International Journal of Economic Practices and Theories (IJEPT)
ISSN: 2247-7225
Volume 2026, Issue 1

Protecting Children from Online Harm in India: A Consumer Protection and Cyber Law View

[1]Shreya, [2]Dr. Shreya Chatterjee

1Ph.D. Research Scholar KIIT School of Law, KIIT Deemed to be University Bhubaneswar, Odisha, India

[2]Associate Professor and Associate Dean (Doctoral Program) KIIT School of Law, KIIT Deemed to be University Bhubaneswar, Odisha, India

Abstract:

Digital platforms, edtech services, mobile applications, and child-facing online environments have reshaped how children in India consume, learn, play, and interact. Yet this shift has opened new vulnerabilities. Data harvesting, behavioural targeting, deceptive interface design, and platform-driven exploitation now define large parts of the digital experience for minors. Children, constrained by age and limited decisional autonomy, are especially prone to manipulative digital practices that erode informed consent and generate commercial and cyber harms. Against this backdrop, the paper asks whether India's legal framework adequately protects children as vulnerable online consumers, focusing on the convergence of consumer protection law, data protection law, and cyber law. It analyses the Digital Personal Data Protection Act, 2023, the Digital Personal Data Protection Rules, 2025, the Consumer Protection Act, 2019, the Consumer Protection (E-Commerce) Rules, 2020, and the CCPA's dark pattern framework of 2023. Practices such as profiling, targeted advertising, behavioural monitoring, subscription traps, deceptive consent mechanisms, and hidden monetisation are evaluated against these instruments. Documented incidents of edtech data exposure, platform insecurity, and cyber fraud affecting children are examined to reveal enforcement limitations. India's framework, the paper argues, is fragmented and reactive. It leans too heavily on parental consent, post facto complaints, and general consumer remedies instead of imposing strong ex ante duties on platforms. A child-centric regulatory model built around data minimisation, age-appropriate design, mandatory transparency, platform accountability, and targeted enforcement is proposed. Treating children not simply as data subjects but as vulnerable digital consumers, the paper enters the growing discourse on digital rights, consumer autonomy, and child protection within India's evolving regulatory architecture.

Keywords: children, data protection, dark patterns, consumer vulnerability, digital platforms, India, DPDP Act, age-appropriate design

1. Introduction

By recent estimates, more than 200 million Indians below the age of eighteen now use the internet. A great many of them, on any given day, open an edtech app, scroll through social media, stream video, or play games online. These platforms earn revenue by keeping users engaged, extracting behavioural data, and selling targeted advertising. Children, for obvious developmental reasons, cannot bargain over these terms the way an adult might (Rozendaal and Buijzen, 2023). Consumer law has a phrase for their position. They are structurally vulnerable.

India's legislative response has arrived in pieces, each one aimed at a different part of the problem. Section 9 of the Digital Personal Data Protection Act, 2023 (DPDP Act) requires verifiable parental consent before a child's data may be processed. The Consumer Protection Act, 2019 (CPA) and the Consumer Protection (E-Commerce) Rules, 2020 target unfair trade practices in electronic commerce. Dark patterns got their own regulatory label when the Central Consumer Protection Authority (CCPA) published guidelines in 2023. Content regulation and intermediary liability live inside the Information Technology Act, 2000 (IT Act) and the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Each instrument covers a fragment. Together, they do not form a unified child-specific protective framework.

The seams between these instruments create regulatory gaps. Nothing stops a platform from obtaining parental consent for data processing on one hand and, with the other, deploying manipulative design features that steer children into uninformed purchases. An intermediary can meet every IT Act requirement while hosting advertising that profiles minors without meaningful constraint. The CCPA may fine a single dark pattern offender, yet it has no power to mandate design-level duties across an entire sector.

Scholarship on this convergence remains sparse. Work on children and digital rights has clustered heavily around the EU's GDPR (Macenaite and Kosta, 2017; Lievens and Verdoodt, 2018) and the UK's Age Appropriate Design Code (Grace, Abel, and Salen, 2023). On the DPDP Act, Indian academic writing has so far stayed at the level of parental consent and data fiduciary duties in general terms. The specific intersection of consumer protection, data protection, and cyber law as it applies to children in India is, for practical purposes, uncharted.

The paper poses four research questions. To what extent does Indian law protect children from data harvesting and behavioural targeting on digital platforms? Are verifiable parental consent and dark pattern rules enough to protect children as vulnerable consumers? Should India adopt a stricter child-specific digital design regime? And how should liability be split among platforms, intermediaries, advertisers, and application developers?

Section 2 lays out the conceptual framework. Section 3 describes the research design. Sections 4 through 7 move through platform practices, Indian law, incidents, and comparative benchmarks, in that order. Section 8 maps gaps. Section 9 proposes reforms. Section 10 wraps up.

2. Conceptual Framework

2.1 The Child as Consumer, Data Principal, and Vulnerable User

A child in the digital economy occupies not one role but three, and the three overlap. As a consumer, the child acquires goods and services through platforms, sometimes via in-app purchases, sometimes through data-for-service exchanges nobody explains. As a data principal under the DPDP Act, 2023, the child is the human being whose personal data a fiduciary processes. As a vulnerable user, the child has not yet developed the ability to recognise persuasive intent, weigh commercial communications, or give consent that means anything (van der Hof, 2017).

These are separate legal categories. In a child's daily digital life, they collapse into one experience. Take a child who downloads a free gaming app. That download, all at once, creates a consumer relationship with the developer, feeds personal data into an advertising pipeline, and places the child inside an interface engineered to exploit developmental weaknesses. Regulate only one of these dimensions, and the other two remain exposed.

Consumer vulnerability has been defined as a state of powerlessness produced by the collision of individual traits and market conditions (Baker et al., 2005). That definition has anchored two decades of consumer research (Basu, 2023; Verma et al., 2026). The concept has been extended to digital settings through the idea of "unobserved vulnerability," where a consumer does not even realise the vulnerability exists (Lee et al., 2026). Children are a textbook case. They do not know that their behavioural data is being harvested. They do not know their interface has been personalised to keep them playing longer. They believe the game is free.

2.2 Information Asymmetry and Market Failure

The information gap between a child and a platform is not merely wide. It is structural. Platforms hold granular behavioural profiles spanning browsing patterns, session durations, purchase histories, device fingerprints, and inferred preferences. The child on the other end of the screen holds, at most, a dim awareness that the platform exists. No disclosure regime can close this gap, because the asymmetry is not a glitch in the market. It is the market's engine (Susser, Roessler, and Nissenbaum, 2019).

The concept of "online manipulation" describes the mechanism precisely (Susser et al., 2019). Information technology reshapes the decision-making context so that individual vulnerabilities become leverage. Persuasion offers reasons.

Coercion imposes costs. Manipulation does neither. It rewires the choice architecture. Dark patterns are the specific interface techniques through which that rewiring happens (Luguri and Strahilevitz, 2021; Gray et al., 2018).

For children, every layer of this problem intensifies. Below eight, a child cannot reliably distinguish advertising from editorial content (Rozendaal, Buijzen, and Valkenburg, 2010). Below twelve, conceptual advertising literacy is limited, and children do not understand that a commercial message has a persuasive purpose (Rozendaal and Buijzen, 2023). Below sixteen, the attitudinal advertising literacy needed to activate critical evaluation of embedded commercial content rarely exists (Hoek et al., 2021). Targeted advertising aimed at these age groups reaches subjects who are, developmentally, unable to mount the cognitive defences that advertising regulation assumes every consumer possesses (van Reijmersdal et al., 2017).

2.3 Dark Patterns and Manipulative Design

Dark patterns are interface designs that deliberately exploit cognitive biases, nudging users into actions they would otherwise avoid (Mathur et al., 2019). Basket sneaking slips items into a cart without consent. Forced action demands data disclosure as the price of entry. Confirm-shaming loads opt-out buttons with guilt. Hidden subscription buries recurring charges behind trial offers.

Are these practices common in applications children use? Very. A large majority of children's apps have been found to contain manipulative design features (O'Donnell et al., 2026). Children between seven and thirteen struggled to identify manipulative interface elements and were markedly more susceptible to them than adults (Schafer et al., 2024). Child-directed websites, meanwhile, are saturated with tracking and advertising technologies, much of it feeding data to third-party ad-tech networks without adequate disclosure (Moti et al., 2024).

The commercial logic is blunt. Dark patterns raise conversion rates, stretch engagement windows, and speed up data extraction. On child-facing platforms, they push in-app purchase revenue higher because users who do not understand financial consequences are easier to convert. The OECD, which now calls these techniques "dark commercial patterns," has argued that disclosure-based remedies are not enough (OECD, 2022).

3. Research Design

The paper uses two methods. The first is doctrinal, involving a close examination of Indian statutes, subordinate legislation, and regulatory guidelines bearing on children's digital protection. The instruments analysed include the DPDP Act, 2023, the DPDP Rules, 2025, the CPA, 2019, and the E-Commerce Rules, 2020. The analysis further covers the CCPA dark pattern guidelines of 2023, the IT Act, 2000, and the IT (Intermediary Guidelines) Rules, 2021. POCSO (2012), the Juvenile Justice Act (2015), the Indian Majority Act (1875), and the Indian Contract Act (1872) supply additional statutory material. The constitutional anchor is Justice K.S. Puttaswamy v. Union of India (2017), which recognised the right to privacy under Article 21.

The second method is qualitative incident-based case analysis, drawing on documented data exposures, enforcement orders, and cyber fraud cases involving children in India. Sources range from regulatory orders to investigative journalism and organisational reports. Four international frameworks serve as comparative benchmarks, namely the EU GDPR (Article 8, Recital 38), the UK Age Appropriate Design Code (2020), the California Age-Appropriate Design Code Act (2022), and the EU Digital Services Act (2022). The comparison is not a transplant exercise. Its purpose is to identify regulatory design choices India has not yet made.

4. Platform Practices That Create Harm

4.1 Tracking and Profiling

Cookies, device identifiers, SDK integrations, cross-site tracking. The instrumentation is varied, but the outcome is uniform. Platforms can monitor children's browsing history, search queries, content preferences, location, and social connections in fine-grained detail. Those data points are assembled into profiles that drive targeted advertising, content personalisation, and algorithmic recommendation. A 2024 IEEE study of children's websites confirmed that tracking

and advertising technologies appeared across a wide share of sites directed at minors, with data flowing out to networks of third-party firms (Moti et al., 2024).

This process has been called the "datafication of childhood." A child's daily activities are translated into quantifiable data points that feed commercial algorithms. What results is not just a data subject in the legal sense but a commercially constructed profile. That profile may follow the child into adulthood, affecting insurance pricing, university admissions, and job prospects. The COVID-19 shift to remote learning accelerated the whole process, because suddenly platform use was compulsory for education (Jarke and Breiter, 2019; Day et al., 2022).

4.2 Behavioural Advertising

Contextual advertising matches an ad to the content on a webpage. Behavioural advertising matches it to the user, specifically to inferred interests and predicted conduct. Profiling is the engine. Section 9(3) of the DPDP Act, 2023 nominally prohibits profiling children. But the boundary between personalisation for service delivery and personalisation for advertising is blurry, and verification tools are rudimentary. Enforcement has stalled.

Why does this matter? Because children lack the persuasion knowledge to recognise what is happening. This gap has been documented in detail (Rozendaal et al., 2011). Profile-targeted ads generate stronger brand attitudes and higher purchase intentions among children than untargeted ones, for the precise reason that the targeting goes undetected (van Reijmersdal et al., 2017). Advertising literacy programmes, run on their own, are not an adequate answer. Children who cannot identify the persuasive technique cannot defend against it. Design-level prohibitions have to accompany any educational intervention (Nelson, 2016; Verdoodt, 2019).

4.3 Addictive Design and Monetisation

Loot boxes, streak rewards, notification pings. All of these rest on variable-ratio reinforcement, a mechanism borrowed from behavioural psychology. Loot boxes exchange real money for randomised in-game rewards. They operate, in substance, as gambling-like mechanics, and children are especially exposed (Ash, Gordon, and Mills, 2023; Xiao and Lund, 2025). The gaming industry introduced self-regulatory labelling requirements. They have not worked. A longitudinal study tracking compliance on the Apple App Store found widespread non-compliance (Xiao & Lund, 2025).

Subscription traps add a second layer of harm. A free trial collects payment details and silently converts into a paid subscription, exploiting inattention and default bias. When the user is a child, one question becomes inescapable. Was valid consent to a recurring financial commitment ever obtained? Under the Indian Contract Act, 1872, agreements with minors are void. Yet platforms routinely process purchases by minors with no effective age check and no payment authorisation gating.

4.4 Data Sharing with Ad-Tech and Third Parties

Child-facing platforms do not keep user data to themselves. Through SDK integrations, cookie-syncing, and contractual data-sharing arrangements, they channel it to ad-tech firms, analytics providers, and data brokers. The child has no idea where the data goes. Consent obtained from the child, or from the parent, seldom extends to the downstream chain.

The EU's Unfair Commercial Practices Directive treats the omission of material information as a misleading practice whenever it leads an average consumer to a transactional decision that would not otherwise have been made. If India were to adopt a comparable standard for child-facing platforms, the result would be an obligation to disclose the entire data-sharing chain, in language accessible to both children and parents. No Indian law currently requires that.

5. Indian Legal Framework

5.1 The Digital Personal Data Protection Act, 2023

Section 9 is where the DPDP Act addresses children. Section 9(1) requires verifiable consent from a parent or lawful guardian before a child's data may be processed. Under Section 2(f), a "child" is anyone below eighteen. That bar is set higher than in the EU, where Article 8 of the GDPR lets member states fix the consent age anywhere from thirteen to sixteen, and higher than the thirteen-year threshold in the United States under COPPA.

On paper, Section 9(3) is a strong provision. It prohibits tracking, behavioural monitoring, and targeted advertising aimed at children. Among comparative data protection regimes, few go as far. But the prohibition runs on subordinate rules and on the enforcement capacity of the Data Protection Board of India (DPBI), both of which remain underdeveloped. An additional ambiguity dogs the section. It draws no line between cross-session commercial profiling and same-session contextual personalisation within educational platforms. Edtech providers deploying adaptive learning algorithms have been left to guess.

Exemption power sits with the Central Government under Sections 9(4) and 9(5). Categories of data fiduciaries may be exempted from Section 9 duties, and processing without parental consent may be authorised for specified purposes. The DPDP Rules, 2025, notified in November 2025, give shape to the consent verification process. Rule 10 permits verification through a Digital Locker, an identity document matched against a government database, or a virtual token linked to an already-verified account. Rule 11, read with the Fourth Schedule, carves out exemptions for healthcare providers, educational institutions, creches, and transport service providers. Rule 13 creates a DPIA framework. It says nothing about child-specific risk assessment.

A developmental perspective is entirely absent from the Act's architecture. Children's capacity to understand and manage privacy risk shifts dramatically across the span from seven to seventeen (Levesque, 2017). Fixing the consent threshold at eighteen, without age-differentiated protections, ignores this. A rights-based global framework that moves past consent mechanisms toward structural duties on data collectors has been advocated (Montgomery & Chester, 2015). The DPDP Act did not follow.

Cognitive biases compound the problem. Status quo bias and present bias, interacting with dark pattern design, produce a "privacy paradox.privacy paradox": usersquot; Users say they care about privacy and then click through every invasive default. If adults are vulnerable to this pattern, children whose executive function and impulse control are still developing are far more so. The DPDP Act's parental consent mechanism does not address this cognitive weakness at all (Waldman, 2020).

5.2 The Consumer Protection Act, 2019

Section 2(47) of the CPA, 2019 defines "unfair trade practice" broadly enough to capture false and misleading representations. The CCPA can investigate, order product recalls, and levy penalties. The E-Commerce Rules of 2020 oblige online sellers to describe goods and services accurately, disclose material terms, and leave prices and search results unmanipulated. Rule 4(9) insists on explicit, affirmative consent before recording any purchase or imposing any charge.

The CCPA issued its dark pattern guidelines on 30 November 2023 (CCPA, 2023). Thirteen categories made the list, including basket sneaking, confirm-shaming, forced action, subscription traps, bait and switch, and others. Any violation counts as an unfair trade practice under the CPA and triggers Section 21 penalties. By June 2025, the CCPA had taken a further step, ordering every e-commerce platform to self-audit for dark patterns within ninety days (CCPA, 2025).

How deep does the problem run? Research from Indian digital markets suggests it runs very deep indeed. A study of Indian quick-commerce platforms found that basket sneaking, false scarcity cues, and confirm-shaming all increased perceived betrayal and negative word-of-mouth among consumers. Indian e-commerce platforms weaponise scarcity

bias and loss aversion through dark pattern deployment (Raj et al., 2025). The problem, these studies indicate, is systemic.

And yet, the CPA framework remains reactive. A platform that deploys dark patterns faces consequences only after a complaint, a CCPA investigation, or a suo motu action. No pre-market design review exists. No periodic compliance certification is required. Fragmented enforcement has a demonstrated cost. An examination of TikTok's treatment of minors under EU law, found that data protection, consumer protection, and competition instruments failed, collectively, to prevent systematic violations, because enforcement moved slowly and in silos (Santos et al., 2023).

5.3 The Information Technology Act, 2000

The IT Act deals with cybercrime and intermediary liability. Section 43A mandates reasonable security practices for bodies corporate handling sensitive personal data. Sections 66C and 66D penalise identity theft and cheating by personation. Section 67B criminalises content depicting children in sexually explicit acts. Section 72A penalises breach-of-contract disclosures of personal information.

Intermediary duties under the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 include informing users about prohibited content, maintaining grievance redressal channels, and removing unlawful material within stipulated timeframes. Significant Social Media Intermediaries face extra obligations, including appointing a compliance officer, deploying automated content monitoring.

None of this addresses design-based harms. Dark patterns, addictive interface features, manipulative monetisation. All of these fall outside what the IT Act contemplates, because the Act views intermediaries as conduits for content, not as architects of user experience. Legal frameworks tend to underestimate the danger posed by manipulative digital architectures, because they fixate on informational harms and miss autonomy harms (Susser et al., 2019b). A platform that exploits a child's cognitive weaknesses through its interface design is not stealing data. It is eroding the child's capacity to form decisions the child can call their own. For that category of harm, the IT Act offers nothing.

5.4 Child-Specific Protections

POCSO (2012) targets sexual offences against children and creates Special Courts. The Juvenile Justice Act (2015) sets up institutional mechanisms for child welfare. The Commission for Protection of Child Rights Act (2005) established the NCPCR with a mandate to advance child rights.

All three were written for a physical world. Commercial exploitation through data extraction and manipulative design barely registers within them. The NCPCR has published advisories on online safety, but it possesses neither the technical expertise to examine platform design nor the regulatory authority to enforce data protection standards.

The constitutional anchor is Justice K.S. Puttaswamy v. Union of India (2017). By recognising the right to privacy under Article 21, the Supreme Court established that informational privacy includes the right to control how personal information is shared. Children, who by definition lack the capacity to exercise autonomous choice over their data, stand to benefit most from this right, and are least able to exercise it.

5.5 International Obligations

India ratified the UNCRC on 11 December 1992 (United Nations, 1989). Article 16 guards against arbitrary or unlawful interference with a child's privacy, family, home, or correspondence. Article 17 addresses mass media and calls on states parties to develop guidelines protecting children from injurious information. Article 32 shields children from economic exploitation. Article 36 catches residual forms of exploitation that damage any aspect of a child's welfare. Taken as a whole, these articles impose a broad obligation on ratifying states to protect children from informational and economic exploitation, an obligation that now extends into the digital sphere.

General Comment No. 25 (2021) of the Committee on the Rights of the Child is, at present, the most authoritative guidance on applying the UNCRC to digital environments (Committee on the Rights of the Child, 2021). It directs

states to prevent businesses from undermining children's digital rights through profiling, automated processing, or commercial exploitation. Paragraph 42 is specific. States parties should prohibit by law the profiling or targeting of children of any age for commercial purposes on the basis of digital records of their actual or inferred characteristics. Paragraph 43 calls on the business sector to implement regulatory frameworks, industry codes, and design standards that place the best interests of children first by default.

The UN Guidelines for Consumer Protection, revised in 2015 (United Nations Conference on Trade and Development [UNCTAD], 2016), address vulnerable and disadvantaged consumers and call for expeditious, fair, and accessible redress mechanisms. Vulnerability, under these Guidelines, is not defined by age alone but by the interaction of individual and market characteristics, a formulation consistent with the consumer vulnerability theory set out in Section 2. The OECD Recommendation on Children in the Digital Environment (OECD, 2021) and the OECD Dark Commercial Patterns report (OECD, 2022) add further weight, urging states to tackle manipulative design and move past disclosure-only responses.

None of these international commitments finds explicit expression in Indian domestic law governing digital matters. The DPDP Act does not mention the UNCRC. The CPA does not adopt the UN Guidelines' concept of the vulnerable consumer. The IT Act and the Intermediary Guidelines ignore the OECD Recommendation. A normative gap of this width weakens the foundation on which India's child protection provisions rest and deprives courts and regulators of the principled framework that would inform interpretation.

6. Incidents And Enforcement

6.1 Edtech Data Exposure

DIKSHA, the Digital Infrastructure for Knowledge Sharing, was built as a government-backed edtech platform under the National Council of Educational Research and Training (NCERT) and launched in 2017. During the pandemic, it became the main channel for students in grades one through twelve to access learning material across India. In January 2023, WIRED revealed that a cloud server holding DIKSHA data had sat unprotected for over a year (Burgess, 2023). On that server were files containing the full names, phone numbers, and email addresses of more than one million teachers, spanning schools in every Indian state. A separate file held the names, school details, enrolment dates, and course completion records of nearly 600,000 students. A UK-based security researcher had spotted the exposure as early as June 2022, emailed the DIKSHA support team, and heard nothing back (Burgess, 2023).

The problem went deeper than one misconfigured server. In May 2022, Human Rights Watch published an investigation showing that DIKSHA could collect children's precise location data, including the date, time, and coordinates of their current and last known position (Human Rights Watch, 2022). The platform was also sharing data with Google, and neither parents nor students had been told. In many states, the government had mandated DIKSHA use and offered no alternative. Children who wanted to protect their data had to give up their education. Human Rights Watch wrote to India's Ministry of Education three times between March and July 2022. No reply came (Human Rights Watch, 2022). By January 2023, Human Rights Watch confirmed that the exposed records spanned March 2020 to December 2022 (Human Rights Watch, 2023), the exact period when millions of children were locked out of physical classrooms and had no choice but to go online. This kind of dynamic has been described as the "cruel optimism" of edtech. Platforms that promise educational equity while their data practices quietly work against it.

Other edtech firms followed a similar pattern. A server-side misconfiguration at Byju's allegedly exposed student names, phone numbers, addresses, email identifiers, and loan-related data. A separate Byju's incident involved data leaking through third-party service providers. Unacademy was named in reports alleging a large-scale breach, with user records sold on the dark web. Running through all of these is a common thread. No mandatory security standards tailored to platforms serving children. The DPDP Act calls for "reasonable security safeguards," but what counts as reasonable for a platform whose primary users are minors has never been specified. Rule 13 of the DPDP Rules creates

a DPIA framework, yet it does not require child-specific risk assessments or independent security audits for edtech providers.

6.2 Dark Pattern Enforcement

On 1 June 2026, the CCPA imposed a penalty of INR 5,00,000 on PhysicsWallah Limited (Case No. CCPA-2/94/2025-CCPA) for dark pattern violations on its platform (CCPA, 2026). The order invoked Sections 2(9), 2(28), and 2(47) of the CPA, read with the E-Commerce Rules, 2020, and the dark pattern guidelines of 2023. Three violations were found.

The first was basket sneaking. A charitable donation had been pre-selected in the user's cart, with no explicit opt-in required. PhysicsWallah disclosed during the proceedings that this mechanism ran from 14 February 2024 to 24 December 2025 and collected approximately INR 2.47 crore from more than 21,36,962 users. The pre-selection remained active even after the CCPA's initial notice in December 2025 and was switched off only once a formal notice landed on 4 December 2025.

The second violation was confirm-shaming. When users tried to remove the donation, the interface responded with emotionally loaded prompts designed to induce guilt.

The third was forced action. Users who wanted access to courses labelled "free" were required to hand over personal data. Data disclosure was the hidden price of a nominally costless service.

Chief Commissioner Nidhi Khare and Commissioner Anupam Mishra directed PhysicsWallah to eliminate all dark patterns and submit a compliance report within fifteen days. The investigation, referred to the Director General (Investigation) under Section 19(1) on 29 December 2025, produced a report on 23 March 2026 confirming every alleged violation.

Two things stand out. The CCPA acted suo motu, a welcome departure from the usual complaint-driven process. But the fine, INR 5 lakh, is dwarfed by the INR 2.47 crore the basket sneaking mechanism had already collected. Whether this penalty structure can deter a well-capitalised platform is an open question.

Edtech platforms continue to use practices that sit uncomfortably close to the 2023 guidelines. "Free" trials that demand credit card details and auto-renew, mandatory data sharing as a ticket to educational content, hidden add-on charges bundled into course packages. All persist. The formal prohibition and the everyday reality occupy different worlds. That gap is the hallmark of a complaint-driven enforcement model.

6.3 Cyber Fraud Involving Children

Children feature in a meaningful share of cybercrime cases in India, both as victims and, in some instances, as accused persons. Gaming platforms have become hunting grounds for account hijacking, ransom demands for the return of accounts, and fraud channelled through fake customer-service contacts. In other documented cases, children clicked suspicious links or downloaded apps that led to the compromise of parental bank accounts.

What distinguishes these incidents from the data exposure and dark pattern cases discussed above is directness. The harm is financial, and it is immediate. Platform design choices make it possible. Absent age verification, frictionless in-app transactions, no parental notification for unusual activity. The IT Act provides criminal remedies through Section 66C (identity theft) and Section 66D (cheating by personation), but both remedies are post-hoc and individual. The systemic design features that set the stage for fraud remain outside the law's reach.

7. Comparative Benchmarks

7.1 The EU Framework

Article 8 of the GDPR establishes parental consent for information society services offered directly to children. The default age threshold is sixteen, but member states may lower it to thirteen. Twenty member states have done so, most

settling on thirteen, fourteen, or fifteen. Recital 38 adds that children deserve heightened protection, as they may be less aware of risks, consequences, and safeguards, especially in connection with marketing, profiling, and data collection (Kosta, 2020).

Academic reception has been critical. The parental consent model imports COPPA's weaknesses wholesale. The difficulty of verifying parental identity, the risk that consent degenerates into a rubber stamp. Further objections have been raised (Lievens & Verdoodt, 2018). No child-specific right to be forgotten, inadequate profiling restrictions. The sheer scale and technical sophistication of modern data collection demands protections that go beyond consent altogether, particularly when the data is gathered through tracking technologies invisible to the user (Montgomery et al., 2017).

Article 28 of the EU Digital Services Act (2022) supplements the GDPR with a design obligation. Platforms may not present ads based on profiling when they are aware, with reasonable certainty, that the recipient is a minor. Unlike consent-based models, this provision puts the burden on the platform. Identify minors. Stop profiling them. Whether or not consent has been obtained is beside the point.

7.2 The UK Age Appropriate Design Code

In 2020, the ICO published the Age Appropriate Design Code (AADC), setting fifteen standards for online services "likely to be accessed by children." High privacy by default, data minimisation, geolocation restrictions, a ban on nudge techniques, and a best-interests-of-the-child standard all appear (ICO, 2020; Grace, Abel, and Salen, 2023).

The AADC's significance is conceptual. It shifts the regulatory question from "did you get consent?" to "did you design the service to protect children in the first place?" Any platform that children are likely to use, whether or not it is specifically aimed at them, must build protections in as a default. Parents should not have to hunt for a privacy toggle that ought to have been on from the start. California's Age-Appropriate Design Code Act (2022) followed a parallel path, requiring DPIAs for any product children might reasonably use. Both instruments reflect a move from user responsibility to platform accountability that Indian law has not yet attempted.

7.3 Implications for India

There is an irony in the comparison. India's Section 9(3) ban on tracking, behavioural monitoring, and targeted advertising aimed at children is, on its face, stricter than anything in the GDPR, which opts for heightened consent requirements rather than a blanket prohibition. But the EU and UK have built enforcement machinery, design standards, and audit mechanisms around their laws. India has not. The distance between a strict statutory text and a weak enforcement apparatus is, for practical purposes, the central regulatory problem.

8. Gaps In Indian Law

8.1 Weak Age Verification

Protecting children on digital platforms requires, as a first step, knowing which users are children. India's framework offers no workable mechanism for this. The DPDP Rules (2025) create procedures for verifying parental consent through identity documents and digital lockers, but those procedures only kick in after the platform has already determined that the user is below eighteen. That initial determination rests on self-declaration. Children routinely lie about their age to access services, and platforms have no commercial incentive to stand in the way.

The UK and California both addressed this problem differently. Their design codes apply to services "likely to be accessed by children," not to services that have positively identified particular child users. The trigger is foreseeable use, not proven use. India has not adopted anything comparable. The DPDP Act requires child-specific protections only when the fiduciary is "processing the data of a child," a formulation that presupposes the very identification it does not mandate.

8.2 Over-Reliance on Parental Consent

Parental consent works as a protective mechanism only if parents can evaluate the data practices of every platform their child uses, understand the implications for downstream data flows, and keep an eye on digital interactions over time. Most parents cannot do any of this. Research on parental awareness of dark patterns in children's applications confirms wide knowledge gaps (van der Hof et al., 2020). Parents are being asked to make informed decisions about data practices that baffle even data protection professionals.

The UNCRC, in Article 5, recognises the evolving capacities of the child. A blanket consent given when a child is seven years old says nothing about that same child's growing autonomy at fourteen. The DPDP Act, 2023, however, treats everyone below eighteen as a single undifferentiated category. There is no graduated consent, no age-differentiated privacy settings, no path for a child to request review of a parental consent decision. A seven-year-old and a seventeen-year-old are treated alike, despite vast differences in cognitive development, digital competence, and privacy awareness.

8.3 Absence of Design Duties

Indian law tells platforms what they must not do. It does not tell them what they must do. The CCPA dark pattern guidelines prohibit specific manipulative practices but impose no obligation to adopt privacy-protective defaults, build age-appropriate interfaces, or conduct child-specific impact assessments.

The UK and California AADCs both go further. High privacy by default, limits on data collection, restrictions on nudge techniques, mandatory impact assessments. All are affirmative duties. India's regulatory architecture, by contrast, places the burden of protection on parents and individual complainants rather than on the platforms that design the digital environments in which children spend their time.

8.4 Thin Remedies and Enforcement Capacity

Penalties under the CPA, 2019, and financial sanctions under the DPDP Act are available on paper. In practice, neither the CCPA nor the DPBI has the technical capacity to audit platform design at scale, monitor compliance with dark pattern rules, or test age verification mechanisms. The CCPA runs no dedicated technology unit able to reverse-engineer application interfaces or trace data flows. The DPBI has yet to be fully constituted as an operational body with the staffing and infrastructure needed to process complaints, investigate, and issue binding orders.

The enforcement record confirms the gap. The PhysicsWallah order (CCPA, 2026) is one of a handful of actions against child-facing platforms. The penalty of INR 5 lakh, imposed on a company that collected INR 2.47 crore through the very practice being penalised, speaks volumes about proportionality. The DPBI has not issued a single order under the DPDP Act, 2023. Regulatory architecture that exists only on paper does not deter.

9. Reform Proposals

9.1 An Indian Age-Appropriate Design Code

India needs a dedicated age-appropriate design code. The UK AADC and the California AADC provide models, but the code should be adapted to Indian institutional realities. It should apply mandatory design standards to any online service likely to be accessed by children. Privacy settings set to high by default, algorithmic recommendation restrictions for child users, prohibition of nudge techniques, geolocation turned off unless affirmatively enabled. These should be baseline requirements, not aspirations.

Twelve design strategies for supporting children’s digital autonomy have been identified, showing that platform functionality need not suffer when protective interventions are built in (Wang et al., 2023). Granular privacy controls calibrated to developmental stages, data-use transparency indicators, and tools that let children exercise agency over their own digital environments all belong in such a code. Issued under the combined authority of the DPDP Act and

the CPA, the code would serve simultaneously as a data protection standard and a consumer protection instrument. Compliance should be a condition for operating a child-facing digital service in India.

Edtech platforms need particular attention. Where use is compulsory for education, families cannot walk away. Edtech providers should be held to the highest privacy-protective defaults on all student-facing features and should refrain from any behavioural data extraction not strictly necessary for the educational purpose. Government-mandated platforms should be subject to protections at least as strong as those applied to commercial ones.

9.2 Mandatory Child-Specific Data Protection Impact Assessments

The DPIA framework under Rule 13 of the DPDP Rules applies to significant data fiduciaries. It should be extended to require a child-specific risk assessment for any fiduciary that processes children's data or runs a service likely to be accessed by children. Risks to privacy, autonomy, development, and financial interests should all be in scope. Each assessment should precede the launch of any new child-facing feature and should be updated annually.

Children negotiate their commercial privacy through acts of digital agency that may serve them now but harm them later (Srivastava et al., 2023). A child-specific DPIA should be designed to capture this tension. Platforms should have to weigh not only immediate risks but the long-term consequences of data collection for a child's development and future life chances.

9.3 Prohibition on Data Brokerage Involving Minors

India does not regulate data brokers as a distinct category. It should. Any sale, licensing, or exchange of personal data profiles involving children should be flatly prohibited. The prohibition should extend to the sharing of child-derived behavioural data with ad-tech firms, analytics providers, and data aggregators. Downstream recipients should carry the same legal obligations as the original data fiduciary.

A cross-national study found that young people are aware of datafication as a problem and push back against the collection of geolocation data, metadata, and behavioural records (Farthing et al., 2024). But awareness without institutional power produces nothing. Children cannot force platform operators to change embedded design practices. A statutory prohibition on data brokerage would act as a structural safeguard, removing the fight from the shoulders of individual children and parents.

9.4 Independent Audits for Child-Facing Platforms

Platforms serving children should undergo mandatory periodic audits of their data practices, interface design, and monetisation mechanics. Qualified auditors accredited by the DPBI should conduct these reviews. Reports should be filed with the DPBI and made available in summarised, non-confidential form to the public.

9.5 Age Verification Reform

A range of online age assurance methods against children's rights to privacy, participation, and non-discrimination (Livingstone et al., 2024). The conclusion was that age assurance should be proportionate, privacy-preserving, and designed to protect children rather than lock them out. India should require platforms likely to be accessed by children to deploy age estimation or verification mechanisms proportionate to the risk the service creates.

9.6 Coordination between CCPA and DPBI

Child protection currently sits across three regulatory bodies, namely the CCPA, the DPBI, and the intermediary guidelines framework. Predictably, gaps and overlaps result. Research on digital vulnerability treats consumer vulnerability in digital markets as a dynamic, relational phenomenon that no single agency can address alone (Helberger et al., 2021; Editorial, Journal of Consumer Policy, 2023). A formal coordination mechanism should assign lead-agency responsibility for different types of child digital harm and ensure that enforcement covers both data protection and consumer protection dimensions.

The NCPCR belongs in this mechanism. It has a constitutional mandate for child rights but no capacity to engage with digital harms. Giving it the power to refer digital child protection matters to the CCPA or DPBI, with a mandatory response obligation, and to participate in child-specific DPIA and audit review would plug a structural hole.

9.7 Granular Duties for App Stores, Ad-Tech Firms, and Game Publishers

Accountability should not end with the direct provider of a child-facing service. App stores should verify design-code compliance before listing applications in child-accessible categories. Ad-tech firms that receive data from child-facing platforms should face independent registration and compliance requirements of their own.

Game publishers using loot box or randomised reward mechanics deserve separate treatment. The 4Cs framework for classifying online risk to children treats dark patterns as a category distinct from content, contact, and conduct risks (Fitton, Read, and Horton, 2021). Gambling-style monetisation falls outside traditional content-based risk classifications, and existing consumer protection frameworks struggle to address it (Hyde and Cartwright, 2023). Game publishers should be required to disclose loot box probability rates, cap spending for child accounts, switch off real-money purchases by default for child users, and submit their monetisation designs for pre-release review.

9.8 Integrating Digital Literacy with Design Obligations

Design regulation and digital literacy should run in parallel. One should never substitute for the other. The benefits young people derive from digital skills depend, in large part, on how the surrounding digital environments are designed (Livingstone et al., 2023). Teaching a child to recognise privacy risks means little if the child is then placed inside an interface that makes exercising privacy impossible. Reform should therefore embed digital literacy in school curricula while, at the same time, requiring platforms to design interfaces where learned skills can actually be used.

10. Conclusion

No single statute can address every digital risk children face. Consumer law, data protection law, and cyber law must work together. India has made progress through the DPDP Act, 2023, the CCPA dark pattern guidelines, and the broader consumer protection framework. The system, though, remains fragmented, reactive, and under-enforced.

The root problem is conceptual. Indian law treats child protection as a function of parental consent. That places the burden on the least resourced actor in the regulatory chain, the parent. Meanwhile, the most resourced actor, the platform, remains free to design its services without regard to the developmental needs of child users.

What this paper proposes is a shift from consent to design. An Indian age-appropriate design code, mandatory child-specific DPIAs, independent audits, and coordinated CCPA-DPBI enforcement would build a preventive model. Children would be recognised not as data subjects whose consent must be obtained but as vulnerable digital consumers whose interests require protection through the very design of the environments they use.

The UK, the EU, and several US states have demonstrated that design-centred regulation is feasible and that it changes how platforms behave. India, home to one of the world's largest child populations and a digital economy growing at extraordinary speed, has both the need and the institutional capacity to place the best interests of the child at the centre of digital governance.

References:

[1] Agrawal, S. and Narayanan, S. (2026). When design deceives: Consumer reactions to dark patterns in quick commerce. Journal of Indian Business Research, ahead-of-print. https://doi.org/10.1108/JIBR-05-2025-0188

[2] Ash, J., Gordon, F., and Mills, S. (2023). Children and young people's experiences and understandings of gambling-style systems in digital games. Annals of the American Association of Geographers, 114(2), 308-327. https://doi.org/10.1080/24694452.2023.2248293

[3] Baker, S.M., Gentry, J.W., and Rittenburg, T.L. (2005). Building understanding of the domain of consumer vulnerability. Journal of Macromarketing, 25(2), 128-139. https://doi.org/10.1177/0276146705280622

[4] Basu, S. (2023). Twenty-five years of consumer vulnerability research. Journal of Consumer Affairs, 57(2), 766-798. https://doi.org/10.1111/joca.12518

[5] Bongard-Blanchy, K., Rossi, A., Rivas, S., Doublet, S., Koenig, V., and Lenzini, G. (2021). "I am definitely manipulated, even when I am aware of it." In Designing Interactive Systems Conference 2021, 763-776. https://doi.org/10.1145/3461778.3462086

[6] Burgess, M. (2023, January 23). A flaw in India's Diksha app exposed the data of millions of students and teachers. WIRED. https://www.wired.com/story/diksha-india-education-app-data-exposure/

[7] Central Consumer Protection Authority. (2023). Guidelines for prevention and regulation of dark patterns, 2023. Ministry of Consumer Affairs, Food and Public Distribution, Government of India.

[8] Central Consumer Protection Authority. (2025, June 7). Advisory to e-commerce platforms on dark patterns. https://www.newsonair.gov.in/central-consumer-protection-authority-advises-all-e-commerce-platforms-to-not-engage-in-deceptive-unfair-trade-practice

[9] Central Consumer Protection Authority. (2026, June 1). In the matter of use of dark patterns resulting in unfair trade practice, misleading advertisement, and violation of consumer right by PhysicsWallah Limited (Case No. CCPA-2/94/2025-CCPA). https://www.indialaw.in/blog/competition-act/ccpa-dark-patterns-physicswallah/

[10] Committee on the Rights of the Child. (2021). General comment No. 25 (2021) on children's rights in relation to the digital environment (CRC/C/GC/25). United Nations.

[11] Day, E., Pothong, K., Atabey, A., and Livingstone, S. (2022). Who controls children's education data? Learning, Media and Technology, 49(3), 356-370. https://doi.org/10.1080/17439884.2022.2152838

[12] Farthing, R., Koren Ošljak, K., Akuetteh, T., Camacho, K., Smith-Nunes, G., and Zhao, J. (2024). Online privacy, young people, and datafication. Social Media + Society, 10(4). https://doi.org/10.1177/20563051241298042

[13] Fitton, D., Read, J.C., and Horton, M. (2021). Integrating dark patterns into the 4Cs of online risk in the context of young people and mobile gaming apps. In Human-Computer Interaction, INTERACT 2021, Lecture Notes in Computer Science. Springer. https://doi.org/10.1007/978-3-030-85610-6_40

[14] Grace, T.D., Abel, C., and Salen, K. (2023). Child-centered design in the digital world. In Interaction Design and Children (IDC '23). https://doi.org/10.1145/3585088.3589370

[15] Gray, C.M., Kou, Y., Battles, B., Hoggatt, J., and Toombs, A.L. (2018). The dark (patterns) side of UX design. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, 534:1-534:14. https://doi.org/10.1145/3173574.3174108

[16] Helberger, N., Lynskey, O., Micklitz, H.-W., Rott, P., Sax, M., and Strycharz, J. (2021). EU Consumer Protection 2.0: Structured Asymmetries in Digital Consumer Markets. BEUC.

[17] Hoek, R.W., Rozendaal, E., van Schie, H.T., and Buijzen, M. (2021). Development and testing of the advertising literacy activation task. Media Psychology, 24(6), 814-846. https://doi.org/10.1080/15213269.2020.1817090

[18] Human Rights Watch. (2022, May 25). How dare they peep into my private life? Children's rights violations by governments that endorsed online learning during the Covid-19 pandemic. https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments

[19] Human Rights Watch. (2023, January 27). Indian government app exposed children's personal data. https://www.hrw.org/news/2023/01/27/indian-government-app-exposed-childrens-personal-data

[20] Hyde, R. and Cartwright, P. (2023). Exploring consumer detriment in immersive gaming technologies. Journal of Consumer Policy, 46, 335-361. https://doi.org/10.1007/s10603-023-09544-9

[21] Editorial (2023). Digital vulnerability. Journal of Consumer Policy, 46, 277-280. https://doi.org/10.1007/s10603-023-09555-6

[22] Jarke, J. and Breiter, A. (2019). Editorial: the datafication of education. Learning, Media and Technology, 44(1), 1-6. https://doi.org/10.1080/17439884.2019.1573833

[23] Kosta, E. (2020). Article 8: Conditions applicable to child's consent. In C. Kuner et al. (eds), The EU General Data Protection Regulation (GDPR): A Commentary. Oxford University Press. https://doi.org/10.1093/oso/9780198826491.003.0037

[24] Lee, K., Bart, Y., and Cauffman, C. (2026). Consumer vulnerability within digital platforms as service ecosystems. Journal of Services Marketing, 40(3), 285-302. https://doi.org/10.1108/JSM-03-2025-0179

[25] Levesque, R.J.R. (2017). Adolescence, Privacy, and the Law: A Developmental Science Perspective. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780190460792.001.0001

[26] Lievens, E. and Verdoodt, V. (2018). Looking for needles in a haystack: Key issues affecting children's rights in the GDPR. Computer Law and Security Review, 34(2), 269-278. https://doi.org/10.1016/j.clsr.2017.09.007

[27] Livingstone, S., Mascheroni, G., and Stoilova, M. (2023). The outcomes of gaining digital skills for young people's lives and wellbeing. New Media and Society, 25(5), 1176-1202. https://doi.org/10.1177/14614448211043189

[28] Livingstone, S., Nair, A., Stoilova, M., van der Hof, S., and Caglar, C. (2024). Children's rights and online age assurance systems. International Journal of Children's Rights, 32(3), 721-747. https://doi.org/10.1163/15718182-32030001

[29] Livingstone, S. and Third, A. (2017). Children and young people's rights in the digital age. New Media and Society, 19(5), 657-670. https://doi.org/10.1177/1461444816686318

[30] Luguri, J. and Strahilevitz, L.J. (2021). Shining a light on dark patterns. Journal of Legal Analysis, 13(1), 43-109. https://doi.org/10.1093/jla/laaa006

[31] Lupton, D. and Williamson, B. (2017). The datafied child. New Media and Society, 19(5), 780-794. https://doi.org/10.1177/1461444816686328

[32] Macgilchrist, F. (2019). Cruel optimism in edtech. Learning, Media and Technology, 44(1), 77-86. https://doi.org/10.1080/17439884.2018.1556217

[33] Macenaite, M. and Kosta, E. (2017). Consent for processing children's personal data in the EU. Information and Communications Technology Law, 26(2), 146-197. https://doi.org/10.1080/13600834.2017.1321096

[34] Mathur, A., Acar, G., Friedman, M.J., Lucherini, E., Mayer, J., Chetty, M., and Narayanan, A. (2019). Dark patterns at scale. Proceedings of the ACM on Human-Computer Interaction, 3(CSCW), Article 81. https://doi.org/10.1145/3359183

[35] Montgomery, K.C., Chester, J., and Milosevic, T. (2017). Children's privacy in the big data era. Pediatrics, 140(Suppl 2), S117-S121. https://doi.org/10.1542/peds.2016-1758O

[36] Montgomery, K.C. and Chester, J. (2015). Data protection for youth in the digital age. European Data Protection Law Review, 1(4), 277-291. https://doi.org/10.21552/EDPL/2015/4/6

[37] Moti, Z., Senol, A., Bostani, H., Borgesius, F.Z., Moonsamy, V., Mathur, A., and Acar, G. (2024). Targeted and troublesome: Tracking and advertising on children's websites. In 2024 IEEE Symposium on Security and Privacy, 1517-1535. https://doi.org/10.1109/SP54263.2024.00118

[38] Nelson, M.R. (2016). Developing persuasion knowledge by teaching advertising literacy in primary school. Journal of Advertising, 45(2), 169-182. https://doi.org/10.1080/00913367.2015.1107871

[39] Organisation for Economic Co-operation and Development. (2021). Recommendation of the Council on Children in the Digital Environment (OECD/LEGAL/0389). OECD Publishing.

[40] Organisation for Economic Co-operation and Development. (2022). Dark commercial patterns (OECD Digital Economy Papers No. 336). OECD Publishing. https://www.oecd-ilibrary.org/science-and-technology/dark-commercial-patterns_44f5e846-en

[41] O'Donnell, N., Klarkowski, M., MacKenzie, J., Horton, E., Mallawaarachchi, S., Howard, S., and Johnson, D. (2026). From playful to manipulative. International Journal of Child-Computer Interaction, 47(C). https://doi.org/10.1016/j.ijcci.2026.100804

[42] Raj, P., Nanda, S.S., and Noorani, M.S. (2025). Safeguarding the digital consumer: A comparative legal and psychological analysis of dark patterns in e-commerce. Advances in Consumer Research, 2(4), 3567-3574. https://doi.org/10.2139/ssrn.5528518

[43] Santos, C., Morozovaite, V., and De Conca, S. (2023). Do too many cooks spoil the broth? How EU law underenforcement allows TikTok's violations of minors' rights. Journal of Consumer Policy, 46, 281-305. https://doi.org/10.1007/s10603-023-09545-8

[44] Rozendaal, E. and Buijzen, M. (2023). Children's vulnerability to advertising: An overview of four decades of research (1980s-2020s). International Journal of Advertising, 42(1), 78-86. https://doi.org/10.1080/02650487.2022.2135349

[45] Rozendaal, E., Buijzen, M., and Valkenburg, P. (2010). Comparing children's and adults' cognitive advertising competences. Journal of Children and Media, 4(1), 77-89. https://doi.org/10.1080/17482790903407333

[46] Rozendaal, E., Lapierre, M.A., van Reijmersdal, E.A., and Buijzen, M. (2011). Reconsidering advertising literacy as a defense against advertising effects. Media Psychology, 14(4), 333-354. https://doi.org/10.1080/15213269.2011.620540

[47] Schafer, R. et al. (2024). Growing up with dark patterns: How children perceive malicious user interface designs. In Nordic Conference on Human-Computer Interaction (NordiCHI '24), 1-17. https://doi.org/10.1145/3679318.3685358

[48] Srivastava, S., Wilska, T., and Nyrhinen, J. (2023). Children as social actors negotiating their privacy in the digital commercial context. Childhood, 30(4). https://doi.org/10.1177/09075682231186486

[49] Susser, D., Roessler, B., and Nissenbaum, H. (2019b). Technology, autonomy, and manipulation. Internet Policy Review, 8(2). https://doi.org/10.14763/2019.2.1410

[50] Susser, D., Roessler, B., and Nissenbaum, H. (2019). Online manipulation: Hidden influences in a digital world. Georgetown Law Technology Review, 4(1), 1-45. https://doi.org/10.2139/ssrn.3306006

[51] United Nations. (1989). Convention on the Rights of the Child. Treaty Series, 1577, 3.

[52] United Nations Conference on Trade and Development. (2016). United Nations guidelines for consumer protection (UNCTAD/DITC/CPLP/MISC/2016/1). United Nations.

[53] van der Hof, S. (2017). I agree... or do I? A rights-based analysis of the law on children's consent in the digital world. Wisconsin International Law Journal, 34(2), 409-445.

[54] van der Hof, S., Lievens, E., Milkaite, I., Verdoodt, V., Hannema, T., and Liefaard, T. (2020). The child's right to protection against economic exploitation in the digital world. International Journal of Children's Rights, 28(4), 833-859. https://doi.org/10.1163/15718182-28040003

[55] van Reijmersdal, E.A., Rozendaal, E., Smink, N., van Noort, G., and Buijzen, M. (2017). Processes and effects of targeted online advertising among children. International Journal of Advertising, 36(3), 396-414. https://doi.org/10.1080/02650487.2016.1196904

[56] Verdoodt, V. (2019). The role of children's rights in regulating digital advertising. International Journal of Children's Rights, 27(3), 455-481. https://doi.org/10.1163/15718182-02703002

[57] Verma, S. et al. (2026). Consumer vulnerability: A systematic literature review and future research agenda. Journal of Consumer Behaviour, 25(1). https://doi.org/10.1002/cb.70092

[58] Waldman, A.E. (2020). Cognitive biases, dark patterns, and the "privacy paradox". Current Opinion in Psychology, 31, 105-109. https://doi.org/10.1016/j.copsyc.2019.08.025

[59] Wang, G. et al. (2023). 12 ways to empower: Designing for children's digital autonomy. In Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems, 1-27. https://doi.org/10.1145/3544548.3580935

[60] Xiao, L.Y. and Lund, M.L. (2025). Non-compliance with and non-enforcement of UK loot box industry self-regulation on the Apple App Store. Royal Society Open Science. https://doi.org/10.1098/rsos.250704

[61] Zac, A. et al. (2024). Dark patterns and consumer vulnerability. Behavioural Public Policy. https://doi.org/10.1017/bpp.2024.49