

Governing Childhood in the Digital Age: Reimagining Child Rights in an Era of Age Verification, Algorithmic Profiling and Platform Commercialisation

Shubhi Agrawal¹, Pooja Mahla^{2*}, Ankit Kumar³

¹Assistant Professor, SRM University, School of Law, Chennai.

Email Id:- agrawalshubhi02@gmail.com., ORCID ID: 0009-0005-2839-4835.

²Research Scholar , Department of Law, Kurukshetra University.

Email Id:- poojamahla31@gmail.com., ORCID. ID : 0009-0007-7071-5254.

³Designation & Institution: Cyber Lawyer, Lex Cyber Attorneys .

Email Id:- ankit@thewriterscommunity.in., ORCID ID: 0009-0003-8212-8648

***Corresponding Author**

Pooja Mahla

Research Scholar , Department of Law, Kurukshetra University.

Email Id:- poojamahla31@gmail.com., ORCID. ID : 0009-0007-7071-5254

ABSTRACT

The generation coming of age today is the first in human history whose childhood is co-authored by machines. Children now constitute roughly one-third of all internet users worldwide, yet the international legal architecture built to protect them the United Nations Convention on the Rights of the Child, 1989 predates the World Wide Web itself. This paper interrogates the widening gap between that analogue-era framework and a digital ecosystem organised around continuous data extraction, algorithmic profiling, behavioural advertising and design engineered for compulsive engagement. Moving beyond the binary of protection versus access, the paper argues that child-rights governance must be reimagined along a third axis: graded, risk-calibrated participation that safeguards the child's evolving autonomy while imposing enforceable obligations of care on digital platforms. Adopting a doctrinal and comparative methodology, the paper examines the normative foundations laid by the UN Committee on the Rights of the Child's General Comment No. 25 (2021) and traces their translation into binding law across five jurisdictions the European Union, France, the United Kingdom, the United States and India with attention to the most recent 2025–2026 developments, including India's Digital Personal Data Protection Rules, 2025, the European Commission's age-verification Recommendation of April 2026, the French Conseil constitutionnel's censure of the under-15 social-media ban, the stalled American KIDS Act, and the European Commission's proposed EU KIDS Act of September 2026. The paper further undertakes a thematic analysis of age-appropriate design, age assurance technologies, profiling-driven behavioural advertising, dark patterns, and the commodification of children's data and attention. It finds that regulatory regimes remain fragmented, privacy-invasive in their verification methods, and insufficiently attentive to children's participatory rights. The paper concludes with a set of calibrated recommendations for a rights-respecting, interoperable and enforceable global framework for digital childhood.

Keywords: digital child rights; age-appropriate design; age assurance and verification; algorithmic profiling; behavioural advertising; dark patterns; children's autonomy and participation; commodification of children's data; platform accountability; EU KIDS Act; UNCRC General Comment No. 25.

I. INTRODUCTION

When the United Nations General Assembly adopted the Convention on the Rights of the Child ("UNCRC") on 20 November 1989, the World Wide Web did not yet exist; Tim Berners-Lee would propose it only months later, in March 1990. The Convention's drafters could not have anticipated a childhood mediated by recommendation algorithms, biometric age-estimation software, in-app currencies and infinite-scroll feeds engineered by behavioural psychologists. Yet today, children account for close to one-third of all internet users globally, and for many, digital access is no longer incidental to childhood but constitutive of it shaping how they learn, play, socialise, express identity and are, in turn, commercially profiled.

For roughly two decades, digital child-safety policy oscillated between two blunt instruments: exclusion (age-gating children out of platforms altogether) and reactive content moderation (removing harmful material after exposure had already occurred). Both approaches treated the child primarily as a vulnerable object of protection rather than as a rights-holder with an evolving capacity for autonomous participation. This protection-only paradigm is increasingly untenable. As internet access becomes indispensable to education, communication and social development, a policy of blanket exclusion risks violating children's rights to information, expression and association under Articles 13, 15 and 17 of the UNCRC, even as it fails to shield children from platforms designed, at an architectural level, to monetise their attention.

The regulatory centre of gravity is now shifting toward a third paradigm: a graded, risk-and-age-differentiated model that seeks to calibrate platform obligations to the developmental stage of the child, rather than imposing uniform bans or uniform access. India exemplifies this shift most starkly. Policy discourse has moved away from proposals for blanket restrictions on children's social media use toward the layered, consent-based, risk-differentiated architecture embodied in Section 9 of the Digital Personal Data Protection Act, 2023 and operationalised through the Digital Personal Data Protection Rules, 2025. Europe's most recent move, the Commission's proposed EU KIDS Act of 17 September 2026, carries the same logic into binding regulation, pairing a staged, age-tiered model of account access with enforceable safety-by-design duties.

This paper is animated by a single organising question: can child-rights law, built on a best-interests and evolving-capacities framework designed for the physical world, be re-engineered to govern an environment whose defining commercial logic surveillance capitalism is structurally indifferent to the child's best interests?¹ In answering this question, the paper examines four interlocking regulatory problem-areas that define the contemporary governance of digital childhood: (i) age-appropriate design and age assurance/verification; (ii) algorithmic profiling and behavioural advertising directed at minors; (iii) manipulative interface design, or 'dark patterns'; and (iv) the broader political economy of the commodification of children's data and attention, and the correlative responsibilities this casts upon digital platforms.

The paper proceeds in eight parts. Part II situates the study within the existing literature on children's digital rights, privacy, and platform governance. Part III lays out the normative architecture supplied by the UNCRC and, specifically, General Comment No. 25 (2021) on children's rights in relation to the digital environment. Part IV undertakes a comparative analysis of the regulatory approaches adopted in the European Union, France, the United Kingdom, the United States and India (including India's emerging proposal for tiered, age-graded social-media access), incorporating developments as current as September 2026. Part V analyses the paper's eight thematic pillars in depth, supported by five original figures. Part VI distils the principal findings; Part VII sets out calibrated recommendations; and Part VIII concludes.

Methodologically, the paper adopts a doctrinal and comparative-legal approach, supplemented by policy analysis of recent regulatory instruments, enforcement actions and legislative developments up to September 2026. Primary sources include international instruments, domestic statutes, subordinate legislation, judicial and regulatory decisions; secondary sources include peer-reviewed scholarship, regulator guidance and contemporaneous legal commentary. Given the pace of change in this field several of the developments discussed below occurred within weeks of this paper's completion the analysis should be read as a snapshot of a rapidly consolidating, but still unsettled, area of law.

LITERATURE REVIEW

The scholarly literature on children's digital rights has evolved through three overlapping waves, each responding to a different facet of the underlying problem.

A. The Privacy and Data-Protection Wave

The earliest and most extensive body of scholarship approaches digital childhood through the lens of information privacy. Sonia Livingstone's empirical work on children's online risks and opportunities established the now-canonical distinction between content risks, contact risks and conduct risks, providing the taxonomy that underlies most subsequent regulatory design.² Valerie Steeves and other privacy scholars have critiqued the consent-based model underlying instruments such as the US Children's Online Privacy Protection Act ("COPPA") as a legal fiction, given that neither children nor, realistically, most parents meaningfully understand or control the data flows they purport to authorise.³ This critique has gained force in light of Shoshana Zuboff's account of 'surveillance capitalism', which frames children's data not as a by-product of service provision but as the primary commercial output of the contemporary internet economy.⁴

B. The Children's-Rights-by-Design Wave

¹ See generally Shoshana Zuboff, 'Big Other: Surveillance Capitalism and the Prospects of an Information Civilization' (2015) 30 *Journal of Information Technology* 75, for the foundational account of the attention-and-data-extraction business model that underlies most consumer digital platforms.

² Sonia Livingstone, Leslie Haddon, Anke Görzig and Kjartan Ólafsson, *Risks and Safety on the Internet: The Perspective of European Children* (EU Kids Online, LSE 2011).

³ Valerie Steeves, 'Terra Cognita: Surveillance of Students' in Emmeline Taylor and others (eds), *Surveillance Futures* (Routledge 2018) 87.

⁴ Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs 2019).

A second wave of scholarship, catalysed by the adoption of General Comment No. 25 in 2021, reframes the debate away from privacy alone and toward the full spectrum of rights under the UNCRC participation, expression, play, non-discrimination and protection from economic and sexual exploitation. Christian Djeflal's analysis of General Comment No. 25 identifies four structural contributions of the instrument to internet governance: it substantiates children's rights as binding obligations on private digital actors, it introduces a 'children's rights by design' methodology analogous to 'privacy by design', it clarifies the horizontal application of the Convention to businesses, and it foregrounds children's participation in the design of digital services and of the regulations that govern them.⁵ Sonia Livingstone and Amanda Third's subsequent work develops the concept of 'digital age of majority' as itself an unstable and contestable construct, arguing that chronological age thresholds are poor proxies for the graduated, context-dependent 'evolving capacities' concept embedded in Article 5 of the Convention.⁶

C. The Platform-Accountability and Dark-Patterns Wave

A third and most recent wave interrogates the design architecture of platforms themselves. Colin Gray and co-authors' foundational taxonomy of 'dark patterns' interface designs that manipulate or coerce users into choices they would not otherwise make has been extended by behavioural-economics and child-development scholars to demonstrate that children and adolescents are disproportionately susceptible to persuasive design because the prefrontal cortex, responsible for impulse control and long-term reasoning, does not fully mature until the mid-twenties.⁷ This literature intersects with a growing regulatory-economics scholarship on the 'attention economy' and its capture of adolescent psychology, echoed in the United States Surgeon General's 2023 advisory on social media and youth mental health, which catalysed much of the subsequent 2024–2026 wave of youth-protection legislation across Australia, France, the United Kingdom and several U.S. states.

Notwithstanding this rich literature, a gap persists: most existing scholarship analyses either the human-rights framework or the data-protection/consumer-protection framework in isolation, and comparative work that synthesises the 2025–2026 wave of legislative and regulatory activity India's DPDP Rules, the EU's age-verification Recommendation and proposed EU KIDS Act, France's ill-fated s. 15 ban, and the American KIDS Act remains sparse, largely because these developments are contemporaneous with this paper's writing. This paper seeks to close that gap by integrating the rights-based, data-protection and platform-design literatures within a single comparative and thematic frame.

THE NORMATIVE ARCHITECTURE: THE UNCRC AND GENERAL COMMENT NO. 25 (2021)

The UNCRC remains the primary international-law foundation for children's digital rights, ratified by 196 States and thus the most widely ratified human-rights treaty in history.⁸ Four provisions are of particular salience: Article 3 (best interests of the child as a primary consideration in all actions concerning children); Article 5 (respect for the child's evolving capacities, requiring that parental guidance be calibrated to the child's maturing autonomy); Article 12 (the child's right to be heard in matters affecting them); and Article 16 (protection from arbitrary interference with privacy).

Because the Convention pre-dates the internet, the Committee on the Rights of the Child adopted General Comment No. 25 on 2 March 2021, following a two-year global consultation that included the direct participation of 709 children from 28 countries itself an application of the Article 12 participatory principle to the standard-setting process.⁹ General Comment No. 25 does not create new treaty rights; rather, it authoritatively interprets existing UNCRC rights as applying with equal force in the digital environment, and it does so along four analytically distinct axes that structure this paper's own thematic analysis in Part V.

General principles: States parties must ensure that in all actions regarding the provision, regulation, design, management and use of the digital environment, the best interests of the child are a primary consideration, and that digital-environment governance itself is non-discriminatory and inclusive of children with disabilities and from marginalised communities.¹⁰

⁵ Christian Djeflal, 'Children's Rights by Design and Internet Governance: Revisiting General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment' (2022) 11 *Laws* 84.

⁶ Sonia Livingstone and Amanda Third, 'Children and Young People's Rights in the Digital Age: An Emerging Agenda' (2017) 19 *New Media & Society* 657.

⁷ Colin M Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt and Austin L Toombs, 'The Dark (Patterns) Side of UX Design' (2018) Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems 1.

⁸ Convention on the Rights of the Child (adopted 20 November 1989, entered into force 2 September 1990) 1577 UNTS 3 ("UNCRC").

⁹ UN Committee on the Rights of the Child, General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment, CRC/C/GC/25 (2 March 2021) para 2.

¹⁰ UN Committee on the Rights of the Child, General Comment No. 25 (2021) CRC/C/GC/25, paras 10–14.

Evolving capacities and ‘digital age of majority’: The Committee cautions against treating chronological age thresholds as a proxy for maturity, and calls on States to develop graduated, evidence-based frameworks rather than one-size-fits-all restrictions a principle directly reflected in India’s post-2023 policy shift away from blanket bans toward risk-differentiated regulation.¹¹

Children’s rights by design: Businesses that design, provide or manage digital products likely to be accessed by children must undertake child-rights due-diligence, embedding privacy, safety and non-manipulation as default settings rather than opt-in features the doctrinal seed of what later crystallised into the UK’s Age-Appropriate Design Code and the EU’s Article 28 DSA guidelines.¹²

Commercial exploitation and profiling: Paragraph 42 of the General Comment specifically flags profiling, algorithmically curated content and behavioural advertising targeted at children as practices requiring stringent regulatory restriction, given children’s demonstrably reduced capacity to recognise persuasive commercial intent.¹³

General Comment No. 25 is, formally, soft law: it is interpretive guidance rather than a source of independently binding obligation. Yet its practical influence on subsequent hard law has been substantial. The Digital Futures for Children research programme at the London School of Economics, mapping the Comment’s global impact on its fifth anniversary in 2026, found that it has been directly cited in domestic legislative and regulatory processes across more than 40 jurisdictions, and has supplied the conceptual vocabulary ‘evolving capacities’, ‘best interests by design’, ‘digital environment’ now standard in comparative children’s-rights instruments, including the EU’s Better Internet for Kids strategy and India’s DPDP Rules, 2025.

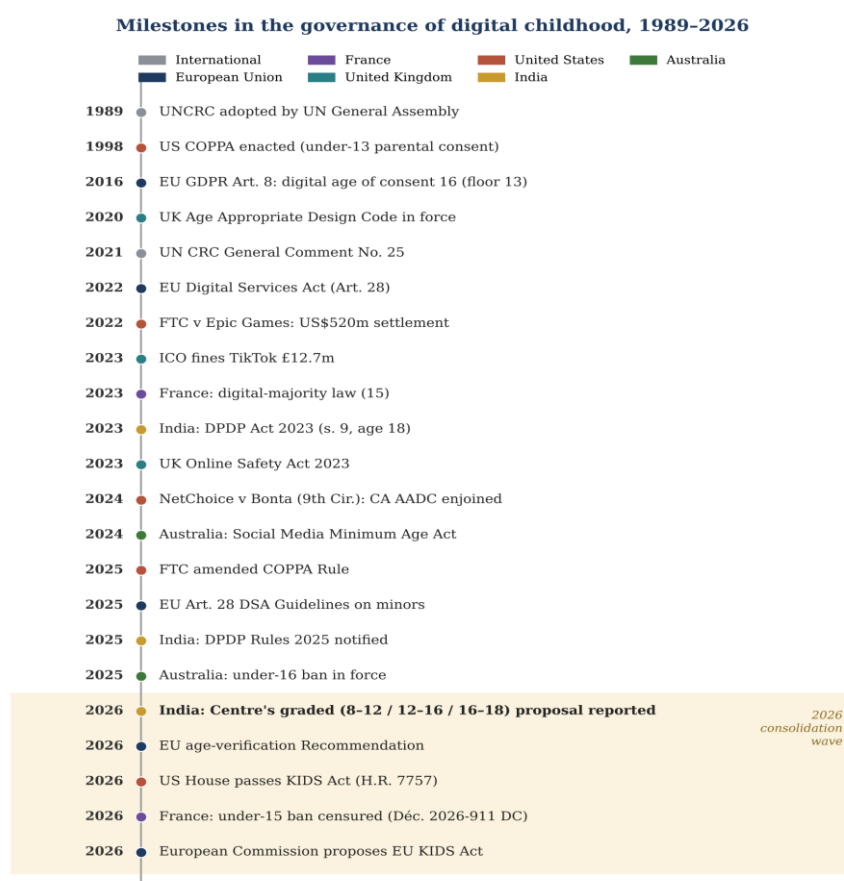


Figure 1: Timeline of key global milestones in the governance of childhood in the digital environment, 1989–2026 (compiled by the author from primary legislative and regulatory sources cited throughout this paper).

¹¹ General Comment No. 25 (2021) CRC/C/GC/25, para 20.

¹² General Comment No. 25 (2021) CRC/C/GC/25, paras 37, 42; see also Christian Djeflal, ‘Children’s Rights by Design and Internet Governance’ (2022) 11 Laws 84.

¹³ General Comment No. 25 (2021) CRC/C/GC/25, para 42; see also paras 62, 112–113 (advertising and marketing).

Comparative Regulatory Analysis: Five Jurisdictions

This Part maps the translation of the UNCRC/General Comment No. 25 framework into binding domestic and regional law across five representative jurisdictions, chosen for the diversity of their regulatory philosophies: the European Union (co-regulatory, platform-obligation model); France (a Member State experimenting, and repeatedly failing, at outright prohibition); the United Kingdom (design-code and safety-duty model); the United States (sectoral, consent-based model, historically narrow but now expanding); and India (a consent-and-verification model layered onto a graded, risk-based architecture).

A. The European Union

The EU's approach operates on two parallel tracks. First, data protection: Article 8 of the General Data Protection Regulation sets a default digital age of consent at 16, while permitting Member States to lower it to a floor of 13 a derogation that most Member States, including France and Germany, have exercised, producing a fragmented internal digital-consent map even within the Union itself.¹⁴ Second, platform regulation: Article 28 of the Digital Services Act imposes a free-standing obligation on providers of online platforms accessible to minors to put in place appropriate and proportionate measures to ensure a high level of privacy, safety and security for minors, and expressly prohibits presenting advertisements based on profiling using minors' personal data.¹⁵

The Commission's July 2025 Guidelines under Article 28 DSA elaborate a risk-based, proportionate approach to age assurance, endorsing self-declaration, inferential age-estimation and hard age-verification as a graduated toolkit depending on the severity of risk posed by a given service, while reserving strong verification for the highest-risk categories such as pornography and gambling.¹⁶ In April 2026, the Commission escalated this approach with a (non-binding) Recommendation establishing a common EU-wide age-verification framework built around an open-source, privacy-preserving 'age verification blueprint' and, eventually, the EU Digital Identity Wallet, urging Member States to operationalise the framework by 31 December 2026.¹⁷ Notably, no Article of the DSA itself fixes a minimum age for social media access; the Commission has therefore had to rely on soft-law guidance and recommendations to knit together an otherwise fragmented Member-State landscape, even as individual States (France, Denmark, Greece) press for a binding EU-wide minimum age.

That pressure has now been answered at Union level. On 17 September 2026, the Commission tabled a proposal for a Regulation on 'Keeping Internet Digital Spaces Accountable and Trustworthy', branded the 'EU KIDS Act' (not to be confused with the U.S. KIDS Act discussed in Part IV.D).¹⁸ Unlike the Article 28 Guidelines and the April 2026 Recommendation, both of which are soft law, the EU KIDS Act is proposed as a directly applicable regulation, and would therefore be the first EU instrument to fix a harmonised minimum age for social-media accounts and to convert the Guidelines' safety-by-design expectations into binding obligations. It is, however, only a proposal: it now passes to the European Parliament and the Council under the ordinary legislative procedure, its adoption is not assured, and in its current form it would apply six months after entry into force, so that it is unlikely to apply before 2028.¹⁹ This paper therefore treats it as a proposed, and not an operative, regime. The proposal rests on four pillars. The first is delayed and graduated access. Children under 15 would be barred from holding their own accounts on social-networking and video-sharing services that carry specified risk functionalities, such as real-time transmission to an indeterminate audience, contact with users outside pre-existing connections, profiling-based recommender systems, or design enabling uninterrupted consumption. Guardians could open limited accounts for children aged 13 to 15, with guardian tools always enabled, a one-hour daily limit and pre-approved contacts; children under 13 could reach only video-sharing services specifically designed for their age group, through a guardian's account; and users aged 15 to 17 could hold their own accounts within a safe-by-design environment.²⁰ The second pillar is a set of safety-by-design duties, applying by default until a user is established to be an adult: a prohibition on addictive design (including autoplay without effective interruption, streaks and rewards for sharing), recommender systems that give primary weight to stated preferences and offer a non-profiling option, off-by-default geolocation, camera, microphone and push

¹⁴ Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1, art 8.

¹⁵ Regulation (EU) 2022/2065 (Digital Services Act) [2022] OJ L277/1, art 28.

¹⁶ European Commission, Guidelines on the Protection of Minors under Article 28 DSA (14 July 2025).

¹⁷ European Commission, Recommendation on Establishing a Common EU-Wide Framework for Age Verification Technologies (29 April 2026).

¹⁸ European Commission, Proposal for a Regulation on Keeping Internet Digital Spaces Accountable and Trustworthy ('EU KIDS Act') (17 September 2026); European Commission, 'EU KIDS Act to restrict social media platforms' access to children in the EU' (press release, 17 September 2026).

¹⁹ Freshfields Bruckhaus Deringer, 'The EU KIDS Act: Europe moves online child safety beyond social media bans' (18 September 2026); Wilson Sonsini, 'European Commission Proposes "EU KIDS Act" to Restrict Children's Access to Online Services' (September 2026).

²⁰ EU KIDS Act proposal, arts 6–7.

notifications, safeguards against unsolicited contact from strangers, and real-time flagging of in-app transactions together with a ban on variable rewards.²¹ The third pillar is age assurance: for the minimum-age rules, providers would have to rely exclusively on a certified EU age-verification solution (the European Digital Identity Wallet qualifying), and existing accounts would have to be screened within six months of the date of application.²² The fourth is enforcement built on existing machinery: DSA-style penalties of up to 6% of worldwide annual turnover, Commission supervision of Very Large Online Platforms, national authorities for other providers, and listing in the Representative Actions Directive to permit collective redress.²³

Three features distinguish the proposal from the regimes surveyed elsewhere in this Part. First, its scope reaches well beyond the DSA's 'online platform' concept, covering seven categories of service (social networking, video-sharing, app stores, online games, operating systems, AI companions and general conversational chatbots) and, unlike much of the DSA, deliberately not exempting micro and small enterprises.²⁴ Second, it reverses the burden of proof: providers must demonstrate that their services are age-appropriate and safe by design, rather than regulators having to prove harm. Third, its account bar is service-differentiated rather than blanket, since it applies only to services carrying the specified risk functionalities, a design that arguably responds to the very objection on which the Conseil constitutionnel struck down the French ban (Part IV.B). Its thresholds nonetheless remain politically contested, with national proposals across the Member States ranging from 13 to 16, and the Commission would hold extensive delegated powers to amend key substantive requirements. The Commission itself has acknowledged that the rules will not work overnight, pointing to the Australian experience described in Part IV.F, where most minors who already held accounts kept them because they were never asked to prove their age.²⁵

B. France

France offers the paper's most instructive cautionary tale on the limits of prohibition-based regulation. The Law of 7 July 2023 ('loi visant à instaurer une majorité numérique') fixed 15 as France's digital majority, requiring parental co-consent for data processing and social-media registration below that age, but its central mechanism was never operationalised because no implementing decree was issued and its design proved difficult to reconcile with EU law the government itself has since admitted in writing that the 2023 law "has not been able to take effect".²⁶ A more ambitious successor bill, sponsored by Députée Laure Miller, sought to go further and impose an outright ban rather than mere parental co-consent on social-media access for under-15s, with mandatory platform-side age verification. Parliament definitively adopted the bill on 21 July 2026.

The Conseil constitutionnel, however, struck the ban down on 14 August 2026, holding in Décision n° 2026-911 DC that a general and undifferentiated prohibition, applied without regard either to the individual minor's circumstances or to the specific risks posed by different categories of online service, and which as a structural matter necessarily required every user including adults to prove their age, constituted a disproportionate interference with freedom of expression and communication guaranteed by Article 11 of the 1789 Déclaration, absent adequate legislative safeguards on the process of age verification.²⁷ The episode illustrates a recurring constitutional tension also visible in the U.S. First Amendment litigation discussed below between age-verification mandates and free-expression guarantees, and demonstrates that even a democratically popular child-protection measure can founder on proportionality review if it fails to build in graduated, risk-differentiated, and narrowly tailored safeguards. A revised French bill is expected before spring 2027.

C. The United Kingdom

The UK pioneered the 'design code' model. The Age Appropriate Design Code (the 'Children's Code'), issued by the Information Commissioner's Office under section 123 of the Data Protection Act 2018 and in force since September 2020, does not itself create free-standing statutory liability but operates as a mandatory factor in UK GDPR enforcement, requiring services 'likely to be accessed by children' to apply data protection impact

²¹ EU KIDS Act proposal, arts 8–13 (addictive design, art 9; recommender systems, art 10; default settings, art 11; contact safeguards, art 12; economic transactions, art 13).

²² EU KIDS Act proposal, arts 6(4), 29(2)–(3) and 32(2).

²³ EU KIDS Act proposal, provisions applying Chapter IV DSA (including the penalty regime in art 52 DSA) and Chapter IX of the AI Act; proposed addition to Annex I of Directive (EU) 2020/1828 (Representative Actions Directive).

²⁴ Freshfields, above n 19 (scope: online social networking services, video-sharing platforms, software application stores, online games, operating systems, AI companions and general conversational chatbots).

²⁵ Freshfields, above n 19; European Commission press release, above n 18.

²⁶ Loi n° 2023-566 du 7 juillet 2023 visant à instaurer une majorité numérique et à lutter contre la haine en ligne, JORF n°0157 (8 July 2023).

²⁷ Conseil constitutionnel, Décision n° 2026-911 DC du 14 août 2026.

assessments, high-privacy default settings, and prohibitions on nudge techniques and profiling-based advertising to under-18 users.²⁸ The Code's most prominent enforcement episode was the ICO's April 2023 monetary penalty of £12.7 million against TikTok for processing the data of an estimated 1.4 million under-13 UK users without parental consent and for failing to provide transparent information to child users a penalty TikTok has continued to contest on appeal even as the ICO opened a fresh 2025 investigation into TikTok's use of 13–17-year-olds' data for content recommendation.²⁹

The Online Safety Act 2023 supplements the Code with a statutory 'duty of care' requiring platforms to protect children from illegal content and from content harmful to children, enforced by Ofcom with penalties of up to £18 million or 10% of global turnover, whichever is higher.³⁰ Ofcom's early enforcement record including a £1 million penalty against AVS Group in December 2025 and a £520,000 penalty against 4chan in March 2026 for non-compliance with age-verification duties signals a regulator prepared to act against both mainstream and fringe platforms alike.

D. The United States

The U.S. federal framework remains the narrowest of the five jurisdictions studied, anchored in the Children's Online Privacy Protection Act, 1998 ("COPPA"), which applies only to actual or constructive knowledge of data collection from children under 13.³¹ The FTC's amended COPPA Rule, effective from June 2025 with a compliance deadline of 22 April 2026, introduced a separate opt-in consent requirement before disclosing children's data to third parties for targeted advertising, mandated written data-retention limits and information-security programmes, and expanded the definition of 'personal information' to capture biometric identifiers.³² Legislative efforts to widen COPPA's scope to teenagers up to 16–17 known as 'COPPA 2.0' and to impose a broader duty of care on platforms the Kids Online Safety Act ("KOSA") passed the Senate unanimously on 5 March 2026 but stalled repeatedly in the House. The two bills, along with over a dozen further child-safety proposals, were eventually consolidated into the omnibus Kids Internet and Digital Safety ('KIDS') Act, H.R. 7757, which passed the House 267–117 on 29 June 2026 notably after KOSA's central 'duty of care' provision was stripped out at the insistence of House negotiators, prompting the original Senate sponsors of KOSA to declare the House version unacceptable. As of September 2026, the U.S. KIDS Act remains pending in the Senate, with its fate uncertain.³³

Enforcement, meanwhile, has proceeded vigorously under existing law. The FTC's 2022 settlements with Epic Games (discussed in Part V.D below) and the DOJ-FTC's joint 2024 COPPA suit against TikTok and ByteDance, which culminated in an August 2026 settlement of US\$400 million, together with Meta's August 2026 settlement of related claims with 29 U.S. states, illustrate a pattern of aggressive ex post enforcement filling the gap left by stalled ex ante legislation.³⁴ At the sub-federal level, California's Age-Appropriate Design Code Act (AB 2273), modelled directly on the UK Children's Code, was substantially enjoined on First Amendment grounds by the Ninth Circuit in *NetChoice, LLC v Bonta*, illustrating the same free-expression tension that later derailed the French s. 15 ban.³⁵

E. India

India's Digital Personal Data Protection Act, 2023 ('DPDP Act') fixes the digital age of majority at 18 the highest threshold among the jurisdictions surveyed and requires verifiable parental consent before processing the personal data of any person below that age.³⁶ Section 9(2) prohibits processing that is detrimental to a child's well-being; section 9(3) bans behavioural tracking and targeted advertising directed at children; and sections 9(4)–(5)

²⁸ Information Commissioner's Office, *Age Appropriate Design: A Code of Practice for Online Services* (2020), issued under Data Protection Act 2018, s 123.

²⁹ Information Commissioner's Office, *Monetary Penalty Notice: TikTok Inc and TikTok Information Technologies UK Ltd* (4 April 2023); Handley Gill, 'ICO Children's Code Strategy 2024–25 Progress Update' (March 2025).

³⁰ Online Safety Act 2023 (UK), ss 11–12, 143.

³¹ Children's Online Privacy Protection Act 1998, 15 USC §§ 6501–6505.

³² 16 CFR pt 312 (Children's Online Privacy Protection Rule), as amended, 90 Fed Reg 16572 (22 April 2025).

³³ Kids Internet and Digital Safety Act, HR 7757, 119th Cong (2026); Congressional Research Service, 'The House Passes the KIDS Act', CRS Legal Sidebar LSB11465 (3 August 2026).

³⁴ *Federal Trade Commission v Epic Games Inc*, Case No 5:22-cv-00518 (EDNC, settlement approved 2023); *United States v TikTok Inc and ByteDance Ltd* (DDC, settled August 2026); Wikipedia, 'Children's Online Privacy Protection Act' (accessed September 2026), summarising the state settlements.

³⁵ *NetChoice LLC v Bonta*, 113 F4th 1101 (9th Cir 2024).

³⁶ Digital Personal Data Protection Act 2023 (India), s 9(1).

empower the Central Government to create class- and purpose-based exemptions, later operationalised for healthcare, education, childcare and transport-safety services.³⁷

The long-awaited Digital Personal Data Protection Rules, 2025, notified on 13 November 2025 alongside the formal constitution of the Data Protection Board of India, operationalise section 9 through Rules 10–12 and the Fourth Schedule. Rule 10 requires a Data Fiduciary to adopt technical and organisational measures ensuring that the person consenting is verifiably an identifiable adult, through either (a) reference to reliable identity and age details already held by the fiduciary, or (b) a virtual token issued by an entity offering digital-locker services, mapped to identity and age information, such as India's DigiLocker infrastructure.³⁸ Rule 12, read with the Fourth Schedule, provides conditional exemptions from the verifiable-consent and no-tracking requirements for specified classes of fiduciaries healthcare and mental-health establishments, educational institutions, and childcare providers where processing is strictly necessary for child welfare, safety or educational purposes.

Implementation is staggered: the Data Protection Board became operative immediately upon notification; the Consent Manager framework takes effect twelve months later (13 November 2026); and the substantive consent and children's-data obligations including verifiable parental consent become enforceable eighteen months after notification, on 13 May 2027, giving platforms a compliance runway that commentators have characterised as generous relative to the technical complexity of building parent-linked, auditable consent infrastructure across India's 22 scheduled languages.³⁹ India's approach is thus best characterised as a hard-identity-assurance model closer in spirit to the UK's design-code approach than to the EU's proportionate, risk-tiered approach to age assurance layered onto the highest digital-majority threshold (18) among the five jurisdictions studied, a combination that maximises formal protection but raises acute questions of proportionality, data minimisation, and inclusion of children without access to formal identity documents, which this paper returns to in Part V.B.

Beyond data-protection law, India is also now weighing a dedicated, access-level regime for minors' use of social media, and here too the direction of central policy is towards graded rather than prohibitive regulation. The Economic Survey 2025–26 recommended that age-based access limits be considered, on the footing that younger users are more vulnerable to compulsive use and harmful content, and that platforms be made responsible for enforcing age verification and age-appropriate defaults, particularly in respect of social media, gambling applications, auto-play features and targeted advertising.⁴⁰ In February 2026 the Union Minister for Electronics and Information Technology confirmed that the Government was discussing age-based restrictions with social-media companies, and in March 2026 senior officials were reported to be preparing a separate central statute for all users under 18 that would deliberately stop short of a blanket ban.⁴¹ As reported, the proposal divides minors into three tiers: the strictest controls for children aged 8 to 12; controlled and monitored access for those aged 12 to 16; and comparatively flexible access, subject to safeguards, for those aged 16 to 18. Reported accompanying measures include parental consent for platform access, daily usage limits, restrictions on evening and night-time log-ins, and enhanced platform accountability, although the specific obligations attaching to each tier have not been disclosed.⁴² The Ministry of Electronics and Information Technology ('MeitY') has since held several rounds of discussion with platforms on the technical feasibility of age-based access controls, and in August 2026 the Electronics and IT Secretary confirmed that consultations were continuing, including on proposals to restrict access for users under 16.⁴³ The legislation was reportedly targeted for the 2026 Monsoon Session after public consultation; as of August 2026, however, consultations were still under way and no Government Bill had been tabled, so the tiered model should be read as a reported policy direction rather than a settled legislative text.

The Centre's graded proposal sits alongside markedly more prohibitive initiatives. In December 2025 the Madras High Court urged the Union to consider Australia-style restrictions; on 6 March 2026 the Karnataka Chief Minister announced in his budget speech that children under 16 would be barred from social media, while Andhra Pradesh

³⁷ Digital Personal Data Protection Act 2023 (India), s 9(2)–(5).

³⁸ Digital Personal Data Protection Rules 2025 (India), r 10; Fourth Schedule.

³⁹ Digital Personal Data Protection Rules 2025 (India), r 1(3) read with the notification timeline; see Nick Palmieri, 'India Notifies Final Rules for Digital Data Protection Act' (Baker Botts OurTake, 20 November 2025).

⁴⁰ Government of India, Ministry of Finance, Economic Survey 2025–26 (January 2026); see Bernama-Anadolu, 'Government Advisor Proposes Age-Based Policies on Access to Digital Platforms in India' (31 January 2026).

⁴¹ Bloomberg Law, 'India Discussing Age-Based Social Media Curbs, Minister Says' (17 February 2026); MediaNama, 'Centre Plans Separate Law for Graded, Age-Based Social Media Restrictions for Children' (March 2026), reporting The Indian Express.

⁴² Kerala Kaumudi, 'Curbing Screen Time: Government Explores Limits on Minors' Social Media Use' (9 March 2026); MediaNama (n above); Subimal Bhattacharjee, 'Social Media Age Limits: Why India Is Choosing a Graded Approach' (The Quint, 13 March 2026).

⁴³ Storyboard18, 'Centre Weighs Curbs on Children's Social Media Use, Explores Age-Based Restrictions amid Rising Concerns' (26 March 2026); Telangana Today, 'Government Mulls Ban on Social Media for Children Under 16' (11 August 2026).

signalled restrictions for children under 13; and three private members' Bills proposing age-based restrictions were listed for introduction in Parliament, among them the Social Media (Age Restrictions and Online Safety) Bill moved by Lavu Sri Krishna Devarayalu MP, which would prohibit under-16s from creating or maintaining accounts and place the entire onus of age assurance on platforms.⁴⁴ India thus presently exhibits, within a single jurisdiction, the same contest between graded and prohibitive models that this paper traces across jurisdictions (Figure 3).

Three features of the Centre's tiered model merit emphasis. First, it would carry the graded, evolving-capacities logic of Article 5 UNCRC and General Comment No. 25 from the plane of data-processing consent to the plane of platform access itself, aligning India's direction more closely with the staged 13/15 model of the proposed EU KIDS Act (Part IV.A) than with Australia's undifferentiated under-16 floor (Part IV.F). Secondly, a central statute would avert a patchwork of State-level bans: online services transcend State boundaries, and the legislative competence of States to regulate online intermediaries is itself open to question, given that 'other like forms of communication' fall within Entry 31 of the Union List. Thirdly, the proposal would have to be reconciled with the DPDP regime: section 9 already fixes 18 as the threshold for verifiable parental consent across all processing, so a statute contemplating differentiated access for 16–18-year-olds would need either to operate through the exemption powers in section 9(4)–(5) or to accompany a recalibration of that threshold. Any access-level restriction will, moreover, have to satisfy Article 19(1)(a) of the Constitution, read with the reasonable-restrictions clause in Article 19(2) and the proportionality standard articulated in *Puttaswamy* and applied to internet restrictions in *Anuradha Bhasin v Union of India*,⁴⁵ the same expression-based objection on which the French ban foundered (Part IV.B). Digital-rights advocates have further warned that broad restrictions could curtail children's access to information and expression and deepen India's digital gender divide if families use them to keep girls offline,⁴⁶ a concern that a graded, service-differentiated design is better placed to accommodate than an outright ban.

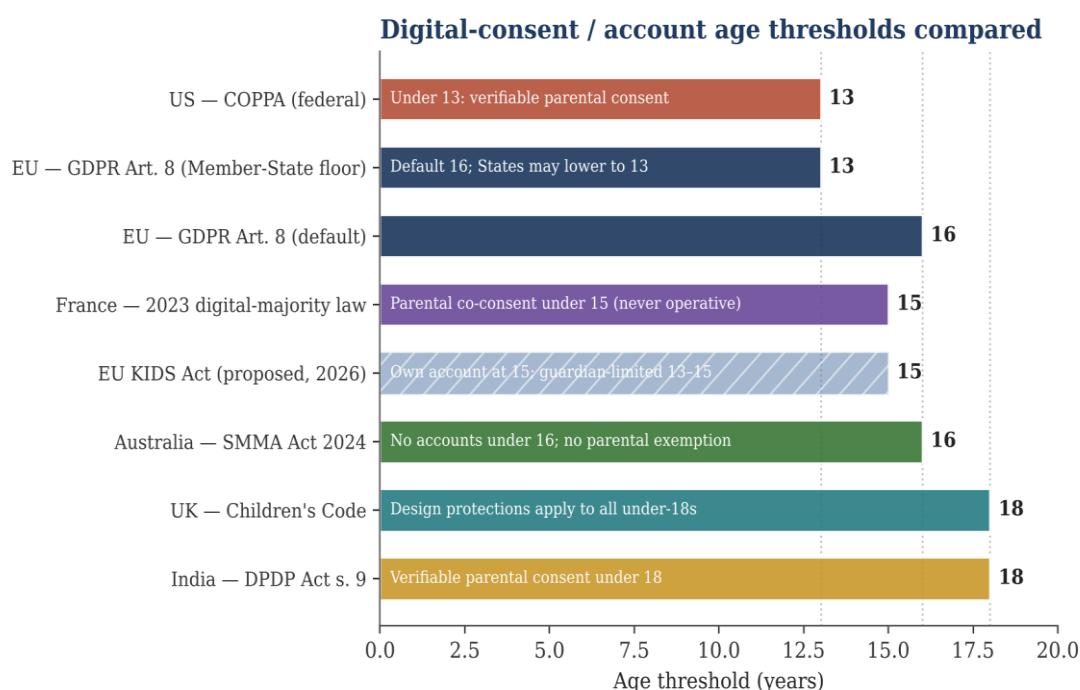
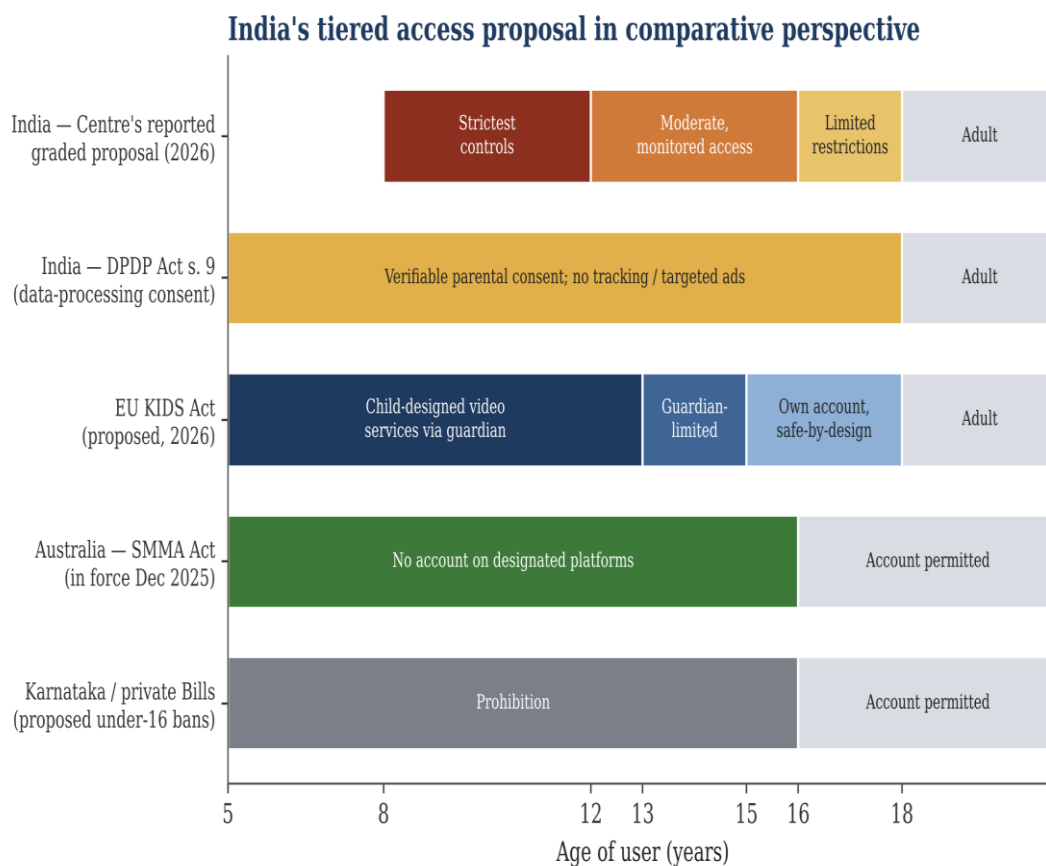


Figure 2: Comparative age thresholds for digital consent or platform-account verification across the jurisdictions and instruments surveyed, including the proposed EU KIDS Act (author's compilation from the primary sources cited in Part IV).

⁴⁴ TechCrunch, 'India's Karnataka Signals Intent to Ban Social Media for Under-16s' (March 2026); Reuters, 'Modi Ally Proposes Social Media Ban for India's Teens as Global Debate Grows' (2026); CXO Digital Pulse, 'Three Parliamentary Bills Propose Age-Based Restrictions on Social Media Access' (2026).

⁴⁵ Justice K.S. Puttaswamy (Retd) v Union of India, (2017) 10 SCC 1; Anuradha Bhasin v Union of India, (2020) 3 SCC 637; Constitution of India, Seventh Schedule, List I, Entry 31.

⁴⁶ TechCrunch (n above), reporting the concerns of Indian digital-rights groups.



Indian tiers as reported in official briefings (Mar 2026); specific measures per tier undisclosed. Treatment of under-8s not reported.

Figure 3: India's reported three-tier model of graded social-media access (8–12, 12–16, 16–18) compared with the DPDP Act's single consent threshold, the proposed EU KIDS Act, Australia's under-16 floor and the prohibition-style Indian State and private-member proposals (author's compilation from the sources cited in Part IV.E; the Indian tiers are as reported and remain subject to legislative drafting).

F. A Sixth Data Point: Australia's Minimum-Age Experiment

Although outside this paper's core five-jurisdiction comparison, Australia's Online Safety Amendment (Social Media Minimum Age) Act 2024 merits brief attention as the world's first enforced, blanket social-media age floor. In force from 10 December 2025, the Act requires designated platforms including Facebook, Instagram, TikTok, Snapchat, YouTube, X, Reddit and Threads to take 'reasonable steps' to prevent under-16s from holding accounts, with civil penalties of up to AUD 49.5 million for systemic non-compliance, and, distinctively, removes parental consent as a basis for exemption altogether.⁴⁷ Early implementation data complicate the policy's claimed efficacy: the eSafety Commissioner reported roughly 4.7 million under-16 accounts removed by mid-December 2025, yet an independent BMJ-published survey of Australian adolescents found more than 85% of under-16 respondents still using restricted platforms three months after the ban took effect, chiefly through circumvention rather than continued lawful access a finding with significant implications for the feasibility of prohibition-based models generally, and a useful empirical counterpoint to France's own subsequently abortive attempt at a similar ban.⁴⁸

⁴⁷ Online Safety Amendment (Social Media Minimum Age) Act 2024 (Cth); eSafety Commissioner, 'Social Media Age Restrictions' (updated September 2026).

⁴⁸ Techxplore, 'Little Evidence That Australia's Under-16 Social Media Restrictions Have Curbed Use Among Adolescents' (25 June 2026), reporting on a study published in The BMJ.

Regulatory-intensity matrix (law in force, Sept 2026)

European Union	Strong	Partial	Strong	Partial	Partial	Strong
France	Absent/ Weak	Partial	Partial	Partial	Absent/ Weak	Partial
United Kingdom	Strong	Strong	Partial	Partial	Partial	Strong
United States	Absent/ Weak	Absent/ Weak	Partial	Partial	Absent/ Weak	Strong
India	Partial	Strong	Strong	Absent/ Weak	Absent/ Weak	Partial
	Age-appropriate design	Age assurance	Profiling-ad restriction	Child-specific dark-pattern rules	Child participation	Enforcement quantum

Figure 4: Comparative regulatory-intensity matrix across five core jurisdictions, scored qualitatively (Absent/Weak – Partial – Strong) against six structural regulatory pillars. The assessment is the author’s own composite synthesis of the primary legal materials discussed in Part IV, and is offered as an illustrative, not a precise quantitative, comparison.

V. Analysis and Discussion

This Part undertakes a thematic, cross-cutting analysis of the eight problem-areas identified in the Introduction, drawing on the comparative material developed in Part IV to test whether the emerging global regulatory consensus is adequate to the structural features of the contemporary attention economy.

A. Age-Appropriate Design

‘Age-appropriate design’ denotes a regulatory technique that shifts the locus of obligation from the point of data collection (classical consent-based privacy law) to the point of product design itself requiring that default settings, interface choices and feature availability be calibrated to a child’s likely age and developmental stage, irrespective of whether the child or a parent later exercises any privacy choice. The UK’s Children’s Code was the first comprehensive legal articulation of this approach, and its fifteen standards including high-privacy defaults, geolocation-off-by-default, and a prohibition on ‘nudge techniques’ that lead children to provide more data or weaken their privacy protections have since been substantially replicated in the EU’s Article 28 DSA guidelines and echoed, in more limited form, in the FTC’s 2025 amended COPPA Rule. The Commission’s proposed EU KIDS Act (Part IV.A) would take the next step of converting these design expectations from guidance into binding regulation, applying safe-by-design defaults to all users until they are established to be adults.

The doctrinal significance of age-appropriate design is that it converts an ex-post, harm-contingent model of liability into an ex-ante, structural obligation platforms must build safety in, rather than merely respond to demonstrated harm or an individual user’s failure to activate a privacy setting. This tracks precisely the ‘children’s rights by design’ methodology articulated in General Comment No. 25, and represents perhaps the single most successful transplant of the Committee’s soft-law guidance into binding comparative law. Its principal limitation is scope-definition: because the relevant trigger in most instruments is a service ‘likely to be accessed by children’, platforms face strong incentives either to over-comply (restricting general-audience content for all users) or to contest the trigger altogether through age-assurance gatekeeping which leads directly to the second theme.

B. Age Assurance and Verification

Age assurance the umbrella term for the spectrum of techniques used to establish or estimate a user’s age, ranging from self-declaration through algorithmic age-estimation (commonly via facial-analysis software) to hard identity verification against government-issued credentials has emerged as the single most contested technical and legal question across every jurisdiction surveyed in Part IV. The European Commission’s own guidance frames age assurance and age restriction as analytically distinct: assurance is merely instrumental to restriction, and the intensity of the assurance method deployed should be proportionate to the severity of risk posed by the underlying service.

The central legal tension is between child protection and the privacy, expression and inclusion interests of all users, including adults. Robust identity verification necessarily requires that every user not merely children prove their age, typically through submission of a government identity document or biometric data to either the platform or a trusted third-party intermediary. The French Conseil constitutionnel's censure of the s. 15 social-media ban crystallises this tension with unusual clarity: the court did not doubt the legitimacy of the child-protection objective, but held that a scheme requiring universal age-proof, without calibrated legal safeguards on data handling, retention and proportionality, disproportionately burdened the Article 11 expression rights of the entire user population, adult and minor alike.⁴⁹

India's Rule 10 approach verifiable parental consent anchored to DigiLocker-style government digital-identity infrastructure attempts to resolve the proportionality problem through data minimisation at the architectural level: rather than platforms collecting and retaining raw identity documents, a token-based system allows a trusted intermediary to attest that verification occurred without transmitting the underlying identity data to the platform itself. This 'prove-without-disclosing' architecture mirrors the EU's own planned Digital Identity Wallet and its April 2026 age-verification blueprint, suggesting an emerging global technical consensus on privacy-preserving verification design even where political consensus on whether verification should be mandatory at all remains elusive.⁵⁰ Nonetheless, empirical concerns persist: the wave of age-verification-related data breaches recorded through 2025–2026 illustrates that any system requiring centralised identity data even ostensibly minimised or tokenised creates a fresh honeypot of sensitive information, and Australia's post-implementation data showing that over 85% of surveyed under-16 users retained access to restricted platforms three months after its ban demonstrates that even a well-resourced, technically sophisticated verification regime faces serious circumvention risk in practice.

The EU KIDS Act would write this logic into binding law while adding a two-tier structure. For its minimum-age rules, providers would have to rely exclusively on certified EU age-verification solutions, of which the European Digital Identity Wallet is one; for the wider safety-by-design duties, more flexible methods remain permissible, provided they involve no identification, tracking or profiling, collect no more personal data than strictly necessary, use state-of-the-art technology and rely on zero-knowledge proofs, with a mandatory free complaint mechanism against erroneous results.⁵¹ The design thus concentrates the most intrusive verification where an access restriction is at stake and relaxes it elsewhere, which is broadly the risk-calibrated logic urged in Part VII. It does not, however, dissolve the proportionality question identified above: an under-15 account bar can be enforced only if every account holder, adults included, establishes their age, so the proposal's resilience under proportionality review will turn on whether the certified scheme delivers genuine data minimisation in practice.

C. Algorithmic Profiling and Behavioural Advertising

Profiling the automated processing of personal data to evaluate, predict or infer aspects of a person's behaviour, preferences or interests sits at the commercial core of the platforms this paper examines. For children, profiling raises acute concerns because recommendation systems trained to maximise engagement are agnostic to the psychological vulnerability of the user being optimised for; the same architecture that serves an adult a shopping advertisement can, for a child user, surface content correlated with eating-disorder communities, self-harm content or compulsive-use patterns, purely because such content statistically maximises engagement metrics among certain adolescent cohorts.

The regulatory response has coalesced, with unusual cross-jurisdictional convergence, around an outright prohibition on profiling-based advertising directed at minors: Article 28(2) of the EU's Digital Services Act flatly bans presenting advertisements to minors based on profiling using their personal data; India's section 9(3) DPDP Act bans behavioural monitoring and targeted advertising directed at children; and the U.S. KIDS Act, as passed by the House in June 2026, would for the first time impose a comparable federal ban on targeted advertising to minors, extending COPPA's currently narrow under-13 scope up to age 17.⁵² The UK's Children's Code similarly discourages profiling absent a demonstrable, child-specific best-interests justification, though as the ICO's still-pending 2025 investigation into TikTok's content-recommendation practices for 13–17-year-olds illustrates the

⁴⁹ Conseil constitutionnel, Décision n° 2026-911 DC du 14 août 2026; see similarly *NetChoice LLC v Bonta*, 113 F4th 1101 (9th Cir 2024) (California AADC).

⁵⁰ Digital Personal Data Protection Rules 2025 (India), r 10; European Commission, Recommendation on Establishing a Common EU-Wide Framework for Age Verification Technologies (29 April 2026).

⁵¹ EU KIDS Act proposal, art 29(4)–(5).

⁵² Digital Services Act (n 15), art 28(2); Digital Personal Data Protection Act 2023 (India), s 9(3); Crowell & Moring, 'House Passes KIDS Act H.R. 7757' (6 July 2026).

boundary between permissible content personalisation (arguably beneficial, enabling age-appropriate curation) and impermissible behavioural profiling (commercially exploitative) remains genuinely difficult to police at the level of algorithmic implementation, since both operate through functionally identical machine-learning architectures. The EU KIDS Act proposal would extend this convergence from advertising to recommender design itself, requiring recommender systems on social-networking and video-sharing services to give primary weight to a child's stated preferences, to disable implicit engagement signals by default, and to offer a non-profiling option.⁵³

D. Dark Patterns

Dark patterns user-interface designs engineered to manipulate, coerce or deceive users into decisions that serve the platform's commercial interest rather than the user's own preference constitute the most granular and behaviourally sophisticated of the four core themes. Common taxonomies distinguish confirmshaming, forced continuity, roach-motel design (easy sign-up, deliberately obstructed cancellation), and asymmetric choice architecture that makes privacy-protective options harder to locate or select than data-maximising defaults.

The paradigmatic enforcement precedent remains the FTC's 2022–2023 action against Epic Games, developer of Fortnite. The FTC's complaint alleged that Epic deployed a 'counterintuitive, inconsistent, and confusing' button configuration that caused players disproportionately children and teenagers, given Fortnite's demonstrated youth user base to incur unintended in-game purchases through a single, ambiguous button press, while separately alleging COPPA violations for collecting children's data without verifiable parental consent and enabling default on-by-default voice and text chat that exposed children to unmoderated contact with strangers.⁵⁴ Epic ultimately paid a combined US\$520 million a US\$275 million civil penalty for the COPPA violations (at the time, the largest penalty ever obtained for violation of an FTC rule) and a further US\$245 million in consumer refunds for the dark-patterns-induced purchases and agreed to structural remedies requiring privacy-protective defaults for all child and teen accounts going forward.⁵⁵

The Epic Games settlement is significant for three doctrinal reasons. First, it demonstrates that dark-patterns liability and children's-privacy liability, though analytically distinct causes of action, frequently arise from the same underlying design choices and can be pursued in parallel. Second, the scale of the penalty signals that regulators are prepared to treat manipulative design targeting children as comparably serious to, rather than derivative of, substantive privacy violations. Third, and most significantly for comparative purposes, no jurisdiction studied in Part IV has yet codified a free-standing statutory prohibition on dark patterns specifically calibrated to child users existing enforcement (in the U.S., under the FTC's general unfair-or-deceptive-practices authority; in the EU, under the DSA's general Article 25 dark-patterns provision, which applies to all users, not only children) still relies on general consumer-protection powers applied to facts involving child victims, rather than child-specific dark-patterns law. This is a significant regulatory gap that this paper's recommendations address in Part VII.

That observation, accurate as to enacted law, is about to be tested by the EU KIDS Act. If adopted, it would be the first instrument among those studied to prohibit addictive and manipulative design specifically for child users: it bans autoplay without effective interruption, notifications unrelated to the minor's activity, rewards for sharing or livestreaming, and streaks that penalise a child for not returning daily; it requires transactions to be flagged in real time, with virtual currency displayed in real money; and it prohibits variable rewards.⁵⁶ Because 'variable rewards' may reach the probabilistic mechanics of loot-box systems, the provision could also touch the monetisation architecture discussed in Part V.F, although the scope of the term will depend on the final text and its interpretation. Even so, the proposal remains a proposal, and the regulatory gap described above persists in every jurisdiction where law is currently in force.

⁵³ EU KIDS Act proposal, art 10.

⁵⁴ In re Epic Games Inc, FTC File No 192-3203 (settlement announced 19 December 2022, finalised 14 March 2023).

⁵⁵ Federal Trade Commission v Epic Games Inc, Case No 5:22-cv-00518 (EDNC 2023) (stipulated order); FTC Press Release, 'Epic Games to Pay \$520 Million' (19 December 2022).

⁵⁶ EU KIDS Act proposal, arts 9 and 13.

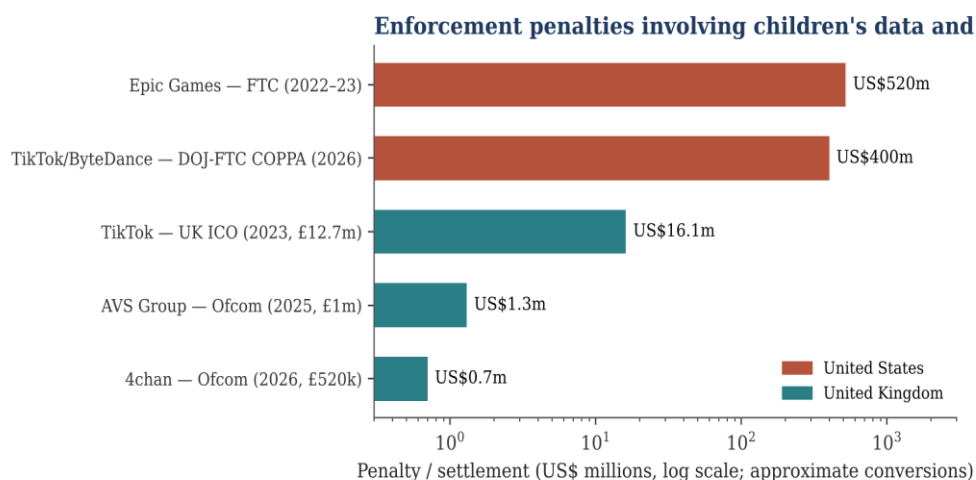


Figure 5: Illustrative order-of-magnitude comparison of recent enforcement penalties and settlements involving children's data and dark-patterns violations (author's compilation; figures approximate and converted to US dollars where necessary for comparability).

E. Children's Autonomy and Participation

A recurring critique in the literature reviewed in Part II is that even well-intentioned child-protection regulation risks reproducing a paternalistic conception of the child as a passive object of regulation rather than a rights-holder entitled, under Article 12 UNCRC, to be heard in matters affecting them. General Comment No. 25 explicitly requires States to facilitate children's participation in the development of laws, policies and standards relating to the digital environment a requirement the Committee itself modelled by consulting 709 children directly in drafting the Comment.

Measured against this participatory benchmark, the comparative record in Part IV is mixed at best. India's DPDP Rules, EU's DSA guidelines, and the UK's Children's Code were each developed through public and multi-stakeholder consultation processes, but none formally embedded child-participant consultation as a structural requirement of the rule-making process itself, in contrast to the Committee's own practice. Australia's eSafety Commissioner is a partial exception, having appointed a Stanford University-led academic advisory group specifically to assess the social media Minimum Age Act's real-world impact on children, incorporating adolescent experience data directly into the regulatory feedback loop. The broader risk is that a uniformly protection-oriented regulatory posture particularly one built around outright bans, as France and Australia have each attempted forecloses precisely the participatory and expressive digital spaces (activism, creative expression, peer support communities, access to information on sensitive health or identity topics) that General Comment No. 25 identifies as core UNCRC entitlements, disproportionately affecting marginalised children for whom the digital environment may be the only accessible forum for such participation.

F. Economic Exploitation and the Commodification of Children's Data and Attention

Beneath the four preceding themes lies a common structural driver: the contemporary digital economy's business model, in which user attention and behavioural data function as the primary commercial asset, monetised principally through targeted advertising and, increasingly, through direct micro-transactions embedded within child-oriented products such as freemium games. Epic Games' Fortnite generating billions of dollars in revenue substantially through in-game currency purchases by a majority-adolescent player base is emblematic of a wider 'pester power' monetisation model in which game design deliberately engineers psychological pressure toward continued spending, often exploiting children's comparatively immature understanding of money's real-world value when abstracted into virtual currency.

General Comment No. 25 addresses this directly, requiring States to prohibit the practice of ill-defined or hidden persuasive marketing techniques directed at children, and to ensure any advertising and marketing content is distinguishable from other content and identified as such to children in a manner appropriate to the child's age. Comparative law has begun to operationalise this principle unevenly: India's section 9(3) prohibition on targeted advertising, the EU's Article 28(2) profiling-advertising ban, and the emerging U.S. KIDS Act framework each restrict data-driven targeting, but none directly regulates the underlying monetisation mechanics of in-app virtual currency and loot-box-style probabilistic purchase systems that most directly implicate the economic-exploitation concern a regulatory blind spot better addressed, so far, through general consumer-protection and gambling-adjacent regulatory frameworks in a small number of jurisdictions (Belgium and the Netherlands, for instance,

have separately classified certain loot-box mechanics as unlicensed gambling) than through children's-rights-specific instruments. The EU KIDS Act's Article 13, which would require real-time flagging of in-app transactions, display of virtual currency in real money and a ban on variable rewards, would, if adopted, be among the first provisions within a children-specific instrument to address this monetisation layer directly, though it remains a proposal.

G. Responsibilities of Digital Platforms

General Comment No. 25's most consequential doctrinal move is its clear statement that States parties' obligations under the UNCRC extend horizontally to require regulation of private business enterprises, including a requirement that businesses undertake child-rights due-diligence identifying, preventing and mitigating adverse impacts on children's rights across their design, operation and business-model choices rather than treating the child-rights impact of a digital product as an externality to be addressed only through downstream, ex post regulatory correction.⁵⁷

The comparative material in Part IV shows this due-diligence obligation operationalised through at least four distinct legal mechanisms: (i) mandatory data protection impact assessments specific to child users, as under the UK Children's Code and, functionally, the EU DSA's systemic risk-assessment obligations for Very Large Online Platforms; (ii) design-mandated default settings, converting privacy and safety protection from an opt-in choice into an architectural baseline; (iii) transparency and reporting obligations, requiring platforms to disclose their child-safety risk assessments and mitigation measures to regulators (and, under the DSA, to the public); and (iv) direct financial liability calibrated to global turnover up to 6% of global annual revenue under the DSA, 4% under UK GDPR-linked Children's Code enforcement, and substantial per-violation penalties under COPPA designed to internalise the cost of non-compliance at a scale commensurate with platforms' global revenues. What remains comparatively underdeveloped across all five jurisdictions is a private right of action allowing children or their guardians to sue platforms directly for design-based harms, as opposed to relying exclusively on public regulatory enforcement; this gap is addressed in the Recommendations in Part VII.

The EU KIDS Act would add to each of these mechanisms. Very Large Online Platforms would be required to notify a compliance plan to the Commission and to commission an independent audit of it, with a public summary of the findings; the DSA penalty regime of up to 6% of worldwide annual turnover would apply; Commission supervision would be funded through an annual supervisory fee capped at 0.03% of each provider's worldwide annual net income; and the Act would be listed in Annex I to the Representative Actions Directive, allowing qualified entities to bring collective actions for injunctive or redress measures.⁵⁸ The last of these is not the individual private right of action whose absence is noted above, but it is a partial step towards private enforcement of design-based duties, and it strengthens the case for the recommendation made in Part VII.B.

VI. Findings

The comparative and thematic analysis in Parts IV and V yields the following principal findings.

Convergence on graduated regulation, divergence on mechanism: Every jurisdiction studied has moved, in principle, toward the graduated, risk-differentiated model endorsed by General Comment No. 25, rejecting both pure exclusion and pure laissez-faire. However, the mechanism chosen to operationalise graduation India's identity-token verification, the EU's proportionate multi-tier age-assurance guidance and its proposed 13/15 graduated-access model under the EU KIDS Act, the UK's design-code liability trigger, and the now-twice-failed French/Californian attempts at outright prohibition diverges sharply, producing significant compliance fragmentation for platforms operating across borders.

Prohibition-based models face a recurring constitutional ceiling: Both the French Conseil constitutionnel's August 2026 censure of the under-15 ban and the U.S. Ninth Circuit's substantial injunction of California's AADC in *NetChoice v Bonta* demonstrate that outright age-based prohibition, particularly where it requires universal age-verification of the entire user population, is acutely vulnerable to constitutional/fundamental-rights challenge on freedom-of-expression grounds a structural constraint that regulators favouring prohibition have twice now failed to design around.

Empirical efficacy of bans remains unproven: Australia's early implementation data with over 85% of surveyed under-16 respondents still accessing restricted platforms three months post-ban suggests that even a well-resourced, enforced prohibition regime achieves, at best, partial and possibly transient behavioural change, raising the question whether the policy objective (reduced youth engagement/harm exposure) is better achieved through the design-code and profiling-restriction routes than through account-level prohibition.

⁵⁷ General Comment No. 25 (2021) CRC/C/GC/25, paras 37, 39, 112–113.

⁵⁸ EU KIDS Act proposal, art 5 (compliance plans and independent audits) and the provisions on supervision, enforcement and the supervisory fee; Freshfields, above n 19.

Profiling-based advertising restriction is the clearest point of global legal consensus: Unlike age-verification mechanics, restrictions on profiling-based behavioural advertising directed at children command near-uniform support across the EU (Article 28(2) DSA), India (section 9(3) DPDP Act) and the pending U.S. KIDS Act, suggesting this is the area of digital child-rights law closest to a stable, transplantable global norm.

Dark patterns and platform monetisation architecture remain the least-regulated pillar: Despite the scale of the Epic Games settlement (US\$520 million), no jurisdiction studied has yet enacted a free-standing, child-specific statutory prohibition on manipulative interface design or probabilistic/loot-box monetisation mechanics; existing enforcement proceeds under general consumer-protection or privacy powers applied to facts involving children, rather than under bespoke child-dark-patterns law. The Commission's September 2026 EU KIDS Act proposal would, if adopted, begin to close this gap for child users in the EU (Part V.D), but it remains a proposal.

Age-verification technology itself generates new privacy risk: The shift toward hard identity- and biometric-based verification (India's DigiLocker-anchored tokens, the EU's forthcoming Digital Identity Wallet, various U.S. state-level document-upload regimes) creates fresh centralised repositories of sensitive identity data, and the wave of age-verification-linked data breaches recorded through 2025–2026 confirms this is not a merely theoretical risk. Privacy-preserving, token-based, zero-knowledge-style verification architecture is emerging as best practice but is not yet universally mandated.

Participation rights remain the least operationalised UNCRC pillar: Notwithstanding General Comment No. 25's explicit call for children's direct participation in the design of laws and digital products affecting them, formal child-consultation mechanisms remain rare in the domestic rule-making processes studied, with Australia's Stanford-partnered academic advisory group the most developed (if still exceptional) example.

Enforcement quantum is rising sharply and converging internationally: The trajectory from the UK's £12.7 million TikTok fine (2023) through Epic Games' US\$520 million settlement (2022–23) to TikTok/ByteDance's US\$400 million U.S. settlement and Meta's multistate settlement (both 2026) indicates that regulators across jurisdictions are converging on treating children's-data and dark-patterns violations as warranting penalties in the hundreds of millions of dollars a level of financial consequence increasingly comparable to major competition-law enforcement.

The EU is moving from soft-law guidance to hard-law, safety-by-design regulation of child users: The Commission's EU KIDS Act proposal (17 September 2026) would convert the Article 28 DSA Guidelines into binding obligations, extend them to online games, AI companions, conversational chatbots, app stores and operating systems, reverse the burden of proof onto providers, and pair a graduated 13/15 access model with certified, privacy-preserving age verification. If adopted substantially as proposed, it would narrow the gaps identified in Findings 5 and 6; but it remains unadopted, is unlikely to apply before 2028, and will inherit the proportionality challenge illustrated by Finding 2.

VII. Recommendations

Building on the findings above, this paper offers the following calibrated recommendations, addressed variously to international standard-setters, domestic legislators/regulators, and platforms themselves.

A. For International and Regional Standard-Setters

1. Develop a model law on privacy-preserving age assurance. The UN Committee on the Rights of the Child, in partnership with technical standard-setting bodies, should develop a model legal framework for token-based, zero-knowledge age-verification architecture building on the convergent technical direction already visible in the EU's Digital Identity Wallet and India's DigiLocker-anchored Rule 10 so that domestic legislatures are not each independently re-solving the same privacy-versus-verification trade-off with inconsistent safeguards.

2. Institutionalise child participation in standard-setting. Regional and domestic regulators should adopt a structural, not merely consultative, requirement to include children's direct testimony and preference data in the rule-making process for digital-child-safety regulation, following the methodology the Committee itself used in drafting General Comment No. 25, and the model Australia's eSafety Commissioner has begun to develop through its academic advisory group.

B. For Domestic Legislatures and Regulators

Enact child-specific dark-patterns prohibitions. Legislatures should follow the DSA's general Article 25 dark-patterns model but adopt a bespoke, more stringent, child-specific variant expressly prohibiting confirmshaming, forced continuity, and probabilistic/loot-box monetisation mechanics directed at or reasonably likely to be encountered by child users, closing the gap identified as Finding 5. The additive-design and in-app-transaction provisions of the proposed EU KIDS Act (Articles 9 and 13) offer an early legislative template.

Calibrate verification intensity to risk, not uniformly to age. Jurisdictions favouring hard identity verification, including India, should study the EU's proportionate, risk-tiered guidance model and consider layering self-declaration and behavioural age-estimation as lower-friction first-line tools for lower-risk services, reserving hard

identity/token verification for higher-risk categories, in order to reduce both the compliance burden and the privacy-risk surface created by universal hard verification. The EU KIDS Act's own two-tier structure, pairing certified verification for its minimum-age rules with more flexible assurance for its safety-by-design duties, is a supportive example.

Create a statutory private right of action. Consistent with Finding 8's account of rising public enforcement penalties, legislatures should complement public enforcement with a calibrated private right of action (potentially with statutory minimum damages, as under several U.S. state privacy statutes) allowing a child's guardian to sue a platform directly for design-based harms, reducing sole reliance on resource-constrained public regulators. The proposed listing of the EU KIDS Act in the Representative Actions Directive would be a partial step in this direction at EU level, enabling collective rather than individual claims.

Draft prohibition-style measures narrowly and with built-in proportionality safeguards. Legislatures contemplating an outright access ban, following France's and Australia's example, should build in from the outset the graduated, risk- and service-differentiated architecture that the French Conseil constitutionnel found lacking rather than a blanket, undifferentiated prohibition to withstand foreseeable constitutional and fundamental-rights review. The EU KIDS Act proposal, whose under-15 account bar applies only to services carrying specified risk functionalities, is an instructive example of such service-differentiated drafting.

Mandate interoperable, minimised age-verification infrastructure. Regulators should require that any mandated age-verification method satisfy an explicit data-minimisation standard verifying age without transmitting or retaining full identity documents to the platform as a precondition of lawful deployment, directly responding to Finding 6.

C. For Digital Platforms

Adopt children's-rights-by-design as an enterprise-wide default, not a jurisdiction-specific compliance overlay. Given the substantial convergence identified across the EU, UK, India and emerging U.S. frameworks (Finding 1 and Finding 4), platforms operating globally should adopt the most protective common standard profiling-advertising bans, high-privacy defaults, and dark-patterns-free monetisation flows for all users plausibly under 18 as a single global product baseline, rather than maintaining fragmented, jurisdiction-specific compliance configurations, both to reduce regulatory risk and to give substantive effect to the 'best interests' principle regardless of a user's country of residence.

Publish child-specific algorithmic-risk assessments. Platforms should proactively publish (not merely submit to regulators) child-specific risk assessments of their recommendation systems, following the transparency logic of the EU DSA's systemic-risk-assessment regime, to enable independent academic and civil-society scrutiny of the profiling/content-recommendation boundary discussed in Part V.C.

CONCLUSION

The governance of childhood in the digital environment sits at an unusually volatile juncture. Within the twelve months preceding this paper's completion alone, India notified its long-awaited DPDP Rules, the European Commission issued a continent-wide age-verification Recommendation and followed it with its proposed EU KIDS Act, the United States House of Representatives passed the most significant federal child-online-safety legislation in a generation, Australia became the first country to enforce and to generate the first sobering efficacy data on a blanket social-media age floor, and France's Parliament and its highest constitutional court staged, within a single month, first the adoption and then the annulment of an equivalent domestic ban. This is not a settled field of law; it is a field in the process of being written.

This paper has argued that the most durable insight to emerge from this turbulent comparative moment is the UNCRC Committee's own: that childhood in the digital environment cannot be governed adequately through either blanket exclusion or unregulated access, but requires a graduated architecture that treats children as rights-holders with evolving autonomy, casts enforceable, design-level obligations on the platforms that profit from their attention and data, and crucially, and still most incompletely realised involves children themselves in shaping the rules that govern their digital lives. The regulatory instruments examined in this paper age-appropriate design codes, proportionate age-assurance frameworks, profiling-advertising bans, and the beginnings of child-specific dark-patterns law each operationalise a fragment of this architecture. None, on the evidence reviewed here, yet operationalises the whole. The EU KIDS Act, proposed as this paper neared completion, is the most ambitious attempt to assemble several of these fragments in a single binding instrument, but it remains a proposal whose passage, and whose proportionality, are yet to be tested. Closing that gap, coherently and without repeating the constitutional missteps of the French and Californian experiments, is the central unfinished task of child-rights law in the digital age.

REFERENCES

1. International Instruments
2. Convention on the Rights of the Child (adopted 20 November 1989, entered into force 2 September 1990) 1577 UNTS 3.
3. UN Committee on the Rights of the Child, General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment, CRC/C/GC/25 (2 March 2021).
4. UN Committee on the Rights of the Child, 'In Our Own Words Children's Rights in the Digital World' (child-friendly version of General Comment No. 25, March 2021).
5. Legislation and Subordinate Legislation
6. Digital Personal Data Protection Act 2023 (India).
7. Digital Personal Data Protection Rules 2025 (India), notified 13 November 2025.
8. Information Technology Act 2000 (India).
9. Social Media (Age Restrictions and Online Safety) Bill 2026, private member's Bill (Lok Sabha) (India).
10. Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1.
11. Regulation (EU) 2022/2065 (Digital Services Act) [2022] OJ L277/1.
12. European Commission, Guidelines on the Protection of Minors under Article 28 DSA (14 July 2025).
13. European Commission, Recommendation on Establishing a Common EU-Wide Framework for Age Verification Technologies (29 April 2026).
14. European Commission, Proposal for a Regulation on Keeping Internet Digital Spaces Accountable and Trustworthy ('EU KIDS Act') (17 September 2026).
15. Loi n° 2023-566 du 7 juillet 2023 visant à instaurer une majorité numérique et à lutter contre la haine en ligne, JORF n°0157 (8 July 2023) (France).
16. Loi visant à protéger les mineurs des risques auxquels les expose l'utilisation des réseaux sociaux, adopted by the French Parliament 21 July 2026 (subsequently censured; France).
17. Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et réguler l'espace numérique (loi SREN) (France).
18. Data Protection Act 2018 (UK), s 123.
19. Information Commissioner's Office, Age Appropriate Design: A Code of Practice for Online Services (2020) (UK).
20. Online Safety Act 2023 (UK).
21. Children's Online Privacy Protection Act 1998, 15 USC §§ 6501–6505 (USA).
22. 16 CFR pt 312 (Children's Online Privacy Protection Rule), as amended, 90 Fed Reg 16572 (22 April 2025) (USA).
23. Kids Internet and Digital Safety Act, HR 7757, 119th Congress (2026) (USA).
24. Children and Teens' Online Privacy Protection Act ('COPPA 2.0'), S 836, 119th Congress (2026) (USA).
25. California Age-Appropriate Design Code Act, AB 2273 (2022) (USA).
26. Online Safety Amendment (Social Media Minimum Age) Act 2024 (Cth) (Australia).
- 27.
28. Cases and Regulatory Decisions
29. Conseil constitutionnel, Décision n° 2026-911 DC du 14 août 2026 (France).
30. NetChoice LLC v Bonta, 113 F4th 1101 (9th Cir 2024) (USA).
31. Federal Trade Commission v Epic Games Inc, Case No 5:22-cv-00518 (EDNC 2023) (stipulated order) (USA).
32. In re Epic Games Inc, FTC File No 192-3203 (settlement announced 19 December 2022, finalised 14 March 2023) (USA).
33. United States v TikTok Inc and ByteDance Ltd (DDC, settled August 2026) (USA).
34. Information Commissioner's Office, Monetary Penalty Notice: TikTok Inc and TikTok Information Technologies UK Ltd (4 April 2023) (UK).
35. Justice K.S. Puttaswamy (Retd) v Union of India, (2017) 10 SCC 1 (right to privacy as a fundamental right, India).
36. Anuradha Bhasin v Union of India, (2020) 3 SCC 637 (proportionality of internet restrictions, India).
- 37.
38. Books, Articles and Reports
39. Christian Djéffal, 'Children's Rights by Design and Internet Governance: Revisiting General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment' (2022) 11 Laws 84.
40. Colin M Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt and Austin L Toombs, 'The Dark (Patterns) Side of UX Design' (2018) Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems
41. Sonia Livingstone, Leslie Haddon, Anke Görzig and Kjartan Ólafsson, Risks and Safety on the Internet: The Perspective of European Children (EU Kids Online, LSE 2011).

42. Sonia Livingstone and Amanda Third, 'Children and Young People's Rights in the Digital Age: An Emerging Agenda' (2017) 19 *New Media & Society* 657.
43. Valerie Steeves, 'Terra Cognita: Surveillance of Students' in Emmeline Taylor and others (eds), *Surveillance Futures* (Routledge 2018) 87.
44. Shoshana Zuboff, 'Big Other: Surveillance Capitalism and the Prospects of an Information Civilization' (2015) 30 *Journal of Information Technology* 75.
45. Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs 2019).
46. Digital Futures for Children (LSE), 'Impact of General Comment No. 25' (research report, March 2026).
47. Interface (EU think tank), 'Mind the Gap: Age Assurance in the EU' (policy paper, October 2025).
48. Congressional Research Service, 'The House Passes the KIDS Act', CRS Legal Sidebar LSB11465 (3 August 2026).
49. Nick Palmieri, 'India Notifies Final Rules for Digital Data Protection Act' (Baker Botts OurTake, 20 November 2025).
50. Crowell & Moring LLP, 'House Passes KIDS Act H.R. 7757: What Online Platforms Must Know Before Senate Showdown' (6 July 2026).
51. Loeb & Loeb LLP, 'Children's Online Privacy in 2026: Congress Stalls (Again), FTC Signals Priorities' (30 June 2026).
52. Handley Gill, 'ICO Children's Code Strategy 2024–25 Progress Update' (March 2025).
53. Techxplore, 'Little Evidence That Australia's Under-16 Social Media Restrictions Have Curbed Use Among Adolescents' (25 June 2026), reporting on a study published in *The BMJ*.
54. eSafety Commissioner (Australia), 'Social Media Age Restrictions' (updated September 2026).
55. Le Club des Juristes, 'Réseaux sociaux interdits aux moins de 15 ans: la France peut-elle trouver une voie de passage?' (September 2026).
56. European Commission, 'EU KIDS Act to restrict social media platforms' access to children in the EU' (press release, 17 September 2026).
57. Freshfields Bruckhaus Deringer, 'The EU KIDS Act: Europe moves online child safety beyond social media bans' (18 September 2026).
58. Wilson Sonsini, 'European Commission Proposes "EU KIDS Act" to Restrict Children's Access to Online Services' (September 2026).
59. Government of India, Ministry of Finance, *Economic Survey 2025–26* (January 2026).
60. Subimal Bhattacharjee, 'Social Media Age Limits: Why India Is Choosing a Graded Approach' (*The Quint*, 13 March 2026).
61. MediaNama, 'Centre Plans Separate Law for Graded, Age-Based Social Media Restrictions for Children' (March 2026).
62. Storyboard18, 'Centre Weighs Curbs on Children's Social Media Use, Explores Age-Based Restrictions amid Rising Concerns' (26 March 2026).
63. *Telangana Today*, 'Government Mulls Ban on Social Media for Children Under 16' (11 August 2026).
64. TechCrunch, 'India's Karnataka Signals Intent to Ban Social Media for Under-16s' (March 2026).