision-maker may articulate how the child's best interests were considered, what weight was accorded to them, and how they were balanced against any competing considerations. Where competing interests, including commercial interests, are weighed against children's best interests, the reasoning must demonstrate that the latter were treated as primary and that any departure from that position is exceptional and proportionate.
4. **Grievance redressal mechanisms:** Children and those acting on their behalf must have access to effective mechanisms by which decisions

¹⁵⁹ European Schoolnet, Children's Rights in the Digital World (Better Internet for Kids) <https://better-internet-for-kids.europa.eu/en/learning-corners/teachers-and-educators/childrens-rights-digital-world> accessed 30 July 2026; Emma Hatheway, 'Online Safety Regulation: The Duty of Care Framework and Implementation Blind Spots' (All Tech Is Human, 30 January 2025) <https://alltechishuman.org/all-tech-is-human-blog/online-safety-regulation-the-duty-of-care-framework-and-implementation-blind-spots> accessed 30 July 2026.

¹⁶⁰ Lorna Woods and William Perrin, Carnegie UK, Online harm reduction – a statutory duty of care and regulator, available at <https://carnegieuk.org/publication/online-harm-reduction-a-statutory-duty-of-care-and-regulator/> accessed 5 August 2026.

¹⁶¹ *ibid.*

¹⁶² UN Committee on the Rights of the Child, 'General Comment No 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration' (29 May 2013) UN Doc CRC/C/GC/14.

¹⁶³ *ibid.*

that inadequately account for children's best interests may be challenged or reviewed.

Principle 3: Intervention to ensure children's digital safety must be proportionate to risk

Measures to ensure children's safety in digital spaces must be proportionate to the nature, severity, and likelihood of actual harm. This requires a clear identification and categorisation of the harms, recognising that harms exist on a spectrum, that not all harms are legally recognised or ought to be addressed through law, and that the appropriate response will vary accordingly.



Interpretation

"Proportionate to the nature, severity and likelihood of actual harm"

The test of proportionality is a long-standing guardrail in legal and constitutional frameworks across jurisdictions, commonly applied to assess the legitimacy of measures that interfere with rights.¹⁶⁴ The proportionality principle continues to apply in assessing any measure intended to ensure children's digital safety. Such a measure ought not to be disproportionate in either direction, leading to serious harms to be under-regulated and the response being inadequate, or over-regulated where the response exceeds what the harm warrants.

For instance, consider assessing social media bans for children against this proportionality standard. While such a measure is likely to have a basis in law (as seen in Australia and Indonesia, for instance), and it can be satisfactorily argued that it is in pursuance of a legitimate state aim, that is, protection of children. A ban bears a reasonable nexus with this objective, but the more demanding inquiry is likely to arise in demonstrating that a total ban is the least restrictive amongst equally effective alternatives (such as age-appropriate design mandates being enforced elsewhere). It may

be equally tricky to countenance the argument that such an absolute prohibition will strike a balance between the incursion into children's rights ([see Principle 1](#)) and the overall benefit secured by the ban. This may especially be the case if the evidence linking social media use to serious harm is contested or incomplete, or if the ban is underinclusive (targeting one platform or age group while leaving comparable harms unaddressed elsewhere)

"Identification and categorization of harms"

Identification of specific harms is a prerequisite for proportionality assessment. Any framework geared towards children's digital safety requires identification and categorisation of harms it seeks to address. This may be carried out through engagement with relevant evidence pertaining to the harms children encounter in digital spaces, the populations of children most affected, the mechanisms through which those harms operate, and the strength of the causal link between specific conduct or design choices and the harm in question.

This report has identified certain harms to children which are either not addressed or addressed in limited aspects under existing laws.¹⁶⁵ Such harms also warrant appropriate attention, and a requisite proportionality assessment under digital safety frameworks.

"Harms exist on a spectrum, ... and the appropriate response will vary accordingly"

While all harms which affect children in digital spaces warrant appropriate attention, not all harms require the same type of response, legal or otherwise. The response must be calibrated as per the unique nature and characteristics of each harm. There are a range of instruments available to address a harm, ranging from criminalisation, outright prohibition, and mandatory ex ante regulatory obligations, to voluntary codes of practice, advocacy, investment in digital literacy, and in some cases, even deliberate non-intervention where the evidence does not support a regulatory response. Each instrument comes with its own considerations vis-a-vis a proportionality assessment, and the selection of an instrument may be driven by factors such as the

¹⁶⁴ Vicki C Jackson, 'Constitutional Law in an Age of Proportionality' (2015) 124(8) Yale Law Journal 3094.

¹⁶⁵ [See Section 5.4.](#)

severity and prevalence of the harm, the strength of the available causal evidence, the feasibility and effectiveness of different responses, and the manner in which existing law already treats the conduct concerned. Where a harm is serious, well-evidenced, and causally linked to specific conduct, a binding legal obligation may be warranted. Where harm is significant, but the evidence base is still developing, or where the causal mechanisms are diffuse, softer instruments such as codes of practice, guidance, or investment in awareness may be more appropriate. Where the evidence does not establish a sufficient basis for intervention, restraint is itself a legitimate regulatory choice. The framework must make space for the full range of these responses and must resist the tendency to treat legislation as the default answer to every harm identified.



Implementation

- 1. A harm identification and categorisation framework:** Any framework for children's digital safety must begin with a structured mapping of the harms it seeks to address, including metrics such as their nature, severity, prevalence, and the strength of available causal evidence.
- 2. A tiered response framework:** Corresponding to the categorisation of harms, a tiered response framework may be considered to set out the range of instruments available and the criteria that govern their selection.
- 3. Proportionality assessments for restrictive measures:** Where measures that significantly restrict children's access to digital spaces or curtail the exercise of their rights are proposed, a structured proportionality assessment must be conducted prior to adoption, addressing the suitability of the measure, the availability of less restrictive alternatives, the strength of the evidence base, and the impact on the full range of children's legally recognised rights. This assessment must be documented and open to scrutiny.

Principle 4: Measures must account for children's developmental realities

Children are not a homogeneous category across the entire age spectrum of 0 to 18.¹⁶⁶ While most legal systems demarcate childhood from adulthood through the concept of age of majority, transposing this legal construction in its entirety to children's digital safety frameworks needs reconsideration. Digital safety framework ought to account for the fact that children's capabilities, understanding, and autonomy develop over time.



Interpretation

"not a homogeneous category"

A 'child' is understood in most legal systems around the world as any person below the age of eighteen, thereby subsuming infants, toddlers, pre-adolescents, and teenagers on the cusp of adulthood into a single category. While this categorisation brought about by the concept of age of majority is intended to serve the purpose of protecting minors from their own inexperience,¹⁶⁷ any framework concerned with the digital safety of children needs to approach the diversity of developmental stages with more nuance. A measure designed for the vulnerabilities of a toddler may be unnecessarily restrictive and rights-curtailling for a sixteen-year-old with developed capacities for autonomous judgment. Conversely, a measure designed with the older adolescent in mind may afford wholly inadequate protection to a younger child who lacks the cognitive and emotional development to navigate the same digital environment safely.

"transposing this legal construction in its entirety to children's digital safety frameworks needs reconsideration"

While the legal distinction between minority and majority may be relevant in specific contexts such as the legal capacity to provide consent, for the broader range of digital safety questions, the relevant consideration should be whether the

¹⁶⁶ Ministry of Women and Child Development, National Policy for Children (2013).

¹⁶⁷ Law Reform Commission (Ireland), The Law Relating to the Age of Majority, the Age for Marriage and Some Connected Subjects (Working Paper No 2, 1977).

measure is appropriate to the developmental stage of the child concerned.



Implementation

1. **Recognising age appropriateness as the relevant standard:** This standard entails measures to be designed taking into account the developmental characteristics of the children they concern themselves with. Certain jurisdictions have already adopted age-appropriate design codes for children. For instance, the UK has adopted a risk-based approach to recognise the age of individual users and establish their age with a level of certainty that is appropriate to the risks of the rights of children that arise from their data processing.¹⁶⁸
2. **Involvement of domain experts in framework design:** Given that age-appropriateness is a standard grounded in developmental science rather than law, it would benefit from engagement with experts from relevant disciplines such as child psychology, developmental science, medicine, etc.
3. **Developmental evidence as a basis for framework design:** Measures for children's digital safety should be informed by credible evidence on child development, including cognitive, emotional, and social development across the age spectrum.
4. **Periodic review against evolving evidence:** Measures adopted under this principle may be subject to periodic review to ensure that the developmental assumptions on which they rest remain correct and that the calibration of age-appropriate standards continues to reflect the best available evidence.

Principle 5: Safety-by-design is the baseline condition for all

children-facing digital spaces

The safety of children must be built into the design, engineering, development and operation of digital products, services, and content. This entails a precautionary approach, focused on anticipating, detecting and eliminating harms to children before they materialise. Further, in the Indian context, regulatory discourse around ensuring children's digital safety may be delinked from the question of intermediary liability, since safety in this context is not limited to 'content' generated by users. Lastly, this approach should also account for cumulative and diffuse harms that arise from prolonged exposure to digital technologies, such as health and physiological harms and are not immediately apparent.



Interpretation

"safety of children should be built into the design, engineering, development and operation of digital products, services, and content"

Harms to children in digital spaces are caused not just by individual and discrete wrong doers but may also be perpetuated or exacerbated by the very design of digital spaces, their infrastructural characteristics, and seemingly innocuous product choices. In digital spaces, the capacity to produce or amplify a harm does not reside solely in the conduct of users and can originate from platforms themselves. For instance, harms may arise from the design of systems that amplify harmful content or from features that are routinely weaponised for harassment and abuse, etc.¹⁶⁹ A safety-by-design framework should account for this structural nature of harm to children and should require design choices to actively foreclose the exploitation of platform architecture for harmful ends. Safety must not be an afterthought but be embedded as a foundational condition at every stage of a product's

¹⁶⁸ Information Commissioner's Office, Age-Appropriate Design Code: A code of practice for online services likely to be accessed by children (2020) Standard 3.

¹⁶⁹ Ofcom, 'Risk factors that may lead children to harm online' <https://www.ofcom.org.uk/online-safety/protecting-children/risk-factors> accessed 5 August 2026; Parisa Rezaee Borj, Kiran Raja and Patrick Bours, 'Online Grooming Detection: A Comprehensive Survey of Child Exploitation in Chat Logs' (2023) 259 Knowledge-Based Systems 110039, available at <https://doi.org/10.1016/j.knosys.2022.110039> accessed 5 August 2026.

lifecycle, from initial design and engineering through to development, deployment, and ongoing operation.¹⁷⁰

As discussed in Principle 2, the best interests of a child require an expansive understanding. This extends to the understanding of safety-by-design obligations as well. In addition to ensuring ex post-facto redressal of harms to children in digital spaces, digital spaces and products must themselves be meaningfully designed to support children's wellbeing and the realisation of their rights. This shifts the burden from children and their caregivers, who are currently expected to navigate unsafe digital environments through individual vigilance, to the entities that design and profit from those environments and are also better placed in terms of informational access and resources to structurally create conditions for safe digital access.

“precautionary approach”

The precautionary approach entails that entities should not wait for harm to materialise, or for a regulatory mandate to compel action, to address it.¹⁷¹ In this regard, it bears noting that the precautionary principle has historically permitted potentially hazardous commercial activity to proceed while still requiring protective action. Governments have acted on possible threats to public health before scientific certainty has been reached.¹⁷² Therefore, even if a clear causal link between a design choice and harm to children is not immediately apparent, it does not justify a laissez-faire approach.

This precautionary obligation applies at the level of design choices themselves, by requiring entities to assess the safety implications of different design choices before those choices are made and implemented. Where a design choice carries a plausible risk of harm to children, that risk should be identified, weighed against alternatives, and

mitigated at the design stage. This proactive and proportionate assessment should extend to both harmful content, that is, content that carries a risk of harm to children, and unlawful content, that is, content that constitutes a legal wrong.



Implementation

1. **Regulatory discourse around ensuring children's digital safety should be delinked from the question of intermediary liability:** Very often, like in the case of India, digital safety of children is often conceived within the architecture of intermediary liability, which is structured around the question of legal accountability for third-party content, often after it has been published.¹⁷³ Safety-by-design is concerned with the anterior question of how products must be structured so as to prevent harm from arising in the first place. The two operate on different logics and in response to different regulatory objectives (while the overall objective of children's digital safety is ensuring their overall well-being). A digital safety framework for children may delink safety-by-design from safe harbour provisions for intermediary liability.
2. **Participatory approach for safety-by-design:** Safety-by-design considerations require consideration of diverse perspectives on what constitutes acceptable conditions for children's participation in digital spaces. An understanding of norms governing safety-by-design may be arrived at through inclusive and participatory processes.
3. **Risk assessment of design options:** Entities responsible for digital products, services, or content directed at or likely to be accessed by children may consider structured risk assessments of the design options under

¹⁷⁰ eSafety Commissioner, Safety by Design: Overview (May 2019), available at <https://www.esafety.gov.au/industry/safety-by-design> accessed 30 July 2026.

¹⁷¹ *ibid.*

¹⁷² Woods and Perrin (n 160).

¹⁷³ Information Technology Act 2000, s 79. The provision exempts intermediaries from liability for third-party content only where they act as passive conduits, observe prescribed due diligence, and expeditiously remove unlawful content upon acquiring actual knowledge thereof through a court order or government notification; failure to do so results in forfeiture of this exemption.W

consideration during development. Such assessments may include identifying the categories of harm to which each design option gives rise, assessing the likelihood and severity of those harms, and documenting the reasoning behind the design choices ultimately made.

4. **Children's risk assessments:** Entities having an outsized impact on children's digital lives, owing to factors such as their scale and reach, may consider conducting structured risk assessments prior to the launch of products or services, identifying the categories of harm to which children may be exposed, evaluating the likelihood and severity of such harms across different categories of children, and documenting the design measures adopted in response.
5. **Certification ecosystems and collective accountability:** Effective implementation of this principle may necessitate the development of shared infrastructure, including certification schemes and audit frameworks that allow safety commitments to be verified across entities, products, and services. Doing so would serve both accountability and market functions. It would provide children and their caregivers with assurance that safety obligations are being met, and create incentives for entities to compete on the basis of safety.
6. **Accountability and transparency:** Entities may maintain documentation of their safety-by-design processes, including risk assessments, design decisions, and the outcomes of any safety testing, and make such documentation available to regulators or any other concerned stakeholders upon request.
7. **Account for cumulative and diffuse harms:** As stated elsewhere in this report, not all harms to children in digital spaces are discrete, attributable events; they may also arise not from a single interaction or piece of content, but from prolonged and repeated exposure to digital technologies and the cumulative effect of design choices that individually may appear innocuous.¹⁷⁴ Such harms resist easy causal

attribution and tend to fall outside the ambit of frameworks oriented around identifiable, incident-based harms. A safety-by-design framework must therefore extend its remit to encompass these cumulative and diffuse harms in the design and operation of digital services and products.

Principle 6: All stakeholders bear a common but differentiated responsibility for ensuring children's digital safety

Every stakeholder in the digital ecosystem, including the State, platforms, developers, schools, parents and caregivers, bears responsibility for ensuring children's digital safety. This responsibility is differentiated taking into account factors such as the role of each stakeholder and their power and influence over the ecosystem of children's digital safety. The frameworks through which this shared responsibility is given effect must themselves be participatory, enabling all stakeholders, including children, to contribute meaningfully.



Interpretation

"Every stakeholder in the digital ecosystem... bears responsibility"

Children's digital safety is a shared responsibility that spans the full range of actors whose decisions influence the conditions under which children encounter digital spaces. For instance, the State bears responsibility for establishing the legislative and regulatory frameworks that set the baseline conditions for children's digital safety, and for enforcing those frameworks effectively. Likewise, platforms and developers bear responsibility for the design, engineering, and operation of the products and services through which children access digital spaces.

"this responsibility should be differentiated"

The principle of common but differentiated responsibility, developed in the context of

¹⁷⁴ See Chapter 4.

international environmental law,¹⁷⁵ provides a useful organising framework here. Applied to children's digital safety, it holds that while all stakeholders share a common obligation to contribute to the safety of children in digital spaces, the nature, stringency, and scope of that obligation may vary based on each stakeholder's capacity to cause harm, their ability to prevent it, and the degree of control they exercise over the conditions that give rise to it.

"role of the stakeholder and their power in and influence over children's digital safety"

In this framework, large platforms occupy a distinct and elevated position of structural influence over children's digital experiences¹⁷⁶, and accordingly bear a correspondingly greater share of this responsibility. As discussed earlier, the elevated responsibility of large platforms is a function of their scale, as well as their structural position in the digital ecosystem; their gatekeeper position makes them indispensable points of regulatory intervention.

Their position also gives rise to systemic risks. The largest platforms are so deeply embedded in the infrastructure of digital life, including children's education, social connection, and access to information, that their dysfunction or misuse carries consequences that extend far beyond any individual user.¹⁷⁷ Recently, regulatory thinking around these large platforms (EU Digital Services Act and the UK Online Safety Act) has moved towards the articulation of a duty of care: an obligation on platforms to take reasonable steps to protect users, particularly vulnerable users such as children, from foreseeable harms arising from the design and operation of their services.

"the frameworks through which this shared responsibility is given effect must themselves be participatory"

Participatory governance creates meaningful opportunities for the full range of affected stakeholders, including children, to shape the design, implementation, and review of the frameworks that govern their digital lives. It serves several distinct functions. It ensures that regulatory frameworks are informed by the lived experiences of those most affected, distributes the responsibility for ongoing oversight across a broader range of actors, creates conditions for the kind of societal consensus that gives safety norms their legitimacy and durability, and provides a check on the tendency of both platforms and regulators to treat children as objects of protection rather than as rights-bearing participants with a genuine stake in the decisions that affect them.

Implementation

- 1. Tiered regulatory obligations calibrated to platform scale and risk:** In designing any regulatory framework for digital safety of children, there is a need to consider differentiated obligations for different categories of platforms, with the most stringent requirements applying to platforms that meet defined thresholds of scale, reach, or systemic significance. Such platforms may be subject to heightened requirements such as mandatory risk assessments, transparency reporting, independent audit requirements, and proactive duties to identify and mitigate risks to children.
- 2. A statutory duty of care for children:** Regulatory frameworks may consider articulating a statutory duty of care owed by platforms to child users, requiring them to take

¹⁷⁵ United Nations Framework Convention on Climate Change (adopted 9 May 1992, entered into force 21 March 1994) 1771 UNTS 107, art 3(1). - The principle of Common But Differentiated Responsibilities ("CBDR") in environmental law establishes that all countries bear a common and shared responsibility for anthropogenic climate change. That said, the responsibility among countries is unequal owing to their differing contributions to climate change, as well as their varying economic capacities. Therefore, CBDR accounts for the greater historical responsibility borne by industrialized countries in climate change.

¹⁷⁶ European Parliamentary Research Service, *Regulating Digital Gatekeepers* (2020) [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/659397/EPRS_BRI\(2020\)659397_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/659397/EPRS_BRI(2020)659397_EN.pdf) accessed 30 July 2026.

¹⁷⁷ Nordine Abidi and Ixart Miquel-Flores, 'Too Tech to Fail?' (Oxford Business Law Blog, 13 July 2022) <https://blogs.law.ox.ac.uk/business-law-blog/blog/2022/07/too-tech-fail> accessed 30 July 2026.

reasonable and proportionate steps to protect children from foreseeable harms arising from the design and operation of their services.

3. **Institutionalised mechanisms for multi-stakeholder accountability:** Accountability frameworks should provide for the establishment of multi-stakeholder bodies or processes through which the full range of stakeholders can contribute to the ongoing oversight and review of children’s digital safety frameworks.

Principle 7: Frameworks should be purposive, proactive, and adaptive

Frameworks for children’s digital safety must be purposive, oriented towards the specific objective of protection of children in digital spaces. They must enable proactive identification and mitigation of harms, intervening upstream at the level of systems and design rather than reacting to harm after it has materialised. They must be adaptive, structured to evolve through periodic review.

Interpretation

“Purposive”

A framework is purposive when it is aligned with and organised around the problem it seeks to address. In the context of children’s digital safety, this requires two things: first, that the framework is oriented towards ensuring the digital safety of children as its primary objective; and second, that it is attentive to the particular rights and vulnerabilities of children as a distinct population.

As noted elsewhere in this report, existing legal frameworks in India that bear on children’s digital safety are predominantly reactive in character and organised around objectives (focused on the conduct of other actors) other than the child’s

safety and wellbeing.¹⁷⁸ A purposive framework, by contrast, treats the child’s interests as the organising principle from which all other design choices flow.

“enable proactive identification and mitigation of harms, intervening upstream at the level of systems and design”

A purposive framework also intervenes at the right level and at the right time. In this regard, a proactive and systems-level orientation for children’s digital safety frameworks merits serious consideration. Such a framework imposes obligations on platforms before harm occurs, anticipating its occurrence and aiming to prevent it from materialising, and does so at the level of systems and architecture rather than individual items of content.¹⁷⁹

A proactive approach is particularly significant in the context of children’s digital safety, given that many harms take years to fully develop or become apparent. The information and power asymmetry seen in digital markets compounds this problem further.¹⁸⁰ This dynamic is especially acute in the case of children, who lack the capacity to meaningfully assess the risks they face.

The case for systems-level regulation follows from this. Arguably, large platforms, particularly social media services, effectively function as public or quasi-public spaces, and their deliberate architectural choices shape the environment in which children operate at scale.¹⁸¹ A proactive framework therefore moves beyond holding platforms accountable for individual items of content on their services, to holding them responsible for the systems they have designed and the risks those systems generate. It is the architecture that merits regulatory attention, not merely the content those systems surface. This also connects directly to the duty of care framework discussed under [Principle 2](#).

¹⁷⁸ See [Section 5.5.3](#).

¹⁷⁹ Delia Rickard, Report of the Statutory Review of the Online Safety Act 2021 (Department of Infrastructure, Transport, Regional Development, Communications and the Arts, February 2025); Lorna Woods, William Perrin (n 160).

¹⁸⁰ *ibid.*

¹⁸¹ *ibid.*

“Adaptive”

Owing to the rapid pace at which digital technologies develop, frameworks should be treated as living instruments, subject to revision in light of novel and changing circumstances. A framework’s capacity to be revised through structured review is critical. In the specific context of children’s digital safety, iteration may be informed by a range of inputs: emerging evidence regarding the harms children encounter and the effectiveness of existing regulatory responses; technological developments that create new categories of risk or render existing provisions obsolete; enforcement experience that reveals gaps, ambiguities, or unintended consequences.



Implementation

1. **Proactive regulatory obligations:** An assessment of the case for proactive, systems-level regulation for children’s digital safety, and its appropriate contours, merits immediate consideration by policymakers.
2. **Mandatory periodic review:** Frameworks may provide for mandatory review cycles at defined intervals, ensuring that the iterative review requirements are structurally embedded rather than left to discretionary initiative.
3. **Outcomes-based and principles-based drafting:** Where appropriate, frameworks may articulate the outcomes and principles they are designed to achieve and the broad direction for doing so, without prescribing implementation detail that may quickly become obsolete. In the context of legal frameworks specifically, detailed technical standards may be developed through delegated legislative or administrative processes to ensure compliance clarity.

V I D H I Centre for
Legal Policy

A-232 Ratan Lal Sahdev Marg, Defence Colony,
New Delhi - 110024