LAARC

WHY BLANKET BANS ARE NOT THE ANSWER TO ONLINE CHILD SAFETY IN SRI LANKA

Authored By:

Kasun Kavishka and Nethmi Yashodya Weerakoon

Acknowledgement

Authors

K. H. Kasun Kavishka

Bachelor of Laws (Hons.) (Colombo) (Reading)

D. Nethmi Yashodya Weerakoon

Bachelor of Laws (Hons.) (Colombo) (Reading)

This research report was conducted under the Spectrum Research Initiative, carried out by the Lalith Athulathmudali Research Centre (LAARC).

Table of Contents

Abstract

Recent incidents of online child exploitation and the viral spread of non-consensual content in Sri Lanka have intensified public and governmental calls for stricter regulation of minors' access to social media. This paper examines whether a blanket ban on social media for children is a legally sound and practically effective response to the growing problem of Online Child Sexual Exploitation and Abuse (OCSEA). The central research question asks whether prohibition-based regulation can adequately address the structural causes of online harm while remaining consistent with constitutional and international child rights standards. The study adopts a doctrinal and comparative analytical approach, reviewing Sri Lanka's existing legal framework alongside international instruments and regulatory models from multiple jurisdictions. It evaluates constitutional protections, statutory gaps, enforcement challenges and platform design issues, while also analysing global policy trends on child online safety. The findings demonstrate that while the State's objective of protecting children is legitimate, a blanket ban is disproportionate, risks infringing fundamental rights and fails to address underlying technological and behavioural factors that enable online harm. Evidence suggests that prohibition displaces rather than eliminates risk, often pushing minors toward less regulated digital spaces. Furthermore, gaps in enforcement capacity, digital literacy and platform accountability remain key contributors to the persistence of OCSEA. The paper concludes that a multi-dimensional regulatory framework is more effective than outright bans. It proposes an alternative approach based on evolving capacities, enhanced digital literacy, parental accountability, safe-by-design technological reforms and targeted legal amendments. Such a framework offers a balanced and sustainable solution that protects children while preserving their rights and participation in the digital environment.

Keywords: Child Protection, Digital Regulation, Online Safety, Social Media, Sri Lanka.

Introduction

In late January of 2026, an alleged explicit video scandal involving a school student and several teachers dominated the Sri Lankan media discourse. Although neither the Ministry of Education nor the implicated school has released any official reports regarding the particular details of the incident, the extensive media coverage and the massive public outrage shed light on a broader social issue that has been persistently affecting children in Sri Lanka. Within a 72 hour window there was a surge of new social media accounts made just to disseminate the explicit material involved with the incident, while admins of social media pages began to monetize the incident through various memes and cartoons.[1] This direct violation of a school boy's privacy exposed the consequences of unregulated social media and internet usage of minors and the inadequacy of social and legal structural safeguards to protect the most vulnerable members of our society from the inevitable dangers they face in cyberspace. Following the scandal, in a special media statement released on 29th of January 2026, Minister of Women and Child Affairs Savithri Paulraj disclosed that discussions have begun at cabinet level to ban social media access for children below 12 years of age.[2] Similar sentiments were echoed in the statement by the official cabinet spokesperson, Dr. Nalinda Jayatisa who highlighted the necessity of an Online Safety framework to address situations where social media and media do not voluntarily self regulate in concerns related to privacy and identity of individuals.[3]

This was not an isolated incident that gained sudden media traction but rather a critical tipping point for the Sri Lankan government to consider a blanket ban of social media for minors to combat issues related to Online Child Sexual Exploitation and Abuse (OCSEA). OCSEA is defined as *"situations involving digital, internet and communication technologies at some point during the continuum of abuse or exploitation. It can occur fully online or through a mix of online and in-person interactions between offenders and children."*[4] National Child

[1] 'Spotlight on leaked school video: Stringent laws needed to check sharing private content online' *Daily Mirror* (Colombo, 2 February 2026) <https://www.dailymirror.lk/news-features/Spotlight-on-leaked-school-video-Stringent-laws-needed-to-check-sharing-private-content-online/131-331820> accessed 5 February 2026.

[2] 'Sri Lanka considering restricting access to social media for children under 12' *Ada Derana* (Colombo, 29 January 2026) <https://www.adaderana.lk/news.php?nid=117755> accessed 5 February 2026.

[3] 'Education Ministry Probes Colombo School Incident After Content Circulates Online' *Asian Mirror* (Colombo, 27 January 2026) <https://asianmirror.lk/news/12067/education-ministry-probes-colombo-school-incident-after-content-circulates-online/> accessed 5 February 2026 .

[4] ECPAT International, 'Access to Justice and Legal Remedies for Children Subjected to Online Sexual Exploitation and Abuse. Disrupting Harm Data Insight 3. Global Partnership to End Violence Against Children.' (2022) <https://safeonline.global/wp-content/uploads/2023/12/DH-data-insight-3_Final.pdf> accessed 5 April 2026.

Protection Authority (NCPA) statistics reveal that in 2025 alone there have been 150 cases of cyber bullying of children involving non-consensual distribution of intimate images reported.[5] More alarmingly, there have already been 34 reported cases of similar nature for the period from 2026.01.01 to 2026.02.28.[6] Furthermore, a comprehensive study done by Social Policy Analysis and Research Centre (SPARC) of University of Colombo, where 1911 children across all 25 districts were surveyed, it was revealed that 28% of the children have faced some form of online violence, which is 3 out of 10 children who participated in the survey.[7] Demographically, it was observed that girls (29%) experienced cyber-violence slightly more than boys (27%).[8] The study identified specific manifestations of OCSEA, revealing that the dangers minors face online go beyond mere cyberbullying with 28.0% of the the survey respondents having received indecent text messages, 26% being exposed to indecent links and media and more critically 20.7% reporting being cyber extorted.[9] Further, Key Informant Interviews (KIIs) with the participants and NCPA officials uncovered how that there is a vicious cycle of perpetrators (most of the time intimate partners/ boyfriends) weaponizing existing intimate images to blackmail victims to self-generate more child sexual abuse material (CSAM).[10]

Studies reveal that OCSEA does not solely take place in hidden corners of the internet but rather it is usually initiated in popular social media platforms that are easily accessible to minors. The WeProtect Global Alliance identified a common, predatory practice among perpetrators called 'off-platforming', where the perpetrators target and initiate contact with minors on popular social media platforms and gradually move the conversations to more private, encrypted messaging platforms.[11] This presents a particularly devastating picture when applied to Sri Lanka's current digital landscape. DataReportal's 2025 digital report on Sri

[5] National Child Protection Authority, 'Child Abuse and Other child related complaints reported to NCPA by Districts by Category - (Year 2025.01.01 to 2025.12.31)' (31 December 2025) <https://childprotection.gov.lk/images/lem-statistics/NCPA_Statistics-e-20251231.pdf> accessed 4 April 2026.
[6] National Child Protection Authority, 'Child Abuse and Other child related complaints reported to NCPA by Districts by Category - (Year 2026.01.01 to 2026.02.28)' (10 March 2026) <https://childprotection.gov.lk/images/lem-statistics/NCPA_Statistics-e-20260310.pdf> accessed 4 April 2026.
[7] Social Policy Analysis and Research Center, 'Online Violence against Children in Sri Lanka: A National Research on Incidence, Nature and Scope' (State Ministry of Women and Child Development 2021) 7, 27 <https://sparc.cmb.ac.lk/wp-content/uploads/2021/04/ECVAC-Research-Summary-Report-Design.pdf> accessed 5 April 2026 .
[8] Ibid, 7.
[9] Ibid, 8, 28.
[10] Ibid, 29.
[11] WeProtect Global Alliance, 'Global Threat Assessment 2025' (2025) 34 <https://www.weprotect.org/wp-content/uploads/GTA-2025_EN.pdf> accessed 5 April 2026.

Lanka has identified that there are over 8.2 million active social media users in Sri Lanka.[12] Further, a study done by UNICEF in 2017 which surveyed over 5300 students aged 11 to 18 in Sri Lanka revealed that minors start to access the internet at 13 years of age and about 60.3% of them were social media users, with Facebook being the most popular platform among them.[13] Compounding this concern, in early 2026, Doctors in Sri Lanka have also raised concerns regarding the social media usage of minors where they noted that minors spend an average of 5-7 hours on screen for non-educational purposes.[14] Thus social media platforms in Sri Lanka clearly house a significant number of underage users who are frequently exposed to dangers of the digital sphere.

The NCPA reports only account for the reported number of cyber crimes related to minors. Behind that, there is a massive dark figure of unreported cases. The SPARC report indicates that there is general reluctance to speak up with about 92% of children who were surveyed revealing that they are unwilling to actively seek legal support or complain to authorities about the online violence that they have experienced.[15] This massive underreporting is a result of fear tactics used by the perpetrators who often threaten to publicly release personal information of the victims or send death-threats to victims. The traditional penal system is heavily reliant on complaints made by victims and the startling rate of non-reporting exposes a critical shortcoming in the sociolegal framework of the country where perpetrators are allowed to operate with impunity.

This impunity enjoyed by the perpetrators of cyberviolence against children is further exacerbated by the structural framework of social media platforms. They are inherently designed for anonymity and this shields perpetrators from accountability for their actions. Further, Social media platforms rely on engagement driven algorithmic models where increased engagement is more profitable. Engagement driven algorithms inadvertently result in rapid dissemination of explicit material because the platform design inherently prioritizes

[12] Simon Kemp, 'Digital 2025: Sri Lanka' (DataReportal, 25 February 2025) <https://datareportal.com/reports/digital-2025-sri-lanka> accessed 5 April 2026.
[13] UNICEF, 'Keeping Children in Sri Lanka Safe and Empowered Online: A Study on Sri Lanka's Digital Landscape' (UNICEF, 2017) <https://www.unicef.org/srilanka/sites/unicef.org.srilanka/files/2018-11/Unicef_Book_260118.pdf> accessed 5 April 2026.
[14] 'Legal basis to be laid for weaning children away from digital addiction' *Sunday Times* (Colombo, 1 February 2026) <https://www.sundaytimes.lk/260201/news/legal-basis-to-be-laid-for-weaning-children-away-from-digital-addiction-630361.html > accessed 5 April 2026.
[15] Social Policy Analysis and Research Center (n 7).

more user interaction "regardless of the veracity or the intention of the content". [16] This compounds the fear and trauma experienced by victims of CSAM. Furthermore, there is a massive shortcoming related to local language content moderation in Social media platforms. Tech companies disproportionately underinvest in developing in-built safety mechanisms for regional languages like Sinhala and Tamil. Therefore they lack "the digital lexicon required for computational analysis" of local languages.[17]

However, a big proportion of local social media content is in Sinhala and Tamil and the fact that in-built safety designs to filter harmful content from the algorithm remains highly ineffective and blind towards vernacular hate speech and culturally specific nuances is alarming.[18] There are identified extreme cases of cyber violence against children in platforms like Facebook, where pages specifically dedicated for distribution of non-consensual CSAM and promotion of gender-based violence have operated openly for many years without being flagged by the Facebook algorithm for violating the platform's community standards. One alarming incident highlighted in an open letter by CPA addressing Facebook in 2017, is where they had reported a Sinhala poem which suggested that when a woman says "no" to sexual advances they actually mean "yes" and it took Facebook two days to review it and finally conclude that it doesn't violate the community standards against promoting sexual violence.[19] Ultimately, this has created a safe haven in the digital sphere for perpetrators to freely exploit minors with impunity.

These shortcomings of both the law enforcement mechanism within the country and the wilful negligence of the social media platforms in combatting continued cyber violence against minors as well as the global movement towards restricting the social media access of minors that has prompted the government to start discussions on whether Sri Lanka should consider a blanket ban of social media for minors as well.

---

[16] Verité Research, 'Better Moderation of Hate Speech on Social Media A Sri Lankan Case Study for Reputational-Cost Approaches' (July 2021) <https://www.veriteresearch.org/publication/better-moderation-of-hate-speech-on-social-media-a-sri-lankan-case-study-for-reputational-cost-approaches/> accessed 4 April 2026.

[17] Verité Research (n 17); also see Yudhanjaya Wijeratne, 'The Control of Hate Speech on Social Media: Lessons from Sri Lanka' (October 30, 2018) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3275106> accessed 4 April 2026.

[18] Uda Deshapriya, 'Amidst Virtual Impunity: The experience of using local languages online in Sri Lanka' (State of Internet's Languages Report, 2022) <https://internetlanguages.org/en/stories/amidst-virtual-impunity/> accessed 4 April 2026.

[19] Center for Policy Alternatives, 'Open letter to Facebook: Implement Your Own Community Standards' (10 April 2018) <https://www.cpalanka.org/open-letter-to-facebook-implement-your-own-community-standards/> accessed 4 April 2026.

Existing legal framework in Sri Lanka on child rights and online child sexual exploitation and abuse

Before assessing the necessity, constitutionality and the feasibility of a blanket ban, it is important to first analyze the existing legal framework governing OCSEA in Sri Lanka. Discussions surrounding the startling amount of cyber violence and exploitation of minors often revolve around the inadequacy of the existing legislation or the shortcomings in legal implementation. It is in fact a combination of both that has resulted in this situation.

Constitutional protections and limitations

Sri Lanka's Constitution ["**SL Constitution**"] recognises a range of rights that affect online safety and children's dignity. These are the freedom of expression (SL Constitution, Article 14(1)(a)), equality before the law (SL Constitution, Article 12(1)) and the right to education (SL Constitution, Article 27) and personal liberty (SL Constitution, Article 13)[20]. These rights form the backdrop against which the state must act when regulating online content and protecting children from harm. At the same time, any limits on expression, as empowered under the Article 15 of the SL Constitution, must be justified as necessary and proportionate, where the rights of minors are involved[21].

Thereupon considering it, a blanket ban by the state may be legally justified under Article 27(13) of the SL constitution which is a directive principle of state policy that outlines the state's duty to promote the interests of children while protecting them from exploitation and discrimination.[22] While the State's objective to eradicate cyber violence against children is legitimate, the contemplated method of implementing it poses some serious questions about constitutional overreach. In fact, a blanket ban would be a direct breach of the Fundamental Right of minors, specifically their freedom of speech and expression guaranteed under Article 14(1)(a)[23] as well as their right to access information under Article 14A.[24] Article 14 is not an absolute right and it can be restricted under Article 15 *"in the interests of national security, public order and the protection of public health or morality, or for the purpose of securing due*

[20] Ruwantissa Abeyratne, 'Constitutional Rights: Life and Personal Liberty in Sri Lanka' *Sri Lanka Guardian* (9 May 2024) <http://www.srilankaguardian.org/2024/05/constitutional-rights-life-and-personal.html> accessed 22nd March 2026
[21] Constitution of Democratic Socialist Republic of Sri Lanka 1978, Art. 12(4)
[22] Constitution of Democratic Socialist Republic of Sri Lanka 1978, Art. 27(13).
[23] Constitution of Democratic Socialist Republic of Sri Lanka 1978, Art. 14(1)(a).
[24] Constitution of Democratic Socialist Republic of Sri Lanka 1978, Art. 14A.

recognition and respect for the rights and freedoms of others, or of meeting the just requirements of the general welfare of a democratic society".[25] However, it is established in constitutional jurisprudence that any restriction of Article 14 should always be proportional.[26] A blanket ban which would completely restrict minors's access to social media instead of first targeting the perpetrators would fail this test of proportionality.

Online Safety Act, No. 9 of 2024

At the statutory level, Sri Lanka has introduced several legal instruments that touch on online harm. The Online Safety Act, No. 9 of 2024 ["**OSA**"] is a recent legislation designed to regulate harmful online communication. It establishes an Online Safety Commission (OSA, Section 4) with powers to investigate complaints and direct action against harmful content. Among its criminal offences are the online publication of abusive or pornographic images, audio and videos relating to children (OSA, Section 21(2)). They carry potential prison terms of up to 20 years and fines of up to one million rupees, as well as compensation orders to victims. This shows an attempt to criminalise the dissemination of harmful material online.

Personal Data Protection Act, No. 9 of 2022

Parallel to this, the Personal Data Protection Act, No. 9 of 2022 ["**PDPA**"] seeks to protect the privacy of individuals by regulating how personal data[27] is processed and controlled. This law creates rights for data subjects and a Data Protection Authority to oversee compliance (PDPA, Section 28). In theory, this helps curb misuse of personal information including of minors but several parts are yet to be fully implemented and enforced.

Computer Crimes Act No. 24 of 2007

Older legislation like the Computer Crimes Act No. 24 of 2007 ["**CCA**"] still applies to many cyber offences such as unauthorised access (CCA, Section 3), misuse of computer systems and related harms (CCA, Section 4). This Act was one of the first legal frameworks in Sri Lanka to

[25] Constitution of Sri Lanka, art 15(7).

[26] *Joseph Perera v The Attorney-General* (1992) 1 Sri LR 199; *Sunila Abeysekara v Ariya Rubasinghe* (2000) 1 Sri LR 314.

[27] Personal Data Protection Act, section 56 - "*"personal data" means, any information that can identify a data subject directly or indirectly, by reference to– (a) an identifier such as a name, an identification number, financial data, location data or an online identifier; or (b) one or more factors specific to the physical, physiological, genetic, psychological, economic, cultural or social identity of that individual or natural person.*"

specifically define computer-related crimes[28] but it was drafted before the widespread use of modern social media and does not directly address many forms of online victimisation, such as sexual exploitation or grooming that occur through contemporary platforms. As Bandaranayake proposes, the provisions in this particular act must be interpreted purposively by the judiciary to cover Child Sexual Abuse and Child Sexual Exploitation that happens online.[29] Section 2 of the Act provides a broad jurisdictional power to the State where they could prosecute offenses that affect computer systems within or outside Sri Lanka.[30] Further section 3 of the act can be used to criminalize particular forms of OCSEA offenses like cyberbullying and cyberstalking by unlawfully accessing children's computers.[31] Section 7 can be interpreted to prosecute individuals who maintain websites and provide digital infrastructure to disseminate CSAM material and section 8 of the act can be interpreted to prosecute individuals who engage in commercial trade of CSAM.[32] However, CCA is predominantly applied to fraud related to commercial transactions, hacking or handling of unlawfully obtained information.[33] Further, the application CCA for cases involving CSA and CSE is severely hindered by the lack of a specific definition for OCSEA and further its failure to mandate specific penalties for digital exploitation of minors.[34] The Online Safety Act, No. 9 of 2024 which was specifically enacted to address these modern digital harms also falls into a similar trap by primarily targeting fraud, dissemination of false information and unauthorized access and failing to address the legislative lacunae related to cybersex trafficking and exploitation that is unique to OCSEA.[35]

Penal Code, No. 2 of 1883

These statutory measures interact with the Penal Code of Sri Lanka ["**SLPC**"]. It criminalises various offences relevant to child protection. Section 286A of the SLPC which deals with the

[28] General Data Protection Regulation (GDPR) 2016/679
[29] BM Prineetha Bandaranayake, 'Combating online child sexual exploitation and abuse in Sri Lanka: Towards a statutory response' (16th International Research Conference, General Sir John Kotelawala Defense University, Sri Lanka, 2023) 46.
[30] Computer Crimes Act No 24 of 2007, s 2.
[31] Bandaranayake (n 29) 47.
[32] Ibid 48.
[33] Nirodha Kalansooriya, 'Addressing Child Harassment on Social Media in Sri Lanka: A Comparative Analysis of Legal Frameworks' (2023) 2 *APIIT LJ* 22
[34] Bandaranayake (n 29) 48.
[35] Chaga Mahingoda, Kushanthi Harasgama and Samurdhi Jayamaha, 'Unveiling Sri Lanka's Legal Landscape: Addressing Cybersex Trafficking Through Current Online Harassment Laws' (17th International Research Conference, General Sir John Kotelawala Defense University, Sri Lanka, 2024) 240.

publication and exhibition of obscene materials involving children, does not explicitly define what "obsence"or "indecent" material is.[36] Therefore leaving its interpretation up to the judiciary, which can be extremely subjective and this leads to inconsistency in the standard applied to each case.[37] Moreover, section 286B SLPC deals with preventing sexual abuse of a child and section 288B SLPC addresses hiring or employing children to traffic in restricted articles.

Further, legislation like Obscene Publications Ordinance No.4 of 1927 remains completely ineffective against modern cyber-crimes.[38] While section 360C of the SLPC criminalizes human trafficking, it still fails to explicitly deal with modern developments like cybersex trafficking particularly related to exploitation and coercion that is prevalent in image-based abuse.[39] Furthermore, there is no substantive law which specifically criminalizes AI-generated and simulated CSAM. According to Internet Watch Foundation (IWF) reports, in 2025 alone they have assessed over 8000 AI generated CSAM and it contained over 3000 videos of AI generated child sexual abuse.[40] These AI generated CSAM is produced using Large Language Models (LLMs), nudify apps and text-to-image models which are trained using already existing "traditional" CSAM. The failure of domestic legislation to address these modern developments of OCSEA is a significant shortcoming.[41]

Crisis in legal implementation and institutional capacity

On another note, it is important to understand the crisis in the legal implementation that facilitates the impunity of perpetrators of cyber violence. The NCPA is the primary statutory body responsible for receiving and investigating child abuse complaints in Sri Lanka. According to official NCPA data, there has been a surge of child abuse complaints following 2020.[42] However despite this massive increase in the number of cases reported, the law enforcement agencies of the country lack the precise training to effectively prosecute cases

[36] Penal Code Ordinance No 2 of 1883, s 286A.
[37] Bandaranayake (n 29) 46.
[38] Obscene Publications Ordinance No 4 of 1927.
[39] Chaga Mahingoda, Kushanthi Harasgama and Samurdhi Jayamaha (n 35).
[40] Internet Watch Foundation, AI CSAM report 2026: Harm without limits: AI child sexual abuse material through the eyes of our Analysts (2026) <https://www.iwf.org.uk/media/hl1nvdti/iwf-ai-csam-report-2026.pdf> accessed on 4 April 2026.
[41] Ibid.
[42] Rohana Ranasinghe, 'Patterns and Trends in Child Abuse Complaints in Sri Lanka: Evidence from National Child Protection Authority Data (2010–2025)' (2026) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=6376338> accessed 6 April 2026.

involving complex digital investigations. Perpetrators of cyber violence often use advanced encryption technologies and anonymization techniques and some even operate in the dark web to obscure their identities. This presents an unique and complex challenge to the Sri Lankan law enforcement agencies that they are ill-equipped to handle with their present technological capabilities.[43] Due to this lack of digital forensic capabilities of the law enforcement agencies, they are unable to take effective proactive steps to prevent such child exploitation. This legal implementation paralysis is highlighted despite the presence of a comprehensive law regarding trafficking and sexual exploitation of children under section 360C of the SLPC, yet there has been only a single conviction which has been reported in the country as of December 2022. Additionally, there are enforcement structures like the Computer Crime Investigation Division (Cyber Crime) and Sri Lanka Computer Emergency Readiness Team ["SLCERT"] that are active to address such claims.

International legal framework on child rights in the digital environment

Shifting focus to international law, it is increasingly recognising that children's rights must be protected in the digital environment just as they are offline. The United Nations Convention on the Rights of the Child ["**UNCRC**"][44] is a treaty ratified by almost every country in the world. It guarantees a wide range of rights for children. It includes the right to privacy (UNCRC, Article 16), protection from sexual exploitation (UNCRC, Articles 34), freedom of expression (UNCRC, Articles 13), access to information (UNCRC, Articles 17) and the right to development (UNCRC, Articles 6). These rights also apply online because harmful conduct such as grooming, cyberbullying, sextortion and exposure to inappropriate content can violate children's rights under international law.

In March 2021, the UN Committee on the Rights of the Child adopted General Comment No. 25 on children's rights in relation to the digital environment[45]. This clarifies how States parties to the UNCRC should protect, respect and fulfil children's rights online. It voices that

[43] Niranjan Meegammana and Sampath Punchihewa, 'Introducing an Effective Cybercrime Regime for Sri Lanka: A Comparative Analysis' (2020) <https://www.researchgate.net/publication/394214360_An_Effective_Cybercrime_Regime_for_Sri_Lanka_A_Comparative_Analysis> accessed 5 April 2026.

[44] (adopted 20 November 1989, entered into force 2 September 1990) 1577 UNTS 3 (CRC)

[45] Committee on the Rights of the Child, General comment No 25 (2021) on children's rights in relation to the digital environment (2 March 2021) UN Doc CRC/C/GC/25 <https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation> accessed 22nd March 2026.

"*the use of digital devices should not be harmful, nor should it be a substitute for in-person interactions among children or between children and parents or caregivers*". States must address risks such as "*violent and sexual content, cyberaggression and harassment, gambling, exploitation and abuse, including sexual exploitation and abuse, and the promotion of or incitement to suicide or life-threatening activities, including by criminals or armed groups designated as terrorist or violent extremist*". The best interests of the child should also guide digital policy and law. The General Comment also stresses that digital harms affect children's "*right to privacy, freedom of thought and opinion*", development and participation rights and that both public authorities and digital service providers have responsibilities to prevent and respond to those harms.

General Comment No. 25 further highlights that the *"digital environment is becoming increasingly important across most aspects of children's live"*. Therefore, the legal standards must adapt. States should involve children in decision-making about digital rules and implement protection measures that are inclusive of all groups of children, including those from marginalized backgrounds. It recognises that technology can help realise children's rights but also that it creates unique risks that must be addressed through law and policy.

Another key international landscape is the European Union's Digital Services Act ["**DSA**"]. Although a regional instrument, the DSA is one of the most advanced legal frameworks globally aiming to protect children online[46]. It obliges online platforms accessible to minors to assess and mitigate risks to children's privacy, safety and wellbeing. Under the DSA, platforms must take measures to prevent exposure to harmful content, set children's accounts to more protective settings, offer effective "*internal complain-handling mechanisms*", limit personalised advertising based on profiling and adapt "*algorithmic recommendation systems*". If this is done so, the children are less likely to encounter harmful material.

Beyond formal treaties and statutes, many global and regional human rights bodies[47] have stressed that states must protect children's rights online.[48] They call for international

[46] European Broadcasting Union, *Digital Services Act Handbook* (February 2023) <https://www.ebu.ch/files/live/sites/ebu/files/Publications/Reports/open/10022023-Digital-Services-Act-Handbook%E2%80%93Public-Version.pdf> accessed 22nd March 2026

[47] committees under the International Covenant on Civil and Political Rights ["**ICCPR**"] and the UN Human Rights Council ["**UNHRC**"]

[48] United Nations Children's Fund (UNICEF), *Child Online Protection in and through Digital Learning: Considerations for Decision-Makers* (May 2022) <https://www.unicef.org/eca/media/22501/file/Child%20Online%20Protection%20in%20and%20through%20Digital%20Learning.pdf> accessed 22nd March 2026

cooperation, data sharing and ethical design of digital services to prevent harms like exploitation, discrimination and abuse. They also call for facilitating access to information and participation. This signals that international legal thinking on online safety is moving towards holistic rights-based standards rather than narrow technical restrictions.

However, a blanket ban would isolate minors from the digital sphere and that would be a violation of the international standards that SL has ratified. Sri Lanka has also acceded to the Optional Protocol on the Sale of Children, Child Pornography and Prostitution (OPSC). However, relying solely on these international frameworks is insufficient because Sri Lanka is a dualist country and these ratifications to international standards remain virtually ineffective in the domestic courts unless the state specifically enact domestic enabling legislation.

Comparative analysis of global regulatory models

In addition to this, social media regulations for children across different countries shows a clear global shift toward stricter control. But this is with important differences in how each country approaches the issue. While the overall goal is the same, that is protecting children's mental health, safety and development, the methods vary in terms of age limits, legal structure, enforcement mechanisms and the role of parents versus technology companies.

One of the most significant developments in this area is seen in Australia. It introduced the world's first full prohibition model. In November 2024, Australia passed the Online Safety Amendment (Social Media Minimum Age) Bill, which officially came into force on 10th December 2025.[49] This law sets a strict minimum age of 16, below which children are completely banned from accessing major social media platforms such as Instagram, TikTok, Snapchat and YouTube. What makes Australia's model unique is that it places full legal responsibility on the companies, not on children or parents. Companies must implement advanced age verification technologies, including ID checks, facial recognition and behavioural analysis. Failure to comply can result in fines of up to AUD 49.5 million (approximately USD 32 million).[50] This model reflects a strong belief that social media platforms themselves are the primary source of harm and therefore must bear the burden of regulation. It is also based on growing evidence that children are being exposed to harmful

[49] Online Safety Amendment (Social Media Minimum Age) Act No. 127, 2024

[50] BBC News, *'Did Australia's under-16 social media ban work?'* (BBC News, March 2026) <https://www.bbc.com/news/articles/cwyp9d3ddqyo> accessed 8 April 2026

content very quickly. Studies show that inappropriate material can appear within 3 to 5 minutes of usage for young users.[51]

In contrast, France represents a controlled access model that combines parental responsibility with corporate accountability. On 29th June 2023, France enacted a law requiring social media platforms to verify the age of users and obtain parental consent for children under 15.[52] This law is part of a broader strategy to reduce cyberbullying, online exploitation and excessive screen time. Companies that fail to comply can be fined up to 1% of their global annual revenue. That is a significant financial penalty, mainly for large tech companies. However, France has also shown signs of moving toward a stricter model. Following a violent incident in June 2025, the French government announced plans to introduce a complete ban on social media for children under 15. This indicates a shift from controlled access to prohibition. This shows how social and safety concerns can accelerate stricter regulation.

A similar but more technologically integrated approach can be seen in Portugal, which introduced new regulations in 2026. Portugal enforces a minimum age of 13, in line with many global standards but requires verified parental consent for users aged 13 to 16 through a national digital identification system known as the Digital Mobile Key (DMK).[53] This system allows parents to directly control and monitor their children's access to online platforms. Portugal's model is significant because it integrates national digital infrastructure into enforcement. It makes age verification more reliable and harder to bypass. At the same time, it maintains a balance between restriction and access. This allows children limited participation under supervision.

Spain is currently moving toward a stricter system. In June 2024, the Spanish government approved a draft law raising the age of digital consent from 14 to 16, aligning itself with countries like Australia. Although the law has not yet fully implemented a total ban, it indicates a strong policy direction toward stricter regulation. Spain has also introduced additional measures to protect minors. This includes criminal penalties for creating or distributing

[51] Deborah Prkno and others, 'Children's and Adolescents' Negative Internet Experiences and the Association with Quality of Life and Behavioural Difficulties: A Cross-Sectional Study' (2025) 9(1) *BMJ Paediatrics Open* <https://pmc.ncbi.nlm.nih.gov/articles/PMC12007062/> accessed on 20.03.2026

[52] 'France requires parental consent for under-15s on social media' (29 June 2023) Le Monde <https://www.lemonde.fr/en/france/article/2023/06/29/france-requires-parental-consent-for-under-15s-on-social-media_6039514_7.html> accessed on 20 March 2026

[53] Ronan Ó Fathaigh, 'Portugal to ban social networks for children under 16' (European Audiovisual Observatory, IRIS Merlin) <https://merlin.obs.coe.int/article/10492> accessed 2 April 2026.

deepfakes and banning access to loot box systems in video games for individuals under 18.[54] These broader digital safety measures show that Spain views online risks as interconnected, not limited to social media alone.

In Denmark, the government is considering a strict ban for children under 15 but with a degree of flexibility. The proposal includes allowing children aged 13 and above to access social media with parental permission, although authorities strongly discourage this. Denmark has also committed 160 million Danish kroner (approximately USD 24.7 million) toward improving digital safety for children through education, awareness programs and platform regulation.[55] This reflects a preventive and supportive approach, rather than purely punitive measures. Denmark's model emphasizes guidance, parental involvement and gradual restriction, making it less rigid than Australia's system.

Similarly, Norway is exploring new regulations aimed at raising the minimum age for social media use from 13 to 15. The government has launched public consultations to clearly define what qualifies as a social media platform and guarantees that any restrictions align with fundamental rights such as freedom of expression and access to information. National data strongly supports this move. Studies show that 38% of Norwegian children feel they spend too much time on social media, while 30% wish they could reduce their usage.[56] Norway's approach reflects a careful balance between child protection and individual rights. As a result it makes it one of the more moderate regulatory frameworks.

The United States, unlike these countries, does not have a unified national policy. Instead, it follows a decentralized approach. Individual states implement their own laws. A key example is Florida, which introduced legislation restricting social media use for minors. Under this law, children under 14 are completely banned from having accounts, while those aged 14 to 15 require parental consent and age verification.[57] This approach is similar to the French model

[54] Thomas Mackintosh, 'Spain announces plans to ban social media for under-16s' (BBC News, 24 February 2026) <https://www.bbc.com/news/articles/c5y2nddvmryo> accessed 2 April 2026.

[55] Christian Mikkelsen, 'Denmark to ban social media for children under 15' (Deutsche Welle, 13 November 2025) <https://www.dw.com/en/denmark-to-ban-social-media-for-children-under-15/a-74666210> accessed 2 April 2026.

[56] Ashifa Kassam, 'Norway to increase minimum age limit on social media to 15 to protect children' (The Guardian, 23 October 2024) <https://www.theguardian.com/world/2024/oct/23/norway-to-increase-minimum-age-limit-on-social-media-to-15-to-protect-children> accessed 2 April 2026.

[57] David Ingram, 'Florida's Ron DeSantis signs bill banning social media for kids under 14' (NBC News, 25 March 2024) <https://www.nbcnews.com/tech/florida-ron-desantis-signs-bill-social-media-kids-ban-rcna144950> accessed 2 April 2026.

but lacks nationwide consistency. Other states are also considering similar laws, but the absence of federal regulation creates a fragmented system with varying levels of protection.

In Italy, concerns about digital addiction have driven legislative proposals, although no law has yet been fully implemented as of March 2026. According to the National Institute of Health, approximately 100,000 teenagers aged 15 to 18 are at risk of social media addiction. In response, the Italian parliament introduced a bill in May 2024 proposing restrictions on social media use, including regulations for child influencers under the age of 15. Italy's focus highlights a growing concern not just about usage, but also about commercial exploitation of children online, particularly through influencer culture.

Austria is currently in the planning stage of introducing a ban for children under 14. Policymakers are studying international examples, mainly Australia's system, to develop effective age verification methods. Proposed measures include identity verification, facial recognition and behavioural tracking to confirm users' ages. Austria's approach demonstrates how countries are increasingly relying on advanced technology to enforce digital regulations.

In South Korea, the focus is slightly different but still relevant to the broader issue of digital exposure. Rather than banning social media entirely, South Korea is implementing a nationwide ban on smartphone use in classrooms, starting from March 2026.[58] This policy aims to reduce digital distraction, improve academic performance and encourage face-to-face interaction among students. Exceptions are made for students who require devices for accessibility purposes. This approach shows that regulation can also target specific environments, such as schools, rather than imposing a full societal ban.

When comparing these countries, three major regulatory models become clear.

1. The first is the **total prohibition model**, represented by Australia, where children below a certain age (16) are completely banned from accessing social media. This model is the most strict and relies heavily on corporate accountability and technological enforcement.
2. The second is the **parental consent model**, seen in countries like France, Portugal and parts of the United States, where children can access social media under supervision.

[58] Suhn-wook Lee and Fan Wang, 'South Korea bans phones in school classrooms nationwide' (BBC News, 27 August 2025) <https://www.bbc.com/news/articles/c776ye6lrvzo> accessed on 8 April 2026.

This model balances freedom and protection, allowing limited use while still imposing safeguards.

3. The third is the **flexible or developing model**, used by countries such as Denmark, Norway, Spain, Austria and Italy, where laws are still evolving and often include exceptions, consultations and gradual implementation.

Another important point of comparison is who is held responsible for enforcing these laws. In countries like Australia and France, the burden is placed almost entirely on social media companies, which must implement strict verification systems and face financial penalties if they fail. In contrast, countries like Denmark and the United States involve parents as active decision-makers. This allows them to determine whether their children should access social media under certain conditions. This difference reflects broader cultural attitudes toward parenting, government intervention and corporate responsibility.

Age limits also vary but generally fall within a narrow range. Most countries set the minimum age between 13 and 16, with 13 being the traditional global standard based on platform policies and 16 emerging as the new preferred threshold for stricter regulation. The shift toward higher age limits reflects increasing awareness of the psychological and developmental risks associated with early exposure to social media.

Enforcement methods are another key area of difference. Countries are increasingly adopting advanced technologies such as biometric verification, artificial intelligence and digital identity systems to guarantee compliance. For example, Australia and Austria are exploring facial recognition and behavioural analysis, while Portugal uses a government-backed digital ID system. These methods are more effective than traditional self-declaration systems, which children can easily bypass.

Despite these differences, all countries share a common concern supported by strong data. Studies show that children who spend more than 3 hours per day on social media are at significantly higher risk of anxiety and depression, while those exceeding 5 hours report much lower levels of happiness and life satisfaction.[59] Additionally, global data indicates that 1 in 7 adolescents (approximately 14%) experience mental health disorders, many of which are linked

[59] Tariq Masri-Zada and others, 'The Impact of Social Media & Technology on Child and Adolescent Mental Health' (2025) *Journal of Psychiatry and Psychiatric Disorders* 9(2) 111-130 <https://pmc.ncbi.nlm.nih.gov/articles/PMC12165459/> accessed 8 April 2026

to excessive digital use.[60] These statistics explain why governments are increasingly treating social media regulation as a public health issue rather than just a technological or social concern.

Accordingly, while countries differ in their specific approaches, ranging from total bans to parental consent systems, they are united by a shared recognition of the risks posed by social media to young users. The differences lie mainly in how strict the rules are, how they are enforced and who is held responsible.

Proposed reforms and policy alternatives

A blanket ban on social media for minors may appear to be a strong and immediate solution but empirical evidence and global trends show that it fails to address the structural nature of online harm. Around one in three young people globally have experienced cyberbullying, while one in five children report direct exposure to such harm. It demonstrates that the problem is widespread and deeply embedded within digital ecosystems rather than limited to access alone.[61] At the same time, one-third of all internet users worldwide are under the age of 18, which indicates that children are not marginal participants but a central demographic within digital spaces.[62] In this context, a ban does not eliminate risk but merely postpones exposure, often pushing children toward unregulated platforms or private networks where safeguards are weaker and detection becomes more difficult. This reinforces the argument that prohibition creates displacement rather than protection.

Evolving capacities approach

An evolving capacities framework offers a more proportionate and evidence-based alternative. Developmental psychology shows that adolescents are more prone to impulsive decision-making and risk-taking behaviour due to incomplete cognitive maturity, which makes them

[60] Candice L Odgers and Michaeline R Jensen, 'Annual Research Review: Adolescent Mental Health in the Digital Age: Facts, Fears and Future Directions' (2020) *Journal of Child Psychology and Psychiatry* 61(3) 336-348 <https://pmc.ncbi.nlm.nih.gov/articles/PMC8221420/> accessed 8 April 2026

[61] United Nations Children's Fund, *'UNICEF poll: More than a third of young people in 30 countries report being a victim of online bullying'* (Press release, 4 September 2019) <https://www.unicef.org/press-releases/unicef-poll-more-third-young-people-30-countries-report-being-victim-online-bullying> accessed 9 April 2026.

[62] United Nations, *'Safeguarding childhood online – How cyberbullying threatens children's safety globally'* (UN Peace and Security, 10 March 2026) <https://www.un.org/en/peaceandsecurity/safeguarding-childhood-online-how-cyberbullying-threatens-childrens-safety-globally> accessed 9 April 2026.

particularly vulnerable in digital environments.[63] However, this vulnerability does not justify total exclusion. Instead, it supports gradual exposure under structured safeguards. A tiered access model that restricts high-risk features such as anonymous messaging, algorithm-driven recommendations and public content sharing for younger users would reflect both the developmental needs of children and their rights under international law. This approach aligns with the reality that digital engagement is now integral to education, communication and social participation and therefore cannot be completely removed without broader social consequences.

Digital literacy and social awareness

The importance of digital literacy and social awareness programmes is equally supported by global data. Studies indicate that many children do not report online abuse due to fear, shame or lack of understanding of available support systems, which allows harmful behaviour to continue unchecked.[64] Furthermore, over one-third of young people report experiencing cyberbullying, yet a significant proportion lack the knowledge or confidence to respond effectively.[65] This gap highlights that risk is not only technological but also educational. Embedding digital literacy within school curricula can equip children with practical skills such as recognising grooming patterns, understanding consent and protecting personal data. Parallel awareness programmes for parents are equally critical, as many caregivers remain unaware of the scale of online risks or the mechanisms through which harm occurs. Without this awareness, supervision becomes ineffective and reactive rather than preventive.

Parental accountability

Parental accountability must therefore form a central pillar of reform. Global evidence shows that cyberbullying and online exploitation often occur in private digital spaces that are invisible to adults, which reduces opportunities for early intervention.[66] At the same time, research

[63] Chengyan Zhu, Shiqing Huang, Richard Evans and Wei Zhang, 'Cyberbullying Among Adolescents and Children: A Comprehensive Review of the Global Situation, Risk Factors, and Preventive Measures' (2021) *Frontiers in Public Health* 9 <https://pmc.ncbi.nlm.nih.gov/articles/PMC8006937/> accessed 9 April 2026.

[64] United Nations, *'Safeguarding childhood online – How cyberbullying threatens children's safety globally'* (UN Peace and Security, 10 March 2026) <https://www.un.org/en/peaceandsecurity/safeguarding-childhood-online-how-cyberbullying-threatens-childrens-safety-globally> accessed 9 April 2026.

[65] United Nations Children's Fund, *'Cyberbullying: What is it and how to stop it'* (UNICEF, 2026) <https://www.unicef.org/stories/how-to-stop-cyberbullying> accessed 9 April 2026.

[66] United Nations, *'Safeguarding childhood online – How cyberbullying threatens children's safety globally'* (UN Peace and Security, 10 March 2026) <https://www.un.org/en/peaceandsecurity/safeguarding-childhood-online-how-cyberbullying-threatens-childrens-safety-globally> accessed 9 April 2026.

highlights that children's online behaviour is closely linked to parental guidance and supervision. A legal framework that imposes a duty of reasonable oversight on parents and guardians would create shared responsibility between families and platforms. This does not impose punitive liability but establishes a standard of care that reflects the realities of modern digital parenting. Such an approach also addresses a critical enforcement gap, as state authorities alone cannot monitor the scale of online interaction that occurs daily.

Technological reforms and safe-by-design systems

Technological reforms are essential to complement these social and legal measures. Current platform designs prioritise engagement, which increases exposure to harmful content and accelerates its spread. Algorithmic systems often amplify sensational or explicit material because it generates higher interaction, thereby creating environments where harmful content circulates rapidly. Introducing "*safe-by-design*" requirements would require platforms to embed child protection into their core architecture. This includes the creation of dedicated teen accounts with restricted functionalities, default privacy settings and reduced algorithmic targeting. Evidence shows that harmful content can appear within minutes of use for young users, which underscores the need for proactive design interventions rather than reactive moderation.

Age verification and privacy concerns

Age verification remains a critical but complex aspect of reform. Traditional self-declaration systems have proven ineffective, as children can easily bypass them. More advanced systems, such as those based on digital identity frameworks, offer greater reliability but raise significant privacy concerns. The UK Digital Identity and Attributes Trust Framework provides a useful model by promoting secure verification while limiting unnecessary data exposure. At the same time, privacy-preserving technologies such as hashing can allow verification without storing sensitive personal information, which balances enforcement with data protection. The failure of earlier age verification efforts in many jurisdictions highlights that technological solutions must be both robust and rights-compliant to be effective.

Legal reforms and statutory amendments

Legal reform must address the substantive gaps identified in the existing framework. The Personal Data Protection Act should incorporate explicit provisions for minors, including stricter consent requirements and limitations on data processing. Children's data requires a higher level of protection due to their vulnerability and limited capacity to provide informed consent. The Online Safety Act should expand beyond content regulation to directly address forms of harm such as grooming, sextortion and algorithmic amplification of harmful material. It should also impose clearer duties on platforms to prevent harm rather than merely respond to complaints. Similarly, amendments to the Penal Code, particularly Section 286, are necessary to define key terms such as "*obscene*" and extend criminal liability to modern forms of abuse, including AI-generated content, which has rapidly increased in recent years.

A shift from prohibition to regulation is therefore both necessary and justified. Global evidence consistently shows that online harm is not caused solely by access but by a combination of behavioural, technological and structural factors. Cyberbullying affects at least one in five children worldwide and its impacts include anxiety, depression, social withdrawal and reduced academic performance.[67] These harms persist regardless of age restrictions because they are embedded in how digital platforms operate and how users interact within them. A blanket ban fails to engage with these underlying dynamics. A comprehensive regulatory framework that integrates education, parental responsibility, technological safeguards and targeted legal reform offers a more sustainable and proportionate response.

Conclusion

The issue of online child safety in Sri Lanka has reached a critical point, as demonstrated by the recent surge in incidents involving cyber exploitation, non-consensual image sharing and digital harassment of minors. The evidence presented throughout this analysis makes it clear that these are not isolated occurrences but manifestations of a deeper structural problem rooted in the interaction between vulnerable users, inadequate legal safeguards, weak enforcement mechanisms and platform designs that prioritise engagement over safety. While the State's intention to protect children is both legitimate and necessary, a blanket ban on social media for

[67] United Nations, *'Safeguarding childhood online – How cyberbullying threatens children's safety globally'* (UN Peace and Security, 10 March 2026) <https://www.un.org/en/peaceandsecurity/safeguarding-childhood-online-how-cyberbullying-threatens-childrens-safety-globally> accessed 9 April 2026.

minors does not offer a proportionate or effective solution. Instead, it risks violating fundamental rights, isolating children from an increasingly essential digital environment and pushing them towards unregulated spaces where risks are more severe and less visible.

Both domestic and international legal frameworks emphasise that children's rights must be protected in a manner that balances safety with participation, development and access to information. The comparative analysis further demonstrates that although countries are moving toward stricter regulation, the most effective models are those that combine restriction with supervision, technological safeguards and education rather than relying solely on prohibition. In this context, Sri Lanka must avoid adopting an overly simplistic regulatory response and instead pursue a more nuanced and adaptive approach that reflects the realities of the digital age.

The proposed reforms provide a pathway toward such an approach. An evolving capacities model allows children to gradually engage with digital platforms under structured safeguards, rather than facing absolute exclusion. Digital literacy and social awareness programmes address the root behavioural causes of online harm by equipping both children and parents with the knowledge required to navigate digital risks. The introduction of parental accountability creates a shared responsibility framework that recognises the role of families alongside the State and technology companies. At the same time, technological reforms grounded in "safe-by-design" principles, improved age verification systems and privacy-preserving tools such as hashing can significantly reduce exposure to harmful content without compromising fundamental rights.

Crucially, these reforms must be supported by targeted legal amendments. Strengthening the Personal Data Protection Act in relation to minors, expanding the scope of the Online Safety Act to directly address forms of exploitation such as grooming and sextortion and clarifying provisions within the Penal Code are necessary steps to close existing legal gaps. Without such reforms, the law will continue to lag behind the rapidly evolving nature of digital harm, leaving children inadequately protected.

Ultimately, the challenge of online child safety cannot be resolved through a single measure. It requires a coordinated and multi-dimensional response that addresses legal, technological and social dimensions simultaneously. A shift away from blanket bans toward a comprehensive regulatory framework is not only more consistent with constitutional and international standards but also more effective in addressing the real risks that children face online. By

adopting such an approach, Sri Lanka can move beyond reactive policymaking and establish a sustainable system that protects children while preserving their rights and opportunities in the digital world.

References

1. Abeyratne R, 'Constitutional Rights: Life and Personal Liberty in Sri Lanka' *Sri Lanka Guardian* (9 May 2024) <http://www.srilankaguardian.org/2024/05/constitutional-rights-life-and-personal.html> accessed 22nd March 2026

2. Ada Derana, 'Sri Lanka considering restricting access to social media for children under 12' (Colombo, 29 January 2026) <https://www.adaderana.lk/news.php?nid=117755> accessed 5 February 2026

3. Asian Mirror, 'Education Ministry Probes Colombo School Incident After Content Circulates Online' (Colombo, 27 January 2026) <https://asianmirror.lk/news/12067/education-ministry-probes-colombo-school-incident-after-content-circulates-online/> accessed 5 February 2026

4. Bandaranayake BMP, 'Combating online child sexual exploitation and abuse in Sri Lanka: Towards a statutory response' (16th International Research Conference, General Sir John Kotelawala Defence University, 2023)

5. BBC News, Lee S-w and Wang F, 'South Korea bans phones in school classrooms nationwide' (27 August 2025) <https://www.bbc.com/news/articles/c776ye6lrvzo> accessed on 8 April 2026

6. BBC News, Mackintosh T, 'Spain announces plans to ban social media for under-16s' (24 February 2026) <https://www.bbc.com/news/articles/c5y2nddvmryo> accessed 2 April 2026

7. BBC News, *'Did Australia's under-16 social media ban work?'* (BBC News, March 2026) <https://www.bbc.com/news/articles/cwyp9d3ddqyo> accessed 8 April 2026

8. Centre for Policy Alternatives, 'Open letter to Facebook: Implement Your Own Community Standards' (10 April 2018) <https://www.cpalanka.org/open-letter-to-facebook-implement-your-own-community-standards/> accessed 4 April 2026

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

10. Constitution of the Democratic Socialist Republic of Sri Lanka 1978

11. Daily Mirror, 'Spotlight on leaked school video: Stringent laws needed to check sharing private content online' (Colombo, 2 February 2026) <https://www.dailymirror.lk/news-features/Spotlight-on-leaked-school-video-Stringent-laws-needed-to-check-sharing-private-content-online/131-331820> accessed 5 February 2026

12. DataReportal, Kemp S, 'Digital 2025: Sri Lanka' (25 February 2025) <https://datareportal.com/reports/digital-2025-sri-lanka> accessed 5 April 2026

13. Deutsche Welle, Mikkelsen C, 'Denmark to ban social media for children under 15' (13 November 2025) <https://www.dw.com/en/denmark-to-ban-social-media-for-children-under-15/a-74666210> accessed 2 April 2026

14. Deshapriya U, ‘Amidst Virtual Impunity: The experience of using local languages online in Sri Lanka’ (State of Internet’s Languages Report, 2022) <https://internetlanguages.org/en/stories/amidst-virtual-impunity/> accessed 4 April 2026

15. ECPAT International, *Access to Justice and Legal Remedies for Children Subjected to Online Sexual Exploitation and Abuse* (2022)

16. European Broadcasting Union, *Digital Services Act Handbook* (February 2023)

17. Fathaigh RÓ, ‘[title of article]’ (European Audiovisual Observatory, IRIS Merlin) <https://merlin.obs.coe.int/article/10492> accessed 2 April 2026

18. General Data Protection Regulation (EU) 2016/679

19. Guardian, Kassam A, ‘Norway to increase minimum age limit on social media to 15 to protect children’ (23 October 2024) <https://www.theguardian.com/world/2024/oct/23/norway-to-increase-minimum-age-limit-on-social-media-to-15-to-protect-children> accessed 2 April 2026

20. Ingram D, ‘Florida’s Ron DeSantis signs bill banning social media for kids under 14’ *NBC News* (25 March 2024) <https://www.nbcnews.com/tech/florida-ron-desantis-signs-bill-social-media-kids-ban-rcna144950> accessed 2 April 2026

21. Internet Watch Foundation, *AI CSAM Report 2026: Harm without limits* (2026)

22. Kalansooriya N, ‘Addressing Child Harassment on Social Media in Sri Lanka: A Comparative Analysis of Legal Frameworks’ (2023) 2 *APIIT Law Journal* 22

23. Le Monde, ‘France requires parental consent for under-15s on social media’ (29 June 2023) <https://www.lemonde.fr/en/france/article/2023/06/29/france-requires-parental-consent-for-under-15s-on-social-media_6039514_7.html> accessed on 20 March 2026

24. Mahingoda C, Harasgama K and Jayamaha S, ‘Unveiling Sri Lanka's Legal Landscape: Addressing Cybersex Trafficking Through Current Online Harassment Laws’ (17th International Research Conference, General Sir John Kotelawala Defence University, 2024)

25. Masri-Zada T and others, ‘The Impact of Social Media & Technology on Child and Adolescent Mental Health’ (2025) 9(2) *Journal of Psychiatry and Psychiatric Disorders* 111

26. Meegammana N and Punchihewa S, ‘Introducing an Effective Cybercrime Regime for Sri Lanka: A Comparative Analysis’ (2020)

27. National Child Protection Authority, *Child Abuse and Other Child-related Complaints Reported to NCPA* (2025)

28. National Child Protection Authority, *Child Abuse and Other Child-related Complaints Reported to NCPA* (2026)

29. Odgers CL and Jensen MR, ‘Adolescent Mental Health in the Digital Age: Facts, Fears and Future Directions’ (2020) 61(3) *Journal of Child Psychology and Psychiatry* 336

30. Online Safety Amendment (Social Media Minimum Age) Act No. 127, 2024

31. Penal Code Ordinance No 2 of 1883

32. Personal Data Protection Act, No. 9 of 2022

33. Prkno D and others, 'Children's and Adolescents' Negative Internet Experiences' (2025) 9(1) *BMJ Paediatrics Open*

34. Ranasinghe R, 'Patterns and Trends in Child Abuse Complaints in Sri Lanka' (2026)

35. Ronan Ó Fathaigh, 'Portugal to ban social networks for children under 16' (European Audiovisual Observatory, IRIS Merlin) <https://merlin.obs.coe.int/article/10492> accessed 2 April 2026

36. Social Policy Analysis and Research Center, *Online Violence against Children in Sri Lanka* (2021)

37. Sunday Times, 'Legal basis to be laid for weaning children away from digital addiction' (Colombo, 1 February 2026) <https://www.sundaytimes.lk/260201/news/legal-basis-to-be-laid-for-weaning-children-away-from-digital-addiction-630361.html> accessed 5 April 2026

38. UNICEF, *Keeping Children in Sri Lanka Safe and Empowered Online* (2017)

39. United Nations, 'Safeguarding childhood online – How cyberbullying threatens children's safety globally' (2026) <https://www.un.org/en/peaceandsecurity/safeguarding-childhood-online-how-cyberbullying-threatens-childrens-safety-globally> accessed 9 April 2026

40. United Nations Children's Fund, 'Cyberbullying: What is it and how to stop it' (2026) <https://www.unicef.org/stories/how-to-stop-cyberbullying> accessed 9 April 2026

41. United Nations Children's Fund, 'UNICEF poll: More than a third of young people…' (2019) <https://www.unicef.org/press-releases/unicef-poll-more-third-young-people-30-countries-report-being-victim-online-bullying> accessed 9 April 2026

42. Verité Research, 'Better Moderation of Hate Speech on Social Media' (2021)

43. WeProtect Global Alliance, *Global Threat Assessment 2025* (2025)

44. Wijeratne Y, 'The Control of Hate Speech on Social Media: Lessons from Sri Lanka' (2018)

45. Zhu C and others, 'Cyberbullying Among Adolescents and Children' (2021) 9 *Frontiers in Public Health*