weprotect Global Alliance

CPC LEARNING NETWORK

COLUMBIA | MAILMAN SCHOOL OF PUBLIC HEALTH

Avaliação da Ameaça global 2025

Prevenção da exploração e abuso sexual infantil facilitados pela tecnologia: **das ideias à acção**

Índice

Nota sobre o conteúdo e recursos de apoio

Este relatório discute a exploração e o abuso sexual infantil facilitados pela tecnologia, incluindo relatos de sobreviventes que podem ser angustiantes. Alguns leitores podem achar algumas secções do relatório difíceis de ler. Se este conteúdo causar preocupação, consulte os recursos globais confidenciais mencionados aqui.

Não está sozinho — há apoio disponível.

- Brave Movement, Get Help: Central de linhas de apoio nacionais.
- Child Helpline International: Linhas de apoio específicas para crianças em cada país.
- INHOPE: Rede global de linhas diretas para denunciar material de abuso sexual infantil no seu país.
- MOORE | Prevenção do abuso sexual infantil, Escola de Saúde Pública Johns Hopkins Bloomberg: Orientação e recursos para indivíduos que procuram ajuda para si ou para outra pessoa a fim de prevenir o abuso sexual infantil.
- Programa de Autoajuda ReDirection: Recurso *online* confidencial que apoia indivíduos preocupados com os seus pensamentos ou comportamentos sexuais em relação a crianças.

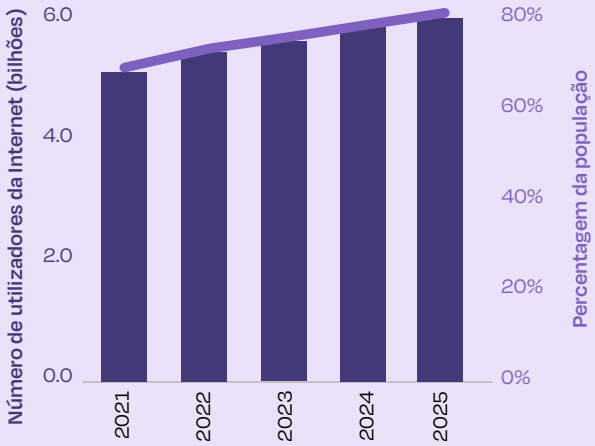
Resumo

> **“O futuro do nosso mundo digital não precisa ser assustador — ele pode ser empolgante e enriquecedor. Mas temos que abordá-lo com cuidado, responsabilidade e transparência. À medida que entramos nesta nova era da IA, precisamos garantir que a geração mais jovem não apenas esteja preparada para navegar por esses espaços, mas também sejam fortalecidos para os transformar em algo melhor.”**
>
> *Defensor dos jovens*[1]

A exploração e abuso sexual infantil facilitados pela tecnologia (sigla inglesa CSEA) são um desafio global complexo que causa danos profundos às crianças, famílias e comunidades. Esta ameaça é **prevenível, não inevitável**.[2] Combater esta questão requer uma acção coordenada e intersectorial centrada nos direitos das crianças, e dados e estratégias promissores estão a surgir a nível global. A Avaliação da Ameaça Global 2025 adopta uma abordagem orientada para a acção, avaliando o panorama actual e enfatizando a prevenção e medidas práticas para manter as crianças seguras.

O panorama digital está a transformar-se rapidamente, criando novas ameaças para as crianças e desafios para a detecção e aplicação da lei. Actualmente mais de 6.0 mil milhões de pessoas utilizam a Internet, e o acesso dos jovens ultrapassa o da população em geral[3,5] e mais da metade da população mundial possui um *smartphone*.[4]

Figura 1 . Tendências no uso da Internet nos últimos cinco anos[5]



Embora as tecnologias digitais criem oportunidades de conexão, aprendizagem e expressão, também expõem as crianças a novos riscos. A tecnologia é frequentemente um amplificador de danos que atravessa os espaços físicos, sociais e digitais. As tecnologias existentes e emergentes, como a inteligência artificial (IA) generativa, a criptografia e a realidade estendida, estão a remodelar os ambientes digitais das crianças. Em alguns poucos anos, a IA generativa, incluindo os *chatbots* de IA, passou de algo amplamente experimental para algo totalmente integrado nas redes sociais, plataformas

de mensagens e ferramentas do quotidiano que as crianças utilizam.[6] Embora estes desenvolvimentos tragam benefícios, também criam desafios substanciais para a prevenção, detecção e aplicação da lei. As plataformas encriptadas aumentam a privacidade do utilizador, mas também podem reduzir as barreiras à prática de crimes contra crianças e também tornam mais difícil detectar, bloquear e remover material de abuso sexual infantil (CSAM). Especialistas da sociedade civil destacam uma tendência contínua em que alguns infractores iniciam o contacto com crianças em plataformas abertas antes de transferir as interações para canais encriptados ou ambientes *offline* com a intenção de causar danos. Além disso, evidências crescentes sugerem que a exploração e o abuso sexual perpetrados por pares parecem estar a aumentar, e a exposição a conteúdo sexual *online* inadequado para o desenvolvimento pode estar a desempenhar um papel importante.[7–9] Os danos causados por pares, colegas de classe e parceiros íntimos geralmente surgem quando proteções digitais fracas, supervisão deficiente e educação limitada sobre conduta *online* e comportamentos sexuais adequados se cruzam.[10,11]

O CSEA facilitado pela tecnologia continua a expandir-se em escala e complexidade, moldado por rápidas mudanças tecnológicas e lacunas sistémicas. Desde 2023, os danos existentes têm persistido em grande parte, enquanto novas ameaças surgiram mais rapidamente do que as leis, políticas e salvaguardas podem se adaptar. O CSAM está a ser detectado, denunciado e removido em níveis recordes. Dados globais confiáveis sobre a prevalência continuam difíceis de obter, e é necessário ter cautela ao interpretar as tendências observadas nas denúncias, pois estas muitas vezes reflectem a capacidade e as práticas de denúncia, em vez da verdadeira escala dos danos. Por exemplo, as denúncias à CyberTipline do Centro Nacional para Crianças Desaparecidas e Exploradas (sigla inglesa NCMEC) caíram de 36,2 milhões em 2023 para 29,2 milhões de incidentes, associados a 20,5 milhões de denúncias, em 2024. Esta diminuição é em grande parte atribuída às práticas de «agrupamento», em que as denúncias relacionadas são agrupadas, e à encriptação de ponta a ponta, que limita a detecção e a denúncia.[12]

A INHOPE recebeu **2,5 milhões** de denúncias de suspeita de CSAM em 2024, mais do que o dobro do ano anterior.[13]

O NCMEC recebeu **20,5 milhões** de denúncias de suspeita de exploração sexual infantil em 2024.[12]

A Internet Watch Foundation (IWF) confirmou quase **300.000** casos de CSAM em 2024.[14]

A IA generativa tem sido utilizada para facilitar a criação e distribuição de CSAM em grande escala, para ocultar as identidades das vítimas e dos agressores e para contornar leis e salvaguardas, tais como métodos de verificação da idade. Também tem alimentado novas formas de CSEA, incluindo extorsão sexual financeira e imagens *deepfake* que retratam crianças reais em situações sexualizadas simuladas. No final de 2023, as primeiras imagens de abuso sexual infantil geradas por IA foram denunciadas através de linhas directas da Internet e, desde então, a sua prevalência aumentou exponencialmente.[15] A **CyberTipline** do NCMEC registou um aumento de 1325% nas denúncias relacionadas com IA generativa entre 2023 e 2024, representando 67.000 denúncias.[12] Este volume sobrecarrega as agências de aplicação da lei e os moderadores de conteúdo.

Nos primeiros seis meses de 2025, mais de **440.000** denúncias de IA generativa relacionadas com a exploração sexual infantil foram recebidas pelo NCMEC.[12]

A sedução e o aliciamento *online* continuam prevalentes. Em 2024, o NCMEC registou 546.000 denúncias, um aumento de 192% em relação a 2023.[12] Os especialistas também estão a observar intersecções alarmantes entre o CSEA facilitado pela tecnologia e outros danos, incluindo pensamento suicida e automutilação, extremismo, tráfico de seres humanos e golpes com motivação financeira. Este fenómeno emergente requer mais investigação e continua a ser mal compreendido. A extorsão sexual financeira é uma tendência persistente que afecta desproporcionalmente os rapazes.

Em 2024, o NCMEC recebeu aproximadamente **100** denúncias de extorsão sexual financeira por dia.[12]

Está a ganhar força a tendência global para combater o CSEA facilitado pela tecnologia.

Desde 2023, vários países propuseram ou aprovaram nova legislação para abordar a questão. A **Lei dos EUA** de 2024 impôs obrigações adicionais às empresas de tecnologia, incluindo a obrigatoriedade de comunicar ao NCMEC casos que anteriormente eram voluntários e multas de até um milhão de dólares por violações.[16] A **Lei de Segurança** *Online* de 2023 do Reino Unido alarga novos requisitos, incluindo avaliações de risco e garantia de idade, a centenas de milhares de prestadores de serviços *online* em todo o mundo que têm como alvo os utilizadores do Reino Unido.[17] No Brasil, duas medidas históricas de proteção à criança em 2025 incluíram a proibição nacional do uso não educacional de smartphones nas escolas e uma nova legislação que introduz a segurança desde a concepção e obrigações de notificação para plataformas *online*.[19,20] A Austrália adoptou um incremento na idade para o uso de redes sociais, restringindo o uso para crianças menores de 16 anos, que está actualmente a ser implementado.[18] Em Singapura, o regulador de telecomunicações exigirá em breve verificações de idade para baixar determinados aplicativos em dispositivos móveis — a primeira legislação desse tipo em todo o mundo.[21] O impacto total dessa onda de legislação ainda está para ser visto, à medida que as políticas avançam para a regulamentação e implementação. A **Convenção das Nações Unidas contra o Crime Cibernético**, adoptada em Dezembro de 2024 e agora em vias de ratificação, constitui um marco importante na proteção infantil global. Pela primeira vez, ela torna os crimes do CSAM e aliciamento *online* passíveis de punição pela legislação internacional.[22,23] O **Global Digital Compact** (Pacto Global Digital), implementado em 2025, fornece uma estrutura para a cooperação internacional, orientando os esforços para lidar com os danos *online* e fortalecer a segurança digital.[24]

Também foram alcançados progressos notáveis por meio da adopção da segunda edição das **Diretrizes de Terminologia para a Proteção das Crianças contra a Exploração e o Abuso Sexual** (abreviada para Diretrizes de Terminologia), o lançamento de parcerias inovadoras intersectorial para melhorar a detecção e a prevenção, como **a Lantern**, e as pesquisas em grande escala destinadas a colmatar lacunas de evidência.[25,26] A Safe Futures Hub's **Living Systematic Review** (Revisão Sistemática em Tempo Real da Safe Futures Hub) fornecerá evidências actualizadas, enquanto iniciativas como **a Prevention Global** expandem o conhecimento sobre a prevenção da perpetração e a prevalência global.[27,28]

As perspetivas das crianças continuam sub-representadas. Apesar de algumas abordagens promissoras para integrar as perspetivas das crianças nas políticas e na tomada de decisões, muitas vezes não são oferecidas às crianças oportunidades de participar de forma significativa nas decisões políticas que as afectam. A nossa revisão da literatura publicada desde 2023 relacionada com o CSEA facilitado pela tecnologia revelou que uma minoria das publicações incluía as vozes das crianças e muito poucas consultaram as crianças sobre as suas recomendações para acção. A Avaliação da Ameaça Global 2025 envolveu consultas com crianças para ajudar a informar e moldar as recomendações apresentadas.

O CSEA facilitado pela tecnologia pode ser prevenido, mas não existe uma solução universal. A prevenção requer uma acção de toda a sociedade. O quadro de prevenção apresentado neste relatório, que complementa o Modelo de Resposta Nacional da WeProtect Global Alliance, oferece orientações práticas em quatro áreas de acção interligadas:[29]

- PARTICIPAÇÃO E LIDERANÇA INFANTIL
- EDUCAÇÃO E APOIO COMUNITÁRIO
- SEGURANÇA DIGITAL
- LEGISLAÇÃO, POLÍTICAS E JUSTIÇA

Estas áreas de acção estão mapeadas em três níveis de prevenção:

- primário (proteção proactiva),
- secundário (detecção e interrupção dos danos) e
- terciário (resposta e apoio após a ocorrência dos danos, o que pode prevenir a revitimização e a reincidência).

A estrutura sintetiza evidências emergentes, boas práticas e orientações de especialistas. O objectivo é fornecer um ponto de entrada para que as partes interessadas considerem acções de prevenção relevantes para o seu contexto e experiência. As áreas de acção estão organizadas de forma a reflectir o modelo socio-ecológico, começando pelas crianças e progredindo pelas comunidades, instituições, governos e actores munidais.[30] Destaca a natureza em camadas da prevenção, em que cada nível reforça os outros. Facilitadores como financiamento e pesquisa fornecem a base para todas as acções e devem ser abordados de forma proactiva e sustentada para tornar a prevenção possível.

Estrutura de prevenção

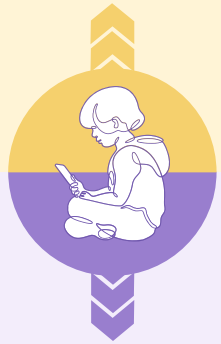
Princípios Orientadores

Todas as crianças têm o direito de estar protegidos de danos, incluindo exploração e abuso sexual.
Os esforços para prevenir a exploração e o abuso sexual da criança facilitados pela tecnologia devem:

- defender os direitos e a dignidade das crianças e dos sobreviventes e evitar aumentar os riscos ou causar mais danos;
- reconhecer que as crianças correm o risco de sofrer danos e de se envolver em comportamentos que podem prejudicar outras crianças;
- ser orientados pelas perspectivas, experiências e preferências das crianças e dos sobreviventes; e
- levar em consideração as diferenças de idade, desenvolvimento e outras características das crianças — como identidade de género, orientação sexual, etnia, condição de deficiência, condição de migrante, situação económica e educacional — que podem afectar as suas necessidades e os riscos que enfrentam.

Factores que facilitam a exploração e o abuso sexual infantil facilitados pela tecnologia

- Falta de mecanismos de proteção
- Motivações financeiras
- Governação e responsabilização fracas
- Vulnerabilidades interseccionais
- Normas sociais prejudiciais



Factores que facilitam a prevenção

- Vontade política
- Forte governação digital e responsabilização a nível mundial, nacional e local
- Terminologia e sistemas de dados harmonizados
- Coordenação global e intersectorial
- Normas sociais favoráveis
- Profissionais e provedores de serviços com formação para lidar com crianças
- Sistemas sólidos de proteção a criança

Pesquisa e dados

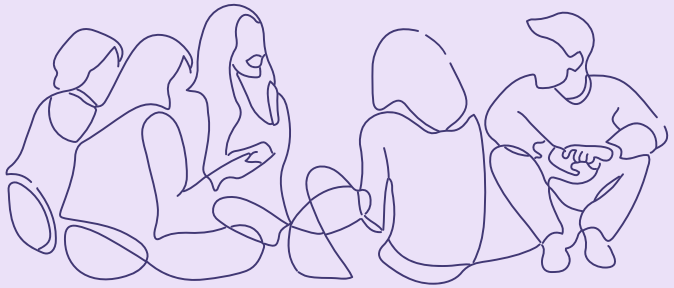
- Utilizar uma abordagem de saúde pública para definir o problema e a prevalência, identificar factores de risco e de proteção, conceber e testar intervenções e expandi o que funciona.
- Priorizar pesquisas informadas ou lideradas por crianças, jovens, sobreviventes e populações marginalizadas
- Desenvolver conhecimento e boas práticas em países de baixa e média renda e contextos sub-representados
- Partilhar dados, conhecimento e boas práticas entre regiões e sectores, adaptando as evidências com sensibilidade a novos contextos
- Realizar análises de custo-benefício para fortalecer os argumentos a favor do financiamento da prevenção

Financiamento sustentável

- Rubricas orçamentais específicas nas estratégias nacionais
- Compromissos da indústria
- Participação de instituições multilaterais
- Mecanismos de financiamento flexíveis
- Financiamento intersectorial
- Apoio sustentável a organizações comunitárias
- Financiamento para inovação e geração de evidências

PARTICIPAÇÃO E LIDERANÇA INFANTIL

Envolver consideravelmente as crianças na definição dos problemas e na elaboração de políticas, programas e serviços que as afectam.



Prevenção primária **PROTEÇÃO PROACTIVA**	Prevenção secundária **DETECTAR E INTERROMPER**	Prevenção terciária **APOIAR E RESPONDER**
Criar, em conjunto com as crianças, iniciativas de educação e sensibilização sensíveis ao contexto, que reflictam a forma como elas utilizam a tecnologia, em quem confiam e a quem recorrem para obter ajuda se forem vítimas de danos ou tiverem preocupações sobre os seus próprios pensamentos e comportamentos.	Estabeleça parcerias com organizações lideradas por crianças e sobreviventes para co-desenhar, implementar e avaliar canais de denúncia acessíveis, fáceis de usar e confiáveis, incluindo canais não formais, como pares treinados.	Criar, em conjunto com as crianças, iniciativas de educação e sensibilização sensíveis ao contexto, que reflictam a forma como elas utilizam a tecnologia, em quem confiam e a quem recorrem para obter ajuda se forem vítimas de danos ou tiverem preocupações sobre os seus próprios pensamentos e comportamentos.

Consultar as crianças apenas quando houver pessoal treinado, medidas de segurança e serviços de apoio disponíveis. Caso contrário, consultar jovens e adultos que possam representar as perspectivas das crianças, incluindo sobreviventes adultos.

Criar espaços seguros e acolhedores, tanto *online* como *offline*, para que as crianças possam partilhar as suas opiniões e influenciar a elaboração de políticas, programas e serviços.

Envolver crianças de todas as faixas etárias, géneros e origens e aborde as barreiras à inclusão. Buscar a opinião de crianças que sofreram danos, bem como de crianças que causaram danos.

SEGURANÇA DIGITAL

Proteger as crianças, priorizando a sua segurança, bem-estar e direitos na cultura da indústria e na concepção e desenvolvimento de produtos, serviços e infraestruturas digitais.

Prevenção primária **PROTEÇÃO PROACTIVA**	Prevenção secundária **DETECTAR E INTERROMPER**	Prevenção terciária **APOIAR E RESPONDER**
Priorizar a segurança, os direitos e o bem-estar das crianças em todos os níveis da cultura da empresa, tomada de decisões e formação da mão-de-obra. Tornar a segurança por desenhar o padrão, integrando as avaliações de impacto dos direitos da criança e auditoria nos processos de desenvolvimento. Consultar crianças e jovens para informar as escolhas do desenho e garantir que os recursos de segurança sejam funcionais, acessíveis e disponíveis de forma equitativa em todos os locais e idiomas em que um produto ou serviço é oferecido. Harmonizar a terminologia e as métricas de transparência dos relatórios para melhorar a comparabilidade entre produtos e serviços.	Detectar e interromper conteúdos e comportamentos prejudiciais utilizando ferramentas em tempo real que respeitem a privacidade e os direitos dos utilizadores (por exemplo, correspondência de hash, pop-ups de aviso, redireccionamento para serviços de apoio, detecção de comportamentos de aliciamento e transações financeiras de risco). Financiar e fornecer apoio à saúde mental e psicossocial para os profissionais da linha de frente digital.	Fornecer canais de denúncia acessíveis e adequados para crianças dentro da plataforma. Estes devem ligar directamente os utilizadores a linhas de apoio e serviços de assistência e fornecer feedback oportuno. Garantir processos seguros e sem estigma para que os sobreviventes possam solicitar a remoção das suas imagens. Reforçar a transparência e a responsabilização, divulgando o impacto material dos produtos e serviços digitais nos direitos da criança em todos os países onde estão disponíveis. Recolher e partilhar dados de segurança anonimizados e desagregados para reforçar a aprendizagem em toda a indústria e entre sectores. Colaborar em toda a indústria para remover CSAM (sigla inglesa para Material de Abuso Sexual infantil) e outros conteúdos prejudiciais.

LEI, POLÍTICA E JUSTIÇA

Fortalecer os sistemas jurídicos e regulatórios para prevenir abusos, garantir a justiça e prestação de contas dos responsáveis.

Prevenção primária **PROTEÇÃO PROACTIVA**	Prevenção secundária **DETECTAR E INTERROMPER**	Prevenção terciária **APOIAR E RESPONDER**
Fortalecer, harmonizar e aplicar leis e regulamentos utilizando terminologia universal e definindo deveres e sanções claros. Consultar os sobreviventes, grupos de direitos da criança, indústria e outras partes interessadas para alinhar a legislação com as leis de direitos da criança, evidências e boas práticas, e permitir a inovação responsável da indústria. Elaborar leis que reconheçam as diferenças de desenvolvimento entre crianças e adultos, enfatizem a reabilitação das crianças que causam danos e evitem criminalizar comportamentos mutuamente desejados entre colegas de idade próxima. Estabelecer reguladores nacionais/regionais com poder, recursos e conhecimentos técnicos para definir normas, monitorar o cumprimento e garantir uma forte supervisão e responsabilização da indústria.	Estabelecer sistemas proactivos para detectar, investigar e responder ao CSEA (sigla inglesa para Abuso e Exploração Sexual infantil) facilitada pela tecnologia, em vez de depender exclusivamente dos relatos dos sobreviventes. Exigir que as instituições financeiras detectem e denunciem activamente transações relacionadas com a exploração sexual de crianças. Estabelecer canais de denúncia acessíveis, adequados às crianças e informados sobre traumas, ligados a serviços de apoio, e fornecer informações claras sobre onde as pessoas devem fazer denúncias ou procurar ajuda no seu país.	Treinar as autoridades policiais, judiciais e promotores em processos adequados às crianças, informados sobre traumas e centrados nos sobreviventes, que defendam os direitos, a dignidade e os melhores interesses das crianças. Criar bases de dados nacionais anónimas de vítimas para informar a prevenção e a resposta. Utilizar monitoria e reabilitação baseadas em evidências para prevenir a reincidência. Tratar as crianças em conflito com a lei de acordo com as normas internacionais de justiça infantil. Utilizar a reabilitação, medidas alternativas e penas alternativas. Evitar a detenção, o registo e a notificação.

EDUCAÇÃO E APOIO À COMUNIDADE

Equipar crianças, cuidadores e comunidades com conhecimento, competências e ferramentas necessárias para manter as crianças seguras e responder adequadamente aos riscos e danos. Oferecer intervenções imediatas para crianças e adultos em risco de causar danos.

Prevenção primária **PROTEÇÃO PROACTIVA**	Prevenção secundária **DETECTAR E INTERROMPER**	Prevenção terciária **APOIAR E RESPONDER**
Implementar e avaliar iniciativas de educação e sensibilização baseadas em evidências que promovam a segurança digital, a denúncia e a procura de ajuda. Garantir que sejam acessíveis, disponíveis em vários idiomas e disponibilizadas em escolas, comunidades e plataformas digitais que as crianças utilizam. Ensinar às crianças como manter a si mesmas e aos outros seguros *online* e *offline*, onde procurar ajuda, adultos seguros a quem podem recorrer para obter ajuda e como denunciar preocupações sobre a sua própria segurança ou a de outras pessoas ou comportamentos.	Estabelecer vários canais de denúncia formais e informais acessíveis e adequados às crianças, incluindo linhas de apoio, colegas treinados e adultos de confiança que possam fornecer apoio e recursos imediatos. Treinar colegas, cuidadores, educadores e provedores de serviços para ajudar as crianças a permanecerem seguras *online* e *offline* e responder adequadamente a preocupações ou denúncias de danos. Realizar intervenções imediatas baseadas em evidências para crianças e adultos em risco de causar ou sofrer danos.	Apoiar os sobreviventes e garanta que eles conheçam os seus direitos, opções, serviços disponíveis e acções que podem tomar para se protegerem de novos danos, solicitar a remoção de imagens e buscar justiça. Prestar serviços informados sobre traumas e centrados nos sobreviventes, tanto para crianças como para adultos, que abordem danos *online* e *offline*, promovam a segurança e a dignidade e previnam novos danos. Estes devem incluir serviços jurídicos, de saúde, de saúde mental e de apoio psicossocial. Fornecer respostas baseadas em evidências e não carcerárias para crianças que causaram danos, a fim de reabilitá-las e prevenir a reincidência.

Recomendações

As recomendações decorrentes da Avaliação da Ameaça Global 2025 destacam a necessidade de uma acção global coordenada para prevenir o CSEA facilitado pela tecnologia. Em conjunto, elas delineiam uma abordagem abrangente e multissectorial para proteger as crianças tanto *online* como *offline*.

Recomendações transversais para todas as partes interessadas

1. **Abordar o CSEA facilitado pela tecnologia como uma prioridade urgente de saúde pública e investir em estratégias de prevenção, incluindo aquelas destinadas a prevenir a perpetração e reduzir o estigma associado à procura de ajuda e à divulgação.** Reconhecer que as crianças correm o risco tanto de serem prejudicadas como de se envolverem em comportamentos que causam danos a outras crianças.
2. **Gerar e usar evidências para informar a prevenção.** Envolver de forma segura e ética crianças e sobreviventes para definir o problema e identificar barreiras à inclusão de populações marginalizadas.
3. **Colaborar entre sectores para coordenar esforços de prevenção e partilhar lições aprendidas.** Adoptar terminologia harmonizada alinhada com as Diretrizes de Terminologia, padronizar métricas/sistemas de relatórios, partilhar dados e evidências oportunas sobre o que funciona e o que não funciona e estabelecer sistemas sustentáveis.[26]

Organizações da sociedade civil, incluindo ONG internacionais

1. **Criar espaços seguros e inclusivos para que crianças e sobreviventes partilhem as suas opiniões e influenciem os esforços de prevenção e defesa.** Envidar esforços para envolver crianças marginalizadas, incluindo crianças com deficiência, populações de minorias sexuais e de género, crianças rurais e que não frequentam a escola, crianças de minorias étnicas ou de origem migrante e crianças que não têm acesso a tecnologias digitais.
2. **Defender a prevenção e resposta baseadas nos direitos e mecanismos robustos de responsabilização para lidar com o CSEA facilitado pela tecnologia.**
3. **Fortalecer os serviços comunitários de denúncia e apoio, incluindo linhas de apoio e apoio entre pares.** Formar cuidadores, educadores e provedores de serviços para dar apoio e recursos imediatos e sem julgamentos; e prover serviços acessíveis e centrados nos sobreviventes para crianças e adultos sobreviventes que abordem os danos *online* e *offline*, promovam o bem-estar a longo prazo e previnam a revitimização.
4. **Oferecer intervenções precoces baseadas em evidências para crianças e adultos em risco de causar ou sofrer danos** e fornecer respostas baseadas em evidências e não carcerárias para crianças que causaram danos.

Sector privado, particularmente empresas de tecnologia

1. **Priorizar a segurança, os direitos e o bem-estar das crianças em todos os níveis da cultura da empresa, tomada de decisões e formação da mão-de-obra.** Prover educação e formação contínuas em todo o processo de recrutamento, investir em pesquisa preventiva e serviços de apoio aos sobreviventes e garantir que os responsáveis digitais da linha da frente e as equipas de Confiança e Segurança tenham apoio e recursos adequados.

2. **Criar a segurança desenhando o padrão, integrando avaliações de impacto dos direitos da criança e diligência necessárias nos processos de desenvolvimento.** Consultar com segurança crianças, jovens e sobreviventes para ter escolhas de *design* melhor informadas. Garantir que os recursos de segurança sejam funcionais, acessíveis e disponíveis de forma equitativa em todas as regiões geográficas e idiomas onde um produto ou serviço é oferecido.

3. **Reforçar a transparência e a responsabilização.** Divulgar todos os impactos materiais nos direitos da criança associados a produtos e serviços digitais por meio das estruturas de reporte corporativo existentes em cada país de operação.[31] Recolher e partilhar dados de segurança anonimizados e desagregados com investigadores, reguladores e entre sectores para informar a prevenção. Incorporar mecanismos de responsabilização independentes na governança corporativa.

4. **Detetar e interromper proactivamente conteúdos e comportamentos prejudiciais.** Utilizar ferramentas em tempo real que respeitem os direitos, tais como correspondência de hash, monitoria, pop-ups de aviso, redireccionamento para os serviços de apoio e detecção de comportamentos de aliciamento e transações financeiras de alto risco. Ao mesmo tempo, fornecer canais de denúncia acessíveis e adequados às crianças que liguem directamente os utilizadores a linhas de apoio e serviços de assistência, removam rapidamente conteúdos prejudiciais e forneçam respostas imediatas às denúncias apresentadas.

Academia e pesquisadores

1. **Priorizar a investigação sobre a prevalência, os factores de risco e de proteção e os impulsionadores sistémicos do CSEA facilitado pela tecnologia.** Abordar lacunas críticas na investigação, incluindo vulnerabilidades interseccionais, escalada *online-offline* e estratégias eficazes de prevenção de perpetração, incluindo o tratamento do início de comportamentos sexuais prejudiciais entre crianças e jovens.

2. **Desenvolver, adaptar e avaliar intervenções em diferentes contextos e populações.** Estabelecer parcerias intersectoriais e realizar pesquisas de custo-benefício e implementação para orientar investimentos sustentáveis.

3. **Estabelecer parcerias de investigação conjuntas, coordenar agendas de investigação e promover a partilha oportuna de dados.**

Governos

1. **Rever, fortalecer e harmonizar leis e regulamentos globais para abordar o CSEA facilitado pela tecnologia.** Consultar amplamente as partes interessadas para alinhar a legislação com evidências, boas práticas e leis e normas de direitos da criança. Usar terminologia harmonizada e garantir que a legislação seja tecnologicamente neutra, abrangendo tecnologias existentes e futuras. Definir deveres, sanções e mecanismos de responsabilização claros para os responsáveis, ao mesmo tempo que se permite a inovação responsável da indústria. Diferenciar entre comportamentos

de adultos e adolescentes e evitar criminalizar comportamentos mutuamente desejados entre pares com idades próximas.

2. **Alocar recursos e coordenar os sistemas nacionais de proteção e justiça infantil para lidar com os danos causados às crianças, tanto *online* como *offline*.** Estabelecer múltiplos canais de denúncia acessíveis, adequados às crianças e informados sobre traumas, ligados a serviços abrangentes de saúde, psicossociais e jurídicos. Manter bases de dados seguras e anónimas das vítimas para orientar a prevenção e a resposta. Formar a força policial, o poder judicial, os educadores e os trabalhadores da linha da frente em práticas adequadas às crianças e informadas sobre traumas e prestar apoio contínuo ao seu bem-estar.
3. **Utilizar monitoria e reabilitação baseadas em evidências para prevenir a reincidência e priorizar o apoio, a diversão e penas alternativas para crianças em conflito com a lei.**
4. **Estabelecer reguladores nacionais ou regionais independentes com autoridade, recursos e conhecimentos técnicos para lidar com o CSEA facilitado pela tecnologia,** incluindo a definição de normas, a monitoria do cumprimento e a aplicação de sanções.
5. **Implementar e avaliar programas nacionais de educação e sensibilização baseados em evidências que visem promover a segurança digital, a denúncia e a procura de ajuda.** Integrar a educação adequada à idade nos currículos escolares e formar professores, cuidadores e provedores de serviços. Realizar campanhas de educação e sensibilização acessíveis e multilingues, colaborando com as comunidades e outros sectores para alcançar as crianças marginalizadas.

Organizações intergovernamentais

1. **Facilitar a cooperação transfronteiriça em matéria de aplicação da lei e partilha de informações.**
2. **Prestar assistência técnica e mobilizar recursos para reforçar a capacidade nacional,** estabelecendo prioridades com base nas necessidades e na prevalência.

1. **Mobilizar financiamento conjunto e sustentável** para apoiar governos nacionais, organizações comunitárias e iniciativas inovadoras de prevenção.

Prefácio

"As minhas imagens estão a ser comercializadas *online* há mais de 20 anos. Sou vítima do CSAM todos os dias da minha vida. Fui abusado quando era criança, quando o meu primeiro agressor criou o meu CSAM e desde então, todas as semanas, os meus advogados recebem novos avisos de que o meu material foi encontrado na coleção de outro pedófilo. Há mais de uma década recorro ao Tribunal Supremo dos Estados Unidos com os meus advogados do escritório Marsh Law sobre este caso.

A minha série do CSAM é tão popular que sei que a distribuição nunca vai acabar. Mas nem todas as vítimas do CSAM precisam de estar confinadas a este mesmo destino. A tecnologia para intervir, detectar e impedir a disseminação do CSAM existe. Temos de fazer com que as grandes empresas tecnológicas a utilizem.

Eu era adolescente quando descobri que o meu CSAM estava a ser comercializado em todo o mundo. Naquela época, eu era uma das poucas vítimas desse crime hediondo. Hoje, há... [centenas de milhões de] crianças vitimas todos os anos.

Agora, estou a criar um adolescente num mundo que está a ficar cada vez mais perigoso. É incrivelmente difícil criar filhos pequenos nesta era tecnologicamente tóxica. Como posso garantir que os meus filhos nunca encontrem o meu CSAM quando ele está literalmente em toda a Internet? Como posso manter os meus filhos a salvo de predadores quando sei que eles estão a apenas dois cliques do perigo?

Tenho muito orgulho de ver vítimas como eu — e pais como eu — enfrentando grandes empresas de tecnologia. Mas, para ser claro: vamos precisar de pesquisas inovadoras, ferramentas de aplicação da lei de ponta e apoio infinito de defensores dedicados para ter uma chance. Não sei como vamos conseguir, mas sei que devemos a todas as crianças não desistir.

Não tenho respostas sobre como manter as crianças seguras *online* hoje em dia, mas sei disto: a WeProtect [Global Alliance] tem sido uma tábua de salvação para os sobreviventes nesta luta pela vida das nossas crianças. Graças a esta rede de apoio, finalmente vejo a luz no fundo do túnel. Os problemas relacionados com CSAM *online* estão a piorar a cada dia e a lacuna de responsabilização está a aumentar, mas as escolas estão a proibir o uso de telemóveis, as empresas de tecnologia estão a acordar, a verificação de idade está a aumentar, os sistemas de apoio estão a expandir-se e sobreviventes em todos os lugares estão a falar corajosamente.

Finalmente estamos a avançar na direcção certa."

Esta declaração foi fornecida, com o apoio da Protect Children, por um sobrevivente que, como muitos outros, optou por permanecer anónimo. A WeProtect Global Alliance convidou este colaborador anónimo a partilhar a sua voz juntamente com muitas outras pessoas com experiências vividas — quer sejam crianças que procuramos proteger no mundo digital ou sobreviventes de abuso sexual facilitado pela tecnologia — porque essas vozes são muitas vezes ignoradas. Nesta Avaliação da Ameaça Global, entrelaçamos essas experiências vividas com as evidências e pesquisas, fundamentando nosso trabalho na realidade das pessoas. Reconhecemos que essas vozes são complexas, diversas e, às vezes, discordantes, mas elas devem ser ouvidas.

Introdução

Objectivos

A exploração e abuso sexual infantil facilitados pela tecnologia (CSEA) são um desafio mundial complexo que prejudica profundamente as crianças, as famílias e as sociedades. Prevenir e responder a este dano requer uma acção urgente e coordenada entre sectores e fronteiras.

A Avaliação da Ameaça Global 2025 tem dois objectivos:

1. Analisar as tendências globais do CSEA facilitado pela tecnologia desde 2023.
2. Co-elaborar uma estrutura de prevenção com partes interessadas especializadas, defensores dos jovens e sobreviventes, fornecendo recomendações práticas alinhadas com o Modelo de Resposta Nacional da WeProtect Global Alliance.

A Avaliação da Ameaça Global 2025 enfatiza a necessidade de abordagens sensíveis ao contexto. Os riscos para as crianças, o seu acesso a tecnologias digitais e recursos de proteção e a força dos sistemas de proteção variam amplamente entre as regiões. O relatório revela importantes lacunas de proteção, destacando a necessidade urgente de equidade nos esforços mundiais de prevenção, particularmente para proteger crianças em ambientes pouco regulamentados ou com recursos limitados.

Uma estrutura de direitos da criança

> **“Os jovens devem ter o direito de compreender os seus direitos *online*. Reconhecer esses direitos já seria um passo em frente para se livrarem de situações perigosas.”**
>
> *Menina de 14 anos, Canadá*[32]

A prevenção do CSEA facilitado pela tecnologia é um imperativo legal e ético baseado na legislação internacional de direitos humanos. A Convenção das Nações Unidas (ONU) sobre os Direitos da Criança exige que os Estados protejam as crianças de todas as formas de violência, exploração e abuso. O Comentário Geral n.º 25 confirma que esses direitos se estendem aos espaços digitais e exige que os governos integrem os direitos das crianças nas políticas digitais, garantam o acesso à justiça e consultem as crianças sobre as decisões que as afectam.[33,34] Embora a Convenção sobre os Direitos da Criança estabeleça obrigações para os Estados como responsáveis, os Princípios Orientadores sobre Empresas e Direitos Humanos e os Princípios sobre Direitos da Criança e Empresas estabelecem a responsabilidade do sector privado de respeitar os direitos das crianças e prevenir e responder a violações de direitos.[35,36] Esses princípios sustentam a análise deste relatório sobre as tendências munidais e informam a estrutura de prevenção e as recomendações a seguir.

Nota sobre a terminologia

Em 2025, um Grupo de Trabalho Interagências mundial actualizou as Diretrizes do Luxemburgo, lançando a segunda edição das **Diretrizes de Terminologia para a Proteção de Crianças contra Exploração Sexual e Abuso Sexual** (abreviadas como Diretrizes de Terminologia).[26] Em consonância com essas diretrizes, este relatório utiliza o termo «exploração e abuso sexual infantil facilitados pela tecnologia (CSEA)». O **CSEA facilitado pela tecnologia** refere-se ao uso de tecnologias digitais em qualquer fase para preparar, cometer ou divulgar (no caso de material de abuso sexual infantil, ou CSAM) a exploração sexual ou o abuso sexual de uma criança. Abrange danos cometidos em ambientes digitais e não digitais (*offline*) — incluindo, por exemplo, a troca de informações, a coordenação de acções e o contacto com crianças para as aliciar ou coagir. Este termo reconhece que a tecnologia desempenha um papel na facilitação do abuso e na perpetuação dos danos causados pelo abuso, tanto em espaços físicos como digitais.

Uma **criança** refere-se a qualquer pessoa com menos de 18 anos de idade. As crianças, incluindo os adolescentes, diferem com base em características como idade, fase de desenvolvimento, orientação sexual, identidade de género, deficiência, etnia, formação académica, situação económica e estatuto migratório. Estes factores interligados podem afectar os riscos e danos que as crianças enfrentam, bem como o seu acesso a recursos de proteção. Um **sobrevivente** é uma pessoa que sofreu exploração ou abuso sexual. Muitos sobreviventes do CSEA facilitado pela tecnologia são agora adultos que também devem ser incluídos nos esforços de prevenção e resposta. Reconhecendo que as pessoas com experiência vivida usam termos diferentes para se descrever, este relatório usa **vítima** e **sobrevivente** de forma intercambiável.

Metodologia

Este relatório baseia-se numa ampla gama de fontes de dados e conhecimentos especializados. Foi orientado por um Comité Diretivo de Peritos composto por 14 representantes do governo, das autoridades policiais, do sector privado, da sociedade civil, do meio académico, de organizações internacionais e de defensores com experiência vivida.

As evidências foram sintetizadas por meio de:

- Uma revisão exploratória da literatura académica e cinzenta relacionada com os dois objectivos do relatório, publicada em inglês entre Janeiro de 2023 e outubro de 2025.
- Entrevistas semiestruturadas com 32 partes interessadas de todos os sectores e regiões, de Junho a Julho de 2025, para triangular perspectivas e abordar lacunas na literatura.
- Um inquérito *online* com 77 especialistas em Setembro de 2025 para obter perspectivas multissectoriais sobre a priorização de acções de prevenção.
- Ideias de quatro workshops com jovens e sobreviventes, conduzidos por organizações focadas em sobreviventes e jovens. Os sobreviventes também reviram os guias de entrevistas e grupos focais para garantir a relevância e a sensibilidade.
- Estudos de caso partilhados por organizações e membros da WeProtect Global Alliance, apresentando práticas promissoras e respostas inovadoras.

A diversidade geográfica foi assegurada através da seleção de partes interessadas, exemplos de boas práticas e estudos de caso, com especial atenção para regiões e contextos sub-representados. O quadro de prevenção foi co-criado e revisto através de processos participativos que se basearam nesta diversidade e representatividade.

As limitações incluem a restrição a publicações em língua inglesa, o que limita a representação regional, o curto prazo para a recolha de dados e o potencial viés de seleção na inclusão de partes interessadas e estudos de caso, apesar dos esforços para garantir a diversidade geográfica e sectorial.

O Manifesto SafetyNet: Vozes dos jovens para um futuro digital mais seguro

Para compreender melhor como as crianças e os jovens vivenciam o mundo digital e imaginam um futuro *online* mais seguro, a WeProtect Global Alliance liderou a segunda fase do projecto #MyVoice#MyFuture. Através de consultas a 109 jovens com idades entre 13 e 24 anos em 10 países, e em colaboração com sete organizações juvenis, a iniciativa reuniu ieias sobre segurança digital, direitos e CSEA facilitado pela tecnologia. O resultado é o **Manifesto SafetyNet**, uma declaração liderada por jovens sobre direitos digitais e um roteiro para construir um futuro digital mais seguro e equitativo. O Manifesto apela a proteção mais forte, *design* inclusivo e acção coletiva para garantir que todas as crianças e jovens possam existir online sem medo.[37]

Figura 2. Manifesto SafetyNet publicado no Safe Futures Hub em Junho de 2025[38]

O panorama digital

As crianças de hoje estão a crescer numa era de rápida transformação digital. Embora o ambiente digital crie oportunidades valiosas para aprendizagem, conexão, expressão e pertencimento, ele também pode expor as crianças a riscos e danos significativos, tanto *online* como *offline*. Essas oportunidades e riscos evoluíram rapidamente nos últimos anos, acelerados pelo surgimento de tecnologias como inteligência artificial (IA) generativa, ambientes de realidade estendida (XR), descentralização, computação quântica e criptografia de ponta a ponta, que desafiaram a capacidade de prevenir, detectar e responder ao CSEA facilitado pela tecnologia.[39]

As crianças estão mais conectadas do que nunca, mas as desigualdades digitais persistem.[40] Existem agora 6.0 mil milhões de utilizadores da Internet — cerca de três quartos da população mundial —, um aumento em relação aos 64% em 2021.[5] Mais de metade da população global possui agora um smartphone.[4] Em alguns países da Maioria Global, a maior parte do tráfego da web ocorre em dispositivos móveis, que muitas vezes são partilhados dentro das famílias ou entre amigos.[41] Por exemplo, 88% do tráfego da web nas Filipinas e 85% na Nigéria tiveram origem num dispositivo móvel em Fevereiro de 2025.[41]

O uso da Internet pelos jovens ultrapassa o resto da população em 13%.[42] Uma pesquisa mundial com mais de 380.000 crianças em 55 países descobriu que a maioria começou a usar um dispositivo digital antes dos 10 anos.[43] Em apenas alguns anos, as tecnologias de IA passaram de amplamente experimentais para totalmente integradas nas redes sociais, plataformas de mensagens e ferramentas do dia-a-dia que as crianças utilizam, como os *chatbots* de IA.[6,44] Embora a IA ofereça benefícios educacionais e sociais, ela está a ampliar rapidamente os riscos e danos para as crianças, incluindo o CSEA facilitado pela tecnologia. Os esforços para aproveitar o seu potencial para proteger as crianças estão a ficar para trás. Conclusões do **Índice de Bem-Estar Digital** 2025 revelam que 80% dos adolescentes e jovens adultos da Geração Z inquiridos relataram ter sofrido algum tipo de risco *online*.[45] Interações potenciais de aliciamento eram comuns e a partilha de imagens íntimas era generalizada. Além disso, aproximadamente um em cada quatro inquiridos indicou ter encontrado imagens sexuais geradas por IA, enquanto 25% dos participantes não sabiam que o envolvimento com imagens sexuais de menores é ilegal.

Embora mais crianças em todo o mundo estejam a ter acesso às tecnologias digitais, o acesso — e, com ele, a exposição a riscos — continua desigual. Quase metade das seis milhões de escolas em todo o mundo não tem acesso à Internet, a maioria delas em países da Maioria Global e áreas rurais remotas.[46] Um estatuto socioeconómico mais elevado tem sido consistentemente associado a uma maior literacia digital, e a exclusão digital atua como «um amplificador de exclusões sociais mais amplas».[47] As crianças que não têm acesso a dispositivos digitais continuam em risco, uma vez que o abuso sexual presencial é frequentemente gravado, armazenado e disseminado por meio de tecnologias digitais, incluindo dispositivos partilhados.

Panorama jurídico e político

Nos últimos anos, governos e organismos internacionais têm promovido respostas legislativas e políticas, buscando harmonizar leis, fortalecer a regulamentação e adaptar-se às tecnologias em rápida evolução. **A Convenção das Nações Unidas contra o crime Cibernético** (2024) estabelece a primeira norma universal contra o crime cibernético, abrangendo explicitamente crimes contra crianças, como CSAM e aliciamento, ao mesmo tempo que reforça a partilha internacional de provas.[23] A **Primeira Conferência Ministerial Global sobre o Fim da Violência contra as Crianças** (2024) catalisou a coordenação multissectorial e os compromissos nacionais para reforçar a estrutura de proteção infantil, incluindo no que diz respeito aos danos *online*.[48] O **Esquema de Classificação Universal Versão 3** (2025) fornece um quadro harmonizado para identificar, categorizar e responder a materiais de exploração e abuso sexual infantil, com rótulos legíveis por máquina e definições alinhadas globalmente além-fronteiras.[49] A segunda edição das **Diretrizes de Terminologias** (2025) fornece uma base de terminologia universal para facilitar a reforma jurídica.[26] Uma «terceira onda» de reformas legislativas surgiu em vários países, marcada por uma maior harmonização, incluindo restrições de idade nas redes sociais, preparação para o futuro e esforços para colmatar lacunas em torno de danos emergentes, como imagens de abuso sexual infantil geradas por IA e extorsão sexual.[50] No entanto, muitas estruturas de proteção das crianças continuam fragmentadas ou desatualizadas, com autoridade regulatória inconsistente e proteção limitada contra conteúdos sexuais gerados na primeira pessoa envolvendo crianças ou abuso facilitado por IA.[50,51] Em alguns contextos, as crianças vitimas de extorsão sexual ainda correm o risco de criminalização, refletindo lacunas entre a lei, as políticas e as realidades vividas pelas crianças.[52]

Desafios persistentes de fiscalização e regulamentação continuam a minar o progresso. Investigações transfronteiriças são retardadas pela fragmentação jurisdicional, recursos desiguais e sistemas fracos de partilha de dados. Apenas 45% dos 20 países da Força-Tarefa Global da WeProtect Global Alliance têm obrigações formais de denúncia para empresas de tecnologia.[53] A dependência de medidas voluntárias da indústria deixa grandes lacunas de responsabilização, particularmente em países da Maioria Global. Os representantes da indústria argumentam que os sistemas de denúncia voluntária podem ser mais ágeis e responsivos, mas há um amplo consenso entre as partes interessadas de que são necessárias obrigações vinculativas.

> “Mas, como empresas, muitas vezes não o fazem, a menos que sejam obrigadas.”
>
> *Indústria*[7]

As rápidas mudanças tecnológicas estão a ultrapassar as ferramentas jurídicas existentes, e as tensões entre a proteção da privacidade e a detecção proactiva continuam por resolver.[39] É necessária uma coordenação internacional mais forte e uma harmonização legislativa, reguladores com mais poderes, mais recursos para os sistemas de proteção infantil e aplicação da lei, e obrigações vinculativas para a indústria, a fim de proteger as crianças num ambiente digital em rápida evolução.

> “Não podemos resolver este problema apenas com prisões.”
>
> *Governo*[54]

Dimensão e natureza da exploração e abuso sexual infantil facilitados pela tecnologia

Desde a última Avaliação da Ameaça Global, os danos existentes continuaram, enquanto novos riscos surgiram mais rapidamente do que as salvaguardas legais, políticas e tecnológicas podem responder. Este capítulo reúne as evidências disponíveis sobre a dimensão de abuso, características das vítimas e/ou sobreviventes, perfis dos perpetradores e ameaças emergentes, reconhecendo que os dados globais permanecem fragmentados, incompletos e difíceis de comparar. Vários estudos sobre a prevalência de perpetração, a serem publicados em breve, visam abordar as lacunas existentes nos dados (ver Apêndice). Apesar dessas limitações, as conclusões fornecem um panorama importante do ambiente de ameaças de 2023 a 2025 e estabelecem as bases para as recomendações apresentadas mais adiante neste relatório.

Panorama dos dados

> **"A verdade é que...é realmente impossível dar uma dimensão precisa da questão."**
>
> *Indústria*[7]

Os dados disponíveis sobre CSEA facilitado pela tecnologia reflectem o progresso coletivo em coordenação, comunicação e monitoria, e são essenciais para compreender a ameaça e mobilizar acções. No entanto, começamos por observar as restrições persistentes do ambiente de dados, uma vez que estes desafios enquadram tanto a interpretação dos números disponíveis como a análise que se segue. Os dados actualmente disponíveis são fragmentados e parciais. Por exemplo, os esforços para medir a prevalência mundial são limitados por lacunas na cobertura geográfica, definições inconsistentes, variação na força dos sistemas de detecção e denúncia e qualidade variável dos estudos. A transparência limitada da indústria também dificulta a avaliação do que as empresas estão a fazer: por exemplo, 60% das 50 principais plataformas mundiais de partilha de conteúdo não publicam informações sobre como lidam com a exploração sexual infantil e, entre as que o fazem, os dados são fragmentados e carecem de comparabilidade.[55] Os dados disponíveis podem tanto sobrestimar, devido à duplicação ou classificação incorreta de material, como subestimar, devido à encriptação e plataformas ocultas.[7] Dados robustos e representativos sobre vítimas e perpetradores continuam limitados, conforme discutido mais adiante neste capítulo. À luz destes desafios, realizámos entrevistas com partes interessadas especializadas e defensores de sobreviventes para abordar as lacunas nas evidências e captar ideias actualizadas e específicas do contexto sobre tendências emergentes e desafios operacionais. Embora não substituam os dados representativos, a triangulação destas perspectivas com conjuntos de dados e pesquisas existentes fornece um quadro mais abrangente e matizado.

Dimensão e padrões de danos

Esta secção descreve os principais danos que moldam o panorama global de ameaças, incluindo CSAM, aliciamento, abuso transmitido ao vivo, IA, extremismo violento *online* e desenvolvimentos tecnológicos , como criptografia de ponta a ponta, descentralização, computação quântica e XR.

Material de abuso sexual infantil

O CSAM está a ser detectado, denunciado e removido em níveis sem precedentes. Conforme discutido anteriormente, as tendências de denúncias reflectem mais a capacidade de denúncia do que a prevalência real, e a maioria dos dados de CSAM se origina de plataformas de alta renda, oferecendo uma visão parcial dos danos globais. Também é importante reconhecer que as tendências ascendentes podem, em parte, reflectir desenvolvimentos positivos, como mais crianças se apresentando para denunciar danos, empresas melhorando os sistemas de detecção e maior transparência do sector no compartilhamento de dados. Os dados de várias fontes, incluindo os relatórios obrigatórios da indústria do Centro Nacional para Crianças Desaparecidas e Exploradas (NCMEC), as linhas diretas da INHOPE e a detecção proactiva e encaminhamentos da Internet Watch Foundation (IWF), servem propósitos distintos e utilizam metodologias diferentes, pelo que os seus números não podem ser combinados de forma significativa.

Os números relatados continuam extraordinariamente elevados.

INHOPE: recebeu mais de 2,5 milhões de denúncias de suspeita de CSAM em 2024, um aumento de 218% em relação a 2023. Destas, 65% foram confirmadas como conteúdo ilegal. Este aumento foi impulsionado em grande parte pela SafeNet Bulgária, que contribuiu com 1,6 milhões de denúncias.[13]

NCMEC **CyberTipline**: recebeu 20,5 milhões de denúncias correspondentes a 29,2 milhões de incidentes em 2024, uma queda em relação aos 36,2 milhões em 2023. Essa diminuição foi parcialmente atribuída às práticas de «agrupamento» que reúnem denúncias relacionadas e ao impacto da criptografia de ponta a ponta, que limita a capacidade das empresas de detectar e denunciar materiais prejudiciais.[120]

IWF: avaliou 424.047 denúncias, confirmando 291.273 casos de CSAM ou links para ele em 2024 — um aumento de 6% em relação a 2023.[14]

Os tipos de conteúdo prejudicial são diversos e cada vez mais baseados em vídeo.

NCMEC: quase 63 milhões de ficheiros foram denunciados em 2024, incluindo 33 milhões de vídeos, 28 milhões de imagens e 1,8 milhões em outros formatos. Entre eles, mais de 51.000 envolviam crianças em perigo iminente, exigindo intervenção urgente.[12]

IWF: classificou 734 048 ficheiros únicos como CSAM, incluindo mais de 47.000 vídeos e mais de 4000 imagens não fotográficas proibidas.[14]

A hospedagem e a distribuição continuam geograficamente concentradas para conteúdos que podem ser rastreados.

A INHOPE informou que 59% dos servidores detectados estavam localizados na Holanda e 13% nos Estados Unidos, posições que mantêm há cinco anos.[13] Da mesma forma, a IWF descobriu que mais da metade dos URL de abuso sexual infantil bloqueados em 2024 estavam hospedados em países membros da União Europeia, com a Holanda, Bulgária e Roménia hospedando 29%, 9% e 7%, respetivamente.[14] **O Índice Into the Light** da Childlight destaca os altos níveis globais de hospedagem de CSAM rastreáveis até a Holanda, bem como 4,5 milhões de denúncias provenientes apenas da Índia, Paquistão e Bangladesh.[57] Uma combinação de infraestrutura de hospedagem em grande escala, conectividade de alta velocidade e regulamentações que priorizam a liberdade de expressão cria condições exploradas por infratores para armazenar e distribuir conteúdo abusivo. A localização de alguns conteúdos não pode ser facilmente rastreada porque está alojada em redes anónimas, como a Tor, que são concebidas para ocultar a origem física do servidor.[11] O NCMEC observou que 11% das denúncias da **CyberTipline** tinham origem desconhecida em 2024.

Os padrões de distribuição mudaram juntamente com os esforços de detecção. A contribuição da SafeNet Bulgária significou que os fóruns representaram 61% das denúncias recebidas pela INHOPE em 2024 — um aumento em relação aos menos de 9% em 2023 —, enquanto as denúncias de plataformas de hospedagem de imagens e sites convencionais diminuíram drasticamente.[13] Paralelamente, a IWF recebeu URL e confirmou 291,270 páginas da internete contendo CSAM em 2024, um aumento de 5% em relação a 2023.[14]

Aliciamento e sedução *online*

A sedução *online*, frequentemente chamada de aliciamento, ocorre quando os perpetradores visam crianças que utilizam a Internet para identificá-las e coagi-las a praticar actos sexuais ilegais. Em 2024, o NCMEC documentou 546.000 denúncias de sedução *online*, um aumento de 192% em relação a 2023, com números que devem aumentar à medida que mais empresas cumprem a **Lei de Denúncias dos EUA**.[16]

Inteligência artificial generativa

O CSAM gerado por IA, sinalizado nas Avaliações da Ameaça Global anteriores e em entrevistas com informantes-chave, continua a crescer a uma velocidade alarmante.[54] As tecnologias *deepfake* (imagens ou vídeos gerados por IA que retratam de forma realista pessoas que nunca existiram ou alteram fotos e filmagens reais), *chatbots* de IA (ferramentas de conversação automatizadas que podem se passar por crianças ou adultos) e modelos generativos (sistemas de IA capazes de produzir novos textos, imagens ou vídeos a partir de padrões aprendidos) estão a ser transformados em armas para explorar crianças e disseminar CSAM em grande escala.[59]

> **"Se a tecnologia agora pode criar imagens e vídeos que nunca aconteceram de facto, como saberemos o que é real no futuro e como isso mudará a forma como confiamos uns aos outros *online*?"**

Rapaz de 15 anos, Etiópia[60]

NCMEC: documentou um aumento de 1.325% nas denúncias relacionadas à IA entre 2023 e 2024, representando 67.000 denúncias.[12] Até Junho de 2025, números preliminares mostram 440.419 novas denúncias envolvendo conteúdo de exploração sexual infantil gerado por IA, contra 6.835 no mesmo período em 2024.[61]

Thorn: 1 em cada 17 adolescentes relata ser vítima de imagens sexuais *deepfake*.[62]

IWF: um único fórum partilhou mais de 3.500 imagens/vídeos digitalmente alterados ou sintéticos de crianças num único mês.[63]

As táticas emergentes dos infractores incluem o uso de IA preditiva e sistemas de recomendação para identificar e disseminar CSAM.[63–65] Alguns infractores partilham modelos de IA personalizados treinados com material real de abuso para gerar conteúdo sintético, enquanto outros testam estratégias de aliciamento em *chatbots* infantis.[8,63,66] Ao mesmo tempo, a IA pode ser implantada para proteger crianças e apoiar a detecção e investigação.

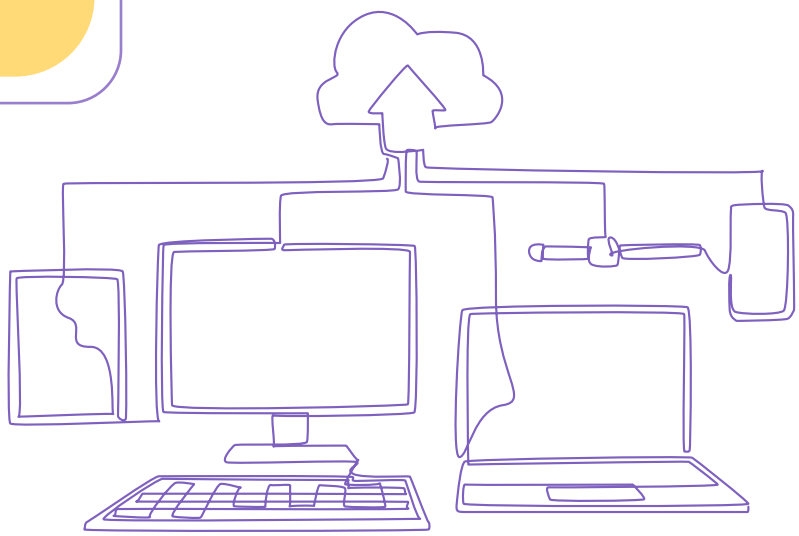


Figura 3. IA: promessas e armadilhas[6,67,68]

OPORTUNIDADES

Automatizar a detecção de comportamentos prejudiciais: interromper interacções de alto risco, aliciamento e tráfico antes que ocorram danos.

Automatizar a detecção de CSAM: identificar, bloquear e remover rapidamente conteúdos prejudiciais.

Apoiar a aplicação da lei: acelerar investigações, analisar e classificar CSAM, identificar vítimas e infractores e reduzir a exposição humana a conteúdos traumáticos.

Segurança desde a concepção: desenvolver e implementar sistemas e modelos de IA generativa seguros.

AMEAÇAS

Amplificar os danos: revitimização de crianças através da criação de novas imagens a partir de CSAM existente, divulgação de CSAM e guias para a prática de crimes, burlar sistemas de verificação de idade e impulsionar conteúdos prejudiciais por meio de algoritmos.

Gerar CSAM: produzir representações sexualizadas ou explícitas de crianças, no todo ou em parte, incluindo deepfakes de crianças reais em situações sexualizadas simuladas.

Complicar a detecção e a aplicação da lei: impedir a identificação de vítimas e infratores, sobrecarregar os sistemas de detecção e remoção e a capacidade de aplicação da lei.

Reduzir as barreiras técnicas e sociais ao dano: permitir a fácil criação de CSAM, facilitar o aliciamento online e normalizar a exploração e sexualização de crianças (por exemplo, aplicativos «nudify»).

> **“Na minha opinião, a IA pode ser muito útil, mas, como qualquer ferramenta poderosa, precisa de regras de segurança e, em vez de removê-la, devemos criar proteções e medidas de segurança robustas, como filtros, monitoria e orientação, para garantir que seja segura para as crianças e para todos os outros.”**
>
> *Mulher de 15 anos, Etiópia*[60]

Extremismo violento *online*

Desde a Avaliação da Ameaça Global 2023, os grupos *online* que promovem a violência proliferaram, com um aumento de 200% nos relatórios do NCMEC (mais de 1300 no total) entre 2023 e 2024.[12] Estes grupos incentivam as crianças a prejudicarem-se a si próprias ou a outros, destacando novas intersecções entre exploração sexual, radicalização *online* e danos *offline*. Foram observadas novas intersecções com pensamento suicida, distúrbios alimentares, golpes motivados por dinheiro e tráfico humano, embora as pesquisas ainda sejam limitadas. Os perpetradores costumam ter como alvo crianças em fóruns onde elas procuram ajuda.[7]

> **"Continuaremos a ver esta fusão de riscos... Acho que [a extorsão sexual] é um óptimo exemplo em que tantas ameaças diferentes se juntaram para criar este novo dano...quando alguém entra em contacto consigo e diz: 'Ei, você é giro, quer conversar?'...isso transforma-se numa troca de imagens...e pode transformar-se na produção real de imagens de abuso sexual infantil. Depois, pode transformar-se em *bullying* e assédio antes de se transformar em chantagem real, antes de poder potencialmente levar à automutilação..."**
>
> *Indústria*[7]

Da linha de frente da detecção de danos: visão do PGI sobre grupos «Com»

O PGI (Protection Group International) apoia governos, ONG e empresas na detecção e interrupção de danos online — desde a exploração infantil e desinformação até ao extremismo violento — usando inteligência humana apoiada por tecnologia.

Os grupos «Com» (também conhecidos como «Com») são um arquipélago de comunidades online onde crianças e jovens são alvo e manipulados para produzir CSAM, envolver-se em automutilação ou até mesmo gravar actos violentos. Estes grupos são, na sua maioria, transnacionais e são conhecidos por nomes diferentes e em evolução: 764, 676, Harm Nation, Leak Society e CVLT enquadram-se neste grupo. Embora os perpetradores sejam frequentemente jovens — predominantemente adolescentes do sexo masculino —, há sobreposições com subculturas extremistas e marginais, incluindo grupos com ideologias violentas.

Táticas do «Com»

Os perpetradores normalmente usam plataformas convencionais para identificar crianças e adolescentes vulneráveis, muitas vezes procurando aqueles que já lutam contra problemas de saúde mental. Por exemplo:

- Eles infiltram-se em comunidades *online* de automutilação ou distúrbios alimentares e convidam crianças para chats em grupos fechados.
- Eles exploram videogames populares voltados para crianças como espaços para encontrar vítimas em potencial, redirecionando-as para plataformas de mensagens privadas.

Uma vez isolados, os jovens podem enfrentar ameaças, manipulação ou extorsão. As vítimas podem ser pressionadas a gravar ou transmitir ao vivo actos prejudiciais, incluindo automutilação, CSAM ou uso de drogas. Este material é então compilado nos chamados «livros de tradições», que também contêm informações pessoais das vítimas. Esses livros circulam entre os membros da comunidade, e os perpetradores ganham status com base no nível de dano que infligem. Os perpetradores criam regularmente novas identidades *online* para evitar a detecção.

Impacto nas vítimas

- As vítimas muitas vezes enfrentam graves danos psicológicos, vivendo sob medo constante devido a ameaças e chantagem. A exposição à coerção e a exigências violentas pode intensificar vulnerabilidades existentes, como depressão, ansiedade ou pensamento suicida, às vezes escalando para actos forçados de automutilação ou tentativas de suicídio.
- A exposição constante a materiais extremos pode normalizar comportamentos prejudiciais para as vítimas, levando, por vezes, à participação contínua. Algumas vítimas passam da participação coerciva para o envolvimento contínuo com grupos de agressores, em casos raros, chegando mesmo a criar os seus próprios canais e a repetir padrões de abuso.

Abuso transmitido ao vivo

Conforme destacado na Avaliação da Ameaça Global 2023, a dimensão e a natureza do abuso sexual de crianças transmitido ao vivo — ocorrendo nas principais redes sociais, bem como em plataformas dedicadas à transmissão ao vivo — continuam sendo importantes e pouco documentadas.[69] Pesquisas com infractores que procuram CSAM na *dark web* sugerem que mais de um terço consome material transmitido ao vivo, com prevalência variando entre as regiões.[70] Investigações mostram que as transmissões ao vivo são frequentemente pré-combinadas, com pequenas transações financeiras ligando consumidores em regiões de maior renda a facilitadores em jurisdições de alto risco.[71] Projectos como o estudo **Scale of Harm** *(Dimensão dos Danos)* da International Justice Mission preenchem lacunas críticas de dados, mas é necessário

um monitoramento mais sistemático. O rastreamento financeiro é uma via promissora para a detecção (ver Prevenção).

Tecnologias em evolução: encriptação, descentralização, computação quântica e realidade estendida

Criptografia de ponta a ponta

Cada vez mais adoptada como recurso de privacidade e segurança, a criptografia de ponta a ponta garante que apenas remetentes e destinatários possam visualizar o conteúdo das mensagens. No entanto, quando introduzida sem salvaguardas adicionais de proteção infantil, torna-se praticamente impossível detectar CSAM ou aliciamento e limita severamente a capacidade das autoridades policiais de identificar vítimas.[72] Em Dezembro de 2023, um dos principais aplicativos munidais de mensagens, a Meta, activou a criptografia de ponta a ponta por predefinição, com outras plataformas a seguirem o exemplo. A crescente adopção e utilização da encriptação de ponta a ponta provavelmente contribuiu para uma **redução de 7 milhões nos incidentes de exploração sexual infantil *online*** relatados ao NCMEC.[12] Várias plataformas importantes também reduziram os volumes de denúncias em cerca de 20% em 2024, levantando preocupações sobre transparência e responsabilidade.[73]

Descentralização

A computação descentralizada distribui tarefas por vários dispositivos ou sistemas, em vez de depender de uma autoridade central, permitindo ligações ponto a ponto e aplicativos como redes sociais, armazenamento de dados, transações financeiras e aprendizagem automática.[39] Embora esta arquitectura possa melhorar a privacidade, também coloca desafios únicos para prevenir e combater o CSEA facilitado pela tecnologia. A descentralização complica a identificação de suspeitos, a moderação de conteúdos e a remoção de material ilegal.[39] Olhando para o futuro, o principal desafio reside na crescente adopção de tecnologia descentralizada sem salvaguardas adequadas para os riscos já observados.[39]

Computação quântica

A computação quântica é um campo emergente que permite que as informações sejam processadas exponencialmente mais rápido do que os computadores clássicos. Embora ainda não tenham sido documentados casos de seu uso em CSEA, os riscos futuros podem incluir a aceleração da geração de CSAM gerado por IA ou a quebra de sistemas de criptografia que atualmente protegem os dados das crianças. Considerações prévias sobre políticas e segurança por design são imprescindíveis antes do amadurecimento dos aplicativos.[39]

Realidade estendida

As tecnologias XR (realidade virtual, aumentada e mista) estão a tornar-se mais acessíveis e económicas, aumentando os riscos de uso indevido e abuso.[75] A investigação destaca possíveis usos indevidos, incluindo experiências imersivas de CSAM e normalização de comportamentos prejudiciais.[76] É essencial tomar medidas preventivas antes que a XR se torne popular. Ao mesmo tempo, a XR mostra-se promissora para a prevenção e formação, oferecendo simulações realistas para a aplicação da lei e intervenções terapêuticas. No entanto, as evidências da sua eficácia continuam a ser limitadas.

> **“...com a realidade virtual, em breve você terá toque e sensação tátil, e haverá almofadas nos corpos, e essa será uma nova maneira de os agressores infligirem danos físicos no espaço virtual.”**
>
> *Sobrevivente*[77]

Características e vulnerabilidades das vítimas e/ou sobreviventes

A secção seguinte resume o que se sabe actualmente sobre as vítimas e/ou sobreviventes, ao mesmo tempo que assinala lacunas persistentes nos dados. As informações sobre as vítimas retratadas em CSAM continuam a ser escassas: apenas uma fracção das milhões de crianças retratadas nos relatórios da INTERPOL são identificadas, localizadas geograficamente ou confirmadas por idade.[9] A dimensão do problema excede a capacidade das autoridades policiais, devido ao pessoal, à capacidade técnica e aos recursos financeiros limitados para identificar as vítimas. Os infractores ocultam deliberadamente detalhes identificativos ou utilizam tecnologias de encriptação ou anonimização, tornando a análise de imagens e a localização da fonte extremamente difíceis.[7,8] O material denunciado retrata de forma desproporcional crianças pré-púberes, enquanto os adolescentes estão provavelmente sub-representados devido à falta de investigação com este grupo demográfico específico e à dificuldade em distinguir as suas imagens das de jovens adultos.[8,9] O estigma, as práticas inconsistentes de denúncia e a falta de desagregação de dados nos sistemas administrativos limitam a capacidade de compreender a demografia e as características das vítimas. Grupos marginalizados, incluindo populações de minorias sexuais e de género, crianças com deficiência e aquelas em condições de vida institucionais ou instáveis, continuam amplamente ausentes dos dados quantitativos, apesar de enfrentarem um risco acrescido.[8]

> “Não sabemos o que acontece às vítimas.”

Autoridades policiais[79]

Idade e género

De acordo com a Avaliação da Ameaça Global 2023, as meninas pré-púberes continuam a ser as vítimas mais frequentemente retratadas nos casos de CSAM denunciados. Em 2024, os dados do Eu Vejo Material de Abuso Infantil (sigla inglesa ICCAM – I See Child Abuse Material) mostraram que 98,7% dos casos denunciados envolviam raparigas e 93,2% eram rapaigas pré-púberes.[13] Os rapazes estão representados de forma desproporcional entre as vítimas de extorsão sexual, representando 91% das denúncias recebidas pela IWF em 2023.[14] Evidências empíricas sugerem que mais meninos podem estar sujeitos a extorsão sexual financeira devido aos hábitos de partilha de imagens dos meninos ou às impressões dos infractores sobre a sua disposição e capacidade de pagar.[9]

> “Ouvimos dizer que eles têm como alvo as meninas [com extorsão sexual financeira], mas de uma forma diferente. Eles não as têm como alvo por dinheiro. Eles as têm como alvo por imagens para... chantagem. Os meninos são o alvo deles.”

Industria[7]

A idade continua a ser um factor crítico para compreender o risco. Dados de um estudo representativo a nível nacional com jovens de 16 a 24 anos na Austrália indicam que as crianças normalmente têm a primeira experiência de partilha indesejada de imagens sexuais próprias por volta dos 15 anos, embora aproximadamente 9% relatem ter tido a primeira experiência antes dos 11 anos.[80] Os dados da ICCAM mostram um ligeiro aumento na proporção de denúncias de CSAM envolvendo

crianças pré-púberes (subindo de 90% em 2023 para 93,2% em 2024), enquanto as denúncias envolvendo adolescentes (14-17 anos) e bebés/crianças pequenas (menores de 3 anos) diminuíram ligeiramente.[13] A INHOPE também documentou um volume crescente de CSAM retratando crianças com menos de 10 anos.[81]

Vulnerabilidades

Em consonância com as conclusões anteriores da Avaliação da Ameaça Global, as crianças marginalizadas — seja devido à pobreza, condição de minoria, negligência, condições de vida instáveis ou residência rural — correm um risco desproporcional.[80,82–84] Factores de risco adicionais incluem dinâmicas familiares que normalizam comportamentos controladores, falta de literacia digital ou supervisão dos pais, falta de apoio social e exposição prévia à violência, CSAM e pornografia violenta.[54,84–86] As crianças com deficiência também enfrentam riscos agravados de exploração sexual, por exemplo, maiores impactos negativos na saúde mental e comportamentos sexuais de risco, além de barreiras significativas à divulgação, incluindo medo da culpa dos pais, julgamento e perda de autonomia.[87–89] Pesquisas mostram que adolescentes que enfrentam múltiplas formas de abuso são mais propensos a sofrer vitimização sexual tanto *offline* como *online*, com impactos duradouros na educação e na saúde mental.

Características e comportamentos de pessoas em risco de cometer crimes e que causaram danos

Novas evidências provenientes das autoridades policiais, da investigação e das comunidades de infractores estão a aprofundar a nossa compreensão sobre quem comete crimes, como agem e o que motiva o seu comportamento. Embora a maioria dos infractores sejam homens adultos, os padrões são cada vez mais complexos, com variações em termos de idade, género, localização geográfica, motivações e métodos. O reconhecimento de crianças e jovens em risco de cometer crimes e que causaram danos está a aumentar, assim como a necessidade de investigação, prevenção e apoio direccionados para esta faixa etária. Até recentemente, a investigação concentrava-se principalmente em infractores adultos identificados pelos sistemas judiciais ou que procuravam ajuda, limitando a percepção a caminhos da perpetração e as oportunidades de intervenção prévia. Abordagens inovadoras — como estudos que pesquisam directamente os infractores na *dark web* e estimativas de prevalência entre amostras representativas de homens — estão a expandir a base de evidências, embora dados robustos e representativos continuem escassos.[57,94] Vieses de relato e inconsistências de definição também limitam os dados.[95] Apesar dessas lacunas, as pesquisas continuam a esclarecer as vulnerabilidades, tecnologias, ambientes sociais e falhas sistémicas que possibilitam a perpetração.

> **“Fazemos o nosso melhor para mitigar o risco e reduzir os danos. Mas enquanto as pessoas continuarem a ter interesse sexual por crianças, enquanto as pessoas quiserem explorar outras para seu próprio ganho financeiro ou outro, continuaremos a ter estes problemas. São o que chamamos de questões que envolvem toda a sociedade.”**

Perfis de infractores adultos e padrões de perpetração

As evidências disponíveis indicam que os infractores que compram e trocam conteúdo são predominantemente do sexo masculino.[96,97] Pesquisas com usuários de CSAM na *dark web* mostram que 68% se identificam como homens e 17% se recusaram a informar seu gênero.[94] No caso de abuso transmitido ao vivo, as descobertas sugerem que os consumidores são em sua maioria homens, predominantemente baseados na Ásia, Europa e América do Norte, enquanto os produtores podem ser tanto homens quanto mulheres.[55] Os padrões etários variam de acordo com o tipo de crime e a população estudada. Dos 4.549 inquiridos que relataram consumir CSAM na *dark web*, 43% tinham entre 18 e 24 anos.[91] Outro estudo mostra que os consumidores de abuso transmitido ao vivo tendem a ser mais velhos.[94,98]

A perpetração também se estende para além de indivíduos que agem sozinhos. Muitas vezes envolve actores interligados além-fronteiras: um abusador inicial produz imagens ou vídeos; outros carregam ou distribuem o material; e os consumidores e compradores alimentam a procura que impulsiona a sua circulação. As redes online trocam, normalizam e amplificam este abuso internacionalmente, tornando extremamente difícil identificar os perpetradores, apesar das investigações especializadas.[79,99]

Uma rede mundial de abuso

Na Operação Víbora (Março-Maio de 2025), liderada pela Polícia Nacional Espanhola com a INTERPOL e a Europol, 20 pessoas foram presas e 68 suspeitos adicionais identificados em 12 países em conexão com CSAM.[100] Na Operação Cumberland (Fevereiro de 2025), a Europol desmantelou uma plataforma dinamarquesa que distribuía CSAM gerado por IA, levando à detenção de 25 pessoas, à identificação de 273 suspeitos e à apreensão de 173 dispositivos em 19 países.[101]

Embora muitas vítimas e agressores permaneçam não identificados, os dados disponíveis sobre casos conhecidos sugerem que uma proporção significativa de CSAM e outras formas de abuso facilitado pela tecnologia são produzidos por pessoas conhecidas da criança.[102] Relatórios da Thorn, com base em dados do NCMEC, mostram que duas em cada três crianças são abusadas por alguém das suas comunidades *offline*.[10,103] Uma revisão de 2023 de 66 estudos sobre a produção parental de CSAM destaca que os membros da família são um grupo significativo, mas subestimado, em risco de cometer crimes, normalmente produzindo material envolvendo crianças pré-púberes.[104]

> **"Há um aspecto digital [no abuso]...é abuso sexual infantil intrafamiliar...os infractores... até os avós estão a usar serviços digitais como o WhatsApp...chat privado e a tirar fotos."**
>
> *Sociedade civil*[11]

Crianças que apresentam comportamentos sexuais prejudiciais

Os comportamentos sexuais prejudiciais entre crianças são reconhecidos como um problema crescente, embora a verdadeira prevalência permaneça incerta. Antes dos 18 anos, uma em cada cinco crianças sofre danos sexuais, tanto *online* como *offline*, e mais de metade desses casos ocorrem entre pares.[105,106] Tais comportamentos podem começar como uma exploração relacionada com os pares, mas às vezes podem escalar para ofensas mais graves. Por exemplo, uma criança pode inicialmente ver imagens sexuais de colegas da sua idade e continuar a procurar material semelhante à medida que cresce. (9 As crianças que apresentam comportamentos sexuais prejudiciais partilham frequentemente vulnerabilidades sobrepostas, tais como vitimização prévia ou exposição a conteúdos sexuais, trauma, negligência, desigualdade social e neurodiversidade.[107] Estas vulnerabilidades são frequentemente agravadas pela falta de consciencialização, educação inadequada e sistemas de prevenção e apoio fracos.[108] Sem apoio oportuno, esses comportamentos podem atrapalhar o desenvolvimento saudável, prejudicar relacionamentos e causar sofrimento psicológico significativo. O estigma e a exclusão podem causar danos adicionais, especialmente quando as crianças são rotuladas como agressoras, em vez de serem reconhecidas como crianças com necessidades específicas de proteção e desenvolvimento.[107] Os esforços existentes de prevenção e intervenção têm-se concentrado principalmente nos agressores adultos. As intervenções centradas nas crianças são frequentemente integradas em programas mais amplos de prevenção da violência, deixando lacunas na compreensão e na resposta.[107] A maioria das intervenções começa demasiado tarde, depois de o dano já ter ocorrido, perdendo uma janela crítica para a prevenção.[108] Ao ignorar que a exploração, o teste de limites e a assunção de riscos são típicos do desenvolvimento, os esforços de prevenção e resposta muitas vezes não conseguem satisfazer as necessidades destas crianças.[108]

Dados recentes também destacam crianças que causaram danos *online*, particularmente por meio da partilha de imagens sexuais de outras crianças.[80,99,109] Muitas não agem com a intenção de causar danos, mas sim por tédio, tentativas de humor ou expectativas sobre masculinidade.[7,99,108] As meninas são mais propensas a enfrentar pressão para produzir conteúdo sexual, enquanto os meninos são mais propensos a compartilhá-lo.[99] Os jovens de minorias sexuais e de género enfrentam riscos elevados de chantagem e *bullying*.[110] Culpar a vítima continua a ser comum, com pesquisas a mostrar que quase metade das crianças e dois terços dos cuidadores em Camboja e nas Filipinas culpam as vítimas quando as suas imagens são partilhadas contra a sua vontade.[111] Como partilhou um adolescente: «Ele era bastante popular. Não teve realmente nenhum efeito na sua popularidade...Acho que tem mais a ver com o que a rapariga enviou e o rapaz não sofreu realmente nenhuma repercussão.»[99]

Motivações e caminhos para a perpetração

A investigação destaca vários caminhos para a perpetração do CSEA facilitado pela tecnologia. O alto desejo sexual, o interesse sexual por crianças, a neuro-diversidade e a desregulação emocional são documentados como factores de risco.[94,108] Nos dados da linha de apoio, alguns infractores relataram que a sua própria vitimização na infância contribuiu para o comportamento abusivo posterior, com o trauma a actuar como motivador e racionalização.[52,112]

Novas evidências de pesquisas aprofundam a compreensão dessas motivações. Um estudo de 2024 com 4.549 infractores da *dark web* descobriu que:

- 30% eram motivados por interesse sexual em crianças,
- 15% tentavam regular emoções como solidão ou depressão,
- 10,6% tinham o desejo de compreender a sua própria experiência de abuso e

- 6,3% procuravam material que retratasse o seu próprio abuso.

Notavelmente, quase 40% dos infractores relataram consumo intenso de pornografia adulta antes de progredir para o CSAM.[94] Isso é consistente com outros estudos que mostram que os infractores geralmente começam consumindo pornografia adulta, mas depois passam a buscar novidades e «variedade».[95,113] O consumo de pornografia cada vez mais violenta ou extrema pode ter origem e interagir com outros factores problemáticos de comportamentos sexuais prejudiciais, reflectindo um padrão de dessensibilização. São necessárias mais pesquisas para compreender essas interacções complexas e os caminhos que levam à escalada e à perpetração.

As motivações financeiras são importantes: há evidências de que o CSAM é usado para impulsionar o tráfico na Internet, enquanto crimes como extorsão sexual, transmissão ao vivo e tráfico — muitas vezes facilitados pela IA generativa — são altamente lucrativos.[2,115] Os perpetradores de extorsão sexual financeira de crianças geralmente estão baseados em países de baixa e média renda, como Nigéria, Filipinas e Costa do Marfim, enquanto as vítimas normalmente estão localizadas em países de alta renda.[116] Em 2024, o NCMEC registou cerca de 100 denúncias de extorsão sexual financeira de crianças por dia, sendo os meninos alvos desproporcionais.[117] A IWF também relatou que 91% das vítimas de extorsão sexual eram do sexo masculino.[117]

> **“As pessoas muitas vezes pensam que os infractores são motivados apenas pela satisfação sexual, mas cada vez mais a motivação é financeira.”**
>
> *Indústria*[7]

Métodos e tecnologias utilizados para cometer crimes

Os métodos de perpetração são dinâmicos e moldados pelas tecnologias em evolução. Os infractores exploram o anonimato, a encriptação e as lacunas das plataformas para partilhar o CSAM na open e *dark web*.[118] Eles ocultam o conteúdo por meio da manipulação de links, redes de entrega de conteúdo, sites *doppelgänger* (mascarados) e trocas encriptadas nas redes sociais para evitar a detecção e a remoção.[11,119] Os algoritmos também podem revelar material prejudicial ou conectar crianças com infractores. Ao mesmo tempo, ferramentas de IA, tecnologia *deepfake* e aplicativos «nudify» (software que cria imagens falsas de nudez ou sexualmente explícitas com base em fotos de pessoas reais) permitem a produção de imagens sexuais infantis sintéticas, que podem ser usadas para coagir as vítimas a produzir o CSAM real.[13,118,121] Este padrão geralmente envolve o primeiro contacto e a preparação nas principais redes sociais, jogos e plataformas de mensagens, seguido pela mudança para ambientes criptografados ou anónimos para intensificar o abuso.[120]

> “Antes, isso só acontecia em fóruns obscuros ou na *dark web*... mas nos últimos dois anos, houve um enorme aumento na disponibilidade de [CSAM]”

Industria[7]

> “Não existe nenhuma plataforma segura, os infractores estão a usar todas as plataformas...quando perguntamos aos infractores onde eles contactam as crianças, eles respondem que, obviamente, é na open web, nas redes sociais e nas plataformas de jogos, onde as crianças estão. As crianças [pequenas] não estão na *dark web*.”

Sociedade civil[11]

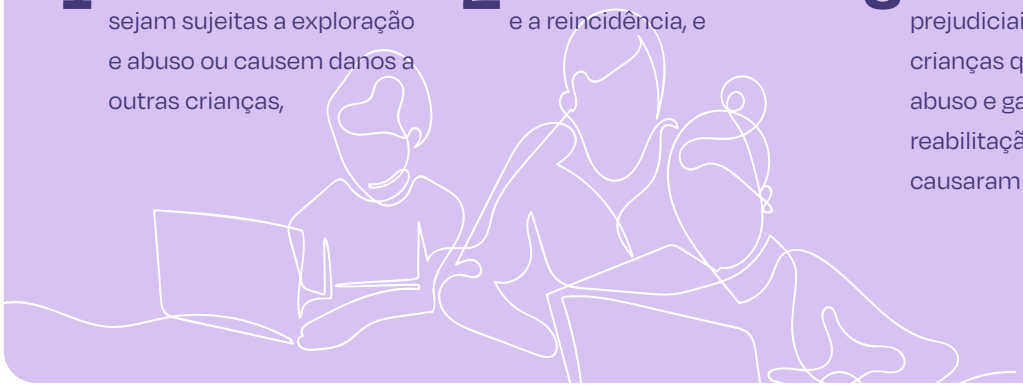
Prevenção

Utilizamos uma definição ampla de prevenção, abrangendo todas as acções que visam:

1 impedir que as crianças sejam sujeitas a exploração e abuso ou causem danos a outras crianças,

2 prevenir a revitimização e a reincidência, e

3 reduzir as consequências prejudiciais para as crianças que já sofreram abuso e garantir a reabilitação daqueles que causaram danos.



Esta definição inclui acções que podem ocorrer após a ocorrência do dano, frequentemente descritas como prevenção terciária ou resposta. Embora estes esforços recebam frequentemente mais atenção e recursos, é necessária uma maior atenção para abordar as causas profundas, reforçar os factores de proteção e prevenir os danos antes que ocorram. Os esforços de prevenção devem abranger todos os níveis do ambiente da criança, incluindo os seus pares, famílias, comunidades, instituições e sociedade em geral, e adaptar-se a um panorama tecnológico em evolução.[30] Respostas criativas e intersectoriais estão a demonstrar que a prevenção é possível, com várias delas lideradas ou informadas pelas próprias crianças e sobreviventes. As tecnologias emergentes introduziram novos riscos, mas também oferecem oportunidades de proteção.

A prevenção eficaz começa por abordar os factores sociais, estruturais e financeiros que causam danos. Deve considerar como factores como a idade, a orientação sexual e a identidade de género, a deficiência, a neuro-diversidade, a etnia, o estatuto indígena ou migrante, as condições socioeconómicas e o estatuto educativo se cruzam para moldar os riscos de danos ou comportamentos prejudiciais das crianças. Desequilíbrios de poder, pobreza, baixa literacia digital e supervisão parental limitada podem aumentar os riscos para as crianças.[123,124] Normas sociais prejudiciais, estigma, vergonha e culpabilização das vítimas podem impedir a divulgação e a procura de ajuda, enquanto leis e governança fracas permitem que o abuso prospere.[85,91,121] Os factores económicos, incluindo extorsão sexual financeira e receitas do tráfego e publicidade *online*, também devem ser abordados. A prevenção do CSEA facilitado pela tecnologia também requer compromisso político e investimento sustentado em sistemas, recursos e processos que protejam as crianças. Os principais facilitadores incluem:

- compromisso político sustentado e financiamento dedicado para priorizar a segurança e o bem-estar das crianças,
- governança digital robusta e responsabilidade em todos os níveis do governo,
- pesquisa e dados para informar a prevenção e priorizar recursos,

- sistemas sólidos de proteção infantil com profissionais treinados que possam detectar riscos precocemente e responder com apoio adequado às crianças, bem informado e sensível ao trauma,[121]
- normas sociais favoráveis que reconheçam que o CSEA facilitado pela tecnologia é evitável, incentivem a denúncia e promovam a procura de ajuda por indivíduos com pensamentos ou comportamentos sexuais prejudiciais,[125] e
- colaboração global e intersectorial para coordenar a prevenção, reforçar a responsabilização e harmonizar a terminologia, as normas de dados e os sistemas de monitorização.

> **“Se der o dispositivo e o telemóvel ou o acesso à Internet ao seu filho...estará a abrir a porta para um ambiente social repleto de adultos. Então, faria isso na sua casa? Acabou de abrir a porta e dizer ‘bem-vindos, todos!’”**
>
> *Sociedade civil*[11]

Colmatar o défice de financiamento

> **“Vejo oportunidades perdidas porque o financiamento está muito restrito neste momento, especialmente [com] o que está a acontecer no mundo...Todos estão a lutar [pelo] financiamento, o que não facilita muito a colaboração... Devemos trabalhar mais em conjunto para prevenir esses crimes.”**
>
> *Sociedade civil*[11]

Apesar da escala e complexidade crescentes do CSEA facilitado pela tecnologia, existe uma «lacuna de financiamento mundial significativa – e que se agrava» para a prevenção, resposta e investigação. A Safe *Online* identifica o subfinanciamento crónico como «o maior obstáculo à concretização de um futuro digital seguro, inclusivo e ético para as crianças».[126] A discrepância entre os investimentos na prevenção e os custos dos danos é gritante. A violência contra as crianças pode custar aos países até 11% do PIB, em alguns casos excedendo em seis vezes as despesas nacionais com saúde.[126] Nos Estados Unidos, mais de 5 mil milhões de dólares são gastos anualmente no encarceramento de adultos condenados por crimes sexuais contra crianças – mais de 3000 vezes o orçamento para a investigação sobre a prevenção do abuso infantil.[127] Os países de rendimento baixo e médio são especialmente subfinanciados, dependendo frequentemente de financiamento de curto prazo e baseado em projectos, em vez de respostas nacionais sustentadas.[128] Colmatar o défice de financiamento requer abordagens inovadoras, incluindo financiamento catalítico de

fontes filantrópicas, cofinanciamento dos governos, investimento sustentado de instituições financeiras internacionais e outras agências multilaterais, e mecanismos mais fortes para financiamento a longo prazo. Também é necessário financiamento para fortalecer os sistemas nacionais essenciais para a prevenção, incluindo saúde, educação, proteção infantil, serviços sociais e sistemas jurídicos. Reconhecendo a realidade de um ambiente de financiamento restrito, é essencial usar os recursos disponíveis de forma mais eficiente, coordenando melhor os esforços de prevenção entre os sectores, usando evidências e dados para priorizar investimentos e adaptando e testando intervenções baseadas em evidências, incluindo as da agenda Violência Contra Crianças.[9] Também são necessárias análises robustas de custo-benefício para demonstrar que a prevenção é mais económica do que respostas reactivas ao CSEA facilitado pela tecnologia.

> **"Há muitos elementos interessantes para...alinhar mais o diálogo Norte-Sul, para trazer o mundo académico para a esfera dos profissionais...[mas] infelizmente acho que o panorama de financiamento não é propício para melhorar isto."**
>
> *Sociedade civil*[11]

Fortalecer a base de evidências para a prevenção

> **"É quase uma frase automática dizer...precisamos de mais dados, mas em algum momento temos que reconhecer o facto de que...Se você tem mais de 500 [estudos sobre exploração sexual de meninos migrantes], é injusto dizer que simplesmente não há dados. É que muitas vezes a qualidade dos dados é fraca."**
>
> *Académico*[8]

É essencial dispor de evidências sólidas para compreender os riscos emergentes, avaliar as estratégias de prevenção e orientar os investimentos. Uma abordagem de saúde pública pode orientar este processo: (1) definir e monitorar o problema e a sua prevalência; (2) identificar os factores de risco e de proteção; (3) conceber, testar e avaliar estratégias de prevenção; e (4) partilhar lições e ampliar o que funciona.[123] Traduzir a investigação em prevenção mais eficaz requer investigação coordenada e partilha de dados entre setores e países. A **Data for Change initiative**, lançada em 2022 e que agora envolve 120 organizações, visa mapear boas práticas, reduzir barreiras à partilha de dados e priorizar dados de países da Maioria Global.[130] A iniciativa enfatiza a adaptação de abordagens a contextos específicos e o envolvimento de jovens investigadores em países de baixa e média renda, para tornar as evidências mundiais mais inclusivas e accionáveis. O resumo de dados da UNICEF sobre **a medição da violência contra crianças facilitada pela tecnologia, em conformidade com a Classificação Internacional de Violência contra Crianças**, promove esforços para melhorar a qualidade e a comparabilidade dos dados mundiais.[131]

Para se manter informado sobre as tendências emergentes e as evidências globais mais recentes sobre estratégias de prevenção eficazes, consulte os recursos vivos no apêndice.

Transformar evidências em acções para acabar com a violência sexual infantil: O Safe Futures Hub global Living Systematic Review e Practice-based Knowledge framework

Lançado em Setembro de 2023, o Safe Futures Hub é co-liderado pela Sexual Violence Research Initiative (SVRI), Together for Girls e WeProtect Global Alliance.[132–135] A sua missão é acabar com a violência sexual infantil, promovendo soluções baseadas em dados, evidências, conhecimento prático e abordagens lideradas pela comunidade.

No início de 2026, o Safe Futures Hub, em conjunto com a Universidade de Oxford, lançará a **Living Systematic Review** global, um recurso actualizado que sintetiza evidências sobre o que funciona para prevenir a violência sexual infantil. A **Living Systematic Review** aplica métodos rigorosos e transparentes para identificar, avaliar e resumir estudos de intervenção emergentes, garantindo que os decisores políticos, profissionais e investigadores tenham acesso às evidências mais actuais. Ao contrário das revisões estáticas, evoluirá em tempo real, colmatando a lacuna entre a investigação e a prática. Com base no relatório de evidências **Building Safe Futures** 2024 e no seu apelo a acções mais fortes e baseadas em evidências, este recurso orientará os investimentos em estratégias eficazes e contextualmente relevantes. Ao destacar intervenções que funcionam, a **Living Systematic Review** do Safe Futures Hub capacitará as partes interessadas a ampliar e adaptar soluções que protegem as crianças da violência sexual.

Em Dezembro de 2025, o Safe Futures Hub lançará dois novos recursos para fortalecer a forma como o conhecimento baseado na prática (singla inglesa PbK) é reconhecido e utilizado na prevenção e resposta à violência sexual infantil.

- O documento de referência explica o que é o PbK e por que é importante para prevenir e responder à CSV, mostrando como ele traz vozes sub-representadas, fortalece a prática e valoriza tanto os profissionais como a experiência vivida.
- A estrutura de orientação oferece ferramentas e processos accionáveis para apoiar os profissionais na recolha, utilização e partilha do PbK de forma segura, ética e prática.

No contexto da prevenção e resposta à violência sexual infantil, o PbK refere-se às ideias geradas através da experiência vivida e do envolvimento directo em programas, serviços ou esforços de defesa. Enquanto a investigação mostra o que funciona, o PbK explica como funciona, por que funciona e como mantê-lo a funcionar em contextos complexos e em mudança. Juntos, o PbK e a investigação podem tornar as estratégias mais eficazes, relevantes e fundamentadas em contextos do mundo real.

Conceber o quadro de prevenção

Ao longo das consultas, surgiu uma mensagem unificadora: precisamos agir agora. Compreender a dimensão e a natureza do CSEA facilitado pela tecnologia é necessário, mas não suficiente. O desafio central que muitos neste campo continuam a enfrentar – «por onde começamos?» – foi o impulso para esta estrutura de prevenção.

A estrutura de prevenção foi desenvolvida para complementar o Modelo Nacional de Resposta da WeProtect Global Alliance, que fornece uma estrutura para acção a nível nacional e sistémico. Juntas, elas orientam a acção global para lidar com o CSEA facilitado pela tecnologia.[29] A estrutura também se baseia em outros modelos bem estabelecidos:

- o Modelo Socioecológico, que destaca que os riscos e proteções existem em vários níveis do ambiente da criança;[30] e
- a abordagem de prevenção em saúde pública, que define a prevenção em diferentes níveis, desde abordagens para toda a população até medidas direcionadas a indivíduos em risco de sofrer ou causar danos.[1,2,3]

A estrutura também está ancorada em normas internacionais e regionais de direitos da criança, incluindo a Convenção das Nações Unidas sobre os Direitos da Criança e os Comentários Gerais 16, 24 e 25, e o Pacto Digital Global (Global Digital Compact).[24,33,136] Foi co-criada através de um processo participativo envolvendo jovens, sobreviventes e um Comité Directivo de Peritos representando governos, sociedade civil, indústria e agências intergovernamentais. As partes interessadas contribuíram por meio de workshops e comentários por escrito.

> **"Quando estamos a envidar esforços de prevenção, acredito que devemos envolver todas as partes interessadas...sobreviventes, pessoas com vasta experiência, indústrias tecnológicas, instituições religiosas, líderes comunitários, professores, pais, mentores de jovens, ONG, sociedade civil e até mesmo organizações regionais como a União Africana, a ONU e a INTERPOL."**
>
> *Sociedade civil[11]*

A estrutura de prevenção está organizada em torno de quatro áreas de acção interligadas:

- Participação e liderança infantil
- Educação e apoio comunitário
- Segurança digital
- Lei, política e justiça

A ordem em que são apresentadas reflecte uma abordagem socioecológica, começando pelas crianças e avançando para a comunidade, instituições, governos e actores mundiais. As áreas de acção são mapeadas em três níveis de prevenção: primário (proteção proactiva), secundário (detecção e interrupção dos danos) e terciário (resposta e apoio após o abuso). Facilitadores como pesquisa e financiamento são cruciais e devem ser abordados continuamente para garantir que todas as acções sejam eficazes e sustentáveis.

Em vez de classificar as intervenções por força de evidência, o que ainda não é possível, esta estrutura apresenta recomendações temáticas para ajudar as partes interessadas a identificar acções de prevenção relevantes para o seu contexto e experiência. A estrutura destaca abordagens baseadas em evidências, quando disponíveis, e aponta para recomendações de especialistas, boas práticas e práticas inovadoras que precisam de avaliação adicional.

> **"É agora necessária uma abordagem de saúde pública, com o estabelecimento de um sistema para prevenir a perpetração, detectar e combater o crime, mas também para apoiar as vítimas e as suas famílias."**
>
> *Academicos[8]*

Perspectivas de especialistas sobre as prioridades de prevenção da Avaliação da Ameaça Global 2025

A nossa pesquisa *online* com 77 profissionais que trabalham no combate ao abuso sexual infantil facilitado pela tecnologia (61% sem fins lucrativos, 19% governamentais, 16% industriais e 3% órgãos estatutários independentes) confirmou um forte apoio às quatro áreas de acção. Os inquiridos pediram uma compreensão mais profunda do comportamento, motivações e perfis dos agressores (47%); as causas fundamentais e os factores sistémicos dos danos (45%); e as perspectivas das crianças sobre o uso da tecnologia (39%). As principais prioridades identificadas para ampliar os esforços de prevenção foram financiamento flexível e de longo prazo (87%), formação e suporte técnico para a equipe (58%) e acesso a ferramentas e orientações de código aberto centradas na criança (50%).

Embora baseadas numa pequena amostra de especialistas, estas conclusões refletem um amplo consenso sobre as prioridades de prevenção e a necessidade urgente de investimento, capacitação e colaboração.

Colocando a prevenção em prática: o modelo Swiss cheese (queijo suíço)

O modelo oferece uma lente poderosa para compreender como esta estrutura de prevenção pode ser aplicada na prática.[137] Amplamente utilizado em áreas críticas para a segurança, como aviação, medicina e engenharia, o modelo enfatiza que danos graves raramente resultam de um único ponto de falha. Em vez disso, os danos ocorrem quando várias fraquezas nos sistemas de proteção se alinham. Cada «fatia» do queijo suíço representa uma camada de proteção — por exemplo, medidas de segurança digital ou leis, políticas e mecanismos judiciais. Cada fatia tem «buracos» que representam pontos de fraqueza. Um único buraco pode não causar danos porque outras camadas actuam como uma barreira, mas quando os buracos em várias camadas se alinham, podem ocorrer danos graves.

Aplicado ao CSEA facilitado pela tecnologia, o modelo destaca três aspectos importantes:

- Sempre que uma criança é prejudicada pelo CSEA facilitado pela tecnologia, isso reflecte uma falha do sistema e várias oportunidades perdidas de intervir.
- Nenhum actor ou sector tem todas as soluções. Várias camadas de prevenção devem trabalhar em conjunto.
- A prevenção requer aprendizagem e adaptação contínuas para identificar onde existem pontos fracos na proteção, quão graves e urgentes são as consequências potenciais e quais os recursos disponíveis para colmatar lacunas ou reforçar outras camadas de proteção.

Usados em conjunto, a estrutura de prevenção e o modelo do queijo suíço fornecem estrutura e método. Enquanto a estrutura de prevenção abrange todas as formas de CSEA facilitado pela tecnologia, o modelo do queijo suíço pode ajudar as partes interessadas a priorizar acções, avaliar riscos e identificar pontos fracos que contribuem para um incidente ou tipo de dano específico. Juntos, eles mudam o foco de soluções isoladas para a construção de sistemas resilientes com múltiplas camadas de proteção para manter as crianças seguras..

Cenário: Amal está no ensino secundário. Recentemente, ela terminou o namoro com o parceiro que tem a mesma idade que ela. Para se vingar, o parceiro dela publicou fotos íntimas de Amal *online*, e outras pessoas as espalharam pela escola. O que aconteceu com Amal foi resultado de falhas em vários níveis. Foi assim que aconteceu, da perspectiva dela..

Figura 4 . Visualizando o modelo do queijo suíço: compreendendo os riscos em conteúdos sexuais gerados em primeira pessoa envolvendo crianças

Participação e liderança infantil

- Parceiros treinados para receber denúncias e encaminhar as crianças a serviços de apoio.
- Concepção de materiais educativos e de sensibilização, canais de denúncia e funcionalidades de segurança digital orientados para as crianças e os sobreviventes.

Educação e apoio comunitário

- Programas escolares sobre relacionamentos saudáveis, sexualidade e segurança digital.
- Apoio precoce a crianças em risco de sofrerem danos ou de causarem danos.
- Formação de educadores e políticas escolares claras para prevenção e resposta.
- Campanhas de sensibilização da comunidade para mudar normas, reduzir a culpabilização das vítimas e incentivar a denúncia.

Segurança digital

- Avaliações do impacto nos direitos da criança e funcionalidades de segurança por design durante o desenvolvimento da plataforma (por exemplo, deteção de nudez, pop-ups de aviso de conteúdo que interrompem partilhas arriscadas e solicitam ajuda).
- Opções de denúncia acessíveis que fornecem feedback oportuno, ligação para apoio e remoção rápida de conteúdos ou contas prejudiciais.

Leis, políticas e justiça

- Leis que respeitem os direitos, protejam as vítimas e evitem criminalizar comportamentos consensuais entre pares com idades próximas.
- Reguladores com poderes para supervisionar o cumprimento das normas pela indústria, investigar abusos e impor sanções.
- Justiça amiga da criança e acesso a reparação através de polícias, juízes e procuradores com formação específica.

Áreas de acção preventiva

Participação e liderança infantil

> "As vozes das crianças devem ser ouvidas em todas as etapas de prevenção, detecção e resposta as devem ser ouvidas em todas as etapas de prevenção, detecção e resposta."

Sobrevivente, Filipinas[138]

As crianças e os sobreviventes têm o direito de partilhar as suas opiniões e influenciar as políticas, os programas e os serviços que os afectam através de uma participação segura e significativa.

As parcerias com organizações lideradas por crianças e centradas nas crianças podem promover uma participação segura, detectar riscos e danos precoces e informar intervenções eficazes e centradas nas crianças.

Devem ser envidados esforços para envolver todas as crianças, especialmente aquelas provenientes de contextos marginalizados, reconhecendo que as crianças correm o risco tanto de serem prejudicadas como de causar danos a outras crianças.

Princípios para uma participação segura e significativa

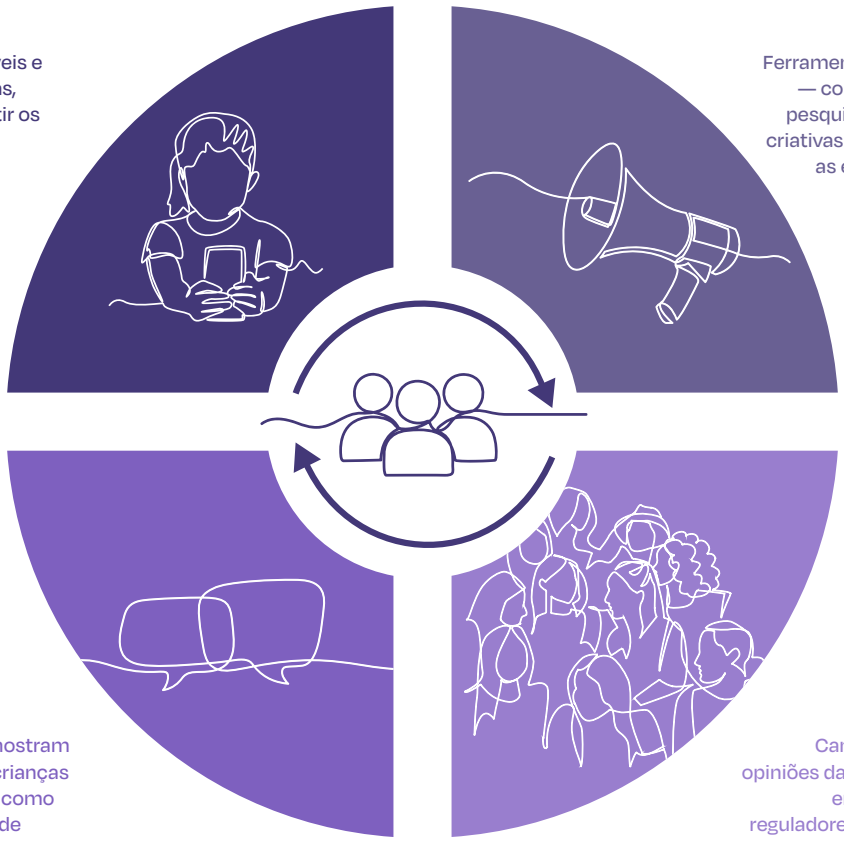
> "Elas [as crianças] são as pessoas mais vulneráveis e mais necessárias para resolver o problema."

Sobrevivente, Filipinas[138]

O artigo 12.º da Convenção das Nações Unidas sobre os Direitos da Criança afirma o direito de todas as crianças serem informadas, expressarem as suas opiniões e participarem nas decisões que afectam todos os aspectos das suas vidas.[33] O **Modelo Lundy** (ver Figura 5) fornece um quadro prático para a aplicação do artigo 12.º, a fim de apoiar a participação significativa das crianças.[139] As crianças e os jovens podem ajudar a identificar riscos emergentes e a informar estratégias de prevenção proactivas.

Como parte de uma campanha implementada na Indonésia, no Nepal e nas Filipinas, a organização de direitos da criança Kindernothilfe desenvolveu um **Guia** e **Kit de Ferramentas do Programa Global** para apoiar a participação significativa de crianças e jovens na defesa da prevenção e proteção contra a violência *online*.[140,141] A UNICEF desenvolveu o **Spotlight Guidance**, que partilha as melhores práticas para envolver as crianças nas Avaliações de Impacto dos Direitos Digitais da Criança.[142]

Figura 5. Características da participação significativa aplicadas online[143]



ESPAÇO
Fóruns seguros, acessíveis e adequados para crianças, onde elas podem discutir os riscos digitais.

VOZ
Ferramentas adequadas à idade — como enquetes, avatares, pesquisas anônimas e mídias criativas — para aprender sobre as experiências online das crianças.

INFLUÊNCIA
Ligações visíveis que mostram como as opiniões das crianças levam a melhorias, tais como melhores ferramentas de denúncia, recursos de privacidade mais fortes ou programas de prevenção nas escolas.

PÚBLICO
Canais diretos para que as opiniões das crianças cheguem às empresas de tecnologia, reguladores, autoridades policiais e legisladores.

0

A segurança, a qualidade e os melhores interesses das crianças devem ser sempre priorizados ao envolver as crianças. A participação das crianças só deve ocorrer quando houver pessoal adequado, medidas de proteção e serviços de apoio informados sobre traumas para as proteger de danos. Se isso não for possível, recorra a ideias de jovens, adultos e organizações que possam representar as opiniões das crianças, bem como a evidências, pesquisas e boas práticas existentes.

Envolver crianças e sobreviventes na prevenção

> **“Acho que as ONG criadas por jovens e para jovens serão realmente úteis. Essas organizações poderiam aumentar a conscientização de uma forma mais confortável, pois os conselhos viriam de outros jovens.”**

Rapaz de 17 anos, Paquistão[60]

As iniciativas que envolvem crianças e jovens na prevenção incluem:

- **Mtoto News**, uma plataforma digital e de mídia com sede no Quénia que facilita a defesa liderada por crianças e permite que mais de 100.000 crianças se envolvam directamente com seus líderes em questões que incluem abuso sexual infantil *online* e *offline*.[144]
- A **Digital Well-Being Index** da Snap Foundation, que envolve jovens de seis países para partilharem ideias sobre o seu bem-estar psicológico e experiências em plataformas *online*, revelando informações importantes para a prevenção.[45]
- **BeSmartOnline**, o Centro para uma Internet mais Segura oficial do governo de Malta, que é orientado por um painel de jovens que ajuda a identificar novos riscos *online* e a co-elaborar estratégias eficazes de sensibilização.[145,146]

Liderança juvenil na segurança *online*: Ideias da VoiceBox

A VoiceBox é uma empresa social e plataforma de conteúdo sediada no Reino Unido e liderada por jovens que ajuda criadores jovens entre 13 e 25 anos a prosperar e a moldar ambientes digitais mais seguros, centrados nas suas experiências de vida.[147] Com uma rede mundial que abrange mais de 50 países, a VoiceBox amplifica diversas perspectivas e muitas vezes consegue identificar riscos *online* emergentes mais rapidamente do que a investigação tradicional, servindo como um «sistema de alerta precoce» para decisores políticos e líderes da indústria. Isto garante que os decisores estejam equipados com informações em tempo real, baseadas nos jovens, sobre as ameaças em evolução.

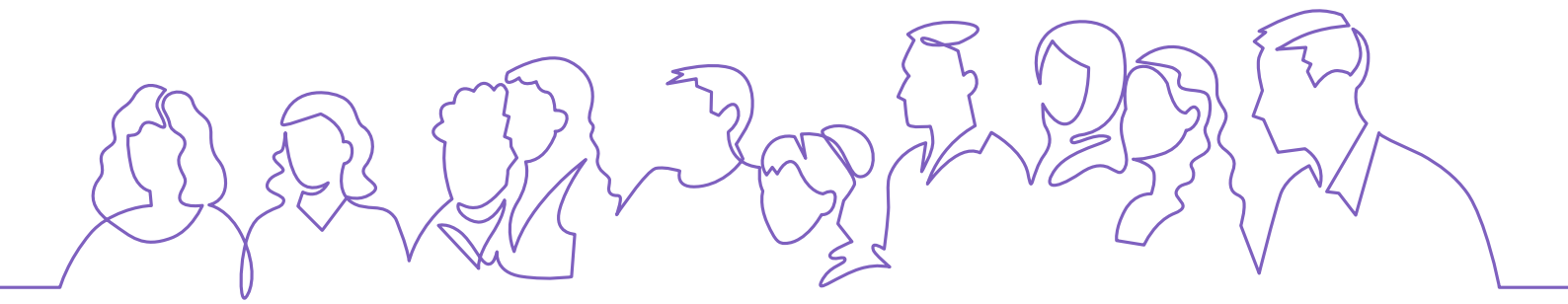
A VoiceBox reúne ideias honestas e não filtradas de jovens sobre desafios complexos de segurança *online*, incluindo literacia mediática, danos *online* e riscos digitais emergentes. A sua abordagem combina oportunidades de liderança para jovens com forte proteção e apoio informado sobre traumas. A VoiceBox utiliza grupos focais liderados por pares, entrevistas e métodos criativos de recolha de ideias (como arte, vídeos e poesia) para permitir que os jovens partilhem experiências de forma segura e autêntica. Esta abordagem lançou luz sobre questões como os companheiros de IA e as plataformas baseadas em assinaturas.[44]

As crianças que sofrem discriminação interseccional — como populações de minorias sexuais e de género e crianças com deficiência — enfrentam riscos e danos únicos *online*, mas muitas vezes são excluídas das políticas e programas.[11]

> **"Se não forem devidamente tidas em conta na forma como as interações e as políticas são concebidas, corremos o risco de perder esta população sub-representada."**
>
> *Sociedade civil*[11]

É importante consultar crianças marginalizadas e aquelas com necessidades específicas que podem navegar nas tecnologias digitais de maneira diferente de seus pares.[8] Por exemplo, crianças surdas, que muitas vezes dependem da comunicação por vídeo, enfrentam riscos *online* únicos e podem ter menos oportunidades de reconhecer ou denunciar possíveis explorações.[11] Garantir estratégias de comunicação acessíveis, personalizadas e inclusivas é fundamental para apoiar a segurança *online* dessas crianças. Exemplos de iniciativas lideradas e informadas por sobreviventes são destacados abaixo:

- **O Disrupting Harm** (Interrompendo o Dano) gera evidências de alta qualidade sobre os danos digitais causados a crianças e jovens em 25 países em 6 regiões. O projecto utiliza processos participativos informados sobre traumas, seguindo diretrizes éticas rigorosas e procedimentos de proteção infantil. A primeira fase revelou que quase uma em cada três crianças não revelou os danos, com quase metade a referir que não sabia a quem contar ou onde procurar ajuda.[10] Uma segunda ronda de entrevistas aprofundadas com mais de 100 jovens sobreviventes na América Latina, Europa Oriental e Médio Oriente foi concluída em 2025, com resultados a serem divulgados em breve.
- **A Global Boys Initiative** (Iniciativa Rapazes do Mundo) documenta as experiências de meninos vítimas de exploração e abuso sexual em dez países, destacando as barreiras à divulgação, denúncia e acesso a serviços.[148]
- O estudo **Our Voice Male Survivors** (Nossa Voz Homens Sobreviventes) fornece um dos maiores conjuntos de dados sobre rapazes que foram vítimas de abuso sexual. Ele mostra padrões distintos, como início precoce, perfis diferentes dos agressores e atrasos mais longos antes da divulgação, ressaltando a necessidade de pesquisas e serviços sensíveis às questões de género.[114]
- **Secrets Worth Sharing** (Segredos que Vale Partilhar) é uma plataforma que fornece recursos informados sobre traumas que reconhecem a diversidade das experiências dos sobreviventes. Apresenta workshops, podcasts e vídeos centrados nos sobreviventes, cobrindo tópicos como abuso sexual infantil, interseccionalidade no trauma e crianças que exibem comportamentos sexuais prejudiciais.[149] Como o fundador partilhou:



> Uma coisa que fazemos de forma diferente como organização é produzir recursos *online* específicos para diferentes factores de identidade, como ser negro, queer ou falar outra língua. O meu maior envolvimento com adolescentes e jovens é sobre sugestões para esses episódios [podcast e vídeo]. Acho que isso se deve ao facto de as crianças e os jovens não quererem apenas ver-se como sobreviventes ou vítimas , mas estarem interessados em como as suas experiências são únicas com base nas suas próprias identidades.

Sociedade civil[150]

Educação e apoio comunitário

> Para promover a educação e a colaboração digitais, concentre-se não apenas em ferramentas de segurança, mas também em capacitar crianças e adolescentes com conhecimentos e habilidades para navegar com segurança e responsabilidade. Envolva pais, educadores e os próprios jovens na criação de ambientes digitais mais seguros e positivos.

Homem de 18 anos, Nicarágua[60]

Os esforços de educação e sensibilização devem procurar mudar comportamentos e promover a denúncia e a procura de ajuda. Devem basear-se em evidências, ser adaptados ao contexto, acessíveis a todas as crianças e coordenados intersectoriais para garantir funções claras e mensagens consistentes e eficazes.

As crianças precisam de múltiplas formas confiáveis de denunciar preocupações, procurar ajuda e aceder a serviços de apoio centrados nos sobreviventes, incluindo linhas de apoio, canais formais de denúncia, colegas treinados para dar apoio e adultos seguros.

Devem estar disponíveis intervenções precoces e baseadas em evidências para crianças em risco de serem prejudicadas, bem como para crianças e adultos em risco de causar danos.

As mensagens de dissuasão e os avisos devem ser adaptados aos diferentes indivíduos em risco de causar danos e acompanhados de vias imediatas de apoio para pensamentos e comportamentos sexuais prejudiciais.

Campanhas de educação e sensibilização

> **"Precisamos de educar tanto as crianças como os pais sobre segurança *online*... Sinto que a maioria das pessoas pensa que não tem para onde recorrer [para obter ajuda] porque é *online*... Os pais também precisam de ser mais educados sobre como lidar com estas situações. E as leis poderiam ser mais rigorosas, especialmente no meu país, nunca ouvi falar muito sobre este assunto."**
>
> *Mulher de 14 anos, Etiópia*[60]

As iniciativas de educação e sensibilização são fundamentais para a prevenção. Estes esforços devem ir além da simples sensibilização, promovendo mudanças reais de comportamento e garantindo o acesso a ajuda.[9]

Especialistas de vários sectores, bem como defensores dos jovens e sobreviventes, salientaram que os esforços eficazes de educação e sensibilização devem:

- Ser informados por/ou desenvolvidos em conjunto com crianças e sobreviventes, ter em conta os traumas e ser sensíveis ao contexto.
- Evitar mensagens baseadas no medo ou estigma que dissuadam a denúncia e a procura de ajuda.
- Ser inclusivos e acessíveis. Devem ser disponibilizados em vários idiomas, formatos e locais, incluindo escolas e outros espaços físicos e digitais onde as crianças aprendem e se relacionam. Devem ser envidados esforços para alcançar grupos marginalizados, incluindo crianças com deficiência, crianças que não frequentam a escola e crianças em áreas rurais ou contextos educativos frágeis.
- Equipar crianças e adultos — incluindo cuidadores, educadores e prestadores de serviços — com o conhecimento e as habilidades necessárias para prevenir, reconhecer e responder à exploração e ao abuso sexual, tanto *online* como *offline*. Isso deve incluir informações sobre leis relevantes, como denunciar preocupações, onde procurar ajuda e como apoiar crianças e colegas, evitando causar danos.
- Ser coordenado e sustentado, com funções claras nas escolas, famílias, comunidades, indústria e governo para garantir mensagens consistentes e eficazes.
- Ser adequada à idade e ao estágio de desenvolvimento das crianças e estrategicamente programada (por exemplo, antes de uma criança receber o seu primeiro telemóvel ou começar a usar a Internet sem supervisão).

Alguns sobreviventes e defensores dos jovens expressaram preocupações de que a educação possa ter dificuldade em acompanhar os riscos associados às tecnologias em rápida evolução (por exemplo, XR) e que os ambientes de educação formal possam parecer intimidantes ou inseguros para as crianças discutirem questões delicadas. Isto destaca a necessidade de envolver as crianças na identificação de riscos e na definição de iniciativas de educação e sensibilização.

> **"Haverá muitas crianças que não vão querer participar em algo assim [educação escolar], porque é...ainda [um] tema tabu e haverá crianças diferentes que terão medo de dizer qualquer coisa e medo de se expressar."**

Sobrevivente[77]

> **"Os pais, especialmente os recém-chegados, podem não ter as competências linguísticas ou o conhecimento tecnológico para acompanhar [os riscos associados às novas tecnologias]. Os recursos...devem ensinar segurança nas redes sociais, ou as escolas devem enviar materiais em vários idiomas para educar os pais."**

Defensor da criança, Canadá[38]

Os programas de prevenção do abuso sexual infantil são bem apoiados por evidências, embora as evidências para programas que abordam os riscos relacionados à tecnologia ainda sejam limitadas e estejam em desenvolvimento.

- **O Tackling Online Child Sexual Exploitation (TOCSE)** - [Combate a Exploração e Abuso Sexual Infantil Online] - aborda a violência *online* a nível individual, comunitário, industrial e sistémico no Vietname. Envolve as crianças em consultas participativas, na concepção de materiais informados pelas crianças e em iniciativas lideradas por crianças nas escolas.[153,154] O TOCSE proporcionou educação e formação profissional a mais de 18.000 crianças com 12 ou mais anos e a 11.000 pais e professores, além de reforçar as linhas de apoio às crianças e os serviços de apoio.[153,154]
- O relatório da UNICEF sobre programas parentais baseia-se numa rápida síntese de evidências e consultas com mais de 50 especialistas de vários sectores para identificar considerações-chave para a concepção de intervenções que apoiem pais e cuidadores na prevenção e resposta ao CSEA facilitado pela tecnologia.[155]

> **“Acho que deveria haver mais aulas e workshops nas escolas sobre exploração infantil ou abuso sexual *online*...acho que eu poderia facilmente ter-me tornado uma vítima disso. Mas agora que participei de alguns workshops, fiquei mais informada sobre como os traficantes vitimizam as pessoas e como escolhem as vítimas... E então, sinto que educar os alunos sobre...como as vítimas são escolhidas pelos traficantes realmente os impediria de se tornarem vítimas de tráfico.”**

Defensor das crianças, Canadá[38]

> **“[É necessária] mais educação sobre o que evitar e por que evitar. As crianças não ouvem quando lhes dizem apenas para não fazer algo. É melhor dar às crianças uma educação passo a passo e ouvir as partes desconfortáveis sobre por que algo é errado, para que elas saibam que não devem fazer isso”**

Defensor das crianças, Quénia[38]

Campanhas eficazes de sensibilização do público podem mudar comportamentos e reforçar a ideia de que o CSEA é evitável. Também podem reduzir o estigma em torno da denúncia, da busca por justiça e da procura de ajuda para pensamentos e comportamentos sexuais prejudiciais. Por exemplo, após a campanha de sensibilização da Agência Nacional contra o Crime do Reino Unido sobre extorsão sexual a proporção de inquiridos que afirmaram que partilhariam imagens explícitas num cenário de extorsão diminuiu significativamente.[156] Da mesma forma, dados da IWF mostram que, após uma campanha sobre a distribuição não consensual de imagens íntimas, o uso da ferramenta **Report Remove** aumentou, embora a campanha não promovesse especificamente a ferramenta.[157] No entanto, o conteúdo, a qualidade e a eficácia das campanhas variam, e poucas iniciativas são avaliadas formalmente. Exemplos recentes de campanhas de sensibilização incluem:

- **Help Children be Children** (Ajude as crianças a serem crianças) em Uganda e na Zâmbia, que combinou campanhas de sensibilização com o reforço da capacidade das linhas directas e das autoridades policiais. As campanhas levaram a mais denúncias e melhoraram o conhecimento dos funcionários das linhas directas.[157]
- **Beware the Share** (Cuidado com a Partilha), do **UNODC**, campanhas interativas em idiomas locais informaram o público sobre aliciamento, sexting (envio de mensagens sexualmente explícitas) e abuso baseado em imagens em cinco países do Sudeste Asiático.[158]
- Em resposta a uma pesquisa que revelou que 70% dos pais no Nepal não estavam cientes dos riscos e danos do CSEA online, a ChildSafeNet fez uma parceria com o TikTok para oferecer treinamento em segurança digital para crianças, pais e educadores em sete distritos do Nepal.

> **“Acho que todos devem ser conscientizados desde muito cedo sobre o uso e o uso indevido [das tecnologias digitais] e, se tais problemas surgirem, como podem lidar com eles. E, em ambos os casos, a família, os amigos e todas as pessoas devem estar cientes..”**
>
> *Mulher de 19 anos, Nepal*[38]

Comportamento Responsável com Jovens e Crianças (sigla inglesa RBYC): Promovendo o desenvolvimento de normas sexuais saudáveis e abordando o abuso por colegas próximos em idade

Desenvolvido por especialistas em abuso sexual infantil e prevenção da violência escolar da MOORE | Preventing Child Sexual Abuse, Johns Hopkins Bloomberg School of Public Health.

O **RBYC** é um currículo escolar baseado em evidências para crianças de 11 a 14 anos que visa prevenir comportamentos sexuais problemáticos e ajudar os jovens adolescentes a desenvolver interacções seguras e adequadas — com crianças mais novas, seus pares e adultos — tanto *online* como *offline*.[74] O programa consiste em cinco sessões interactivas apoiadas por vídeos animados e discussões em sala de aula.[74]

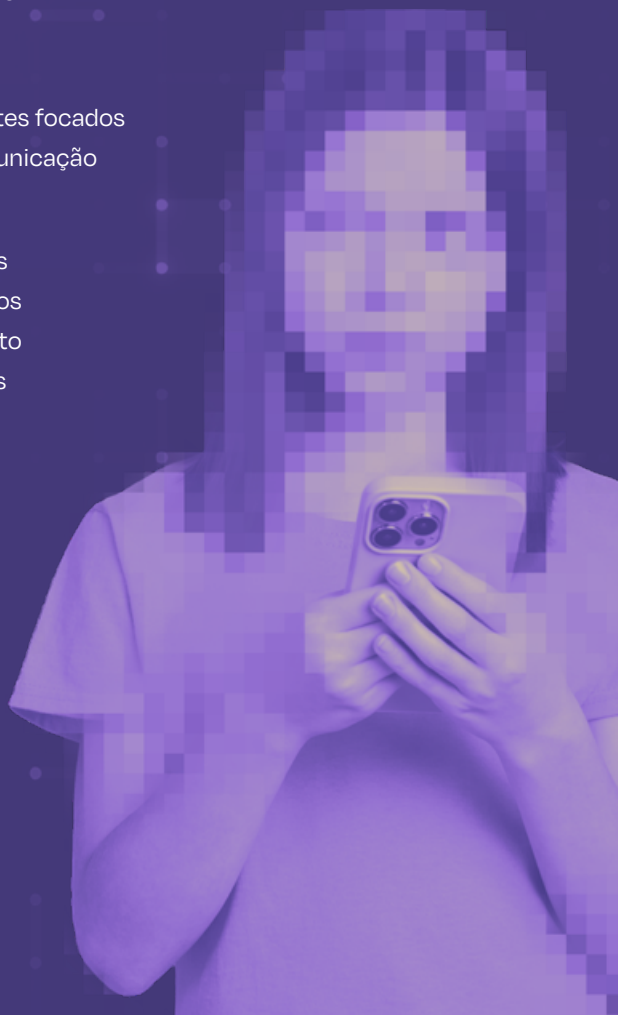
Uma elevada proporção dos abusos sexuais de crianças é perpetrada por outras crianças e adolescentes. O início da adolescência é uma fase crítica do desenvolvimento, quando os jovens estão a formar identidades e normas sexuais e podem não ter as competências ou os conhecimentos necessários para lidar com relações emergentes de forma segura.[160,161] O **RBYC** aborda estas lacunas através de uma abordagem informada sobre traumas e baseada nos pontos fortes. O currículo pode ser ministrado como um programa autónomo ou integrado em currículos existentes de saúde, educação sexual ou prevenção da violência. As sessões abrangem:

- Relações saudáveis e tomada de decisões
- Limites pessoais e consentimento
- Diferenças de desenvolvimento entre adolescentes e crianças mais novas
- Comportamentos responsáveis e irresponsáveis em contextos *online* e *offline*
- Identificação e prevenção de comportamentos sexuais problemáticos
- Adultos e amigos seguros

O **RBYC** inclui materiais para levar para casa para as famílias e componentes focados em adultos para educadores e pais/cuidadores, a fim de incentivar a comunicação aberta e reforçar as mensagens de prevenção em casa e na escola.

Um ensaio controlado aleatório com 160 alunos nos EUA descobriu que as crianças que participaram no **RBYC** demonstraram aumentos significativos na autoeficácia para prevenir danos sexuais e melhoraram o conhecimento sobre diferenças de desenvolvimento, consentimento e comportamentos sexuais problemáticos em comparação com aqueles que não receberam o currículo.

Além do ensaio nos EUA, o **RBYC** está a ser ampliado e adaptado mundialmente. O currículo foi adaptado para uso na Alemanha (com um ensaio aleatório controlado em andamento em 24 escolas) e nas Filipinas (atingindo 250 alunos como parte de programas de prevenção combinados).[162] Em colaboração com o Kennedy Krieger Institute, o **RBYC** também foi adaptado para adolescentes neuro-diversos e aprimorado com vídeos educativos para aumentar a acessibilidade e o envolvimento.[8]



Conteúdo sexual gerado na primeira pessoa envolvendo crianças

> "As crianças vão fazer este [sexting] no contexto dos relacionamentos, e como podemos fazer com que elas o façam de uma forma que não volte para assombrá-las?"

Sociedade civil[111]

A partilha de imagens íntimas pode ser uma parte normal dos relacionamentos adolescentes. No entanto, a distribuição e criminalização desse conteúdo pode causar danos, especialmente quando as leis e políticas não distinguem entre CSAM produzido por adultos e imagens geradas na primeira pessoa envolvendo crianças. As evidências mostram que abordagens baseadas no medo ou apenas na abstinência são frequentemente ineficazes e podem desencorajar a denúncia e a procura de ajuda.[163]

> "Havia um assistente social e um agente da polícia que estavam a falar connosco sobre isso e a dizer que...se enviarmos as nossas próprias imagens nuas, isso ainda é distribuir pornografia infantil, então...tenho quase a certeza de que metade das pessoas que estavam lá enviaram imagens nuas... provavelmente pensaram: 'Oh, há um agente da polícia ali e ele vai prender-me no meio do ginásio'."

Mulher de 17 anos[164]

Leaked: Visão sobre conteúdo sexual gerado na primeira pessoa na Tailândia

- Os jovens costumam partilhar e encontrar conteúdo sexual *online* e descrevem principalmente os danos como ocorrendo quando perdem o controlo sobre o conteúdo.
- Abordagens baseadas na educação sexual podem ser mais eficazes do que advertências severas e ameaças contra qualquer partilha de conteúdo sexual.

Leaked é uma parceria de três anos entre o Projecto HUG, uma ONG sediada em Chiang Mai, e a empresa de pesquisa Evident, sediada em Banguecoque, com o apoio da World Childhood Foundation.[165,166,167] Esta iniciativa teve como objectivo compreender melhor como os jovens na Tailândia se envolvem com — e interpretam — conteúdos sexuais gerados na primeira pessoa. Inclui um inquérito populacional e representativo com 1916 jovens dos 9 aos 17 anos em escolas do norte da Tailândia e entrevistas aprofundadas com partes interessadas especializadas. As conclusões dos dados servirão de base para novos currículos educativos personalizados no último ano do projetco.[110]

Mais de um em cada três jovens (36%) relatou ter recebido ou visto imagens sexuais de alguém que se acreditava ter menos de 18 anos. As motivações para partilhar conteúdo sexual eram variadas. Muitos acreditavam que o conteúdo era partilhado para ganhar likes e seguidores (46%), para ganhar dinheiro, presentes ou crédito (45%), para se sentirem bem consigo mesmos (40%) ou para mostrar confiança numa relação (27%).[110] Um jovem explicou:

> **"Alguns dos meus amigos e conhecidos mais jovens também partilharam imagens de nudez. Quando perguntei sobre as suas motivações, eles disseram que estavam à procura de aceitação. Sentiam-se confiantes com os seus corpos, mas não tinham considerado totalmente as possíveis consequências. Essas pessoas são talentosas, mas não têm espaço e oportunidades suficientes para se expressarem. Como resultado, envolveram-se nesse comportamento como forma de atrair atenção.."**

Informante-chave de 18 anos[110]

Uma proporção significativa dos inquiridos (34%) acreditava que os jovens partilham conteúdo sexual porque são pressionados, enganados ou coagidos. Os jovens também descreveram como a tecnologia torna muito fácil partilhar impulsivamente imagens sexuais explícitas, ao mesmo tempo que oferece pouco apoio quando surgem problemas.[110]

Fundamentalmente, o projecto **Leaked** enfatiza que os danos identificados pelos jovens não decorrem da partilha de conteúdo íntimo em si, mas da perda de controlo sobre ele. A partilha indesejada de imagens sexuais geradas na primeira pessoa surgiu como a principal preocupação relatada pelos jovens (81%), seguida por arrependimento (76%), *bullying* (70%) e sofrimento emocional (68%).[110] Esta evidência desafia as abordagens tradicionais baseadas no medo, que dependem de advertências severas e ameaças legais para desencorajar a partilha de qualquer conteúdo sexual. Tais mensagens não refletem a realidade da vida dos jovens e podem, na verdade, agravar o estigma ou desencorajá-los de procurar ajuda. Em vez disso, os dados do **Leaked a**poiam uma abordagem que apela a:

- Educação sexual abrangente e baseada em direitos, que reconheçam as realidades da tecnologia nas interacções sexuais modernas
- Recursos de segurança mais fortes nas plataformas para proteger as crianças de conteúdos sexualizados, sensacionalistas ou prejudiciais
- Mudanças culturais — da punição ao apoio — na resposta a questões decorrentes de conteúdo sexual gerado na primeira pessoa
- Espaços sem julgamentos para um diálogo aberto com os jovens sobre como lidar com as decisões *online*

> **"Acho que devemos apenas tentar entender a situação deles e não culpar as vítimas. Como isso é comum no meu país...As pessoas simplesmente entram na onda de insultar a pessoa que, na verdade, foi a vítima."**

Rapaz de 17 anos, Paquistão[60]

Apoio a adultos e crianças em risco de causar danos

> "Foi a coisa mais difícil que já fiz ligar para a linha de apoio pela primeira vez, mas estou muito feliz por ter feito isso. [Foi a] primeira vez em anos que reconheci o meu vício em pornografia adulta, que me levou a ver outras imagens [CSAM]. Tive um grande apoio e nunca me senti julgado."

Chamada anónima para a Stop It Now![112]

Os programas de prevenção da perpetração são uma importante estratégia de prevenção apoiada por evidências crescentes.[28] Eles podem fornecer ajuda precoce para pessoas preocupadas com seus próprios pensamentos ou comportamentos sexuais em relação a crianças, interromper os caminhos para a perpetração de crimes e prevenir danos antes que eles ocorram. Pensamentos e comportamentos sexuais prejudiciais geralmente começam na infância, ressaltando a necessidade de intervenções precoces e personalizadas para adultos e crianças em risco de causar danos.[168] As barreiras à procura de ajuda podem ser reduzidas através do fornecimento de várias opções acessíveis que priorizam o anonimato e estabelecem limites claros de confidencialidade.[168] Exemplos de iniciativas de prevenção de perpetração estão listados abaixo:

- O projecto **ReDirection** pesquisa indivíduos anónimos que procuram CSAM na *dark web* e redireciona-os para serviços de apoio, ao mesmo tempo que gera dados para informar estratégias de prevenção eficazes.[169] Com mais de 26.000 respostas recolhidas em vários idiomas, o projecto forneceu informações importantes sobre os caminhos dos infractores e os seus comportamentos de procura de ajuda. O programa **ReDirection Self-Help** foi avaliado quanto à sua redimensionabilidade e está a ser submetido a uma avaliação mais aprofundada.
- **Help Wanted**, um curso *online* que oferece ajuda a adolescentes e jovens adultos atraídos por crianças mais novas, foi desenvolvido nos EUA e agora está a ser adaptado para o México e avaliado.[170]
- A linha de apoio **Stop It Now!** fornece aconselhamento e apoio confidenciais a pessoas preocupadas com os seus próprios pensamentos ou comportamentos sexuais ou com os de outras pessoas em relação a crianças. O apoio está disponível em mais de 200 idiomas. Em 2023-24, quase metade dos 4.000 clientes que ligaram para a linha de apoio eram adultos que procuravam ajuda para os seus próprios pensamentos e comportamentos, incluindo aqueles que já tinham causado danos a crianças.[112] Cerca de 12% das pessoas que procuraram ajuda eram desconhecidas das autoridades no momento do primeiro contacto, o que sugere que as linhas de apoio podem chegar a indivíduos em risco antes que as autoridades policiais se envolvam.[112]
- **Prevention Global** é uma plataforma de conhecimento e uma iniciativa de investigação ambiciosa que avalia sete programas desenvolvidos para prevenir a perpetração de abuso sexual infantil, incluindo terapia individual e em grupo, aconselhamento remoto, materiais autoguiados e currículos escolares. **A Prevention Global** também publica uma série de produtos de conhecimento e a publicação **Scalability** explora as barreiras e oportunidades para ampliar os programas de prevenção, incluindo uma avaliação de programas com foco específico na prestação de serviços de ajuda.[125]

> **“Podemos ver que, para alguns infractores, é possível desviar o seu comportamento infractor. E se nos concentrássemos mais nisso, estaríamos a fazer um trabalho melhor. Mas é realmente difícil para as pessoas entenderem...É uma narrativa muito complicada politicamente, socialmente, de aceitar... o que torna pouco popular falar sobre isso, pouco popular financiar isso. Mas há cada vez mais evidências de que, para algumas [pessoas], é possível intervir e desviá-las do caminho em que estão.”**

Sociedade civil[11]

Dissuadir pesquisas por CSAM: Percepção da Lucy Faithfull Foundation

A Lucy Faithfull Foundation trabalha para prevenir o abuso sexual infantil através de serviços profissionais para indivíduos em risco de causar danos, famílias afectadas pelo abuso e ferramentas e recursos para profissionais criarem ambientes mais seguros para as crianças.

- As tipologias e trajetórias dos agressores variam significativamente, exigindo táticas personalizadas e mensagens diversificadas e multicanais para alcançar diferentes perfis de agressores.
- Os avisos devem ser emitidos em todos os pontos onde alguém possa tentar aceder a conteúdos ilegais.
- As mensagens devem ser imparciais e cuidadosamente elaboradas. As mensagens de dissuasão por si só não podem impedir os crimes, mas combiná-las com apoio acessível e anónimo pode incentivar as pessoas a procurar ajuda para lidar com os seus pensamentos e comportamentos sexuais..

> **“A maioria do público prefere <excluir> os crimes sexuais. É algo que acontece a outras pessoas. Outras pessoas são criminosas. Outras pessoas são vítimas... Isso não ajuda em nada na proteção das crianças. Não ajuda em nada a manter as crianças seguras... você não vai perceber se o seu filho está abusando do seu outro filho... você não vai perceber se estiver apenas à procura de monstros e predadores.”**

Sociedade civil[11]

A Lucy Faithfull Foundation foi pioneira na divulgação de mensagens de dissuasão por meio de campanhas em canais *online* e *offline*, incluindo meios de comunicação social convencionais, redes sociais, publicidade digital paga, curtas-metragens e parcerias com as autoridades policiais e outras organizações estatutárias e voluntárias.[171]

Ao longo de onze anos de mensagens e campanhas de dissuasão, a Lucy Faithfull Foundation identificou quatro mensagens centrais que alertam eficazmente aqueles que procuram CSAM:

- Acessar imagens sexuais de crianças é crime.
- Isso causa danos às crianças.
- Tem consequências para si e para a sua família.
- Ajuda anónima está disponível se você quiser parar.

A Lucy Faithfull Foundation, em parceria com a IWF e a Aylo (uma plataforma de conteúdo adulto), testou se mensagens de dissuasão anónimas baseadas em *chatbots* poderiam interromper e reduzir as pesquisas por CSAM no Pornhub UK. A Aylo mantém uma lista dinâmica de milhares de termos proibidos devido à sua associação com imagens sexuais de crianças. Quando um utilizador pesquisa um desses termos no Pornhub UK, uma mensagem de aviso estática é exibida. Além disso, um chatbot aparece, semelhante a uma caixa de atendimento ao cliente padrão comumente vista em outros sites. Com base nas respostas do utilizador, o chatbot pode direccionar os indivíduos para serviços de apoio anónimos, incluindo a linha de apoio **Stop It Now!**, apoio por e-mail ou chat ao vivo, recursos de autoajuda *online*, a National Suicide Prevention Lifeline ou os serviços urgentes de saúde mental do National Health Service.

Uma avaliação da intervenção constatou que:[171]

- 82% das sessões que procuravam conteúdo ilegal foram interrompidas. Alguns utilizadores encerraram completamente a sessão, enquanto outros mudaram para conteúdo legal ou saíram do site.
- A combinação da mensagem de aviso e do chatbot incentivou efectivamente as pessoas a procurarem apoio nos serviços da **Stop It Now!**
- Quando o chatbot foi desativado por um mês, as pesquisas por CSAM aumentaram.

Impacto do projecto em números

- Houve uma redução estatisticamente significativa nas pesquisas por imagens sexuais de menores de 18 anos ao longo dos 18 meses do projecto.
- O chatbot e a mensagem de aviso foram exibidos 2,8 milhões de vezes.
- 99,8% das pesquisas durante os 18 meses do projecto não acionaram o chatbot ou a mensagem de aviso.
- 1656 pessoas solicitaram informações sobre serviços de apoio após verem o chatbot ou a mensagem de aviso.
- 490 pessoas visitaram o site **Stop It Now!** após verem uma mensagem de aviso ou o chatbot.
- 68 pessoas que ligaram para a linha de apoio **Stop It Now!** foram identificadas como tendo interagido com o chatbot.

Opções de denúncia acessíveis e confiáveis e apoio centrado nas vítimas

> Os governos, as empresas de tecnologia e as instituições educacionais devem...garantir que as crianças possam denunciar em qualquer lugar e a qualquer momento... E então as medidas necessárias podem ser tomadas para ajudar a reduzir isso

Mulher de 24 anos, Uganda[38]

É necessária uma variedade de mecanismos de denúncia acessíveis e confiáveis para conectar as crianças que sofreram danos a serviços de apoio abrangentes, adequados às crianças e centrados nos sobreviventes. As evidências mostram consistentemente que as crianças raramente usam canais formais de denúncia. Por exemplo, o **Disrupting Harm** descobriu que apenas cerca de 3% das crianças vítimas de exploração ou abuso sexual *online* denunciaram o caso a uma linha de apoio ou à polícia, em comparação com 40% que contaram a amigos e 24% que contaram a irmãos.[60]

> Prefiro falar com adultos porque sinto que eles têm mais ideias...os adultos com quem falo me ouvem bem, especialmente a minha irmã.

Mulher de 17 anos, Nigéria[60]

> Normalmente não falo com adultos. Costumo falar com pessoas da minha idade, porque elas passam por coisas semelhantes e podem se identificar mais facilmente, e sei que os adultos têm boas intenções, mas às vezes sinto que eles podem não entender completamente ou podem ver as coisas de maneira diferente, e...é melhor falar com pessoas da minha idade.

Mulher de 15 anos, Etiópia[60]

> Acho que muitas pessoas podem não [falar com os pais] porque sentem que terão restrições ao uso do telemóvel se contarem... talvez muitas crianças possam sentir-se culpadas, especialmente no caso de abuso sexual. Elas podem sentir-se culpadas e achar que também é culpa delas.

Mulher de 15 anos, Reino Unido[60]

Os defensores dos jovens enfatizam que a denúncia deve ser fácil de acessar e usar, livre de estigma e confiável.[60] Alguns jovens sugerem modelos liderados por pares, como adolescentes treinados que podem responder de forma eficaz e encaminhar seus pares para os serviços de apoio adequados.[60] Outros exemplos na prática incluem:

- **Meri Trustline**, uma linha de apoio na Índia que apoia crianças, mulheres e pessoas de identidades marginalizadas que estão em risco de danos *online*.[172] As denúncias enviadas por WhatsApp, e-mail ou telefone são recebidas por conselheiros treinados. A plataforma também integra a ferramenta **Report Remove** da IWF, que permite às crianças denunciar conteúdos *online* e solicitar a sua remoção.[173]
- Modelos de serviços multidisciplinares centrados na criança para crianças vítimas de abuso e exploração sexual, como o **Barnahus** (Casa das Crianças), que oferece serviços co-localizados, adaptados às crianças e informados sobre traumas, incluindo entrevistas forenses, exames médicos, serviços terapêuticos e apoio às vítimas/famílias. Os **One Stop Centers** são outro exemplo: eles oferecem resposta imediata a crises e serviços de apoio a mulheres e crianças vítimas de violência de género, particularmente em países de baixa e média renda. Os seus serviços abrangentes e localizados incluem serviços jurídicos, serviços sociais e aconselhamento.[174] A UNICEF está a analisar como estes modelos de cuidados podem apoiar crianças vítimas de CSEA facilitados pela tecnologia.[174] Experiências documentadas das Filipinas, África do Sul, Nigéria e Bulgária serão divulgadas em breve.[174]
- Os produtos de conhecimento **Serving Youth** (servindo os jovens) da Prevention Global incluem um **guia prático para líderes** de organizações juvenis que destaca oito práticas sistemáticas para prevenir e lidar com o abuso sexual infantil.[175,176] Pesquisas mostram uma redução de mais de 20% na prevalência de vitimização em organizações que atendem jovens e implementaram estratégias de prevenção do abuso sexual infantil.[180]

> **“Na minha opinião, a melhor maneira seria ouvi-los sem julgá-los, acreditar no que dizem, dar acesso a aconselhamento ou ajuda e garantir que eles saibam que não estão sozinhos, porque isso significaria muito... sentir-se seguro, ser ouvido, ter apoio para se recuperar e também garantir que as pessoas que fizeram isso sejam responsabilizadas.”**
>
> *Mulher de 15 anos, Etiópia*[38]

Segurança digital

> À medida que continuamos a construir esses mundos digitais, temos que garantir que estamos a fazê-lo com a segurança em mente. Não se trata apenas de dar aos jovens acesso a novas tecnologias interessantes, mas sim de nos dar as ferramentas para nos protegermos, ensinando-nos a reconhecer quando algo parece errado e criando espaços onde possamos desfrutar de todos os benefícios dessas inovações sem os perigos ocultos.

Defensora dos jovens[1]

A segurança, os direitos e o bem-estar das crianças devem ser priorizados em todos os níveis da cultura da empresa, da governança e da formação da mão-de-obra.

As empresas devem integrar avaliações de impacto sobre os direitos da criança, diligência necessária em matéria de segurança infantil e características de *design* centradas na criança em todos os processos de desenvolvimento.

As empresas devem detectar e interromper proactivamente conteúdos e comportamentos prejudiciais, além da moderação reactiva.

A transparência, a responsabilização e a colaboração intersectorial são essenciais para reforçar as defesas mundiais contra o CSEA facilitado pela tecnologia.

Promover uma cultura industrial de segurança infantil

A criação de um ecossistema digital mais seguro para as crianças requer uma cultura industrial que priorize os direitos, a segurança e o bem-estar das crianças em todos os níveis da cultura empresarial, governança, tomada de decisões e formação da força de trabalho. A segurança infantil deve ser enfatizada como uma responsabilidade profissional desde a fase inicial, incluindo currículos de ciência da computação e vias de contratação na indústria.[32] Os funcionários envolvidos na concepção, desenvolvimento e entrega de produtos e serviços digitais devem receber formação contínua para reconhecer e mitigar os riscos para as crianças. A segurança infantil também deve ser integrada às políticas de proteção e códigos de conduta da empresa. Em 2024, o governo do Camboja treinou 48 empresas de tecnologia digital sobre as diretrizes da indústria para a proteção infantil *online* – quatro dessas empresas treinadas posteriormente integraram a proteção infantil às suas políticas internas e desenvolveram um código de conduta de proteção infantil para seus funcionários.[159]

Os moderadores de conteúdo da linha de frente e os trabalhadores de segurança digital, descritos como os «trabalhadores essenciais de segurança da Internet», realizam um trabalho vital e difícil, mas muitas vezes enfrentam condições precárias e riscos para a sua própria saúde e bem-estar. Devem ser apoiados com condições de emprego justas, desenvolvimento profissional, acesso a serviços de saúde mental e apoio psicossocial e apoio pós-emprego.[181] Tais medidas podem melhorar a retenção da mão-de-obra, aumentar a especialização e melhorar a qualidade e a eficácia das respostas de segurança digital na linha da frente.

Tornar a segurança por *design* o padrão

Uma abordagem de segurança desde a concepção exige que todas as partes interessadas envolvidas na concepção e desenvolvimento de produtos e serviços digitais se perguntem: «o que faríamos de diferente se soubéssemos que o utilizador final é uma criança?»[182] Isso transfere a responsabilidade para as empresas garantirem que os seus produtos não causem danos às crianças. É importante ressaltar que essas medidas de segurança devem ser aplicadas a todas as tecnologias digitais, uma vez que as crianças frequentemente acessam produtos e serviços que não foram criados especificamente para elas.[183] Vários especialistas da sociedade civil observaram uma percepção de que os interesses comerciais têm precedência sobre os direitos das crianças e as considerações de segurança.[184] Representantes da indústria afirmam que uma abordagem de segurança desde a concepção não precisa entrar em conflito com os interesses comerciais.

As principais características da segurança desde a concepção incluem:[31]

- Integrar avaliações de impacto sobre os direitos da criança e diligência necessária nos processos de *design* e desenvolvimento. As avaliações de impacto sobre os direitos da criança são processos que permitem às empresas avaliar como as suas operações, produtos e serviços afectam os direitos da criança, conforme definido na Convenção das Nações Unidas sobre os Direitos da Criança e outros instrumentos de direitos humanos.[185]
- Privacidade e proteção de dados, incluindo padrões rígidos de privacidade, experiências de usuário adequadas à idade e salvaguardas contra o uso indevido de dados pessoais de crianças.
- *Design* e educação centrados na criança, como envolver crianças e jovens na conceção e teste de produtos, fornecer informações claras e acessíveis e incorporar recursos educacionais que aumentem a autonomia e a consciência das crianças.
- Proteções integradas, tais como controlos parentais, limites de contacto, salvaguardas financeiras para impedir que as crianças transfiram dinheiro *online* e modos ou dispositivos com funcionalidades limitadas.
- Responsabilidade por meio de obrigações claras de relatórios de transparência, moderação robusta e mecanismos acessíveis de denúncia e reparação.

Os recursos de segurança infantil devem ser funcionais, acessíveis e disponíveis de forma equitativa em todas as regiões geográficas e idiomas em que um produto ou serviço é oferecido.

> **“Se você abrir uma conta [nas redes sociais] aqui na América Latina e no Sul Global, a questão era se elas teriam o mesmo tipo de proteções e salvaguardas que as pessoas que têm uma conta nos EUA e no Reino Unido [têm], e a resposta foi: absolutamente não!...As pessoas aqui na América Latina estão menos seguras do que as crianças em outros países. E por que isso deve ser assim?”**
>
> *Sociedade civil*[11]

Uma estrutura complementar, os direitos da criança por design, reconhece que as tecnologias digitais devem apoiar o cumprimento dos direitos das crianças, incluindo o seu direito à segurança.[186] A aplicação destas abordagens requer compromisso da liderança, recursos dedicados e pessoal treinado. As empresas mais pequenas e as start-ups muitas vezes não têm essa capacidade, embora existam orientações disponíveis para ajudar as empresas a avaliar os impactos das tecnologias digitais, incluindo a IA generativa, nos direitos da criança.[36,184,187–189] A implementação eficaz dos princípios de segurança desde a concepção deve ser orientada por evidências e requer transparência da indústria e mecanismos independentes de responsabilização.

Tabela 1. Exemplos de segurança e direitos da criança por *design* na prática

Elemento de design	Acção	Exemplos na prática
Proteções do produto	Integrar avaliações de risco de segurança no desenvolvimento de produtos.	A **D-CRIA ToolBox** da UNICEF orienta as empresas na realização de avaliações robustas do impacto sobre os direitos da criança e na diligência necessária relacionada ao ambiente digital. Ela inclui um modelo D-CRIA, um guia de início rápido e orientações destacadas para a participação e o envolvimento das crianças.[185] **A Estrutura de IA Responsável e a Lista de Verificação de Segurança por Design** da Thorn para plataformas tecnológicas visam diminuir os riscos associados à IA generativa.[188]
Proteções do produto	Conceber dispositivos ou modos seguros para crianças com funcionalidades ou acesso limitados. As funcionalidades avançadas podem ser desbloqueadas por um pai ou responsável.	O **HMD Fuse** é um smartphone seguro para crianças com um filtro de conteúdo de IA integrado que bloqueia a visualização, gravação ou armazenamento de conteúdo com nudez. Ele inicia em um modo restrito, sem acesso a aplicativos ou redes sociais, a menos que os responsáveis habilitem recursos adicionais.[190] A Apple **Communication Safety** está activada por predefinição para contas infantis. Ela analisa imagens e vídeos no dispositivo para detectar e desfocar automaticamente a nudez, avisa a criança e fornece orientações e recursos de segurança adequados à idade, além de permitir o controlo parental através das definições do Screen Time.[191]
Privacidade e proteção de dados	Aplicar padrões e salvaguardas de privacidade rigorosos e recolher o mínimo de dados das contas infantis ou quando a idade do utilizador for incerta.	As contas de adolescentes nas redes sociais, como **o modo Snapchat Teen**, podem tornar as contas privadas, restringir mensagens directas, filtrar conteúdo prejudicial e desactivar o compartilhamento de localização por padrão.[192] **O YouTube Kids**, para crianças menores de 13 anos, filtra conteúdo, desactiva comentários, compartilhamento de localização e anúncios personalizados por padrão.

Elemento de design	Acção	Exemplos na prática
Comunicação, educação e mecanismos de denúncia adequados às crianças	Fornecer informações, educação e mecanismos de denúncia/reclamação adequados à idade e adequados às crianças.	O currículo de segurança digital **Be Internet Awesome** do Google inclui jogos interactivos sobre segurança *online*, privacidade e partilha respeitosa.[193] A LEGO desenvolveu um código de conduta adequado para crianças. A ferramenta **Captain Safety** do aplicativo LEGO Life, agora extinto, incorporava um compromisso de segurança, lembretes de segurança no aplicativo e explicações adequadas para crianças sobre as políticas de privacidade e moderação da LEGO.[194] O programa **School Partnership** do Instagram oferece recursos de segurança digital e prioriza denúncias de conteúdos e contas prejudiciais enviadas por estudantes e educadores, garantindo a análise em até 48 horas[195]

> **"Quando era adolescente, ela procurava uma razão para dizer não. E ele continuava a pressioná-la [para enviar mais imagens sexuais], e ela não conseguia lutar... Ela não conseguia dizer não... Mas 'o meu telemóvel não me deixa tirar nudes' parece ser uma forma muito poderosa de devolver esse poder às vítimas para que possam dizer que não podem. 'Sim. Eu não – o dispositivo não me deixa.'"**
>
> *Sociedade civil*[11]

Detectar e interromper proactivamente os danos

As empresas de tecnologia devem detectar e bloquear proactivamente conteúdos, contas e comportamentos prejudiciais em tempo real, utilizando ferramentas como sistemas de correspondência de hash e filtros de monitoria de conteúdos, respeitando os direitos dos utilizadores[73] Estão a surgir esforços para aproveitar a IA e a aprendizagem automática para a detecção proactiva de conteúdos, incluindo um serviço de detecção de aliciamento que utiliza aprendizagem automática e um sistema de inteligência de detecção de CSAM proposto que demonstrou distinguir com precisão entre publicações CSAM e não CSAM na *dark web*, ao mesmo tempo que gera percepções acionáveis sobre criadores e vítimas.[196,197]distributing or discussing child sexual abuse materials (CSAM O produto **Safer** da Thorn é um conjunto de ferramentas alimentadas por IA que as empresas podem utilizar para detectar, identificar e denunciar CSAM. O **Safer** foi integrado ao aplicativo web de IA generativa DALL-E2 da OpenAI.[198]

A Tech Coalition está a testar uma prova de conceito para detectar e responder o CSEA facilitado pela tecnologia em ambientes de transmissão ao vivo.[199] Este piloto utilizará sinais de metadados, tais como características da sessão e a utilização de serviços de anonimização, para gerar uma pontuação de risco que indica a probabilidade de ocorrência de CSEA *online* numa determinada sessão de transmissão ao vivo para investigação adicional por equipas de segurança infantil. Os testes e a avaliação serão realizados nesta primavera para avaliar a viabilidade de uma adopção mais ampla pela indústria.

As crianças devem poder denunciar imediatamente as suas preocupações e conteúdos e comportamentos prejudiciais que encontram *online* — incluindo CSAM, extorsão sexual, aliciamento ou distribuição não consensual de imagens — através de canais simples e fiáveis dentro da plataforma[60] As denúncias devem desencadear respostas atempadas para remover conteúdos e bloquear contas prejudiciais, bem como conectar os utilizadores a serviços de apoio e acompanhamento.

Muitos produtos digitais não oferecem mecanismos de denúncia acessíveis e, mesmo quando estão disponíveis, as crianças muitas vezes não os utilizam. Um estudo mundial sobre extorsão sexual descobriu que **apenas 4% das crianças denunciaram incidentes à plataforma onde ocorreram.**[52] Os defensores dos jovens enfatizaram que a experiência de denunciar e solicitar a remoção de imagens sexuais é tão importante quanto a função em si: deve ser fácil, segura e livre de estigma. Como exemplo positivo, o serviço **Take It Down** do NCMEC tranquiliza as crianças com mensagens não estigmatizantes («ter nudes *online* é assustador, mas há esperança de removê-los»), suporte multilíngue, vídeos explicativos e perguntas frequentes.[200] As orientações da OCDE (Organização para a Cooperação e Desenvolvimento Económico) enfatizam que os sistemas de reparação devem ser concebidos com a participação das crianças e adaptados aos riscos específicos da plataforma.[182]

> **“Penso que [algumas plataformas digitais]...estão mais focadas nos seus lucros do que na segurança [das crianças]. Algo que poderia definitivamente ajudar é melhorar os mecanismos de denúncia na plataforma, porque acho que muitas vezes é muito complicado descobrir onde denunciar e não há muitas informações sobre como isso realmente funciona. E, na maioria das vezes, você não recebe resposta. Então, você meio que sente que é inútil e que não adianta fazer a denúncia.”**
>
> *Mulher de 15 anos, Reino Unido*[60]

Transparência e responsabilidade

É essencial um compromisso mais forte com a transparência e a responsabilidade. As empresas devem realizar avaliações obrigatórias do impacto sobre os direitos da criança e publicar relatórios de transparência oportunos que capturem os riscos, os danos e os comportamentos dos utilizadores que possam informar as estratégias de prevenção. Estes podem incluir, por exemplo, dados demográficos das vítimas e dos agressores, taxas de abandono de sessões ou cliques em serviços de apoio acionados por pop-ups de aviso. A padronização das métricas de segurança infantil e dos processos de denúncia em toda a indústria pode resolver os desafios actuais com a comparabilidade dos dados. O programa **Lantern** da Tech Coalition destaca a necessidade de um ecossistema onde dados, percepções e responsabilidades sejam partilhados entre sectores para fortalecer a proteção infantil *online*.

Lantern – acção coordenada da indústria contra o CSEA *online*: Visão da Tech Coalition

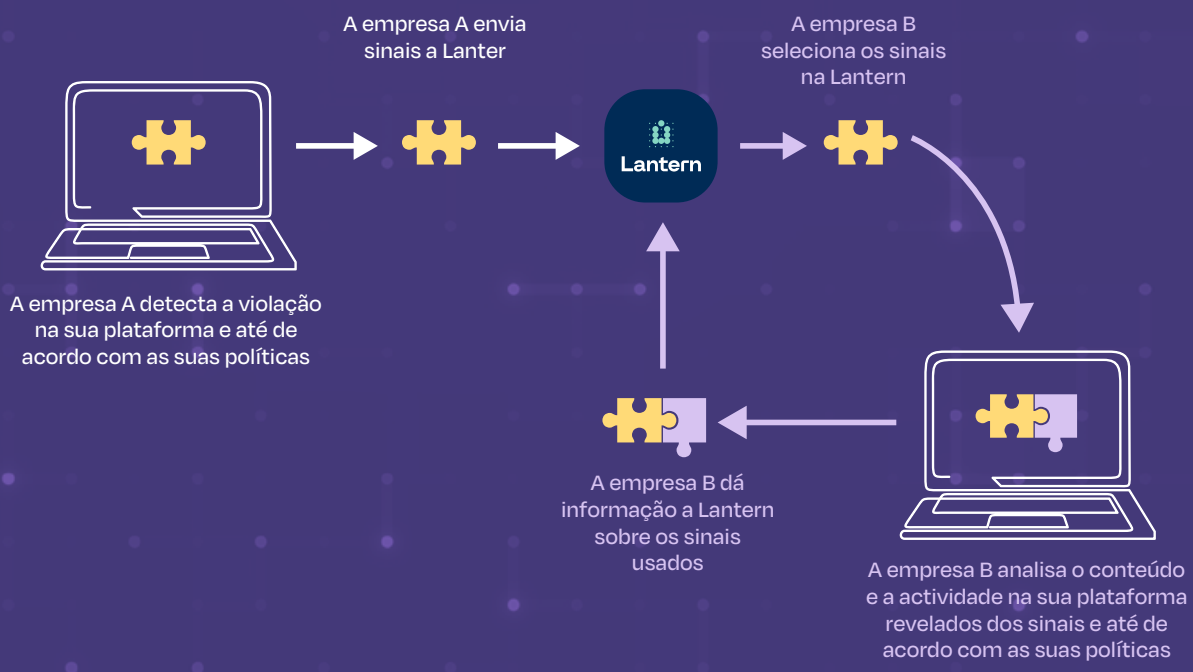
A Tech Coalition é uma aliança mundial de mais de 55 empresas de tecnologia comprometidas em proteger as crianças da exploração e abuso sexual online, compartilhando conhecimento, identificando ameaças e desenvolvendo soluções colaborativas.

Os perpetradores costumam usar várias plataformas para partilhar conteúdo abusivo e explorar crianças *online*. Historicamente, não havia uma estrutura universal para coordenar os esforços da indústria para detectar exploração e abuso, deixando lacunas na detecção e resposta. A **Lantern** foi criado para preencher essa lacuna, permitindo que as empresas participantes partilhem sinais accionáveis de abuso, possibilitando a detecção e resposta a danos que, de outra forma, poderiam passar despercebidos.[201]

Operando com base no princípio de que a partilha de informações sobre ameaças melhora a resposta da indústria ao CSEA *online*, a Lantern facilita a colaboração para fortalecer as defesas coletivas contra ameaças emergentes. Sinais – como hashes, URL ou nomes de utilizador – representam conteúdo ou comportamento potencialmente prejudicial relevante para o CSEA *online*. Quando uma plataforma sinaliza um sinal, outras podem analisar independentemente as actividades relacionadas nos seus próprios serviços.[25]

Quando uma empresa identifica CSEA na sua plataforma, toma as medidas adequadas para fazer cumprir as suas políticas de segurança infantil e partilha os sinais associados através da **Lantern**. Isto permite que outras plataformas detectem e removam proactivamente conteúdos ou contas relacionados, reforçando o ecossistema geral de segurança *online*.

Figura 6. Estrutura e processo de partilha de sinais da **Lantern**[25]



A colaboração através da **Lantern** já está a demonstrar impacto, com as empresas participantes a notarem melhorias constantes na sua capacidade de mitigar os riscos à segurança infantil.[201] Em 2024:

- Quase 300.000 novos sinais relacionados com o CSEA *online* foram partilhados — elevando o total para mais de 1 milhão de sinais **Lantern** até à data.
- Mais de 100.000 contas foram penalizadas por violações relacionadas com a exploração e abuso sexual infantil.
- Mais de 135.000 URL que hospedavam ou transmitiam CSEA foram bloqueados ou removidos.
- Mais de 7.000 itens de CSAM foram removidos.
- Casos de alto risco, incluindo 81 incidentes de crimes sexuais com contacto e 45 casos relacionados com tráfico, foram sinalizados.

A maioria dos sinais baseados em incidentes envolveu perpetradores que procuravam distribuir ou obter CSAM, por vezes como precursores de aliciamento ou abuso com contacto.[201] A taxonomia de sinais da **Lantern** permite uma categorização mais precisa das ameaças, apoiando múltiplas abordagens de detecção e resposta.[201]

Figura 7. Sinais carregados por tipo em 2024

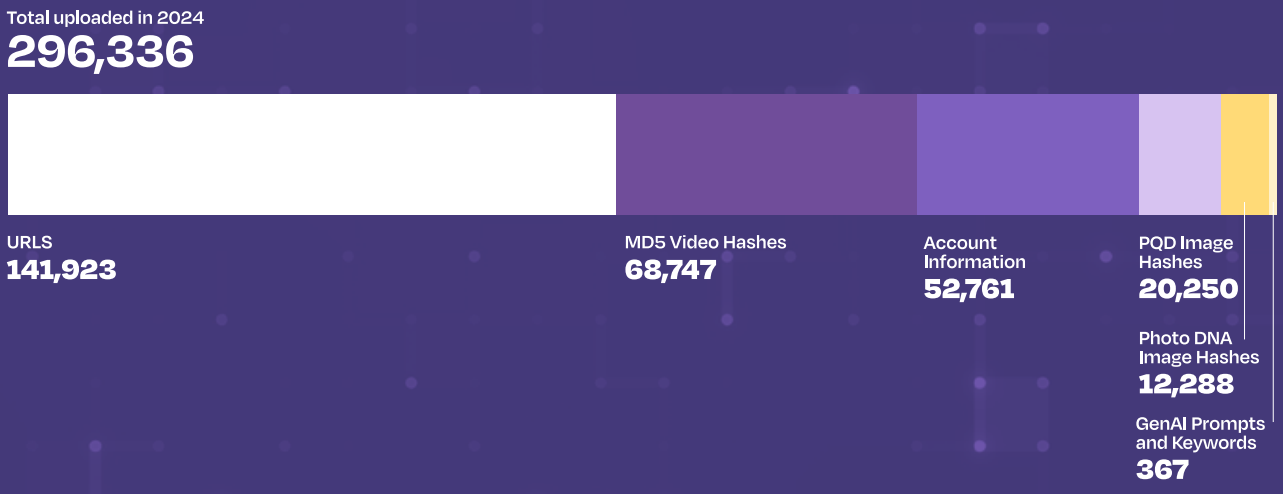
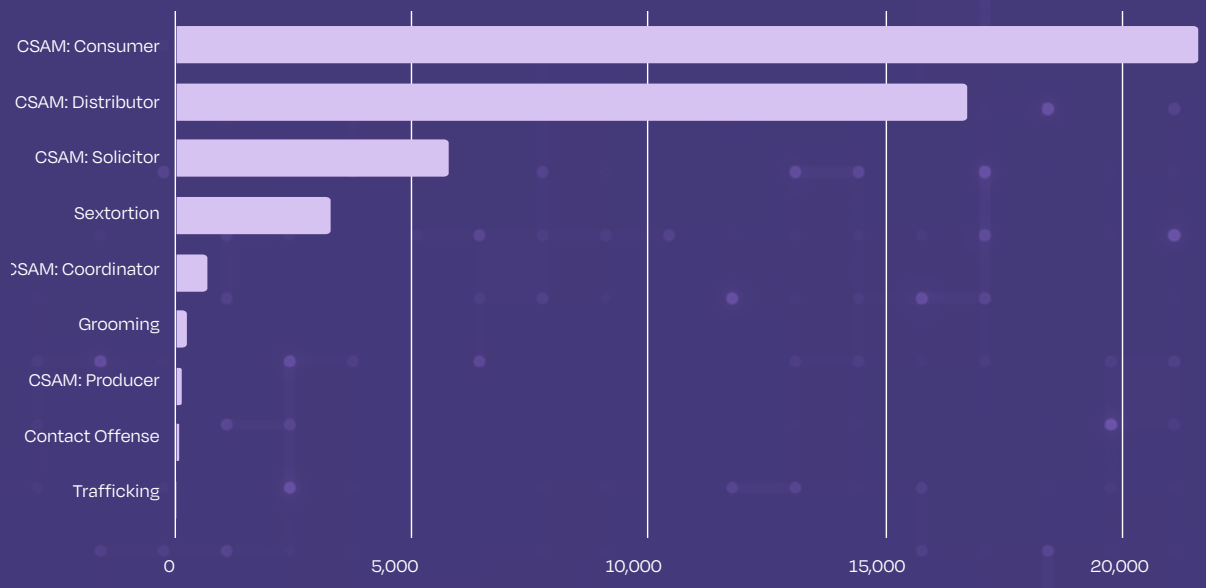


Figura 8. Categorias de sinais baseados em incidentes relatados em 2024



A **Lantern** demonstra o poder da colaboração entre sectores na luta contra a exploração e o abuso infantil *online*. Ao quebrar as barreiras entre plataformas, o programa melhorou a detecção, a responsabilização dos perpetradores e a velocidade de resposta. É importante ressaltar que ela também demonstra como o compartilhamento de sinais relacionados a conteúdo e comportamento pode fortalecer as defesas contra ameaças mais amplas, como aliciamento, extorsão e tráfico, além da distribuição de CSAM.

> **"O que realmente me tocou foi a importância de é preciso uma aldeia...todos precisam de se envolver na prevenção."**
>
> *Indústria*[7]

Lei, política e justiça

> “Acho que precisamos de mais regulamentação, legislação. E acho que é o mesmo com o tabagismo, com o abuso de substâncias. Não deixamos as crianças fumarem. Não deixamos as crianças beberem. Temos legislação. Portanto, demoramos muito para regulamentar a internet.”

Sociedade civil[11]

A harmonização da legislação é essencial para colmatar lacunas jurídicas, garantir a cooperação transfronteiriça e acompanhar as ameaças digitais emergentes.

A aplicação eficaz das leis depende de sistemas judiciais com recursos adequados, informados sobre traumas e centrados nos sobreviventes, que protejam as crianças e não as traumatizem novamente.

Combater o CSEA facilitado pela tecnologia requer uma acção colaborativa entre o governo, os reguladores, a indústria e a sociedade civil para responsabilizar os detentores de obrigação.

Harmonizar a legislação mundialmente, em conformidade com as normas dos direitos da criança

Os esforços para harmonizar a legislação nacional que aborda o CSEA facilitado pela tecnologia estão a ganhar impulso a nível mundial. A **Convenção das Nações Unidas contra Crimes Cibernéticos** é um tratado multilateral histórico contra o crime que promove esforços para padronizar as leis mundiais de proteção infantil, incluindo a criminalização do CSAM e do aliciamento pela primeira vez a nível munidial.[23] Leis abrangentes, como a **Lei de Segurança Online do Reino Unido**, ajudam a minimizar as inconsistências que existem naturalmente quando se legisla entre ministérios governamentais e áreas temáticas.[8,202] A recente Política Abrangente de Proteção à Criança de Fiji, promulgada em 2025, alinhou a anterior **Lei de Cuidados e Proteção de 2024 e a Lei de Justiça Infantil de 2024**. Ela também buscou minimizar lacunas e melhorar a coordenação entre os setores.[203] No entanto, globalmente, permanecem inconsistências nos esforços legislativos, tanto dentro dos governos quanto entre eles. A falta de um sistema centralizado para monitorar os desenvolvimentos legislativos e partilhar os avanços agrava ainda mais o desafio global da inconsistência legislativa. Ferramentas comparativas como o **#BeBrave G7 Country Scorecard** do Brave Movement e o **Online Safety Regulatory Index** destacam os progressos e as lacunas.[204,205]

> “Grande parte [da extorsão sexual] vem de países estrangeiros... mas cada um tem as suas próprias jurisdições e leis, e ninguém quer trabalhar em conjunto [por isso] torna-se muito difícil para nós dizer: ‘não façam isso às crianças’.”

Sobrevivente[77]

Os avanços do Brasil em 2025 na proteção infantil *online*

Em 2025, o Brasil teve um marco na proteção digital infantil por meio de acções políticas que refletem a crescente liderança dos países da Maioria Global na criação de ambientes *online* mais seguros. Em setembro, o Brasil promulgou uma lei abrangente que estabelece obrigações claras para empresas e plataformas prevenirem, detectarem e responderem ao CSEA *online*.[19] A lei introduz um dever de prevenção, exige a remoção imediata de conteúdo ilegal sem ordens judiciais e obriga a denúncia às autoridades nacionais. A lei também incorpora princípios de segurança e privacidade desde a concepção, proíbe publicidade direcionada a crianças e estabelece regras rígidas de verificação de idade, incluindo a vinculação de contas dos pais para usuários menores de 16 anos. As plataformas devem fornecer ferramentas de controlo parental em português, publicar relatórios de transparência e permitir o acesso de pesquisadores a dados sobre o bem-estar digital das crianças. A fiscalização será liderada pela Agência Nacional de Proteção de Dados do Brasil.[19]

Consultas multissectoriais, incluindo com a indústria e organizações de direitos da criança, são essenciais para garantir que as leis acompanhem as ameaças tecnológicas emergentes e se alinhem com os padrões de direitos da criança, ao mesmo tempo que permitem inovações que aumentam a segurança infantil. As opiniões sobre a melhor forma de proteger as crianças por meio da legislação continuam divergentes: um especialista do sector defendeu a criação de portos seguros legislativos (com salvaguardas rigorosas) para testar e pressionar ferramentas de detecção, enquanto um representante da sociedade civil alertou que algumas leis de denúncia obrigatória podem inadvertidamente restringir denúncias voluntárias e oportunas.

Garantia de idade na era digital: equilibrando proteção e participação

- A garantia de idade descreve os métodos utilizados para verificar ou estimar a idade de um utilizador *online*, a fim de garantir o acesso a conteúdos adequados à sua idade. Os métodos envolvem compromissos entre precisão, privacidade e equidade.
- Leis recentes que exigem a verificação da idade chamaram a atenção do público para os riscos à segurança infantil *online* e trouxeram à tona uma série de desafios éticos, práticos e políticos. Elas podem levar a consequências indesejadas, como usuários contornando restrições ou exclusão de grupos marginalizados.
- A garantia de idade pode aumentar a segurança das crianças *online*, mas sem uma consulta significativa com crianças e jovens, a implementação corre o risco de prejudicar os seus direitos.
- As restrições de idade não devem reduzir a importância das intervenções familiares, escolares e comunitárias, nem minimizar a importância da responsabilidade das empresas e das avaliações de impacto sobre os direitos das crianças em relação aos ambientes digitais.

Tendências legislativas mundiais

Desde a última Avaliação da Ameaça Global, muitos países introduziram leis de garantia de idade e segurança *online*:206

- Brasil: aprovou legislação que inclui obrigações abrangentes de verificação de idade em Setembro de 2025.[19]
- Reino Unido: exigiu que as plataformas impedissem os jovens de encontrar conteúdos prejudiciais, incluindo o uso de verificação de idade «altamente eficaz» (por exemplo, identificação ou estimativa facial) em sites pornográficos e grandes plataformas de redes sociais, a partir de Julho de 2025.[202]
- Austrália: restringirá o acesso de crianças menores de 16 anos às redes sociais a partir de Dezembro de 2025.[207]
- Cingapura: exigirá verificação de idade nas lojas de aplicativos para downloads do Google Play, Apple e Huawei.[21]

Outras localidades que consideraram ou adoptaram recentemente legislação semelhante incluem Dinamarca, Malásia, Mongólia, Nova Zelândia, Coreia do Sul, Turquia, União Europeia e Uzbequistão.[50,51]

> **“Muitas leis desenvolvidas para os jovens não são [realmente] desenvolvidas para os jovens. Por exemplo, as actuais proibições nas redes sociais para menores de 16 anos – os jovens não foram suficientemente consultados. Os jovens devem estar presentes enquanto as leis estão a ser elaboradas e desenvolvidas, e não apenas na fase de consulta.”**

Mulher de 22 anos, Austrália[38]

Perspectivas das crianças

- As crianças e os jovens reconhecem o valor das leis de segurança *online*, ao mesmo tempo que enfatizam a necessidade de nuances na sua concepção e implementação. Um inquérito nacional representativo a crianças dos 8 aos 17 anos na Austrália revelou que quase 90% apoiavam a verificação da idade para aceder a sites, enquanto 56% dos adolescentes norte-americanos inquiridos apoiavam os requisitos de verificação da idade nas redes sociais.[208,209] No entanto, os jovens também destacam preocupações com a privacidade, a segurança e a inclusão digital.

> **“Se se quer proteção, é necessário sacrificar um pouco da liberdade. Mas, como jovem, também tenho o direito de explorar e descobrir coisas [no mundo digital].”**

Jovem[38]

Os críticos das proibições generalizadas alertam que restringir o acesso pode excluir ou isolar jovens marginalizados, como populações de minorias sexuais e de género, ou crianças sem documentos, e empurrá-los para espaços digitais não regulamentados.[210] Evidências do Reino Unido mostram que o uso de VPN disparou após as restrições, destacando os desafios da aplicação da lei em um mundo conectado digitalmente.[211]

> **“uando uma criança precisa de aceder a plataformas de transmissão, mas não tem uma conta, recorre a sites ilegais que exibem anúncios pop-up inadequados com conteúdo explícito”**

Defensor das crianças, Quénia[38]

> **“As contas alternativas são um grande problema. Se alguém é banido, pode criar uma nova conta. [Existem] muitas maneiras diferentes de contornar os banimentos ou moderações.”**

Menina de 13 anos, Austrália[38]

Equilibrando segurança, privacidade e direitos

Os defensores argumentam que “a verificação da idade não deve servir para impedir o acesso das crianças, mas sim para permitir o seu acesso com segurança”.[186] A **Política de Segurança e Empoderamento Infantil Online** da União Africana (2024) adopta esta abordagem baseada nos direitos, promovendo o acesso juntamente com a prevenção.[212]

> **“A verificação da idade é uma ferramenta, não um fim em si mesma, para experiências *online* positivas dos jovens. Na melhor das hipóteses, protege; na pior, impede os jovens de aceder a informações, expressões e conexões essenciais.”**

Regulador[206]

Tabela 2. Métodos de verificação da idade[213]

Método	Descrição	Principais preocupações
Autodeclaração	O utilizador insere a data de nascimento ou assinala uma caixa.	Fácil de implementar, mas pouco fiável.[214]
Estimativa da idade	Prevê a idade por meio de algoritmos ou biometria.	Conveniente, mas propenso a preconceitos e erros — estudos mostram taxas de erro de 34 a 73% entre adolescentes e preconceitos raciais.[207,215]
Verificação da idade	Requer identificação oficial ou sinal verificado.	Mais preciso, mas levanta questões de privacidade, segurança e exclusão, especialmente para aqueles sem identificação formal.[216]

Ainda não existe um padrão global para a garantia da idade. A Meta propôs verificações no dispositivo ou na loja de aplicativos, enquanto o Google explora provas de conhecimento zero que confirmam a elegibilidade sem revelar a identidade. Os formuladores de políticas e as empresas devem garantir que os sistemas sejam transparentes, respeitem os direitos, preservem a privacidade, sejam equitativos e sejam projectados em conjunto com as crianças.

Capacitação, resposta adequada às crianças e justiça centrada nos sobreviventes

As leis para proteger as crianças devem ser apoiadas por investimentos em formação, capacitação e reguladores dedicados. Os governos devem garantir que as autoridades policiais, os promotores e o poder judiciário recebam formação contínua em abordagens adequadas às crianças e informadas sobre traumas, e tenham os recursos para aplicá-las de forma eficaz. Sobreviventes de todas as regiões relatam que as proteções legislativas existentes são insuficientes ou mal aplicadas e pedem justiça centrada nos sobreviventes.[60]

> **"Se denunciar à polícia...eles vão rir de si. É por isso que precisamos de unidades de combate ao crime cibernético."**
>
> *Defensor dos sobreviventes*[60]

No Quénia, o Conselho Nacional de Administração da Justiça lançou um manual de formação especializado para os intervenientes do sector da justiça sobre a investigação e o julgamento de CSEA facilitados pela tecnologia.[217] Esta iniciativa reflete o reconhecimento da necessidade de práticas adaptadas às crianças e informadas sobre traumas no sistema judicial, indo além da legislação para apoiar respostas eficazes centradas nas vítimas.

> **"Os sistemas jurídicos devem facilitar a denúncia de abusos sem medo, e as plataformas *online* devem agir rapidamente para remover qualquer conteúdo prejudicial."**
>
> *Rapaz de 15 anos, Etiópia*[60]

A detecção proactiva, independente das queixas das vítimas, é crucial. Ferramentas como o classificador CSAM da Thorn (via INTERPOL) e o resumidor de vídeo alimentado por IA da Rigr AI melhoram a resposta oportuna ao CSEA transmitido ao vivo.[218,219]

As autoridades policiais observam consistentemente que são necessários mais recursos para lidar com o número crescente de denúncias recebidas pelas linhas diretas, uma vez que as denúncias aumentam exponencialmente, em parte devido à IA generativa. Também é necessária capacidade adicional para apoiar o bem-estar dos funcionários das linhas diretas e dos socorristas, bem como para financiar investigações proactivas que possam interromper a produção e o consumo de CSAM.[79] A formação da polícia do Camboja sobre CSEA facilitado pela tecnologia ilustra como construir sistemas inclusivos e centrados na criança.[220] Da mesma forma, a Associação Canadiana de Chefes de Polícia adoptou uma estrutura para o policiamento informado sobre traumas, construída em torno de seis etapas, o **Six 'R' Model:** Realizar, Reconhecer, Repensar, Responder, Reduzir, Rever.[221] Quando os sistemas são informados sobre traumas e amigos das crianças, eles reduzem os danos da culpabilização das vítimas, o que desencoraja a denúncia, agrava os impactos a longo prazo e enfraquece a deteção e a resposta.

> **"Especialmente no meu país, nunca vi culparem a pessoa que está a aliciar. É sempre: 'Por que farias isso? É o teu próprio telemóvel, por que deixarias isso acontecer?'"**
>
> *Menina de 14 anos, Etiópia*[60]

Coordenação mundial intersectorial para lidar com a extorsão sexual financeira

A coordenação mundial entre sectores, incluindo autoridades policiais, governo, indústria e provedores de serviços, é essencial para uma prevenção eficaz, particularmente em casos de extorsão financeira sexual. A ECPAT recomenda o fortalecimento das medidas intersectoriais por meio de:[222]

- Obrigar as instituições financeiras a detectar e denunciar activamente transações relacionadas com a exploração sexual de crianças.
- A adaptação de ferramentas de vigilância para tendências emergentes, incluindo carteiras digitais e criptomoedas.
- Reformar as leis de sigilo bancário para permitir a colaboração com os serviços policiais além da polícia financeira.

Prevenção da extorsão sexual de crianças *online*: Visão do Centro Australiano de Combate à Exploração Infantil, liderado pela Polícia Federal Australiana

Dados divulgados pelo Centro Australiano de Combate à Exploração Infantil (sigla inglesa ACCCE) em 2023 identificaram uma tendência emergente: criminosos estrangeiros visando principalmente adolescentes do sexo masculino para extorsão sexual financeira.[223] Mais de 90% das denúncias relacionadas à extorsão sexual financeira envolveram vítimas do sexo masculino. As denúncias de extorsão sexual financeira *online* visando crianças australianas aumentaram quase 60% entre Dezembro de 2022 e o início do ano lectivo de 2023, sugerindo um aumento durante as férias escolares.[223]

Desde Janeiro de 2024, a ACCCE registou um declínio nas denúncias de extorsão sexual financeira, provavelmente devido à actividade coordenada das autoridades policiais, mensagens de prevenção e esforços educacionais. No entanto, acredita-se que muitos incidentes não sejam denunciados, e a extorsão sexual de crianças continua a ser uma preocupação e prioridade significativas.

Uma característica central da abordagem da ACCCE é a colaboração intersectorial para divulgar mensagens de prevenção em grande escala.

> **“É toda uma rede e um ecossistema que é necessário para que a prevenção seja bem-sucedida.”**
>
> *Agente da lei*[79]

As parcerias reúnem autoridades policiais, indústria, ONG e organizações comunitárias para alcançar públicos diversos com intervenções personalizadas. Exemplos incluem:

- Alcance direccionado aos jovens: a ACCCE trabalhou com a Kids Helpline, a Meta e o programa de prevenção juvenil dos EUA **NoFiltr** para lançar recursos educativos para jovens de 13 a 17 anos, fornecendo informações sobre como prevenir e responder à extorsão sexual. Esses materiais também orientam pais e cuidadores sobre como reconhecer riscos, denunciar incidentes e acessar apoio.[223]
- Prevenção centrada na família: A ACCCE colaborou com o Project Paradigm na campanha **It's Never Too Early** (Nunca é cedo demais), que incentiva pais, cuidadores e famílias grávidas a iniciar conversas precoces sobre a prevenção do abuso sexual infantil.[224]
- Campanhas de comunicação em massa: Para alcançar directamente os grupos de alto risco, a ACCCE desenvolveu um anúncio animado de 30 segundos para rapazes de 13 a 17 anos, exibido no Snapchat, que alcançou cerca de cinco milhões de pessoas.[79,225]

Figura 9. Campanha animada contra a extorsão sexual no Snapchat

- Educação e formação: O **ThinkUKnow**, liderado pela Polícia Federal Australiana, equipa escolas, famílias e grupos comunitários com ferramentas práticas para lidar com a segurança *online* e os riscos de extorsão sexual. Os recursos incluem apresentações, fichas informativas, cartões de conversação, pacotes de actividades e materiais culturalmente adaptados para comunidades linguisticamente diversas, oferecendo vários pontos de entrada para discussões sobre os riscos *online*.[152]

Embora a ACCCE recolha activamente dados de participação, como o número de apresentações realizadas e o público alcançado, medir o verdadeiro impacto dos esforços de prevenção continua a ser um desafio, uma vez que muitos resultados não são directamente visíveis nos dados. A abordagem da ACCCE centra-se em equipar pais e cuidadores com ferramentas práticas e informações, reconhecendo o seu papel fundamental no apoio à segurança *online* das crianças. Os esforços contínuos visam alcançar famílias menos propensas a se envolver e fortalecer iniciativas de educação e sensibilização em todas as comunidades.

Conclusão

O CSEA facilitado pela tecnologia é uma ameaça mundial que pode ser evitada. A tarefa que temos pela frente é clara: preencher as lacunas de evidência, identificar e ampliar o que funciona e acelerar a tradução do conhecimento em acção. Num ambiente de financiamento limitado, isso significa maximizar o impacto por meio da partilha de conhecimento e evidências, agendas coordenadas e lições aprendidas com o CSEA *offline* e esforços mais amplos de prevenção da violência. Para construir um mundo digital mais seguro, devemos fortalecer os elos mais fracos, reconhecendo que os riscos e danos migram para os espaços menos protegidos, e garantir que todas as crianças se beneficiem do mesmo nível de proteção. A prevenção eficaz depende de colocar os direitos e as vozes das crianças no centro, investir em acções sustentáveis e baseadas em evidências e fortalecer a colaboração entre todos os sectores e partes interessadas. Por meio da responsabilidade compartilhada, a comunidade mundial pode acelerar o progresso em direcção a um ambiente digital mais seguro, onde as crianças possam aprender, brincar e se conectar livres de exploração e abuso.

> **“Da dor ao propósito, da sobrevivência à força.”**
>
> *Sobrevivente, Filipinas*[138]

Agradecimentos

Citação sugerida: WeProtect Global Alliance (2025). Global Threat Assessment 2025, Preventing technology-facilitated child sexual exploitation and abuse: From insights to action (by Lau LS, Mayevskaya Y, Fanton d'Andon C, Ware M, and Hermosilla S). WeProtect Global Alliance: https://www.weprotect.org/global-threat-assessment-25/

Autores

WeProtect Global Alliance

A WeProtect Global Alliance é um movimento global que reúne mais de 350 organizações governamentais, do setor privado e da sociedade civil que trabalham para transformar a resposta global à exploração e abuso sexual infantil *online*.

Care and Protection of Children (CPC) Learning Network, Universidade de Columbia

A Rede de Aprendizagem CPC, sediada na Escola de Saúde Pública Mailman da Universidade de Columbia, promove a saúde e o bem-estar infantil por meio de pesquisa, políticas e práticas. Com parceiros em mais de 20 países, a CPC gera evidências e ferramentas rigorosas e baseadas localmente para fortalecer os sistemas de proteção infantil e promover o bem-estar de crianças, jovens e famílias em todo o mundo.

Este relatório foi pesquisado e escrito por Ling San Lau, Yana Mayevskaya, Sabrina Hermosilla, Cécile Fanton d'Andon e Matthew Ware, com contribuições adicionais de Claire Cunningham, Hannah Thompson, Cassie Landers, Hanna-Tina Fischer, Jonathan Huynh e Lisberma Peralta Aquino.

A WeProtect Global Alliance gostaria de agradecer a todas as organizações e indivíduos que apoiaram o desenvolvimento da Avaliação da Ameaça Global 2025. Agradecemos às crianças e sobreviventes cujas experiências e ideias contribuíram para este relatório e orientam os esforços coletivos para manter as crianças seguras. O apoio prestado ao desenvolvimento do relatório, como membro do Comité Directivo ou colaborador, não implica o endosso (parcial ou total) do conteúdo deste relatório.

Comité Diretivo de Peritos

Aengus Ó Dochartaigh	MOORE | Prevenção do Abuso Sexual Infantil, Universidade Johns Hopkins
Afrooz Kavani Johnson	UNICEF
Anil Raghuvanshi	ChildSafeNet
Beth Hepworth	PGI
Carolina Piñeros	RedPapaz
Dan Sexton	Internet Watch Foundation (IWF)
Debra Clelland	DeafKidz International
Elena Martellozzo	Childlight, Instituto Global de Segurança Infantil, Universidade de Edimburgo
James Smith	PGI
Jess Lishak	Tech Coalition
Nina Vaaranen-Valkonen	Protect Children
Ricardo de Lins e Horta	Governo do Brasil
Sambath Sokunthea	Governo do Camboja
Soyoung Park	Regulador sul-coreano, KCSC
Wirawan Boom Mosby	Projeto HUG Tailândia

Colaboradores

As seguintes organizações forneceram informações sobre sobreviventes e jovens para a nossa pesquisa:

VoiceBox

Uma empresa social sediada no Reino Unido e liderada por jovens que amplifica as vozes de jovens entre 13 e 25 anos. A VoiceBox organizou duas sessões com jovens entre 14 e 18 anos de sete países, incluindo comunidades marginalizadas, refugiados e sobreviventes de genocídio. As suas opiniões contribuíram para o relatório e para o quadro de prevenção.

Secrets Worth Sharing

Uma organização sediada no Reino Unido que promove a discussão aberta sobre abuso sexual infantil por meio de podcasts, workshops e eventos. A Secrets Worth Sharing analisou ferramentas de pesquisa qualitativa e contribuiu com as perspectivas dos sobreviventes incorporadas ao relatório.

Marie Collins Foundation

Apoia vítimas e/ou sobreviventes de abuso sexual infantil assistido por tecnologia, bem como as suas famílias e os profissionais que trabalham com elas, fornecendo serviços de defesa, educação e recuperação. A Marie Collins Foundation analisou ferramentas de pesquisa qualitativa, contribuiu com informações de sobreviventes e facilitou um workshop com sobreviventes para analisar a estrutura de prevenção.

International Justice Mission (IJM) Philippines

Uma organização global que combate o tráfico de pessoas, a escravidão moderna e a exploração e abuso de crianças. A IJM contribuiu com informações de sobreviventes relevantes para a estrutura de prevenção e integrados ao longo do relatório.

Footprints to Freedom

Uma organização sediada na Holanda, liderada por sobreviventes, que empodera sobreviventes do tráfico humano; implementa intervenções de base em Uganda, Quénia e Ruanda; e amplia iniciativas em toda a África por meio da sua Coligação Africana de Sobreviventes. A Footprints to Freedom contribuiu com as perspectivas dos sobreviventes incorporadas ao longo do relatório.

Protect Children

Com sede em Helsínquia, a Protect Children defende o direito de todas as crianças estarem livres da violência sexual, desenvolve programas de prevenção e pesquisa e reabilita os agressores. A Protect Children contribuiu com um prefácio de um sobrevivente e informações adicionais incluídas ao longo do relatório.

Para além do nosso Comité Directivo de Peritos, os seguintes indivíduos e organizações ofereceram as suas perspectivas para orientar esta investigação:

- ECPAT
- União Europeia
- Rede Global de Reguladores de Segurança Online (GOSRN)
- Google
- INHOPE
- Organização Internacional de Polícia Criminal (INTERPOL)
- Fundação Lucy Faithfull
- Centro Nacional para Crianças Desaparecidas e Exploradas (NCMEC)
- Agência Nacional contra o Crime (NCA)
- Organização Nacional para o Tratamento de Abuso (NOTA)
- Safe Futures Hub
- Snap
- Virtual Global Taskforce (VGT)
- Fórum Económico Mundial

Safe Futures Hub

A estrutura de prevenção foi desenvolvida como parte da Safe Futures Hub, uma iniciativa conjunta da Sexual Violance Research Initiative (SVRI), Together for Girls e WeProtect Global Alliance que tem como objectivo propor soluções para acabar com a violência sexual contra crianças.

O design visual e o layout do relatório foram desenvolvidos pela Rec Design. O design visual da estrutura de prevenção foi feito pela Together Creative.

Manter-se actualizado com as evidências emergentes

Tabela 3. Seleção de publicações pendentes e recursos vivos

Nome da iniciativa	Descrição	Prevista
Disrupting Harm 2 (pesquisa realizada em conjunto pela UNICEF Innocenti, ECPAT e INTERPOL)	Expansão de inquéritos populacionais com crianças e cuidadores, bem como entrevistas aprofundadas com jovens sobreviventes em 12 países adicionais, para melhorar a compreensão global da exploração e abuso sexual infantil online.	**2025-2026**
Global Boys Initiative (ECPAT)	Uma publicação futura apresentará um estudo de caso do Paquistão com depoimentos de sobreviventes e profissionais, destacando iniciativas para prevenir e responder à exploração sexual de meninos.	**2025-2026**
INSPIRE: Sete Estratégias para Acabar com a Violência contra Crianças (desenvolvido pela OMS com parceiros globais)	O **INSPIRE** é um pacote técnico baseado em evidências que descreve sete estratégias e duas actividades transversais para prevenir a violência contra crianças de 0 a 17 anos. Ele apoia os países na coordenação de acções multissectoriais e no acompanhamento do progresso.	**Em curso**
Prevenção Global (fornecido pela MOORE | Prevenção do abuso sexual infantil, Escola de Saúde Pública Johns Hopkins Bloomberg e Instituto Real de Investigação em Saúde Mental)	Lançada em 2024, **a Prevenção Global** é uma plataforma de conhecimento e uma iniciativa de investigação ambiciosa que avalia sete programas desenvolvidos para prevenir o abuso sexual infantil e conduz inquéritos de referência sobre a prevalência do abuso em quatro continentes (Brasil, Alemanha, Tanzânia e EUA).[176] Também publica produtos de conhecimento que exploram aspectos-chave da prevenção, incluindo **Serving Youth**, que aborda a prevalência da vitimização em ambientes que atendem jovens nos EUA e fornece um guia prático para líderes; **Scalability,** que explora barreiras e oportunidades para ampliar programas; e **Making The Case**, que revela a percepção pública do abuso sexual infantil como uma questão evitável.[125,176,226]	**2026**

Comportamento Responsável com Jovens e Crianças (RBYC)[74]	**O RBYC** é um programa para jovens de 11 a 14 anos que visa prevenir comportamentos sexuais problemáticos e ajudar os adolescentes a desenvolver interações seguras e adequadas — com crianças mais novas, seus pares e adultos — tanto online como *offline*. Ele foi testado nos EUA e actualmente está a ser adaptado e avaliado em 24 escolas na Alemanha (22 em ensaios aleatórios controlados e 2 em estudos-piloto).	**2026**
Safe Futures Hub Revisão Sistemática Global e Estrutura PbK	O Safe Futures Hub, em colaboração com a Universidade de Oxford, está a desenvolver uma **revisão sistemática global** para fornecer evidências continuamente actualizadas sobre a prevenção da violência sexual infantil, com foco em países de baixa e média renda. Em Dezembro de 2025, o Hub também lançará a sua **estrutura de conhecimento baseado na prática (PbK)**, que reconhece a experiência vivida, traz vozes sub-representadas e destaca por que e como as intervenções são bem-sucedidas em contextos do mundo real.	**2025-2026**

Glossário de termos

Material de abuso sexual infantil (CSAM) gerado por inteligência artificial (IA)	O uso indevido de tecnologias de IA para criar, total ou parcialmente, qualquer representação sexualizada ou sexualmente explícita de uma criança. Isso inclui imagens, vídeos, áudio, animações ou outras mídias produzidas por IA. É uma forma de CSAM gerado digitalmente (DG-CSAM) (ver relacionado, *deepfakes*).
Agrupamento	Recurso que consolida denúncias relacionadas a incidentes generalizados, como conteúdo viral, em uma única denúncia ou em um conjunto menor de denúncias, reduzindo envios redundantes e mantendo as informações sobre todos os utilizadores e incidentes denunciados.[12]
Chatbots	Uma ferramenta de conversação automatizada, frequentemente alimentada por IA, que pode simular crianças ou adultos e interagir com os utilizadores como companheiros, conselheiros ou amigos, mas pode representar riscos como desinformação, recolha de dados ou exposição a conteúdo impróprio.[59]
Material de abuso sexual infantil (CSAM)	Material, como imagens ou vídeos, que retrata e/ou documenta actos de abuso sexual e/ou exploração de crianças. Esse material pode ser usado em investigações de inteligência criminal e/ou servir como prova em processos judiciais criminais.[26]
Abuso sexual infantil online	Qualquer forma de abuso sexual de crianças que tenha uma ligação com o ambiente digital. Isto inclui o abuso sexual de crianças facilitado pela tecnologia e cometido noutro local e depois repetido através da partilha online nas redes sociais ou noutras dimensões digitais.[26]
Exploração sexual infantil online	Todos os actos de natureza sexualmente exploradora realizados contra uma criança que tenham uma ligação com o ambiente digital. Isto inclui qualquer uso da tecnologia que resulte em exploração sexual ou faça com que uma criança seja sexualmente explorada ou que resulte ou faça com que imagens ou outro material que documente tal exploração sexual seja produzido, comprado, vendido, possuído, distribuído ou transmitido. Em comparação com o abuso, a troca ou distribuição de coisas de valor, incluindo, mas não se limitando a imagens ou vídeos, são frequentemente componentes da exploração.[26]
Deepfake	Um *deepfake* é um conteúdo gerado por IA (por exemplo, uma foto, vídeo, animação ou áudio) que retrata de forma realista uma pessoa a fazer ou a dizer algo que nunca fez.[227] Pode ser usado para se referir a conteúdos que retratam crianças reais em situações sexualizadas simuladas.

Bem-estar digital	Impacto das tecnologias na saúde mental, física, social e emocional de um indivíduo.[228]
Criptografia de ponta a ponta	Um método de segurança que garante que apenas o remetente e o destinatário pretendido possam aceder ao conteúdo de uma comunicação, impedindo que terceiros, incluindo provedores de serviços, visualizem ou analisem os dados.
Conteúdo sexual gerado/produzido na primeira pessoa envolvendo crianças	Crianças e adolescentes menores de 18 anos podem tirar fotos ou gravar vídeos de conteúdo sexual de si mesmos. Embora essa conduta em si não seja necessariamente ilegal ou socialmente inaceitável, há riscos de que esse tipo de conteúdo seja divulgado online ou pessoalmente para prejudicar as crianças ou ser usado como base para extorsão. Usamos esse termo, bem como «sexting», que é uma referência coloquial comum para tirar e partilhar imagens de natureza sexual. As crianças frequentemente dizem que não se identificam com a noção de conteúdo «autogerado» e, em contextos como o compartilhamento não consensual, isso pode ser inútil.[233]
Inteligência artificial generativa (IA)	A IA generativa é uma forma de inteligência artificial que utiliza modelos de aprendizagem automática para analisar os padrões e a estrutura dos seus dados de treino, a fim de criar novos conteúdos, incluindo texto, imagens, áudio ou outros meios de comunicação, que imitam essas entradas.[230]
Aliciamento	Aliciamento ou aliciamento online refere-se ao processo de estabelecer/construir uma relação com uma criança, seja pessoalmente ou através da utilização da Internet ou de outras tecnologias digitais, para facilitar o contacto sexual com essa pessoa. No relatório, aliciamento sem qualificativos refere-se ao aliciamento para fins sexuais.[26]
Comportamentos sexuais prejudiciais	Acções sexuais iniciadas por uma criança ou jovem que são inadequadas do ponto de vista do desenvolvimento, coercivas ou abusivas e podem causar danos a si próprias ou a outras pessoas. Comportamento sexual problemático refere-se a acções sexuais que podem ser inadequadas ou preocupantes, mas que não atingem o limiar de dano ou abuso. Este relatório utiliza o termo comportamentos sexuais prejudiciais para abranger todo o espectro de comportamentos preocupantes, reconhecendo que comportamentos em fase inicial ou menos graves ainda requerem intervenção para evitar que se agravem.[108]
Correspondência de hash	Um algoritmo conhecido como função hash é utilizado para calcular uma impressão digital, conhecida como hash, a partir de um ficheiro. A comparação desse hash com outro hash armazenado numa base de dados é chamada de correspondência de hash. No contexto da segurança online, a correspondência de hash pode ser um meio principal para a deteção de imagens e vídeos ilegais ou prejudiciais conhecidos.[231]
Abuso transmitido ao vivo	Frequentemente transmitido aos espectadores por meio de plataformas dedicadas de transmissão ao vivo ou redes sociais, o conteúdo é entregue instantaneamente, permitindo que os espectadores assistam e se envolvam enquanto o abuso está a ocorrer. Em comparação com outros formatos, isso pode deixar menos vestígios digitais do abuso.[26]

Partilha não consensual de imagens íntimas (NCII)	Um termo comumente associado a adultos que se refere a compartilha de imagens sexuais ou sexualmente sugestivas sem o consentimento da pessoa retratada. Isso pode ocorrer quando o conteúdo inicialmente compartilhado de forma consensual é posteriormente compartilhado ou encaminhado sem consentimento, ou quando as fotos são tiradas sem consentimento (como no contexto de aliciamento ou extorsão sexual). O conceito-chave é a «perda de controlo» sobre as representações.[26] Este termo requer cautela quando utilizado em relação a crianças que não atingiram a idade de consentimento sexual (ver conteúdo sexual relacionado, gerado/produzido na primeira pessoa envolvendo crianças).
Agressor	Pessoa que cometeu crimes ou é culpada de um crime envolvendo exploração e abuso sexual infantil.[26]
Sedução online	Quando um indivíduo comunica com uma criança através da Internet (ou outra tecnologia) com a intenção de cometer um crime sexual ou rapto.[232]
Perpetrador	Pessoa que pode ter-se envolvido na exploração sexual de crianças (independentemente de seu envolvimento no processo de justiça criminal). Usamos os termos perpetrador e potencial perpetrador para nos referirmos a pessoas que cometeram ou podem cometer esses actos, independentemente de terem-se enquadrado na definição específica de um crime ou terem sido presas/condenadas por um crime.[26]
Extorsão sexual de crianças	Um processo pelo qual as crianças são coagidas a continuar a produzir material sexual e/ou a realizar actos angustiantes sob a ameaça de exposição a outras pessoas do material que as retrata. Quando a motivação é principalmente financeira, também usamos o termo «extorsão sexual financeira».[26]
Sobrevivente	Pessoas que sofreram danos e vitimização. O uso do termo «sobrevivente» pode refletir um processo de cura. Reconhecendo a variedade de preferências que as pessoas com experiência vivida têm em relação à terminologia, usamos os termos «vítima» e «sobrevivente» de forma intercambiável no relatório.[26]
Exploração e abuso sexual infantil facilitados pela tecnologia (CSEA facilitado pela tecnologia, também referido como TFCSEA)	O CSEA facilitado pela tecnologia refere-se ao uso de tecnologias digitais em qualquer fase para preparar, cometer ou divulgar (no caso de CSAM) a exploração sexual ou o abuso sexual de uma criança. Abrange danos cometidos em ambientes digitais e não digitais (*offline*) - incluindo, por exemplo, a troca de informações, a coordenação de acções e o contacto com crianças para as aliciar ou coagir. Este termo reconhece que a tecnologia desempenha um papel na facilitação do abuso e na perpetuação dos danos causados pelo abuso, tanto em espaços físicos como digitais.[26]
Vítima	Pessoas que foram vítimas de actos prejudiciais e/ou criminosos enquanto titulares de direitos. Reconhecendo a variedade de preferências que as pessoas com experiência vivida têm em relação à terminologia, utilizamos este termo de forma intercambiável com «sobrevivente» no relatório.[26]

Referências

1. Navigating the Unknown: Reflections on AI, the Metaverse, and Keeping Young People Safe | VoiceBox [Internet]. [cited 2025 Sept 27]. Available from: https://voicebox.site/article/navigating-unknown-reflections-ai-metaverse-and-keeping-young-people-safe
2. MOORE | Preventing Child Sexual Abuse | Johns Hopkins Bloomberg School of Public Health [Internet]. [cited 2025 Sept 27]. Available from: https://publichealth.jhu.edu/moore-center-for-the-prevention-of-child-sexual-abuse
3. United Nations Department of Economic and Social Affairs [Internet]. Global Internet Use Continues To Rise But Disparities Remain. [cited 2025 Nov 20]. Available from: https://social.desa.un.org/sdn/global-internet-use-continues-to-rise-but-disparities-remain
4. GSMA. Smartphone owners are now the global majority, New GSMA report reveals [Internet]. Newsroom. 2023 [cited 2025 Nov 4]. Available from: https://www.gsma.com/newsroom/press-release/smartphone-owners-are-now-the-global-majority-new-gsma-report-reveals/
5. ITU. Statistics [Internet]. [cited 2025 Nov 21] . Available from: https://www.itu.int/en/ITU-D/Statistics/pages/stat/default.aspx
6. Generative AI: Risks and opportunities for children | Innocenti Global Office of Research and Foresight [Internet]. [cited 2025 Aug 29]. Available from: https://www.unicef.org/innocenti/generative-ai-risks-and-opportunities-children
7. Industry. Data collected by the CPC Learning Network through key informant interviews.
8. Academic. Data collected by the CPC Learning Network through key informant interviews.
9. Intergovernmental. Data collected by the CPC Learning Network through key informant interviews.
10. Safe Online. Disrupting Harm [Internet]. Available from: https://safeonline.global/wp-content/uploads/2023/12/DH-data-insights-8-151223.pdf
11. Civil Society. Data collected by the CPC Learning Network through key informant interviews.
12. National Center for Missing and Exploited Children. CyberTipline Data [Internet]. [cited 2025 Sept 3]. Available from: https://ncmec.org/gethelpnow/cybertipline/cybertiplinedata
13. INHOPE Releases Annual Report 2024 [Internet]. [cited 2025 May 5]. Available from: https://inhope.org/EN/articles/inhope-annual-report-2024
14. IWF 2024 Annual Data & Insights Report [Internet]. [cited 2025 May 6]. Available from: https://www.iwf.org.uk/annual-data-insights-report-2024/
15. How AI is being abused to create child sexual abuse material (CSAM) online [Internet]. [cited 2025 May 1]. Available from: https://www.iwf.org.uk/about-us/why-we-exist/our-research/how-ai-is-being-abused-to-create-child-sexual-abuse-imagery/

16. 118th Congress. S.474 - REPORT Act [Internet]. 2024. Available from: https://www.congress.gov/bill/118th-congress/senate-bill/474

17. UK Public General Acts. Online Safety Act 2023 [Internet]. 50 Oct 26, 2023. Available from: https://www.legislation.gov.uk/ukpga/2023/50

18. Social media ban in Australia | A simple guide [Internet]. UNICEF Australia. [cited 2025 Sept 27]. Available from: https://www.unicef.org.au/unicef-youth/staying-safe-online/social-media-ban-explainer?srsltid=AfmBOop6gJckegYUrtle7BkiDMa6ZKUVy0aaGjHrYShDthWRHUqp8_9A

19. Presidência da República, Casa Civil, Secretaria Especial para Assuntos Jurídicos. LEI No 15.211, DE 17 DE SETEMBRO DE 2025 [Internet]. Available from: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/L15211.htm

20. Presidência da República, Casa Civil, Secretaria Especial para Assuntos Jurídicos. LEI No 15.100, DE 13 DE JANEIRO DE 2025 [Internet]. Available from: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/l15100.htm

21. New Online Safety Code of Practice for App Distribution Services Enhances Protection for Singapore Users [Internet]. Infocomm Media Development Authority. [cited 2025 Aug 29]. Available from: https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2025/online-safety-code-of-practice-for-app-distribution-services

22. Making the digital and physical world safer: Why the Convention against Cybercrime matters | UN News [Internet]. 2024 [cited 2025 Sept 27]. Available from: https://news.un.org/en/story/2024/12/1158526

23. UN Cybercrime Convention - Full Text [Internet]. United Nations : Office on Drugs and Crime. [cited 2025 Aug 25]. Available from: //www.unodc.org/unodc/en/cybercrime/convention/text/convention-full-text.html

24. Global Digital Compact | Office for Digital and Emerging Technologies [Internet]. [cited 2025 Sept 10]. Available from: https://www.un.org/digital-emerging-technologies/global-digital-compact

25. Lantern: advancing child safety through signal sharing [Internet]. https://technologycoalition.org/. [cited 2025 Sept 27]. Available from: https://technologycoalition.org/programs/lantern/

26. ECPAT. Terminology Guidelines [Internet]. 2025 [cited 2025 Aug 29]. Available from: https://ecpat.org/terminology/

27. Call for consultants, global Living Systematic Review consultant(s):... [Internet]. Safe Futures Hub. [cited 2025 Sept 27]. Available from: https://www.safefutureshub.org/call-for-consultants-global-living-systematic-review-consultants-what-works-to-prevent-childhood-sexual-violence

28. Prevention Global. Prevention Global launches with new online resource hub and landmark impact evaluations [Internet]. [cited 2025 Sept 27]. Available from: https://www.prevention.global/

29. Model National Response to end child sexual exploitation & abuse online - WeProtect Global Alliance [Internet]. 2020 [cited 2025 May 1]. Available from: https://www.weprotect.org/resources/frameworks/model-national-response/

30. Bronfenbrenner U. Toward an experimental ecology of human development. Am Psychol. 1977;32(7):513–31.

31. UNICEF. Corporate reporting on child rights in relation to the digital environment [Internet]. Available from: https://www.unicef.org/childrightsandbusiness/workstreams/responsible-technology/reporting

32. Workshop. Data collected by the CPC Learning Network through key informant interviews.

33. Convention on the Rights of the Child, 20 November 1989 [Internet]. [cited 2025 Sept 10]. Available from: https://ihl-databases.icrc.org/en/ihl-treaties/crc-1989

34. OHCHR. General comment No. 25 (2021) on children's rights in relation to the digital environment [Internet]. OHCHR. [cited 2025 Nov 3]. Available from: https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation

35. United Nations. Guiding Principles on Business and Human Rights : Implementing the United Nations "Protect, Respect and Remedy" Framework [Internet]. Available from: https://digitallibrary.un.org/record/720245?v=pdf

36. UNICEF. Children's Rights Business Principles 2012 [Internet]. [cited 2025 Nov 3]. Available from: https://www.unicef.org/media/96136/file/Childrens-Rights-Business-Principles-2012.pdf

37. WeProtect Global Alliance. Children and Young People present their roadmap for a safer digital world [Internet]. Available from: https://www.weprotect.org/news/children-and-young-people-present-their-roadmap-for-a-safer-digital-world/

38. SafetyNet: insights from young people around the world [Internet]. Safe Futures Hub. [cited 2025 Sept 22]. Available from: https://www.safefutureshub.org/resources/safetynet-insights-from-young-people-around-the-world

39. Thorn. Evolving Technologies Horizon Scan [Internet]. Available from: https://www.thorn.org/research/library/evolving-technologies-horizon-scan/

40. UNICEF. Childhood in a Digital World [Internet]. [cited 2025 Nov 20]. Available from: https://www.unicef.org/innocenti/reports/childhood-digital-world

41. 10 countries with the highest percentage of web traffic from mobile phones | Business Insider Africa [Internet]. [cited 2025 Aug 29]. Available from: https://africa.businessinsider.com/local/lifestyle/10-countries-with-the-highest-percentage-of-web-traffic-from-mobile-phones/04wvy3f

42. Facts and Figures 2024 - Youth Internet use [Internet]. [cited 2025 Aug 29]. Available from: https://www.itu.int/itu-d/reports/statistics/2024/11/10/ff24-youth-internet-use

43. Slater SO, Arundell L, Grøntved A, Salmon J. Age of first digital device use and screen media use at age 15: A cross-sectional analysis of 384,591 participants from 55 countries. Public Health Pract [Internet]. 2025 June 1 [cited 2025 Sept 2];9:100596. Available from: https://www.sciencedirect.com/science/article/pii/S2666535225000151

44. Coded Companions: Young People's Relationships With AI Chatbots | VoiceBox [Internet]. [cited 2025 Sept 27]. Available from: https://voicebox.site/article/coded-companions-young-peoples-relationships-ai-chatbots

45. Snap Digital Well-Being Index | Snapchat Safety [Internet]. [cited 2025 Sept 27]. Available from: https://values.snap.com/safety/dwbi

46. Häubi RB. How the UN plans to connect every school to the internet by 2030 [Internet]. SWI swissinfo.ch. 2024 [cited 2025 Sept 2]. Available from: https://www.swissinfo.ch/eng/international-geneva/the-un-plans-to-connect-every-school-to-the-internet-by-2030/83325727

47. Peng D, Yu Z. A Literature Review of Digital Literacy over Two Decades. Educ Res Int [Internet]. 2022 [cited 2025 Sept 3];2022(1):2533413. Available from: https://onlinelibrary.wiley.com/doi/abs/10.1155/2022/2533413

48. World Health Organization. 1st Global Ministerial Conference on Ending Violence Against Children [Internet]. [cited 2025 Nov 4]. Available from: https://www.who.int/teams/social-determinants-of-health/violence-prevention/1st-global-ministerial-conference-on-ending-violence-against-children

49. INHOPE. Launching Version 3 of the Universal Classification Schema [Internet]. 2025 [cited 2025 Oct 29]. Available from: https://inhope.org/EN/articles/what-s-new-in-version-3-of-the-universal-classification-schema

50. WeProtect Global Alliance. Child protection online: Global legislative, regulatory and policy update January 2025.

51. WeProtect Global Alliance. Child protection online: Global legislative, regulatory and policy update June 2025.

52. Patchin JW, Hinduja S. The nature and extent of youth sextortion: Legal implications and directions for future research. Behav Sci Law. 2024;42(4):401–16.

53. MikeHarrison. Global Taskforce on child sexual abuse online - WeProtect Global Alliance [Internet]. 2022 [cited 2025 Nov 3]. Available from: https://www.weprotect.org/global-taskforce-on-child-sexual-abuse-online/

54. Government. Data collected by the CPC Learning Network through key informant interviews.

55. Transparency reporting on child sexual exploitation and abuse online [Internet]. 2023 Sept [cited 2025 Sept 30]. (OECD Digital Economy Papers; vol. 357). Report No.: 357. Available from: https://www.oecd.org/en/publications/transparency-reporting-on-child-sexual-exploitation-and-abuse-online_554ad91f-en.html

56. Grossman S, Pfefferkorn R, Thiel D, Shah S, DiResta R, Perrino J, et al. The Strengths and Weaknesses of the Online Child Safety Ecosystem. 2024 Apr 22 [cited 2025 Sept 5]; Available from: https://purl.stanford.edu/pr592kc5483

57. Childlight Into the Light Index [Internet]. [cited 2025 Apr 30]. Available from: https://www.childlight.org/into-the-light

58. 2024 Annual Report [Internet]. National Center for Missing & Exploited Children. [cited 2025 Aug 25]. Available from: http://www.missingkids.org/content/ncmec/en/footer/about/annual-report.html

59. UNICEF. The risky new world of tech's friendliest bots [Internet]. Available from: https://www.unicef.org/innocenti/stories/risky-new-world-techs-friendliest-bots

60. Data from the youth consultations led by Voicebox.

61. Davis P. Spike in online crimes against children a "wake-up call" [Internet]. National Center for Missing & Exploited Children. [cited 2025 Sept 27]. Available from: http://www.ncmec.org/content/ncmec/en/blog/2025/spike-in-online-crimes-against-children-a-wake-up-call.html

62. Deepfake Nudes & Young People: Navigating a New Frontier in Technology-facilitated Nonconsensual Sexual Abuse and Exploitation [Internet]. Thorn. [cited 2025 Sept 5]. Available from: https://www.thorn.org/research/library/deepfake-nudes-and-young-people/

63. Online child sex abuse material, boosted by AI, is outpacing Big Tech's regulation [Internet]. [cited 2025 May 1]. Available from: https://www.iwf.org.uk/news-media/iwf-in-the-news/online-child-sex-abuse-material-boosted-by-ai-is-outpacing-big-techs-regulation/

64. Thiel D, DiResta R, Stamos A. Cross-Platform Dynamics of Self-Generated CSAM. 2023 June 6 [cited 2025 Aug 25]; Available from: https://fsi.stanford.edu/publication/cross-platform-dynamics-self-generated-csam

65 How Instagram's Algorithm Connects and Promotes Pedophile Network - Tech News Briefing - WSJ Podcasts [Internet]. [cited 2025 Aug 25]. Available from: https://www.wsj.com/podcasts/tech-news-briefing/how-instagrams-algorithm-connects-and-promotes-pedophile-network/A683C0B4-2E6F-4661-9973-10BD455DB895

66. AI enabling 'DIY child abuse' tools, with child victims in models, IWF warns MPs [Internet]. [cited 2025 May 1]. Available from: https://www.iwf.org.uk/news-media/news/ai-giving-offenders-diy-child-sexual-abuse-tool-as-dozens-of-child-victims-used-in-ai-models-iwf-warns-mps/

67. Aws Ai, Hugging Face, Inflection, Metaphysic, Stability AI, Teleperformance. Safety by Design for Generative AI: Preventing Child Sexual Abuse. Thorn [Internet]. 2024; Available from: https://info.thorn.org/hubfs/thorn-safety-by-design-for-generative-AI.pdf

68. Thorn. Synthetic Media Framework Case Study: Thorn. [cited 2025 Nov 4]; Available from: https://partnershiponai.org/wp-content/uploads/2024/11/case-study-thorn.pdf

69. Sivathasan N, Clahane P, Kemoli D. TikTok profiting from sexual livestreams involving children, BBC told. BBC [Internet]. 2025 Mar 2; Available from: https://www.bbc.com/news/articles/cedl8eyy4pjo

70. Ovaska A, Insoll T, Soloveva V, Vaaranen-Valkonen N, Di GR. Findings from Italian language respondents to Re-Direction surveys of CSAM users on dark web search engine. JRC Publ Repos [Internet]. 2025 [cited 2025 Nov 3]; Available from: https://publications.jrc.ec.europa.eu/repository/handle/JRC138231

71. FATF Annual Report 2023-2024 [Internet]. [cited 2025 Sept 30]. Available from: https://www.fatf-gafi.org/en/publications/Fatfgeneral/FATF-Annual-report-2023-2024.html

72. Protect Children. Tech Platforms Used by Online Child Sexual Abuse Offenders [Internet]. 2024. Available from: https://www.suojellaanlapsia.fi/en/post/tech-platforms-child-sexual-abuse

73. Ending the Scourge: The Need for the STOP CSAM Act — Testimony of Michelle DeLaune, President and CEO, National Center for Missing & Exploited Children (PDF) [Internet]. Room 226, Dirksen Senate Office Building, Washington, DC; 2025 [cited 2025 Sept 5]. p. 16. Available from: https://www.judiciary.senate.gov/imo/media/doc/2025-03-11_testimony_delaune.pdf

74. Responsible Behavior with Youth and Children | MOORE | Preventing Child Sexual Abuse [Internet]. [cited 2025 Sept 5]. Available from: https://publichealth.jhu.edu/moore-center-for-the-prevention-of-child-sexual-abuse/responsible-behavior-with-youth-and-children

75. The emergence of immersive technologies and Extended Reality - WeProtect Global Alliance [Internet]. [cited 2025 May 1]. Available from: https://www.weprotect.org/thematic/extended-reality/

76. Child safeguarding and immersive technologies [Internet]. NSPCC Learning. [cited 2025 Aug 25]. Available from: https://learning.nspcc.org.uk/research-resources/2023/child-safeguarding-immersive-technologies

77. Data from Marie Collins Foundation survivor consultation session.

78. Edwards G, Christensen L. Cyber strategies used to combat child sexual abuse material [Internet]. Australian Institute of Criminology; 2021 [cited 2025 Nov 4]. Available from: https://www.aic.gov.au/publications/tandi/tandi636

79. Law enforcement. Data collected by the CPC Learning Network through key informant interviews.

80. Walsh K, Mathews B, Parvin K, Smith R, Burton M, Nicholas M, et al. Prevalence and characteristics of online child sexual victimization: Findings from the Australian Child Maltreatment Study. Child Abuse Negl. 2025 Feb;160:N.PAG-N.PAG.

81. Under 10s groomed online 'like never before' in 2023 find IWF [Internet]. [cited 2025 May 1]. Available from: https://www.iwf.org.uk/news-media/news/under-10s-groomed-online-like-never-before-as-hotline-discovers-record-amount-of-child-sexual-abuse/

82. Girls & Young Women-Led Assessment on Online Sexual Exploitation, Abuse & Technology-Facilitated Gender-Based Violence in Africa [Internet]. ECPAT. [cited 2025 May 1]. Available from: https://ecpat.org/resource/girls-young-women-led-assessment-on-online-sexual-exploitation-abuse-technology-facilitated-gender-based-violence-in-africa/

83. Protecting Children From Violence and Exploitation in Relation to the Digital Environment | UNICEF [Internet]. [cited 2025 Sept 5]. Available from: https://www.unicef.org/documents/protecting-children-violence-and-exploitation-relation-digital-environment

84. Huang TF, Chun-Yin H, Fong-Ching C, Fong-Ching C, Chiu CH, Ping-Hung C, et al. Adolescent Use of Dating Applications and the Associations with Online Victimization and Psychological Distress. Behav Sci [Internet]. 2023;13(11):903. Available from: https://pubmed.ncbi.nlm.nih.gov/37998650/

85. Technology-facilitated Child Sexual Exploitation and Sexual Abuse in Burkina Faso, Côte d'Ivoire, Guinea and Niger [Internet]. ECPAT. [cited 2025 Sept 5]. Available from: https://ecpat.org/resource/technology-facilitated-child-sexual-exploitation-and-sexual-abuse-in-burkina-faso-cote-divoire-guinea-and-niger/

86. Pinto Cortez, Cristián & Guerra, Cristobal. Parental styles and online sexual abuse prevention factors. 2024. Límite (Arica). 19. 1-9. 10.4067/s0718-50652024000100209. Available from: https://www.researchgate.net/publication/383135600_Parental_styles_and_ online_sexual_abuse_prevention_factors

87. Wright MF. The Associations among Cyberbullying Victimization and Chinese and American Adolescents' Mental Health Issues: The Protective Role of Perceived Parental and Friend Support. Int J Environ Res Public Health [Internet]. 2024;21(8). Available from: https://pubmed.ncbi.nlm.nih.gov/39200678/

88. Friedman-Hauser G, Katz C. "She has a history of making things up": Examining the disclosure and reporting of online sexual abuse among children with disabilities. Child Abuse Negl [Internet]. 2025;163 ((Friedman-Hauser G., galf@haruv.org.il) The Bob Shapell School of Social Work, Tel Aviv University, Israel). Available from: https://awspntest.apa.org/record/2026-05574-001

89. Wright MF, Wachs S. Longitudinal
Associations between Different Types of Sexting, Adolescent Mental Health, and Sexual Risk Behaviors: Moderating Effects of Gender, Ethnicity, Disability Status, and Sexual
Minority Status. Arch Sex Behav [Internet]. 2024 Mar 1 [cited 2025 Sept 30];53(3):1115–28. Available from: https://doi.org/10.1007/s10508-023-02764-7

90. Gemara N, Mishna F, Katz C. 'If my parents find out, I will not see my phone anymore': Who do children choose to disclose online sexual solicitation to? Child Fam Soc Work [Internet]. 2025 [cited 2025 Sept 5];30(1):4–14. Available from: https://onlinelibrary.wiley.com/doi/abs/10.1111/cfs.13069

91. Lusky-Weisrose E, Klebanov B, Friedman-Hauser G, Avitan I, Katz C. Online sexual abuse of children with disabilities: Analyzing reports of social workers' case files in Israel. Child Abuse Negl. 2024 Aug;154:N. PAG-N.PAG.

92. Hong JS, Kim J, Lee JM, Saxon S, Thornberg R. Pathways from Polyvictimization to Offline and Online Sexual Harassment Victimization Among South Korean Adolescents. Arch Sex Behav. 2023 Oct;52(7):2779–88.

93. Tanaya NLTP, Puteri NMM. Child Sexual Abuse and Exploitation through Livestreaming in Indonesia: Unequal Power Relations at the Root of Child Victimization. J Int Womens Stud [Internet]. 2023 Apr;25(3):1–14. Available from: https://vc.bridgew.edu/jiws/vol25/iss3/6

94. Children P. What Drives Online Child Sexual Abuse Offending? Understanding Motivations, Facilitators, Situational Factors, and Barriers [Internet]. Protect Children. 2024 [cited 2025 Aug 31]. Available from: https://www.suojellaanlapsia.fi/en/post/2know-final-report-1

95. Napier SS, Seto MC, Cashmore J, Shackel R. Characteristics that predict exposure to and subsequent intentional viewing of child sexual abuse material among a community sample of Internet users. Child Abuse Negl. 2024 Oct;156:106977.

96. Lahtinen HM, Honkalampi K, Insoll T, Nurmi J, Quayle E, Ovaska AK, et al. Investigating the disparities among child sexual abuse material users: Anonymous self-reports from both charged and uncharged individuals. Child Abuse Negl. 2025 Mar;161:107299.

97. Chauviré-Geib K, Gerke J, Fegert JM, Rassenhofer M. The Digital Dimension: Victim's Experiences of Technology's Impact on Penetrative Child Sexual Abuse. J Child Sex Abuse. 2025 Apr 28;1–21.

98. Christensen LS, Woods J. "It's Like POOF and It's Gone": The Live-Streaming of Child Sexual Abuse. Sex Cult. 2024 Aug 1;28(4):1467–81.

99. Ringrose J, Regehr K. Recognizing and addressing how gender shapes young people's experiences of image-based sexual harassment and abuse in educational settings. J Soc Issues. 2023 Dec;79(4):1251–81.

100. 20 arrested in international operation targeting child sexual abuse material [Internet]. [cited 2025 Sept 30]. Available from: https://www.interpol.int/News-and-Events/News/2025/20-arrested-in-international-operation-targeting-child-sexual-abuse-material

101. 25 arrested in global hit against AI-generated child sexual abuse material [Internet]. Europol. [cited 2025 Sept 30]. Available from: https://www.europol.europa.eu/media-press/newsroom/news/25-arrested-in-global-hit-against-ai-generated-child-sexual-abuse-material

102. UNICEF. Who Perpetrates Online Child Sexual Exploitation and Abuse? [Internet]. [cited 2025 Nov 4]. Available from: https://safeonline.global/wp-content/uploads/2023/12/DH-data-insights-8-151223.pdf

103. Child sexual abuse material (CSAM) [Internet]. Thorn. [cited 2025 Sept 30]. Available from: https://www.thorn.org/research/child-sexual-abuse-material-csam/

104. Salter M, Wong T. Parental Production of Child Sexual Abuse Material: A Critical Review. Trauma Violence Abuse. 2024 July;25(3):1826–37.

105. Finkelhor D, Turner H, Colburn D. The prevalence of child sexual abuse with online sexual abuse added. Child Abuse Negl. 2024;149.

106. Finkelhor D, Shattuck A, Turner HA, Hamby SL. The lifetime prevalence of child sexual abuse and sexual assault assessed in late adolescence. J Adolesc Health. 2014;55(3):329-333.

107. Russell DH, Trew S, Smith R, Higgins DJ, Walsh K. Primary prevention of harmful sexual behaviors by children and young people: A systematic review and narrative synthesis. Aggress Violent Behav. 2025 Apr;81:N. PAG-N.PAG.

108. Safe Futures Hub. Children Displaying Harmful Sexual Behaviour: Evidence and Responses [Internet]. 2025 [cited 2025 Nov 4]. Available from: https://cdn.safefutureshub.org/files/Children-displaying-harmful-sexual-behaviour-Evidence-and-responses.pdf

109. Tunagur MT, Oksal H, Büber Ö, Kurt Tunagur EM, Sarıgedik E. Risk Factors and Predictors of Penetrative Online Child Sexual Abuse. J Pediatr Health Care. 2025;39(2):198–205.

110. Leaked: Understanding and Addressing Self-Generated Sexual Content involving Young People in Thailand [Internet]. Evident. [cited 2025 Sept 6]. Available from: https://www.itsevident.org/major-projects

111. Disrupting Harm country reports | Innocenti Global Office of Research and Foresight [Internet]. 2022 [cited 2025 Sept 6]. Available from: https://www.unicef.org/innocenti/reports/disrupting-harm-country-reports

112. Trends and insights from a unique helpline preventing child sexual abuse [Internet]. Lucy Faithfull Foundation. [cited 2025 Sept 5]. Available from: https://www.lucyfaithfull.org.uk/research/trends-and-insights-from-a-unique-helpline-preventing-child-sexual-abuse/

113. Bailey A, Allen L, Stevens E, Dervley R, Findlater D, Wefers S. Pathways and Prevention for Indecent Images of Children Offending: A Qualitative Study. Sex Offending Theory Res Prev [Internet]. 2022 Dec 2 [cited 2025 Sept 5];17:1–24. Available from: https://sotrap.psychopen.eu/index.php/sotrap/article/view/6657

114. Protect Children. Our Voice Male Survivors: Experiences of Victims and Survivors of Child Sexual Abuse and Exploitation [Internet]. 2025. Available from: https://www.suojellaanlapsia.fi/en/post/our-voice-male-survivors

115. Tech Coalition | Assessing OCSEA Harms in Product Development [Internet]. Tech Coalition. [cited 2025 May 1]. Available from: https://www.technologycoalition.org/knowledge-hub/assessing-ocsea-harms-in-product-development

116. Detecting, Disrupting and Investigating Online Child Sexual Exploitation [Internet]. [cited 2025 Aug 30]. Available from: https://www.fatf-gafi.org/en/publications/Fatfgeneral/Online-child-sexual-exploitation.html

117. Internet Watch Foundation. Teenage boys targeted as hotline sees 'heartbreaking' increase in child 'sextortion' reports [Internet]. 2024 [cited 2025 Nov 10]. Available from: https://www.iwf.org.uk/news-media/news/teenage-boys-targeted-as-hotline-sees-heartbreaking-increase-in-child-sextortion-reports/

118. Self-Generated Child Sexual Abuse Fieldwork Findings Report by PIER [Internet]. [cited 2025 May 1]. Available from: https://www.iwf.org.uk/about-us/our-campaigns/self-generated-child-sexual-abuse-fieldwork-findings-report/

119. MikeHarrison. Link-sharing and child sexual abuse: understanding the threat - WeProtect Global Alliance [Internet]. 2023 [cited 2025 May 1]. Available from: https://www.weprotect.org/resources/library/link-sharing-and-child-sexual-abuse-understanding-the-threat/

120. Iyer C, Mehra S. Not a Child's Play: Taking Stock of Children's Gaming in India, Gaps, Emerging Risks and Responses [Internet]. Space2Grow; 2025 June. Available from: https://www.space2grow.in/_files/ugd/fcdbc5_0dead6ef6615455280abdbded0c2c605.pdf

121. Situation Analysis of Child Online Protection in Pakistan | UNICEF Pakistan [Internet]. [cited 2025 May 1]. Available from: https://www.unicef.org/pakistan/documents/situation-analysis-child-online-protection-pakistan

122. Online sexual abuse of primary children 1000% worse since lockdown [Internet]. [cited 2025 May 1]. Available from: https://www.iwf.org.uk/news-media/news/sexual-abuse-imagery-of-primary-school-children-1-000-per-cent-worse-since-lockdown/

123. CDC. A Public Health Approach to Community Violence Prevention [Internet]. Community Violence Prevention. 2025 [cited 2025 Sept 22]. Available from: https://www.cdc.gov/community-violence/php/public-health-strategy/index.html

124. Emery CR, Wong PWC, Haden-Pawlowski V, Pui C, Wong G, Kwok S, et al. Neglect, online invasive exploitation, and childhood sexual abuse in Hong Kong: Breaking the links. Child Abuse Negl. 2024 Jan;147:N.PAG-N.PAG.

125. Scalability | Prevention Global [Internet]. [cited 2025 Sept 22]. Available from: https://www.prevention.global/scalability

126. 2024: A Year of Urgency, Vision, and Partnership in Safeguarding Children Online – Safe Online [Internet]. [cited 2025 Sept 22]. Available from: https://safeonline.global/2024-a-year-of-urgency-vision-and-partnership-in-safeguarding-children-online/

127. Safe Online. Financing a Safe Digital Future: Safer Internet Day 2025 – Safe Online [Internet]. [cited 2025 Nov 4]. Available from: https://safeonline.global/financing-a-safe-digital-future-safer-internet-day-2025/

128. Ending Online Child Sexual Exploitation and Abuse | UNICEF [Internet]. [cited 2025 May 1]. Available from: https://www.unicef.org/documents/ending-online-child-sexual-exploitation-and-abuse

129. Kardefelt-Winther D, Maternowska C. Addressing violence against children online and offline. Nat Hum Behav. 2020;4:227–30.

130. Data for Change – Safe Online [Internet]. [cited 2025 Sept 27]. Available from: https://safeonline.global/data-for-change/

131. UNICEF. Data brief on Measuring Technology-facilitated Violence against Children in line with the International Classification of Violence against Children (ICVAC) [Internet]. 2025 [cited 2025 Oct 29]. Available from: https://data.unicef.org/resources/data-brief-on-measuring-technology-facilitated-violence-against-children-in-line-with-the-international-classification-of-violence-against-children-icvac/

132. Safe Future Hub [Internet]. Available from: https://www.safefutureshub.org

133. Sexual Violence Research Initiative. SVRI Building the Field [Internet]. Available from: https://www.svri.org

134. Together for Girls [Internet]. Available from: https://www.togetherforgirls.org/

135. WeProtect Global Alliance. A global commitment to every child [Internet]. Available from: https://www.weprotect.org

136. General comment No. 24 (2019) on children's rights in the child justice system | OHCHR [Internet]. [cited 2025 Sept 22]. Available from: https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-24-2019-childrens-rights-child

137. Reason J. The contribution of latent human failures to the breakdown of complex systems. Philos Trans R Soc Lond B Biol Sci [Internet]. 1997 Jan [cited 2025 Sept 27];327(1241):475–84. Available from: https://royalsocietypublishing.org/doi/10.1098/rstb.1990.0090

138. Data from the Philippines Survivor Network consultations with survivors.

139. Lundy L. 'Voice' is not enough: conceptualising Article 12 of the United Nations Convention on the Rights of the Child. Br Educ Res J. 2007;33(6):927–42.

140. O'Kane C. Active and Safe: The Global Program Guide for Meaningful Participation of Children and Young People in Advocacy and Prevention and Protection from Online Violence [Internet]. kindernothilfe; 2025 [cited 2025 Nov 6]. Available from: https://fliphtml5.com/dcrxp/efpp/Active_%26amp%3B_Safe_GUIDE/

141. O'Kane C. Active and Safe: Accompanying Toolkit for Meaningful Participation of Children and Young People in Advocacy and Prevention and Protection from Online Violence [Internet]. kindernothilfe; 2025 [cited 2025 Nov 6]. Available from: https://fliphtml5.com/dcrxp/kqad/Active_%26_Safe_TOOLKIT_web_19Aug2025/

142. UNICEF. Spotlight guidance on best practices for stakeholder engagement with children in D-CRIAs [Internet]. 2025 [cited 2025 Oct 29]. Available from: https://www.unicef.org/childrightsandbusiness/reports/D-CRIA-Spotlight-guidance-stakeholder-engagement

143. Diagram adapted from Lansdown G, Haj-Ahmead J, Rusinow T, Sukura Y Friscia. Conceptual Framework for Measuring Outcomes of Adolescent Participation [Internet]. 2018 [cited 2025 Nov 4]. Available from: https://www.unicef.org/media/59006/file

144. WeProtect Global Alliance. Visualising child and survivor participation [Internet]. Available from: https://www.weprotect.org/response/child-survivor-participation/mapping-participation-initiatives/#dataviz

145. European Union. BeSmartOnline - Maltese Safer Internet Centre [Internet]. 2025 [cited 2025 Oct 29]. Available from: https://better-internet-for-kids.europa.eu/en/saferinternetday/malta

146. Be Smart Online. A Safer Internet for Malta [Internet]. [cited 2025 Oct 29]. Available from: https://www.besmartonline.info

147. VoiceBox. VoiceBox | By young people, for young people [Internet]. [cited 2025 Nov 4]. Available from: https://voicebox.site/

148. How can service providers work with boys at-risk and survivors of sexual exploitation and abuse in a gender-sensitive way? [Internet]. ECPAT. [cited 2025 May 1]. Available from: https://ecpat.org/story/global-boys-initiative-case-studies/

149. SecretsWorthSharing. Secrets Worth Sharing | How to talk about childhood sexual abuse [Internet]. SecretsWorthSharing. [cited 2025 Nov 4]. Available from: https://www.secretsworthsharing.com

150. CPC Learning Network. Secrets Worth Sharing founder testimony.

151. Global Threat Assessment 2023 Data - WeProtect Global Alliance [Internet]. 2023 [cited 2025 May 1]. Available from: https://www.weprotect.org/global-threat-assessment-23/data/

152. Resources | ThinkUKnow [Internet]. [cited 2025 Sept 22]. Available from: https://www.thinkuknow.org.au/resources-tab

153. World Vision. Tackling Online Child Sexual Exploitation [Internet]. [cited 2025 Oct 29]. Available from: https://wvi.org.vn/special-projects/tackling-online-child-sexual-exploitation-ene29.html

154. End Violence. More progress and impact from our grantees [Internet]. End Violence. [cited 2025 Nov 4]. Available from: https://www.end-violence.org/node/7971

155. UNICEF. Parenting for the Digital Age | UNICEF [Internet]. [cited 2025 Nov 4]. Available from: www.unicef.org/documents/parenting-digital-age

156. National Crime Agency. National Crime Agency launches online campaign to tackle "sextortion" among young teenage boys [Internet]. Available from: https://www.nationalcrimeagency.gov.uk/news/national-crime-agency-launches-online-campaign-to-tackle-sextortion-among-young-teenage-boys

157. Think Before You Share Campaign from IWF [Internet]. [cited 2025 Sept 17]. Available from: https://www.iwf.org.uk/about-us/our-campaigns/think-before-you-share/

158. UNODC. Beware The Share [Internet]. [cited 2025 Nov 4]. Available from: www.unodc.org/roseap/uploads/documents/beware-the-share/index.html

159. Safe Online. Grantee Highlight – Safe Online [Internet]. [cited 2025 Nov 4]. Available from: https://safeonline.global/grantee-highlight/

160. Letourneau EJ, Schaeffer CM, Bradshaw CP, Ruzicka AE, Assini-Meytin LC, Nair R, et al. Responsible Behavior With Younger Children: Results From a Pilot Randomized Evaluation of a School-Based Child Sexual Abuse Perpetration Prevention Program. Child Maltreat [Internet]. 2024 Feb 1 [cited 2025 Sept 6];29(1):129–41. Available from: https://doi.org/10.1177/10775595221130737

161. Ruzicka AE, Assini-Meytin LC, Schaeffer CM, Bradshaw CP, Letourneau EJ. Responsible Behavior with Younger Children: Examining the Feasibility of a Classroom-Based Program to Prevent Child Sexual Abuse Perpetration by Adolescents. J Child Sex Abuse [Internet]. [cited 2025 Nov 7];30(4). Available from: https://www.prevention.global/resources/responsible-behavior-younger-children-examining-feasibility-classroom-based-program

162. Forum EEC. Cultural Adaptation and Evaluation of the RBYC Program in Germany: Towards Offender-Focused and School-Based Prevention of Child Sexual Abuse [Internet]. Preventing disease and ill health. 2025 [cited 2025 Sept 6]. Available from: https://euspr.hypotheses.org/2100

163. Schatz J, Deesawade R, Mosby W, Kavenagh M. Leaked: Understanding and Addressing Self-Generated Sexual Content Involving Young People in Thailand [Internet]. Evident & HUG Project: Bangkok; 2025 [cited 2025 Nov 4]. Available from: www.itsevident.org/_files/ugd/0bd10b_86d0e7f3921645f7bebc0fa399371860.pdf

164. Dodge A, Lockhart E. "Young People Just Resolve It in Their Own Group": Young People's Perspectives on Responses to Non-Consensual Intimate Image Distribution. Youth Justice J Natl Assoc Youth Justice. 2022 Dec;22(3):304–19.

165. Our story [Internet]. World Childhood Foundation - 25 Years. [cited 2025 Sept 27]. Available from: https://childhood.org/about-childhood/our-story/

166. The HUG Project - Protecting Thai children from sexual abuse and online sex trafficking [Internet]. The HUG Project. [cited 2025 Sept 22]. Available from: https://www.hugproject.org/

167. Evident | Translating evidence into action for social change [Internet]. Evident. [cited 2025 Sept 22]. Available from: https://www.itsevident.org

168. Deterring online child sexual abuse and exploitation: lessons from seven years of campaigning) - Lucy Faithfull Foundation [Internet]. [cited 2025 Sept 27]. Available from: https://www.lucyfaithfull.org.uk/research/deterring-online-child-sexual-abuse-and-exploitation-lessons-from-seven-years-of-campaigning/

169. ReDirection | Protect Children [Internet]. [cited 2025 Sept 22]. Available from: https://www.suojellaanlapsia.fi/en/redirection

170. Help Wanted. Help Wanted Prevention Intervention [Internet]. Help Wanted. [cited 2025 Nov 4]. Available from: https://staging.wp.helpwantedprevention.org/

171. Chatbots and Warning Messages - Innovations in the Fight Against Online Child Sexual Abuse [Internet]. Lucy Faithfull Foundation. [cited 2025 Sept 27]. Available from: https://www.lucyfaithfull.org.uk/research/chatbots-and-warning-messages-innovations-in-the-fight-against-online-child-sexual-abuse/

172. Rati. Meri Trustline [Internet]. Rati Foundation. [cited 2025 Nov 4]. Available from: https://ratifoundation.org/meri-trustline/

173. Internet Watch Foundation. IWF 2024: Meri Trustline – Supporting Children Facing Online Harms [Internet]. [cited 2025 Nov 4]. Available from: https://www.iwf.org.uk/annual-data-insights-report-2024/data-and-insights/meri-trustline/

174. UNICEF. Multidisciplinary Models of Care for Child Victims and Survivors of Sexual Abuse and Exploitation in the Digital Age | UNICEF [Internet]. [cited 2025 Nov 4]. Available from: https://www.unicef.org/documents/multidisciplinary-models-care-child-victims-and-survivors-sexual-abuse-and-exploitation

175. Prevention Global. Serving Youth Animation, Brieg, Infographic [Internet]. 2025 [cited 2025 Oct 29]. Available from: https://www.prevention.global/insight/serving-youth-animation-brief-infographic

176. Prevention Global. Serving Youth [Internet]. [cited 2025 Oct 29]. Available from: https://www.prevention.global/serving-youth

177. MyVoiceMySafety-global-poll-of-children.pdf [Internet]. [cited 2025 Sept 22]. Available from: https://www.weprotect.org/wp-content/uploads/MyVoiceMySafety-global-poll-of-children.pdf

178. ECPAT. Guidelines for ethical research on sexual exploitation involving children [Internet]. 2019 [cited 2025 Oct 29]. Available from: https://ecpat.org/guidelines-for-ethical-research/

179. Disrupting Harm: Conversations with Young Survivors about Online Child Sexual Exploitation and Abuse [Internet]. ECPAT. [cited 2025 May 1]. Available from: https://ecpat.org/resource/disrupting-harm-conversations-with-young-survivors-about-online-child-sexual-exploitation-and-abuse/

180. Luciana C. Assini-Meytin, McPhail I, Sun Y, Matthews B, Kaufman KL, Letourneau E. Child Sexual Abuse and Boundary Violating Behaviors in Youth Serving Organizations: National Prevalence and Distribution by Organizational Type. Child Maltreat [Internet]. 2024 [cited 2025 Oct 29];20(3):499–511. Available from: https://journals.sagepub.com/doi/10.1177/10775595241290765

181. Alliance WG. Health and wellbeing of frontline responders. 2025 [cited 2025 Sept 27]; Available from: https://www.weprotect.org/wp-content/uploads/Health-and-wellbeing-of-frontline-responders_May-2025.pdf

182. Towards digital safety by design for children | OECD [Internet]. [cited 2025 Sept 22]. Available from: https://www.oecd.org/en/publications/towards-digital-safety-by-design-for-children_c167b650-en.html

183. Tech Coalition | Child Safety Best Practices [Internet]. Tech Coalition. [cited 2025 May 1]. Available from: https://www.technologycoalition.org/knowledge-hub/child-safety-best-practices

184. Child Rights Impact Assessment: A Policy Tool for a Rights Respecting Digital Environment - Livingstone - 2025 - Policy & Internet - Wiley Online Library [Internet]. [cited 2025 Sept 22]. Available from: https://onlinelibrary.wiley.com/doi/10.1002/poi3.70008

185. UNICEF. Assessing child rights impacts in relation to the digital environment | UNICEF Child Rights and Business [Internet]. [cited 2025 Nov 4]. Available from: https://www.unicef.org/childrightsandbusiness/workstreams/responsible-technology/D-CRIA

186. Digital Futures Commission. Child Rights by Design - 5Rights Foundation & Digital Futures Commission [Internet]. Child Rights By Design | Digital Futures Commission. [cited 2025 Nov 4]. Available from: https://childrightsbydesign.5rightsfoundation.com/

187. Thorn & ATIH. Safety by Design for Generative AI: Preventing Child Sexual Abuse. 2024. Thorn Repository. Available at https://info.thorn.org/hubfs/thorn-safety-by-design-for-generative-AI.pdf.

188. Thorn. Safety by Design for responsible AI | Safer by Thorn [Internet]. Purpose-Built Trust and Safety Solutions | Safer by Thorn. 2025 [cited 2025 Nov 4]. Available from: https://safer.io/resources/safety-by-design-a-responsible-ai-framework/

189. Australian Government. Be Secure Quiz | eSafety Commissioner [Internet]. [cited 2025 Nov 4]. Available from: https://www.esafety.gov.au/educators/classroom-resources/be-secure/quiz

190. Human Mobile Devices. HMD Fuse | The phone that grows with your kids [Internet]. HMD - Human Mobile Devices. [cited 2025 Nov 4]. Available from: https://www.hmd.com/en_int/hmd-fuse

191. Apple Support. About Communication Safety on your child's Apple device [Internet]. Apple Support. [cited 2025 Nov 4]. Available from: https://support.apple.com/en-us/105069

192. Snapchat. Parents - Safeguards For Teens [Internet]. [cited 2025 Nov 4]. Available from: https://parents.snapchat.com/safeguards-for-teens

193. Google. Be Internet Awesome [Internet]. Be Internet Awesome. [cited 2025 Nov 4]. Available from: https://beinternetawesome.withgoogle.com/en-us

194. Lego. LEGO® - Code of conduct [Internet]. [cited 2025 Nov 4]. Available from: https://kids.lego.com/en-us/legal/kids-code-of-conduct

195. Instagram. Partner With Instagram to Keep Your Students Safe | About Instagram [Internet]. [cited 2025 Nov 4]. Available from: https://about.instagram.com/community/educators

196. Ngo VM, Gajula R, Thorpe C, Mckeever S. Discovering child sexual abuse material creators' behaviors and preferences on the dark web. Child Abuse Negl. 2024 Jan;147:106558.

197. Haluska R, Badovska M, Pleva M. Concept of Speaker Age Estimation Using Neural Networks to Reduce Child Grooming. Elektron Ir Elektrotechnika. 2024 Aug 26;30(4):61–7.

198. Thorn. Generative AI: Now is the Time for Safety By Design [Internet]. Thorn. 2023 [cited 2025 Nov 4]. Available from: https://www.thorn.org/blog/now-is-the-time-for-safety-by-design/

199. Tech Coalition. Insights to Action: Asia-Pacific Briefing on Combating OCSEA [Internet]. https://technologycoalition.org/. [cited 2025 Nov 4]. Available from: https://technologycoalition.org/news/insights-to-action-tech-coalition-asia-pacific-briefing-on-combating-ocsea/

200. National Center for Missing & Exploited Children. Take It Down [Internet]. Take It Down. [cited 2025 Nov 3]. Available from: https://takeitdown.ncmec.org/

201. Lantern 2024 Transparency Report [Internet]. https://technologycoalition.org/. [cited 2025 Aug 31]. Available from: https://technologycoalition.org/resources/lantern-2024-transparency-report/

202. U.K. Government. Online Safety Act: explainer [Internet]. GOV.UK. [cited 2025 Nov 4]. Available from: https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer

203. Fiji approves 1st national child safeguarding policy [Internet]. [cited 2025 Sept 22]. Available from: https://english.news.cn/asiapacific/20250822/3042a592ecb344bb8eaa4bd2bf0ebebf/c.html

204. G7 #BeBrave Scorecard Report 2025 [Internet]. Brave Movement. [cited 2025 Sept 27]. Available from: https://www.bravemovement.org/resources/g7-scorecard-2025

205. Global Online Safety Regulators Network. GOSRN Regulatory Index 2024 [Internet]. [cited 2025 Nov 3]. Available from: https://www.esafety.gov.au/sites/default/files/2024-10/GOSRN-Regulatory-Index-2024-final.pdf

206. Tracking the shifts: Age assurance in motion | IAPP [Internet]. [cited 2025 Sept 27]. Available from: https://iapp.org/news/a/tracking-the-shifts-age-assurance-in-motion

207. Taylor J. Not just under-16s: all Australian social media users will need to prove their age – and it could be complicated and time consuming. The Guardian [Internet]. 2025 Sept 1 [cited 2025 Sept 28]; Available from: https://www.theguardian.com/technology/2025/sep/02/under-16s-ban-how-hard-will-it-be-for-australian-social-media-users-to-prove-their-age

208. Department of Infrastructure T. Age assurance consumer research findings [Internet]. Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts; 2025 [cited 2025 Sept 27]. Available from: https://www.infrastructure.gov.au/department/media/publications/age-assurance-consumer-research-findings

209. Faverio MA and M. 81% of U.S. adults – versus 46% of teens – favor parental consent for minors to use social media [Internet]. Pew Research Center. 2023 [cited 2025 Sept 27]. Available from: https://www.pewresearch.org/short-reads/2023/10/31/81-of-us-adults-versus-46-of-teens-favor-parental-consent-for-minors-to-use-social-media/

210. International A. Social media ban: what is it and what will it mean for young people? [Internet]. Amnesty International Australia. 2024 [cited 2025 Sept 27]. Available from: https://www.amnesty.org.au/social-media-ban-explained/

211. VPNs top App Store charts as UK age verification kicks in [Internet]. 2025 [cited 2025 Sept 27]. Available from: https://www.bbc.com/news/articles/cn72ydj70g5o

212. African Union. African Union Child Online Safety and Empowerment Policy | African Union [Internet]. 2024 [cited 2025 Nov 3]. Available from: https://au.int/en/documents/20240521/african-union-child-online-safety-and-empowerment-policy

213. Commonwealth of Australia. Age Assurance Technology Trial [Internet]. Age Assurance Technology Trial. [cited 2025 Nov 3]. Available from: https://ageassurance.com.au/report/

214. Eltaher F, Gajula R, Miralles-Pechuán L, Thorpe C, McKeever S. The Digital Loophole: Evaluating the Effectiveness of Child Age Verification Methods on Social Media. Conf Pap [Internet]. 2025 Jan 1; Available from: https://arrow.tudublin.ie/scschcomcon/442

215. Evershed N, Nicholas J. Social media ban trial data reveals racial bias in age checking software: just how inaccurate is it? The Guardian [Internet]. 2025 Sept 18 [cited 2025 Sept 23]; Available from: https://www.theguardian.com/news/2025/sep/19/how-accurate-are-age-checks-for-australias-under-16s-social-media-ban-what-trial-data-reveals

216. School SL. The "Segregate-and-Suppress" Approach to Regulating Child Safety Online [Internet]. Stanford Law School. 2025 [cited 2025 Sept 28]. Available from: https://law.stanford.edu/publications/the-segregate-and-suppress-approach-to-regulating-child-safety-online/

217. Safe Online. Kenya launches groundbreaking training handbook to combat online child sexual exploitation and abuse [Internet]. [cited 2025 Nov 4]. Available from: https://safeonline.global/kenya-launches-groundbreaking-training-handbook-to-combat-online-child-sexual-exploitation-and-abuse/

218. Thorn. For Victim Identification [Internet]. Thorn. [cited 2025 Nov 3]. Available from: https://www.thorn.org/solutions/victim-identification/

219. Rigr AI. Video Summarisation Tool by Rigr AI [Internet]. Video Summarisation Tool by Rigr AI. [cited 2025 Nov 3]. Available from: https://www.vst.rigr.ai

220. Safe Online Report 2024 – Safe Online [Internet]. [cited 2025 Sept 22]. Available from: https://safeonline.global/safe-online-report-2024/

221. Canadian Framework For Trauma-Informed Response in Policing – Introduction | Barrie Police Service [Internet]. [cited 2025 Sept 27]. Available from: https://www.barriepolice.ca/cftirp-introduction/

222. Landry G. Mobilising the Financial Sector Against the Sexual Exploitation of Children. ECPAT;

223. AFP records spike in financial sextortion reports over the school holidays | Australian Federal Police [Internet]. 2023 [cited 2025 Sept 22]. Available from: https://www.afp.gov.au/news-centre/media-release/afp-records-spike-financial-sextortion-reports-over-school-holidays

224. It's Never Too Early - Early education Project Paradigm collaboration | ACCCE [Internet]. [cited 2025 Sept 22]. Available from: https://www.accce.gov.au/resources/parents-carers/its-never-too-early-early-education-project-paradigm-collaboration

225. Sextortion Campaign [Internet]. Available from: https://www.accce.gov.au/sites/default/files/2022-11/sextortion%20campaign%20video.mp4

226. Prevention Global. Making The Case | Prevention Global [Internet]. [cited 2025 Nov 3]. Available from: https://prevention.global/making-the-case

227. U.S. Government Accountability Office. Science & Tech Spotlight: Deepfakes [Internet]. 2025 [cited 2025 Nov 3]. Available from: https://www.gao.gov/assets/gao-20-379sp.pdf

228. JISC. Digital wellbeing [Internet]. Digital wellbeing. [cited 2025 Nov 3]. Available from: https://digitalcapability.jisc.ac.uk/what-is-digital-capability/digital-wellbeing/

229. Knodel M, Baker F, Kolkman O, Celi S, Grover G. Definition of End-to-end Encryption [Internet]. Internet Engineering Task Force; [cited 2025 Nov 3]. Report No.: draft-knodel-e2ee-definition-04. Available from: https://datatracker.ietf.org/doc/draft-knodel-e2ee-definition-04

230. INHOPE. What is generative AI? [Internet]. 2024 [cited 2025 Nov 3]. Available from: https://inhope.org/EN/articles/what-is-generative-ai

231. Overview of Perceptual Hashing Technology [Internet]. www.ofcom.org.uk. 2022 [cited 2025 Nov 3]. Available from: https://www.ofcom.org.uk/online-safety/safety-technology/overview-of-perceptual-hashing-technology

232. Know2Protect, US Department of Homeland Security. ONLINE ENTICEMENT INFORMATIONAL BULLETIN [Internet]. Available from: https://www.dhs.gov/sites/default/files/2025-01/25_0121_K2P_online-enticement.pdf

233. 'Self-generated' sexual material - WeProtect Global Alliance [Internet]. 2022 [cited 2025 May 1]. Available from: https://www.weprotect.org/issue/self-generated-sexual-material/

weprotect
Global Alliance

CPC
LEARNING
NETWORK

COLUMBIA | MAILMAN SCHOOL OF PUBLIC HEALTH