



Dear ,

Child protection online: Global legislative, regulatory and policy update

Between August 2025 and February 2026, governments worldwide accelerated reforms addressing **AI-enabled abuse, children's access to online services, and platform accountability**.

A clear trend emerged toward **criminalising AI-generated child sexual abuse material and so-called deepfakes**. **Argentina's** courts set a global precedent by confirming that AI-generated CSAM is equivalent to traditional CSAM under criminal law, prompting new legislative proposals. Similar momentum is visible in **India, Türkiye and Denmark**, where lawmakers are seeking to modernise offences to reflect AI-driven harms.

At the same time, **age-based access controls** moved firmly into the mainstream. **Australia** implemented a nationwide ban on social media for under-16s, while proposals or laws restricting youth access advanced in **France, Malaysia, the United Kingdom**, and several US states.

Regulators also strengthened **safety-by-design and enforcement frameworks**. **Brazil** enacted far-reaching child-rights focussed digital obligations with significant regulatory powers, while **Italy** and **Singapore** expanded age-verification and redress mechanisms.

At regional and global level, negotiations advanced on **EU child protection legislation** and the **United Nations Convention against Cybercrime** opened for ratification, signalling growing international alignment on tackling technology-facilitated child sexual abuse and exploitation.

Please note that this is a briefing produced for WeProtect Global Alliance members and not an exhaustive list of developments and is intended to be a summary only.

NATIONAL DEVELOPMENTS



Criminalisation of AI-enabled Abuse and Exploitation

A number of jurisdictions have taken steps to modernise criminal law frameworks to address AI-enabled sexual exploitation, particularly AI-generated child sexual abuse material (AI-CSAM) and so-called 'deepfakes'.

In **Argentina**, a significant judicial development occurred in August 2025 when a high court in the Province of Buenos Aires ruled that AI-generated CSAM should be treated equivalently to non-AI CSAM under Article 128 of the Penal Code, even where the images do not depict identifiable victims. This decision established binding national jurisprudence recognising AI-CSAM as a criminal offence and directly prompted legislative action. In October 2025, the Argentine Government introduced [Bill No. 5945-D-2025](#) before the Chamber of Deputies. The Bill proposes a special judicial remedy where an individual's image has been altered using AI, machine learning or neural networks, covering both AI-CSAM and non-consensual intimate image abuse. It would allow affected individuals or their representatives to file digital claims at no cost and empower judges to order immediate blocking, removal or de-indexing of content, with permanent deletion where unauthorised use is confirmed. The Bill remains under deliberation.

In **India**, Parliament has seen the introduction of two legislative measures targeting deepfakes and online harassment. In early December 2025, the [Regulation of Deep Fake Bill \(No. 193 of 2024\)](#) was introduced as a Private Members' Bill in the House of the People. The Bill proposes criminal penalties for the creation or dissemination of non-consensual deepfakes, including sexually explicit material and content capable of inciting violence, disrupting official processes or facilitating fraud. Article 4 of the Bill establishes a dedicated Taskforce on Deep Fakes to oversee implementation. Separately, a draft Bill [amending the Information Technology Act \(2000\) \(No. 16 of 2025\)](#) seeks to define and criminalise online harassment, stalking and harmful deepfakes. Both measures remain under parliamentary consideration.

In **Türkiye**, legislative amendments to strengthen protections against CSAM were introduced in late October 2025. **Bill No. 5237**, currently before the Grand National Assembly's Justice Committee, seeks to clarify Article 226 of the Turkish Penal Code by expanding the scope of the offence of obscenity to explicitly criminalise access to, distribution of and promotion of CSAM.

In **Denmark**, the Government has proposed amendments to the Copyright Act to grant individuals copyright over their own likenesses, including voice and image, as a mechanism to prevent the spread of AI-generated deepfakes. The proposal introduces consent-based protections for both private individuals and artists and performers, with enforcement governed by the EU Digital Services Act. Public [consultation](#) closed in early February 2026 and next steps are currently under consideration by the Government. The EU's technical regulation information system has been notified (notification number 2025/0654/DK).



Age-based Access Restrictions

Across multiple jurisdictions, governments have advanced or implemented age-based restrictions on children's access to social media and other online services.

In **Australia**, the [Online Safety Amendment \(Social Media Minimum Age\) Act](#) entered into force on 10 December 2025, prohibiting children under 16 from accessing social media platforms. Ahead of commencement, the eSafety Commissioner published a list of applications covered by the Act, confirming that major platforms including Facebook, Instagram, TikTok, YouTube, Snapchat, X, Threads and Reddit are subject to the restrictions. To support compliance, the [Social Media Minimum Age Regulatory Guidance](#) was published in September 2025, setting out minimum standards for detecting and removing underage accounts, preventing re-registration and providing clear user information, alongside a [self-assessment](#) tool. These measures complement newly registered [Phase 2 industry codes](#) under the Online Safety Act, which impose enhanced safety and age-verification requirements across social media, app stores, gaming services and device manufacturers from March 2026. They include a range of measures designed to protect children from age-restricted content such as pornography and self-harm material. The first set of three age restricted material codes were registered in June 2025 and came into effect on 27 December 2025, applying to search engines, hosting services and internet carriage services.

In **France**, the National Assembly approved [Bill No. 2107](#) in January 2025, proposing a prohibition on social media access for children under 15. The Bill will now move to the French Upper House, the *Sénat*, for consideration before the *navette* process begins, in which both Houses negotiate the final text of the bill.

In **Malaysia**, in November the Cabinet approved proposed restrictions preventing children under 16 from creating social media accounts. These measures are being tested through a digital regulatory sandbox, which enables technology companies to test approaches in a controlled environment, introduced in 2024. While detailed obligations are yet to be finalised, the proposal is expected to mandate age-verification mechanisms such as electronic know-your-customer checks and may take effect from July 2026, following the passage of the [Online Safety Act 2025](#).

In **United Kingdom of Great Britain and Northern Ireland**, the Government announced in January 2026 that it is considering introducing social media age restrictions for under-16s. It has launched a [public consultation](#) involving children, parents and civil society which closes on 26 May 2026. The announcement also confirmed that schools in England are expected to be phone-free by default, with compliance considered by Ofsted during inspections.

At state level in the **United States of America**, several measures were adopted. California enacted [SB 243](#), addressing harms associated with AI companion chatbots used by children. South Carolina passed [HB 3431](#), which would introduce an Age-Appropriate Design Code upon gubernatorial assent. In Virginia, [SB 854](#) entered into force on 1 January 2026, limiting social media use for children under 16 to one hour per day without verified parental consent.



Safety-by-Design and Platform Accountability

Governments are increasingly embedding child protection requirements directly into the design and operation of digital services.

In **Brazil**, [Law No. 15.211](#) was signed into law in August 2025 following cross-party approval by Congress. The law mandates safety-by-design measures across digital services, requiring providers to mitigate risks of children's exposure to inappropriate content, products and practices. Services legally restricted for children must implement robust age-verification mechanisms, and social media platforms must link accounts belonging to children under 16 to those of legal guardians. The legislation also introduces duties of prevention, including investment in digital literacy, bans on loot boxes and Portuguese-language parental controls, alongside mandatory reporting and content removal obligations. Enforcement powers rest with the National Data Protection Agency, with penalties including fines of up to 10% of Brazilian revenue, service suspension and prohibition of operations. The law enters into force in March 2026 and applies extraterritorially.

In **China**, national technical safety regulations for children's smartwatches ([GB 46859-2025](#)) were adopted in December 2025. The standards apply to devices for children aged 3–14 and address data security, parental controls and content safeguards, with effect from January 2027.

In **France**, [Decree No. 2025-767](#) entered into force in October 2025, requiring pornographic platforms to display warnings on content depicting simulated rape or incest.

In **Italy**, the Communications Regulatory Authority's [Resolution 96/25/CONS](#) came into force in November 2025, establishing technical and procedural requirements for age-verification systems to prevent children from accessing pornographic content in line with [Legislative Decree No. 123/2023](#) and [Law No. 159/2023](#). The regulator had previously identified 48 platforms subject to these obligations.

In **Singapore**, the [Online Safety \(Relief and Accountability\) Act 2025](#) received Presidential assent in November 2025. The Act aims to improve complaint and redress mechanisms for those impacted by online harms, promote online safety and increase accountability for actions individuals and companies' actions online. The Act also establishes an independent Online Safety Commission empowered to receive complaints, investigate online harms and order remedies including content removal, account suspension and disclosure of offender information. Under the provisions of the Act, the Commission is able to receive reports (Section 22), investigate online harms (Section 24) and will be able to take a series of actions under Section 28 of the Act, including ordering content removal, suspending accounts, and requiring platforms to disclose offender information. The Bill also introduces civil remedies - known as statutory torts - for victims and clearer liability for individuals and platforms that facilitate harmful content. The law is currently uncommenced, but is expected to take effect in the second half of 2026.



Child-friendly Justice and Investigation

In **Finland**, the Government consulted on legislation to permanently embed the Barnahus multidisciplinary model into investigations of suspected offences involving children, following a successful pilot as part of an EU/Council of Europe project from 2021-2024. This model, originally adopted in Iceland in 1998, is a multidisciplinary model bringing together police, social workers, healthcare professionals, and psychologists and making these a permanent fixture in forensic and psychiatric units. The Act on Social and Health Care Units Assisting in the Investigation of Suspected Offences Involving Children is currently under consideration following the public consultation closing on 15 December and, pending approval, is scheduled to enter into force at the start of 2027, according to the Finnish Government.



Terminology Reform

In **Canada**, [Bill C-291](#) received Royal Assent in October 2025, amending the Criminal Code and related legislation to replace the term "child pornography" with "child sexual abuse and exploitation material", aligning domestic law with [international terminology standards](#).

REGIONAL & GLOBAL DEVELOPMENTS

On 26 November 2025 the Council of the **European Union** reached an [agreed position](#) on the EU Child Sexual Abuse Regulation. This paved the way for the commencement of trilogue negotiations – a series of technical and political meetings between the Council of Ministers, European Commission and European Parliament - which started on 15 January 2025 with a view to agreeing a finalised text of the Regulation. The European Parliament had previously agreed a position on the Regulation in November 2023.

On 19 December 2025 the European Commission announced its [proposal to extend the interim Regulation on the ePrivacy Directive](#) to 3 April 2028. The interim measure would allow interpersonal communications services to use specific technologies for the processing of personal and other data to the extent strictly necessary to detect online child sexual abuse on their services and report it and to remove CSAM. On 11 March 2026 the [European Parliament voted](#) to agree its position, which would extend the interim Regulation until 3 August 2027 and narrows the scope to permitting the detection only of known-CSAM. The Parliament, Council and Commission have entered into trilogue negotiations to agree a finalised text and are expected to reach a compromise position before 3 April 2026 when the existing interim derogation expires.

Trilogue negotiations on the re-cast Directive on combating child sexual abuse ([Directive 2011/93/EU](#)) continue, following its passage by the European Parliament on 17 June 2025. The Directive is intended to

expand the definition of offences to cover those enabled by digital tools such as generative AI, increasing penalties for offenders, and introducing more specific requirements for member states on prevention and victim support.

Within **Southern Common Market (Mercosur)**, leaders adopted a Special Declaration on the Protection of Children and Adolescents in Digital Environments, recognising emerging risks including AI and committing to enhanced regional cooperation. Signed by the leaders of Argentina, Brazil, Paraguay, Uruguay, Bolivia, Panama and Chile, the Declaration recognised the digital environment as a vital resource for children and highlighted increasing prevalence of cybercrimes and their impact on children.

Globally, the **United Nations Convention against Cybercrime** opened for signature in October 2025, with 72 states signing at launch. As outlined in our [blog](#) on the treaty, the Convention includes key provisions on online child sexual abuse, grooming and non-consensual intimate imagery and will enter into force following the 40th signatory acceding to the Convention.



HAVE SOMETHING TO SHARE?

If you'd like us to include an update in the next issue or have any questions, please contact katie@weprotectga.org

This legislation and policy update was funded by the European Union's Internal Security Fund - Police. The content of this update does not represent the views of the European Commission. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This material is provided for informational purposes only and may or may not reflect the most current legislation policy or regulatory developments. Accordingly, information in this newsletter is not promised or guaranteed to be correct or complete, and should not be relied upon as such. Readers should conduct their own appropriate research.



Sent to: gina@weprotectga.org

[Unsubscribe](#)

WeProtect Global Alliance, 16 Upper Woburn Place, London, WC1H 0AF, United Kingdom