CHILDREN'S RIGHTS AND ONLINE SAFETY IN INDIA: LEGAL GAPS IN THE INFORMATION TECHNOLOGY ACT AND THE EXPLOITATION OF DIGITAL CHILDHOODS

Priyanshi Soni[*] Hussain Patanwala[*]

ABSTRACT

In an age dominated by digital interconnectivity, children in India are rapidly emerging as one of the most visible and vulnerable groups in the online world. On the one hand, this study is situated in the context of the twofold threat online represents for children—cyberbullying, harmful content, data misuse and grooming—and, on the other hand, the emerging problem of their commodified digital presence, in particular driven by social media use and influencer culture. As the international legal architecture is developing to cater to digital child rights, the Information Technology Act, 2000, and its associated legislation regime in India are antiquated and do not commensurate with such emerging realities. This paper reviews the existing Indian legal framework including the IT Act, the Child Labour (Prohibition and Regulation) Act, and the Digital Personal Data Protection Act and reveals that the current laws are ill-equipped to govern the commercial sexual exploitation of children online and to hold the platform/service providers responsible. By comparing these frameworks, the paper analyses several international legal innovations such as France's Kidfluencer Law, the US COPPA framework, and the UK's Age Appropriate Design Code and draws actionable insights for India's legislative reform. The study suggests a new, dedicated legal model to safeguard children in digital economies – centred on right-based governance, financial protections and consent. Through a synergy of legal, technical and policy-based solutions, this research aims to catalyse a national conversation surrounding the imperative to regulate and safeguard childhoods in the emergent digital milieu of India.

[*]BBA LLB, FIFTH YEAR, PRESTIGE INSTITUTE OF MANAGEMENT AND RESEARCH, DEPARTMENT OF LAW, DAV, INDORE, INDIA.
[*]GRADUATE.

Keywords: Digital Childhood, Child Influencers, Online Safety, Children's Rights, Information Technology Act (India).

INTRODUCTION

The swift proliferation of India's digital infrastructure has fundamentally altered the way children engage with their environment. With more than 560 million internet users and a rising number of households linked to the internet through low-cost smartphones, children in India are increasingly common users of digital platforms for education, entertainment and communication. With such wide access, it has both great advantages and issues. More and more, children are not just passive users of digital content; they are also players in online economies. From kid-directed YouTube channels and game live streams to family vlogs and sponsored content deals, children are featured and exploited online – often lacking any informed consent, protective oversight or legal recognition of their rights to do so.[1] Notwithstanding this increasing engagement of children in digital platforms, the legal framework of India, especially the Information Technology Act, 2000, is not relevant to address the material risks and exploitative attitudes confronting children. Forty-Two and counting: The effects of the MHRDA. As the MHRDA was passed at a time when the digital society still catered predominantly to adults, there are no direct childhood-specific clauses outside of Section 67B, which prohibits the publishing or transmission of sexually explicit material of a child.[2] It doesn't even articulate or govern the commercialisation of children's digital content or place responsibilities on platforms or carers that broker and profit from the online presence of young children. Children are left in a vacuum where they are at the receiving end of Bullying, Grooming, mental trauma, loss of privacy, loss of economic and reputational implications and have no recourse or recognition under the Indian law.[3] Monetising children's digital visibility, meanwhile, raises pressing questions about exploitation, work, privacy and autonomy. Provision of Existing Laws: The existing law on child labour, including the Child Labour (Prohibition and Regulation) Act 1986, does not cover the digital process of production in which children contribute content for commercials and earn from their brand endorsements, advertising revenue and viewer-related revenue on social media platforms.[4] Unlike child artists

[1] Jaspreet Singh, 'Child Influencers in India: Legal Grey Zones and Digital Exploitation' (2023) 45(2) *Indian Journal of Cyber Law* 56
[2] Information Technology Act 2000, s 67B
[3] NCPCR, *Report on Child Safety in Online Gaming and Content Platforms* (2021) https://ncpcr.gov.in accessed 18 July 2025
[4] Child Labour (Prohibition and Regulation) Act 1986; see also India Code, Ministry of Labour and EmploymEnt

in the traditional child star system, which is subject to film and television regulations, however, children in the influencer economy evade even outside of formal regulatory oversight. Their images are commodified with no corresponding power to consent, no bona fide right to the kind of economic protections that players ought to have in an economy that profits precisely from their visibility. The Digital Personal Data Protection Act 2023, an effort to regulate data security and consent generally, defines anyone under the age of 18 as a child and requires verifiable parental consent to process data.[5] But there is no statutory requirement to establish effective age verification, nor does the law require content platforms to have in place age-appropriate protection. Even more frightening, the Act doesn't make a difference between a kid's digital identity for social use and one for profit. There is still no obligation for platforms to monitor, report on or moderate monetised child content. This leads to the unfettered datafication of children and the algorithmic amplification of their presence determined in terms of engagement rather than welfare. Others also do this, but what is new is the response that jurisdictions (worldwide) are taking about the exploitation of children in the digital age, through creative legal instruments that are implemented. France was the first to predict their exploitation ahead of its 2020 "Kidfluencer Law" requiring to obtain local government's authorization for the hours the children engage in producing monetised online video and to put most of their earnings in a blocked account that can be released when they become adults.[6] It also enshrines the right to request takedown of content and places legal duties on platforms hosting monetised, child-made content driven by children.[7] In the same vein, the United States applies data protection to children via the Children's Online Privacy Protection Act (COPPA), and the GDPR, for its part, features stringent requirements on consent and data minimisation regarding minors. The UK's Age-Appropriate Design Code requires platforms to act for the benefit of the digital products that they create.[8] In this context, the current study aims to scrutinise the effectiveness of Indian laws in safeguarding children in the online domain. The study will also examine the IT Act 2000, the Child Labour Act 1986 and the Digital Personal Data Protection Act 2023 concerning online harms and digital exploitation. The research also seeks to expose the gaps in Indian cyber laws vis-à-vis online threats to children and the

[5] Digital Personal Data Protection Act 2023, s 9
[6] France: Law No. 2020-1266 on the Rights of Child Influencers (2020)
[7] Library of Congress, 'France: Parliament Adopts Law to Protect Child "Influencers" on Social Media' (30 October 2020) https://www.loc.gov/item/global-legal-monitor/2020-10-30/france-parliament-adopts-law-to-protect-child-influencers-on-social-media/ accessed 18 July 2025
[8] UK Information Commissioner's Office, *Age-Appropriate Design Code* (2020) https://ico.org.uk accessed 18 July 2025

monetisation of digital childhoods and to examine regulatory models in other jurisdictions that might guide an Indian legislative response.

The study is doctrinal and based on analysis of legislation, case law, policy statements and international instruments such as the United Nations Convention on the Rights of the Child (UNCRC) and its General Comment No 25 on children's rights in the digital environment.[9] The comparative study is used to benchmark the regulatory practice in France, the EU, the US, and the UK in the coaching on which recommendations for India are based. The research zooms in on those below 18 years of age in the Indian legal framework and examines their online activities on platforms such as YouTube, Instagram, as well as online gaming applications. The purpose of this research is to determine the extent of protection offered to children under the Indian cyber law, to pinpoint the areas of deficiency in regulating their online activities and economic exploitation, and to suggest legal and policy reforms by international best practices. What are the legal challenges faced by children in Indian digital environments? How the issue of online gambling is addressed in the Information Technology Act, 2000? What can India learn from other countries on child protection and digital governance? What changes are needed in the digital economy to save children from abuse and harm? This study is important because it is an effort to highlight the less developed patch in Indian cyber law and child rights jurisprudence. By framing children as rights-holders and economic actors in digital space, the study contributes to a much-needed shift in how we legislate, design platforms and understand what it means to live in digital childhoods. That would lay the groundwork for the next wave of child-focused reform of cyber law in India.

CARTOGRAPHY OF CONCEPTUAL AND JURIDICAL REASONING ON CHILDHOOD DIGITALISATION

Childhood in Digital Era: The digital revolution has fundamentally changed the social, legal, and economic landscape of children. Children of today are plunged into online 'habitats' at ever earlier ages, interacting with (virtual) worlds not only as part of educational and entertainment platforms, but also as contributors to monetised networks. As their identities and activities become more datafied and platform-ified, legal systems have been confronted with the task of extending longstanding principles of child protection to technologically mediated

[9] 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)

environments.[10] This chapter introduces the conceptual framework of the study, as well as the jurisprudential scaffold and analytical lenses for children as rights-holders, as economic agents and as vulnerable digital citizens. To begin with, the foundation of this inquiry is the United Nations Convention on the Rights of the Child (UNCRC), of which India is a signatory. The UNCRC establishes children's entitlements and freedoms to privacy, economic protection, participation and development.[11] Acknowledging the migration of these rights into the digital sphere, the UN Committee issued General Comment No 25 (2021), stating that children's rights are applicable "in all digital environments," encompassing social media, gaming, ed-tech tools, and algorithmic infrastructures.[12] The GC emphasises the State's responsibility to promote that digital technologies are in the best interest of the child with a focus on consent, profiling, autonomy and access to remedy 77. In India, while legislation like the Juvenile Justice (Care and Protection of Children) Act 2015, the Right of Children to Free and Compulsory Education Act 2009, and Protection of Children from Sexual Offences Act 2012 (POCSO), embodies robust welfare and protection considerations, none of these instruments seem to provide such protection specifically within the digital space.[13] These laws were not meant to tackle child data profiling, algorithmic manipulation, influencer monetisation, or behavioural tracking—all of which characterise online childhoods in India today. There is, as a consequence, a conceptual and legislative void where children's rights are concerned, unrooted in the systems that rule their digital lives. "When you're talking about digital childhood, more often, scholars and child-rights advocates are talking about vulnerability and agency." Digital vulnerability is the increase in the risk of psychological, reputational, and economic harm faced by the child as a result of his or her online activity.[14] Conversely, however, agency requires that children also be seen as agents with the ability to voice their preferences, to participate online, and to seek redress – all within age-appropriate and protective contexts.[15] The UNCRC has a general principle, "evolving capacities," under Article 5 that is particularly relevant considering legal responses that are neither overly broad nor paternalistic, rather balanced to respect the

[10] Sonia Livingstone and Amanda Third, 'Children and Young People's Rights in the Digital Age: An Emerging Agenda' (2017) 19(5) *New Media & Society* 657
[11] UNCRC (1989), arts 16, 17, 19, 31, 32
[12] 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
[13] Juvenile Justice (Care and Protection of Children) Act 2015; RTE Act 2009; POCSO Act 2012
[14] Usha Ramanathan, 'Surveilling Children: The Intersections of Law, Technology and Rights' (2023) *Indian Journal of Constitutional Studies* 12
[15] Sonia Livingstone and Mariya Stoilova, 'The Paradox of Children's Digital Rights' (2020) 43(3) *Journal of Law and Society* 371

autonomy of adolescents but also keep them safe.[16] Building on this, a typology of risks to children online has been developed, typically organised around the "4Cs" model: Content, Contact, Conduct, and Commercial/Contractual risks. Content-based risks refer to age-inappropriate or harmful content exposure with such materials like porn, hate speech, or misinformation. Contact risk is the risk that may result from contact with strangers, including grooming, sextortion, and cyberbullying. Behaviour risks are those stemming from children's actions online – such as sharing too much information, creating intimate content of one's self or taking part in risky viral challenges. Commercial risks — which are rarely discussed in Indian legal and academic discourses — comprised the collection and monetisation of children's data and identities, profiling for advertising purposes and participation in influencer economies.[17]

Child digital labour and monetised childhoods have become particularly prevalent in recent years. Minors in for-profit media content are common on platforms like YouTube, Instagram, and gaming channels. Some are (more or less) under agency control and parental supervision, and others do not approach the engagement with informed consent, compensatory structures or knowledge of their exposure.[18] Without legislation or case law in India that defines and regulates digital work by minors, these children are legally invisible—they receive no protection under labour laws (because the work is off the books) but are not covered under child welfare laws, either.[19] Family vloggers, brand partnerships, gaming streams, and short-form video platforms now make up unregulated digital economies that traffic in the commodification of minors for the sake of the algorithm. If the monster guardian is not held accountable, it can have long-term consequences -- both developmental and economic.[20] Some countries around the world have begun to respond. France's "Kidfluencer" law requires the registration of child influencers and that a percentage of their earnings be stashed into trust funds until the child reaches the majority age (except for example, who are allowed to binary).[21] The US COPPA regime makes it illegal to collect data on under-13s without parental consent,

[16] UNCRC, art 5
[17] UNICEF, *State of the World's Children 2021: On My Mind – Promoting, Protecting and Caring for Children's Mental Health* (UNICEF 2021) https://www.unicef.org/reports/state-worlds-children-2021 accessed 18 July 2025
[18] Outlook India, 'Money, Fame But No Safety Net in the Murky Market of Kid Influencers' (2022) https://www.outlookindia.com accessed 18 July 2025
[19] Child and Adolescent Labour Act 1986
[20] Adhyayan Foundation for Policy & Research, 'Kids as Currency: Legal Gaps in Indian Digital Labour Law' (2024)
[21] French Law No. 2020-1266 (19 Oct 2020); Library of Congress, Global Legal Monitor https://www.loc.gov/law/ accessed 18 July 2025

and the EU GDPR increases protection over minors' data, as well as requiring visibility in processing activity.[22] The Age-Appropriate Design Code enforced by the United Kingdom also specifies that platforms set child protections as default, minimizing developers' ability to collect data and profile users, by default.[23] Very little Indian literature is available on this topic. Though government reports, such as those by the National Commission for Protection of Child Rights (NCPCR), and non-governmental organisations such as ChildFund India, have acknowledged the increase in online risks, most of them are for content moderation and cybercrime prevention.[24] Commentary in academia does not address in depth the participation of children in the platform economies, the legal ramifications of child-generated income, the roles that platforms and guardians have in monetised contexts.[25] This academic white spot is among the reasons that have motivated the present research, which seeks to expand legal discussion from protectionist to right-based structural reasoning of children's digital participation. Bringing theoretical concepts, international norms, and emerging scholarship to bear, the chapter lays out the starting point from which the empirical examinations of Indian laws, judicial decisions, and policymaking lacunae will follow. It creates the jurisprudential foundation for understanding children as more than victims or children-in-the-care and ones who have digital positioning that requires protection, participation, and dignity in online environments.

LEGAL AND POLICY ANALYSIS – INDIAN SCENARIO

India's major Law dealing with cybercrimes is the Information Technology Act 2000, and it addresses issues related to the protection of children on the use of the internet & other technologies under section 66E privacy violation, section 67 obscenity in electronic form, section 67B child pornography, and section 72A unauthorised personal data breach.[26] Furthermore, the provisions are aimed at discrete forms of criminal behaviour and not the whole context of children's engagement in online economies. The Act provides for no child digital identity, is silent on monetisation of child content and has no armour plating around guardianship, the consent regime or the promotion of age-appropriate platforms. As

[22] Children's Online Privacy Protection Act (COPPA) 1998 (US); GDPR (EU Regulation 2016/679)
[23] UK Information Commissioner's Office, *Age-Appropriate Design Code* (2020)
[24] NCPCR, *Guidelines for Prevention of Online Harassment* (2021) https://ncpcr.gov.in accessed 18 July 2025; ChildFund India (n 8)
[25] The Dialogue, 'Children's Rights in the Digital Economy: Indian Legal Perspectives' (2023) https://thedialogue.co accessed 18 July 2025
[26] Information Technology Act 2000, ss 66E, 67, 67B, 72A; see also *Fiadora Editorial*, 'The IT Act is 20 Years Old, But Child Protection Remains an Invisible Frame' (2024) *Indian Journal of Cyber Law* 41

commentators observe, although the impact and definitions of section 66A were set aside by Shreya Singhal v Union of India, and the net liability under section 79 illuminated,[27] no legislative reform has put the Act to work on algorithmic amplification or the economic valorisation of child digital personas.

More critiques of the IT Act centre on its weak conception of privacy at best, with powers of surveillance under sections 69 and 69A considered too wide, and its restrictions on encryption capabilities threatening vulnerabilities.[28] Such structural inadequacies create species-level risk for kids, for the AI Act provides no meaningful redress for irresponsible data scraping or algorithm-mediated exposure, both of which disproportionately impact children.[29] The 1986 Child and Adolescent Labour (Prohibition and Regulation) Act views child work in the same way the developed world has traditionally seen such work, with its focus on physical effort. It prohibits minors from working in the hazardous occupations listed, but it does not cover digital media creation, live streaming, or other monetised online activity.[30] They qualify as kidfluencers — children who appear in family-run channels or sponsored streams — and are thus not covered by the law's protections. There is no legal compulsion for trust accounts for a child's earnings, no regulation of working hours or income disclosure (as in the case of child actors in the Indian film industry), and children who are working in monetised digital spaces fall between the cracks of a lack of financial protection and of work regulation.[31]

Indeed, in the Digital Personal Data Protection Act 2023, section 9, the Act makes the categorisation of those under eighteen as children and demands the determination of a verifiable parental consent for the use of the data of such children.[32] The Act prohibits certain practices, such as behavioural profiling or targeted advertising towards children, as well as digital processing that could adversely affect their physical and mental well-being.[33] Provisional rules would require people to use government-linked digital tokens or virtual IDs to verify their identity, and platforms would need to verify the status of a guardian of any minor

[27] *Shreya Singhal v Union of India* AIR 2015 SC 1523; Information Technology Act 2000, s 79 as interpreted by the Supreme Court
[28] See *TheLaw Institute*, 'Critical Perspectives on the Information Technology Act' (2024); Reddit commentary on surveillance and ambiguity under ss 69 and 69A
[29] Ibid.; also *Reddit*, user commentary on IT Act's outdated provisions and encryption limits.
[30] Child and Adolescent Labour (Prohibition ad Regulation) Act 1986; *Mondaq*, 'Legal Landscape of Child Social Media Influencers in India' (2025)
[31] *ThePrint*, 'India's kidfluencers are raking in millions. No law to protect them' (17 Apr 2022) https://theprint.in accessed 18 July 2025
[32] Digital Personal Data Protection Act 2023, s 9 (1)
[33] Ibid, ss 9(2)–(3)

who gives consent.[34] The fines for non-compliance are not trifling — more than ₹200 crore of fines can be levied for breaches related to children's data.[35] But, despite these strides, the DPDP Act is deeply flawed. It does nothing to differentiate between a child's use of platforms and a child being inadvertently engaged with monetised content. Consent technologies are vaguely defined, posing the challenges of implementation in India's low digital literacy context.[36] There is no legal requirement for age-appropriate design or to keep earned child income separated or deposited for later, nor do platforms have a requirement to help moderate monetised children's content, even if it might be exploitative or psychologically damaging.[37] Standardised age limits disregard differences in adolescent capabilities and preclude the evolution of autonomy among older minors—undermining privacy rights at a crucial period in development.[38]

The Protection of Children from Sexual Offences Act 2012 (POCSO) and juvenile justice laws, as well as other legislation intended to protect children, also do not recognise digital-first threats like grooming, online extortion or the non-consensual creation or sharing of intimate imagery.[39] The many grey areas in POCSO when it comes to technology-facilitated child abuse have been identified by the government, but reform is still pending on this front.[40] While the Juvenile Justice Act and NCERT or state directives have endorsed protecting children's best interests, there are no binding powers or penalties related to platform governance, influencer monetisation, or parental responsibility in the digital sphere. This complex of laws creates a patchwork protection of children, which is generally very fragmentary and has only limited effectiveness: the IT Act only treats some criminal harms, the Labour Act is linked to physical labour exclusively, and the DPDP Act has only some nominal data protection. None together articulates children's position as digital rights-holders, or their role as economic agents. There are no legal obligations for platforms to incorporate mechanisms for age verification, trust accounts or, indeed, recognition of consent or autonomy relating to digital exposure or income.

[34] Draft Digital Data Protection Rules, MEITY (Jan 2025) https://prsindia.org accessed 18 July 2025
[35] *Taft Privacy & Data Security Insights*, 'Breaking Down India's Digital Personal Data Protection Act, 2023' (2023)
[36] *MediaNama*, 'DPDP Rules: Platforms need parental consent to use children's data' (4 Jan 2025) https://www.medianama.com accessed 18 July 2025
[37] *Economic Times Legal*, 'Is India's draft data protection rules enough to safeguard children's privacy?' (6 Jan 2025) https://legal.economictimes.indiatimes.com accessed 18 July 2025
[38] CCG NLU Delhi Blog, 'Navigating the Indian Data Protection Law…' (21 Nov 2023)
[39] *Legal Service India*, 'Digital Crime Against Children: The POCSO Act in Online Realm' (2025) https://www.legalserviceindia.com accessed 18 July 2025
[40] *Εσya Centre*, 'Technology-Facilitated Child Sexual Exploitation' (2 Jul 2025) https://www.esyacentre.org accessed 18 July 2025

The gap allows a Wild West of uninhibited monetisation of children's digital lives — intellectual and fiscal — that must be addressed through legislative action.

COMPARATIVE LAW AND INTERNATIONAL LAW PERSPECTIVES

The issues regarding digital footprint and exploitation of children are not just an Indian phenomenon. Government and regulators in different jurisdictions are struggling with how to square children's rights with the business models of digital platforms. Comparison of legal regimes has much to offer in terms of the limitations of Indian law and how they may be reformed. France was the first to pass a law specifically allowing minors to create online content through Law No. 2020-1266 with effect from October 2020. This legislation would protect those under 16 whose image is monetised online. It mandates parents or guardians to obtain official approval from local governments for any ongoing internet business arising from a child's regular web use. A part of the child's income has to be held in a blocked savings account until the child has reached the age of majority, and digital platforms need to find a way to ensure this is happening.[41] The law replicates terms already established for child actors by the French Labour Code and targets the increasing risks of parental overexploitation, economic extortion, and negative reputation.[42] It also grants the child the right to request the removal of content, which reemphasises the importance of future agency and control over one's digital identity.[43]

The United States has lurking on its books the COPPA, the Children's Online Privacy Protection Act, in force since 2000. COPPA applies to online services that knowingly collect information from children under 13 and mandates obtaining verifiable parental consent before any personal information is collected.[44] It requires the least collection of data, that policies be transparent, and that parents have rights to review and delete the data collected.[45] COPPA has been the basis for some major enforcement actions, such as a $5.7 million fine levied against TikTok (then known as Musically in 2019 and a $275 million fine against Epic Games in 2022

[41] French Law No. 2020-1266, Journal Officiel de la République Française (19 October 2020)
[42] Claire Lefevre, 'French Law Protects "Kidfluencers" from Exploitation' (2021) 12 European Digital Rights Review 23
[43] Library of Congress, 'France: Parliament Adopts Law to Protect Child "Influencers"' (30 October 2020) https://www.loc.gov/item/global-legal-monitor/2020-10-30/france-parliament-adopts-law-to-protect-child-influencers-on-social-media/ accessed 18 July 2025
[44] COPPA (1998), 15 U.S.C. §§ 6501–6506
[45] Federal Trade Commission, *Complying with COPPA* (2013) https://www.ftc.gov accessed 18 July 2025

for illegally collecting children's data.[46] Though COPPA has been derided for cutting off at an older age and for its lacklustre enforcement in nascent tech sectors, new updates proposed by the Federal Trade Commission have been designed to bolster its protections by extending additional controls over push notifications, in-app nudging, and ed-tech data use.[47]

The European Union (EU)'s General Data Protection Regulation (GDPR) is one of the most wide-ranging privacy regulations in the world, with powerful safeguards for children. Through Article 8, the GDPR establishes consent to be between the ages of 13 to 16 in MS to collect information from minors.[48] GDPR requires data minimisation, purpose limitation and profiling guardrails that mean it's impossible to use data on children for behavioural advertising without a lawful basis.[49] The flexibility of enforcement mechanisms can be exposed to abuses as well. There is an already-notorious example of this, being a fine of €345 million on TikTok handed out by Ireland's Data Protection Commission, precipitated by the apparent inadequacies of data processing and age-verification system.[50] What sets GDPR apart is that it applies to any global company, even if they don't have a subsidiary in the EU but process EU users' data, so it becomes a de facto standard, while other territories vary.

The UK's Age-Appropriate Design Code (or Yes, the Children's Code) became law under the DPA 2018 in September 2021. It establishes 15 design standards for online services "likely to be accessed by children," such as social media, apps, games and websites. These rules force all platforms to implement privacy-by-default settings, ban the use of nudge techniques designed to make kids divulge more data and discourage tracking or profiling for reasons other than strictly necessary.[51] Companies are also obligated to conduct Data Protection Impact Assessments (DPIAs) to evaluate risks to children and to provide age-appropriate terms and settings.[52] However, the Code does not have enforcement provisions in itself, but the UK's data regulator, the Information Commissioner's Office (ICO), has indicated that it will use its current powers in UK data law to levy fines for violations. Giant global platforms, like Google, TikTok and Instagram, adjusted their systems around the world to follow the Code, establishing a

[46] FTC Press Release, 'Epic Games to Pay $520 Million over Allegations of Privacy Violations and Unfair Practices' (2022)
[47] AP News, 'FTC Proposes COPPA 2.0 Rules to Tackle Push Notifications, Ed-Tech Surveillance' (20 December 2023)
[48] GDPR (EU Regulation 2016/679), art 8
[49] GDPR, arts 5, 6, 22
[50] Irish Data Protection Commission, Decision on TikTok Technology Ltd (15 September 2023)
[51] UK Information Commissioner's Office, *Age-Appropriate Design Code* (2020) https://ico.org.uk accessed 18 July 2025
[52] Ibid

muscular precedent of jurisdictional power. [53] These comparative perspectives suggest a range of best practices that India can emulate. France shows that legislation can deal with economic and reputational exploitation by mandating income protection, enforceable delete rights and public scrutiny. The US and EU Indicate the Importance of Consent Mechanism, Data Minimisation and Tough Regulation Through Fines. The UK illustrates how platform design itself might be regulated in the interests of the child. A hybrid model, which mandates statutory controls, platform duties, and independent oversight, seems to be emerging in all jurisdictions as the norm. India is yet to formulate a comprehensive child digital protection policy. Unlike France, there's no law referring to children as digital performers generating profit; unlike the U.S., there's no enforcement body to ensure it can be proved that a child consented; and unlike the EU and UK, there's no structure for age-appropriate platform governance or algorithmic accountability. These lacunae are not simply exploitable but also leave Indian still behind global child digital rights norms. Accordingly, the comparative study highlights the imperative nature of India establishing a legal architecture that recognises children as vulnerable and yet participatory subjects of digital economies. Regulatory design will need to centre children's autonomy, safety and growing capacities — not just in principle, but in enforceable legal mechanisms.

CASE STUDIES OF USE AND MONETISATION PLATFORM DYNAMICS

The nexus of childhood, social media and commerce has spawned an under-regulated but profitable system in India, where children serve as both content creators and brand assets, as well as virtual micro-celebrities. Yet even as the influencer economy is exploding in financial size and social status, child influencer online labour is still being operationalised without formalised protections. Real-life cases point to a systemic normalisation of the commercialisation of minors, the mining of their data and the crossing of their emotional boundaries — all in the name of likes, sponsorships, and algorithmic love. This space is also popularly led by Apoorva Mukhija, also known as The Rebel Kid. She started as an engineering student, became known for comic sketches, and now works with top brands like Meta, Amazon and Maybelline. Her reels typically rack up millions of views. She stirred media controversy in 2024 with claims for inflated income earned — ₹ 2.5 lakh per day — and net worth ₹ 41 crore.[54] She pushed back on the numbers, but the conversation pointed to how society is

[53] Wired UK, 'How the UK Forced Big Tech to Rethink Its Design for Children' (2021)
[54] IndiaTimes, 'Apoorva Mukhija aka Rebel Kid's net worth: Does she really earn Rs 2.5 lakh daily?' (6 July 2025) https://www.indiatimes.com accessed 19 July 2025

becoming more attuned (and envious) of influencer earnings, especially among the younger set. After being trolled over her appearance on India's Got Talent, Mukhija was sent threats of rape and harassment against her and her mother.[55] These highlights not only the commodification of young public figures, but also the inescapable vulnerability of female influencers in particular when they are fed into monetised public arenas as children. Jannat Zubair Rahmani, a former child actor who's now an influencer, also faced deep online hate and invasive public censure, especially after she shared horror-themed content during the 2020 lockdown.[56] Despite her age, material was heavily monetised and disseminated to the four corners of the internet – and frequently without much concern for filters and emotional or digital well-being. In this instance, influencer children become permanent digital artefacts—caged within content algorithms that continue to generate value from their portraits, regardless of age, agency, or future consent.

Other prominent examples are of Anantya Anand (MyMissAnand), who started making videos at four and became a national champion at eight.[57] From challenges and lifestyle hacks to do-it-yourself tutorials, her channel now racks up millions of views and boasts sponsorships from companies like Disney and Nestlé. [58] Meanwhile, Amreen Malhotra, who has been creating content since the age of five, works with Pampers, Volvo and Amazon, and mainly features in "cute" family-oriented reels, aimed at the primary household decision-makers.[59] Her airbrushed aesthetic is more than just lifestyle branding — it is a type of work dressed up as childhood. The most structurally branded sibling influencers are probably Aayu and Pihu, two siblings who have a Kota-based YouTube channel replete with challenge videos and lifestyle vlogging.[60] Their viewership and brand reach are on par with adult creators, but the law has been slow to clarify consent protocols, contractual obligations and how the money gets made. As with so many children who are part of the digital economy, these new influencers find themselves in a legal grey zone. Specific examples are reflected at a statistical level. As of March 2025, 83,000 plus Instagram accounts were owned by minors aged less than 16 in

[55] Forbes India, 'The Great Indian Influencer Burnout' (2024) https://www.forbesindia.com accessed 19 July 2025
[56] Hindustan Times, 'How Jannat Zubair became a target of lockdown hate' (2021) https://www.hindustantimes.com accessed 19 July 2025
[57] ThePrint, 'India's kidfluencers are raking in millions. No law to protect them' (17 April 2022) https://theprint.in accessed 19 July 2025
[58] ETBrandEquity, 'Kidfluencers: Balancing compliance and reach' (21 May 2025) https://brandequity.economictimes.indiatimes.com accessed 19 July 2025
[59] Exchange4Media, 'Meet the mini influencers shaping India's digital childhood' (Feb 2025) https://www.exchange4media.com accessed 19 July 2025
[60] YouTube, 'Aayu and Pihu Show' https://www.youtube.com/@aayuandpihushow accessed 19 July 2025.

India.[61] Girls represented approximately 69% of this group, and micro-influencers (defined as having 10,000–100,000 followers) were the most represented. Those accounts had average engagement rates of 3.17%, suggesting they were good brand ambassadors but also algorithmically ideal engagement nodes.[62] Many kidfluencers make Rs 1–2 lakh per sponsored post if industry estimates are anything to go by, and there is no legal regulation on contracts, disclosure or the right to income.[63] In addition to earnings, the children face serious psychological, safety and ethical challenges. A 2025 survey by Karnataka State Commission for Protection of Child Rights (KSCPCR) and ChildFund India demonstrated shocking statistics: in a study of 900 children aged 8-18, 18 had been sexually coerced online, 31 had gone to meet strangers they had come into contact with through online, while 80% of parents said that police had not been responsive enough.[64] Similar reports have popped up in other states. In Delhi, a 13-year-old YouTuber, who was known for being a content creator focused on education, went missing and was later discovered participating in participation at an unofficial meet-up for influencers.[65] In Nagpur, the city's cyber cell filed 759 cases for harassment in 2024—some of which were filed on behalf of minors.[66]

Psychologically, constantly being subject to manufactured attention and validation leads to unhealthy developmental effects. Kids internalise metrics such as view counts, shares and follower growth as stand-ins for social value. Experts like Riddhi Doshi Patel and Chandni Tugnait warn of the mental health fallout —identity diffusion, performance anxiety and disconnection from real-world interactions.[67] Even children as young as seven report feeling "not good enough" when a video underperforms.[68] The likes of YouTube, Instagram, and Facebook seek to enforce age restrictions (usually 13+); however, parental subversion is rife. Parents typically control the accounts and monetisation but can flout platform safeguards as they broker brand partnerships.[69] YouTube's "Made for Kids" setting eliminates personalised advertising and comment features, but instead influencers upload content in broader categories,

[61] Qoruz Influencer Reports (2025) https://www.qoruz.com accessed 19 July 2025
[62] Ibid
[63] Livemint, 'The lives of India's baby influencers' (2024) https://www.livemint.com accessed 19 July 2025.
[64] Times of India, 'Karnataka parents raise alarm over rampant online child exposure & abuse' (14 June 2025) https://timesofindia.indiatimes.com accessed 19 July 2025
[65] TOI City Bureau, 'Missing 13-Year-Old YouTuber found at East Delhi influencer meet' (3 May 2025) https://timesofindia.indiatimes.com accessed 19 July 2025
[66] TOI Nagpur, 'Cyber cell shields women and children; 759 complaints in 2024' (28 December 2024).
[67] India Today, 'Paedophilia, stalking, abuse: What kidfluencers pay to make money online' (17 September 2024) https://www.indiatoday.in accessed 19 July 2025
[68] Ibid
[69] Instagram and YouTube Terms of Use https://www.instagram.com/legal/terms and https://www.youtube.com/t/terms accessed 19 July 2025

exposing children to data misuse.[70] Legally, contracts signed for children by their parents cannot able to be enforced. According to the precedent of *Mohori Bibee v Dharmodas Ghose*, minors cannot contract, and contracts by parents are not always enforceable in court if not endorsed through legal guardianship procedures.[71] So any money made or rights sold to brands or platforms may not be legally owed to the children who are performing. They also may have no recourse if their image is misused or if their money is withheld. Taken together, these examples paint a sobering picture: children are seen but not legally visible in India's influencer economy. They produce enormous economic and algorithmic value, but the state provides them with no clear rights, support or legal routes to claim agency over their data, image or pay. It is far beyond the time when strong, child-focused regulation is needed. In the next chapter, these regulatory lacunae will be discussed, and possible routes to reforms.

CHALLENGES AND LEGAL VULNERABILITIES

Yet, as there is an increasing presence of child influencers and an emerging evidence base of how they are contributing to digital economies at an unprecedented pace, India's legal framework is significantly wanting in protecting the rights and well-being of these children. Four major lacunae characterise the regulatory design, contributing to the systemic invisibility of children in juristic protections and facilitating exploitative dynamics. Absence of Any Legal Status to Work of Digital Child Labour - The existing child labour law, the Child and Adolescent Labour (Prohibition and Regulation) Act 1986, covers the protection of minors in the context of physical and industrial labour, but does not incorporate digital content creation, streaming, or sponsored influencer work. This exception means monetised content involving children is left completely unregulated."[72] In contrast to formally regulated entertainment industries, in which child actors exist as a group under legislative guardianship and with earnings protection, the existence of child influencers in digital media means that this group of children are working without legal protection of their developmental rights, working out of school hours with brand responsibility, serve the two-thirds of the world's child population who are not protected by any legislative framework. Legal No Law for Consent and Financial Rights - No contracts are binding on Indian minors. The decision in *MohoriBibee v Dharmodas Ghose* says all contracts by a Guardian on behalf of a minor are void, except when that person

[70] Ibid
[71] *Mohori Bibee v Dharmodas Ghose* (1903) 30 IA 114 (PC)
[72] Child and Adolescent Labour (Prohibition and Regulation) Act 1986; the statute lacks provisions for digital content creation or online monetised participation.

comes of age.[73] There is no room in this legal principle for the contemporary models of kids making money through digital avenues. As a result, when children appear in influencer campaigns, branded collaborations or sponsorships, there are few, if any, legally binding protections around their work or the money generated from it and no form of protection for a child aged between 0 – 12 years to refuse, remove or demand payment. This void contradicts the principles of autonomy and capacity in development as enshrined in the UNCRC that India needs to comply with.[74] No Platform Responsibility to Detect or Censor Monetised Child Accounts - The Information Technology Act 2000 or the Digital Personal Data Protection Act 2023 does not prescribe that digital platforms be legally obliged to digitally track and report for detection, users that share monetised child content.[75] Platforms have no mandatory obligation to label monetised child material, cease the algorithmic promotion of said content, or secure verifiable consent.[76] As evidenced by the explosion in kidfluencers' content and engagement numbers, monetised child content is spreading like wildfire. In the absence of transparency or mandated oversight – like age verifications, flagged content disclaimers, or platform accountability – kids are exposed to viral overexposure, forced engagement or algorithmic reductions.

Absence of Children's Friendly Digital Complaints Mechanism - There is no easily accessible system of grievance redressal in India suited to address the issues of children in digital environments. Although children and their families have access to general consumer protection and cybercrime pathways, they face substantial procedural, cognitive and psychological challenges when trying to seek a remedy.[77] There are no online reporting portals that are child-friendly and where the process is accelerated for them to remove content for the misuse of data and financial fraud. Parental control is not always possible; some parents encourage children's digital labour entrapping, ng the same stakeholder, supposedly to protect the child. In combination, these four deficiencies in law, of these gaps – non-recognition of digital child labour, void entitlement to earnings or content rights, absence of platform accountability, and inexistence of child-focused redress – are indicative of a structural failure of India's legal system to accommodate children's actual digital participation.-recognition of digital child

[73] *Mohori Bibee v Dharmodas Ghose* (1903) 30 IA 114 (PC)
[74] 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
[75] Information Technology Act 2000; Digital Personal Data Protection Act 2023 — neither act offers child-specific categorisation or algorithmic oversight mandates
[76] Draft DPDP Rules (2025); no platform-enforced verification or transparency duty currently mandated
[77] *Juvenile Justice (Care and Protection of Children) Act 2015* and general cyber grievance mechanisms—none tailored to minor users

labour, void entitlement to earnings or content rights, absence of platform accountability, and inexistence of child-focused redress, [we are seeing] the structural failure of India's legal system to accommodate children's actual digital participation. This fractured landscape, besides facilitating the abuse, erodes children's privacy, emotional well-being, and rights to financial independence. It is in direct contravention to India's commitments under international conventions such as the UNCRC and UN General Comment No 25 on digital environments.[78]

SUGGESTIONS

As this research reveals, Indian children's involvement with the nation's digital economy is extensive, hyper-monetised and significantly unregulated. "The existing legal landscape does not do much to protect child influencers." The gaps are in consent (and their ability to decide what content is shared), income security, platform liability and redressal of grievances. To close this divide, India needs an integrated reform vision, in which children should be regarded as digital rights holders, economic actors and protected participants in platform-based ecosystems. First, India's flagship cyber statute, the Information Technology Act 2000, needs to be revamped. Reform must, within the Act, acknowledge a separate digital child rights framework that defines and protects monetised child participation. Definitions need to incorporate "child digital labour" and "monetised child content", identifying algorithmic exposure and parental orchestration as economic and developmental exploitation. What the Act ought to do is require standardised consent procedures, a ban on exploitative material about children, and architecture-neutral digital child identities.

But merely overhauling the IT Act will not be enough. Parliament will have to bring a new standalone law — tentatively named the Children's Online Safety and Earnings Protection Act. Such proposed legislation should secure the commercial interests of children rather than fundamentally change the on-line marketing marketplace for kids, by formalising children's online economic engagement with the introduction of steps to verify parental consent, to place limits on that engagement, such as time-of-use, privacy rights and psychological distress, and to require that a certain stable proportion of the gross income of the child go into a protected escrow or trust that is not accessible until adulthood. The law should formally delegate oversight to the national agencies like the NCPCR (National Commission for Protection of Child Rights) or a new Digital Child Protection Unit (DCPU) under the Ministry of Electronics

[78] Ibid. UNCRC (1989), arts 5, 12, 19, 32; General Comment No 25 (n 3)

and Information Technology to supervise compliance and mediate in the disputes that arise. At the same time, the same kind of binding governance standards need to apply to digital platforms such as YouTube, Instagram, TikTok alternatives and gaming services that are very much in the field of play (The Guardian 2022). Platforms need to be mandated by law to release biannual transparency reports detailing the number of child accounts monetised, reach, engagement, content types and safety measures implemented. Platforms will need to use account systems with verified ages based on government IDs or secure digital identity systems – not merely self-attestation of age. I do think all of those child accounts should require registered guardian supervision, including some sort of punishment for misrepresentation or indifference. This approach recognises the outsized role that platforms play in algorithmically mediated childhood visibility and requires a move from self-regulation to enforceable responsibility. Because it's a new economic model, institution-building is necessary." Digital Child Protection Units (DCPUs) should be built within MeitY, with the support of NCPCR and NCW, for conducting child audits, issuing advisories and investigating violations. “Nationally, we need to teach our children, parents and teachers at schools across the country – a cyber education for empowerment – digital literacy and rights, consent, privacy, mental health and digital resilience.

Reforms need to ensure that kids control — not merely are seen on — the digital landscape economically and ethically. A statutory trust fund regime would maintain that a specific percentage of all child earnings be automatically deposited into a secured escrow account managed by independent trustees who could only release earnings upon attaining majority or with the approval of the court/guardian. These rules echo legal precedents like the Coogan laws in the US and France’s Kidfluencer law. Built into this should be a digital child consent protocol that should have mandatory elements of age-appropriate assent, parental consent and digital recording (for example, e-signatures, Aadhaar OTP) to ensure the authenticity and informed cooperation.

To accommodate the increasing preponderance of influencer families in our media landscape, India ought to construct a national Code of Conduct for Family Vloggers, which draws on child-rights experts, psychologists, ethicists and influencer associations, among others. That code would provide norms on sensitivity toward a child’s exposure, processes for public content removal on children’s request, content boundaries appropriate to their age, and first privacy storytelling. It would also provide advice on how to avoid manipulative or exploitative

"sharenting" behaviours and require platforms to offer easy-to-use reporting mechanisms for children and parents. These measures make up a comprehensive regulatory environment. Legislated requirements that are based on children's digital rights, platform responsibilities through transparency and design, institutional checks and balances on oversight and education and economic factors and ethical guardrails combine a solution from a variety of dimensions. This framework can additionally help India meet international standards set by the UNCRC, General Comment No 25 (2021), GDPR and the UK's Age-Appropriate Design Code, and at the same time take into consideration India's social-legal context. Without these reforms, children will continue to be legally unprotected, and increasingly exposed , in one of the most glaring social innovations of the digital age: monetised childhoods. They are an important start, creating a possible way forward to restoring agency, creating safety and recasting childhood policy in the age of digital economies.

CONCLUSION

This article has critically analysed the point of interface of children's rights, online safety and digital monetisation in India. As has been seen over the previous chapters, India's legal framework -both within and beyond the Information Technology Act 2000, the Child Labour Act 1986, and the Digital Personal Data Protection Act 2023 - falls extremely short of capturing the lived experiences of digitally informed childhoods present on booted platforms. It placed young people as digital participants within a juridical and theoretical framework, highlighting children as rights-holders and understanding vulnerability, agency and developing capacity against international standards such as the UNCRC and General Comment No. 25 (2021). We found that the law does not count digital labour undertaken by children, requires no consent or escrow processes, and is low-touch on platforms. The study also brought home to the panel's attention progressive models internationally—Kidfluencer law of France, COPPA, GDPR and UK Design Code that India is yet to incorporate. Major platforms that garner millions of views, children like The Rebel Kid, MyMissAnand, and Jannat Zubair, Aayu & Pihu continue to systematically monetise and generate exposure without infrastructural defences in place, with harassment, psychological risk and legal murk proceeding yet unchecked. "The Legal Gaps that Reinforce Children's Invisibility identified four legal gaps that perpetuate children's invisibility: the absence of digital child labour laws; the lack of any enforceable right to consent and earn; no platform obligation to monitor monetising child content; and the inability to access child-focused grievance mechanisms. This involves changes to the IT Act to include

protections for child digital rights; the introduction of a Children's Online Safety and Earnings Protection Act; compulsory platform transparency, age verification, and accountability to guardians; structural supports such as Digital Child Protection Units and cyber education programmes; economic and ethical measures such as mandatory escrow accounts, digital assent protocols, and a national code of conduct for family vlogging. Collectively, these interrelated reforms represent a legislative, institutional, and normative ecosystem that would foreground the dignity, agency, and security of children who use digital venues. The system harmonises with international best practices and India's commitments under international human rights law, thus respecting the developmental requirements and evolving maturity levels of juveniles. Without reform, monetised childhood will continue as a territory of extraction – a space in which children's identities are blithely commodified, their earnings not guaranteed, their experiences unconstrained. India, it can be argued, stands at a crossroads, for the choices it makes now may have an impact on whether children's participation in the digital world serves as an engine for empowerment or exploitation. As a result, all of us request strong and immediate legislative action, ongoing oversight, and public engagement that centres children at the core of digital reform. By informed policy, ethical design, and enforceable legal rights, India can turn its influencer economy into a child-centric digital terrain — where childhood, autonomy and safety advance in tandem, not in tension.