Conselho
da União Europeia

Bruxelas, 13 de fevereiro de 2026
(OR. en)

6361/26

FREMP 48
JAI 198
HYBRID 19
EDUC 47
JEUN 26
GENDER 13
TELECOM 67
CYBER 61
DISINFO 11
COPEN 43
AUDIO 20

NOTA DE ENVIO

de:	Secretária-geral da Comissão Europeia, com a assinatura de Martine DEPREZ, diretora
data de receção:	11 de fevereiro de 2026
para:	Thérèse BLANCHET, secretária-geral do Conselho da União Europeia
n.° doc. Com.:	COM(2026) 71 final
Assunto:	COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU, AO CONSELHO, AO COMITÉ ECONÓMICO E SOCIAL EUROPEU E AO COMITÉ DAS REGIÕES Plano de Ação contra a Ciberintimidação «Mais seguros em linha, mais fortes juntos»

Envia-se em anexo, à atenção das delegações, o documento COM(2026) 71 final.

Anexo: COM(2026) 71 final

COMISSÃO
EUROPEIA

Estrasburgo, 10.2.2026
COM(2026) 71 final

COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU, AO CONSELHO, AO COMITÉ ECONÓMICO E SOCIAL EUROPEU E AO COMITÉ DAS REGIÕES

Plano de Ação contra a Ciberintimidação

«Mais seguros em linha, mais fortes juntos»

1. Introdução

«Esta não é uma atividade beneficente. Mas os pais vivem diariamente com os riscos e danos dela decorrentes: ciberintimidação. Incentivo à automutilação. Predadores em linha. Algoritmos que criam dependência. Cabe-nos a nós proteger a nossa próxima geração.»

Presidente Ursula von der Leyen, discurso no evento de alto nível «Proteger as crianças na era digital» realizado em 2025

A transformação digital mudou radicalmente a sociedade. Proporciona vastas oportunidades para as crianças e os jovens desenvolverem as suas competências e criatividade. Atualmente, 97 % dos jovens da UE utilizam a Internet diariamente e, no caso dos jovens com idades compreendidas entre os 15 e os 24 anos, a principal fonte de informação são as plataformas de redes sociais (65 %). Juntamente com as ferramentas de inteligência artificial (IA), os jogos de vídeo, as aplicações de mensagens e as comunidades em linha, estabelecem ligações e interagem.

Mas estas plataformas também comportam riscos: exposição a predadores em linha, incentivo à automutilação, algoritmos que criam dependência, desafios perigosos em linha e ciberintimidação.

Os direitos fundamentais, incluindo os direitos das crianças, são essenciais para os valores da UE e têm de ser respeitados tanto em linha como fora de linha. As crianças e os jovens têm o direito de procurar informações, aprender, estabelecer ligações e tornar-se membros ativos da sociedade em segurança. Por conseguinte, as liberdades e as possibilidades do mundo digital têm de ser acompanhadas da nossa determinação em proteger e capacitar as crianças e os jovens. A promessa da era digital não pode ser comprometida por comportamentos que humilhem, excluam ou prejudiquem.

A ciberintimidação mina a confiança e prejudica a autoestima. Exclui as pessoas e limita o seu potencial. Compromete a nossa ambição comum de uma Europa digital dinâmica e inclusiva para as nossas crianças e jovens.

As redes sociais são um dos principais canais através dos quais as crianças e os adolescentes são expostos à ciberintimidação, havendo cada vez mais indícios de que a sua exposição a conteúdos em linha inadequados está a ter efeitos duradouros e prejudiciais. A UE já dispõe de um quadro jurídico e político abrangente para proteger e capacitar as crianças em linha, sendo o Regulamento dos Serviços Digitais (RSD) o principal instrumento existente neste domínio.

Tal como anunciado no discurso sobre o estado da União de 2025, a presidente Ursula von der Leyen está a procurar aconselhamento especializado sobre a aplicação de restrições de idade nas redes sociais na Europa à luz dos riscos em linha, estando previstas recomendações até ao verão de 2026. Vários Estados-Membros estão a ponderar a adoção de medidas com vista a introduzir idades mínimas obrigatórias para o acesso às redes sociais e requisitos para o consentimento e o controlo parental. Isto inclui o alinhamento dos limites mínimos de idade para o acesso às redes sociais com a idade de consentimento digital, a obrigatoriedade da privacidade por defeito para os menores e a criação de soluções para a verificação da idade de forma anónima.

Uma abordagem europeia coordenada dos limites mínimos de idade asseguraria a igualdade de proteção de todas as crianças europeias e evitaria a fragmentação jurídica no mercado único digital. O painel de peritos abrirá caminho a uma abordagem europeia coordenada e potencialmente legislativa dos limites mínimos de idade e a uma campanha de sensibilização baseada em dados concretos, capacitando os progenitores a assumirem o controlo efetivo do acesso dos seus filhos aos conteúdos em linha.

O Conselho Consultivo da Presidente sobre a Juventude também partilhou com a presidente da Comissão as perspetivas dos jovens sobre esta questão. A Comissão está a testar com os Estados-Membros uma solução de verificação da idade que seja fácil de utilizar, proteja a privacidade e estabeleça uma «norma de referência» para a verificação da idade em linha. O Parlamento Europeu defendeu a fixação de uma idade mínima digital de 16 anos, harmonizada a nível da UE, para o acesso às redes sociais, às plataformas de partilha de vídeos e aos companheiros de IA, permitindo simultaneamente o acesso dos jovens com idades compreendidas entre os 13 e os 16 anos com o consentimento dos progenitores.

A Comissão lançará igualmente um inquérito à escala da UE para dar início a um debate baseado em dados concretos sobre o impacto das redes sociais e da exposição excessiva aos ecrãs no bem-estar e na saúde mental dos jovens.

Quando as crianças estão em linha, a ciberintimidação continua a constituir uma ameaça significativa que exige uma resposta coordenada a nível nacional e da UE. A responsabilidade que incumbe às plataformas em linha de garantir a segurança desde a conceção é primordial. O combate à ciberintimidação exige a colaboração a todos os níveis de governação, incluindo as autoridades reguladoras e responsáveis pela aplicação da lei, bem como uma abordagem global da sociedade, que envolva os progenitores, os profissionais, os educadores, a sociedade civil e os próprios jovens.

Tal como anunciado nas Orientações políticas da Comissão para 2024-2029, a presente comunicação estabelece um plano de ação específico para combater firmemente a tendência crescente de comportamentos abusivos em linha. O plano centra-se principalmente nas crianças e nos jovens, tendo igualmente em conta a crescente vulnerabilidade de determinados grupos. No entanto, muitas das ações propostas ajudarão a combater a ciberintimidação junto da população em geral.

A Comissão utilizará todos os instrumentos à sua disposição para complementar o RSD, assegurando que as plataformas digitais assumam plenamente a sua responsabilidade pela deteção e combate à ciberintimidação. Apoiará todos os Estados-Membros na adoção das boas práticas disponíveis na UE, a fim de maximizar a eficácia do seu combate à ciberintimidação, e intensificará os esforços para chegar a todos os segmentos da sociedade com informações e sensibilizar para o que é a ciberintimidação, como pode ser prevenida e como as vítimas podem ser apoiadas.

Com o presente plano de ação, a Comissão convida os Estados-Membros, as autoridades regionais e locais, as plataformas em linha, a sociedade civil, os estabelecimentos de ensino, as famílias e as próprias crianças e jovens a empenharem-se num esforço comum: garantir que o espaço digital seja seguro, respeitador, inclusivo e solidário. A Comissão propõe que a nossa União se una em prol do bem-estar mental e da dignidade de todas as crianças e jovens.

2. Ciberintimidação: o problema

A ciberintimidação afeta crianças em todo o mundo: 18,3 % das crianças no mundo já foram vítimas de ciberintimidação através de mensagens instantâneas, publicações nas redes sociais, mensagens de correio eletrónico ou mensagens de texto. A ciberintimidação não é praticada apenas através de mensagens de texto, mas também através de conteúdos audiovisuais, como fotografias ou vídeos, partilhados em linha.

Na Europa, cerca de uma em cada seis crianças com idades compreendidas entre os 11 e os 15 anos afirma ter sido vítima de ciberintimidação e cerca de uma em cada oito admitiu ter praticado atos de ciberintimidação contra outras crianças. Entre 2018 e 2022, o número de adolescentes vítimas de ciberintimidação aumentou um quarto no caso dos rapazes e quase um quarto no caso das raparigas. Nos últimos cinco anos, a ciberintimidação tem sido sistematicamente o principal motivo de contacto das linhas de apoio dos Centros Internet Segura.

Os 6 343 inquiridos com idades compreendidas entre os 12 e os 17 anos consultados no âmbito do presente plano de ação referiram uma exposição generalizada à ciberintimidação: uma em cada quatro crianças e adolescentes com idades compreendidas entre os 12 e os 17 anos já foi vítima direta de ciberintimidação e mais de uma em cada três testemunharam a prática de atos de ciberintimidação.

2.1 O que é a ciberintimidação?

As tecnologias digitais aumentaram as oportunidades de ligação, mas também intensificaram os riscos em linha, como a exclusão social, os crimes de ódio, o assédio, a humilhação e os abusos, que podem transcender as fronteiras físicas e persistir permanentemente.

Para efeitos do presente plano de ação, a Comissão tenciona promover **um entendimento comum da ciberintimidação**:

A ciberintimidação refere-se a **comportamentos realizados através de tecnologias digitais, com a intenção ou o efeito principal de humilhar, excluir socialmente, abusar, assediar ou prejudicar, de forma repetida ou contínua, em especial crianças ou jovens**.

A repetição é considerada uma característica fundamental da intimidação e da ciberintimidação. Diz respeito aos efeitos persistentes sobre a vítima, que também pode recear que um acontecimento único possa ser repetidamente partilhado em linha, prolongando o trauma e conduzindo a uma revitimização sem um envolvimento direto adicional do autor do crime.

O desequilíbrio de poder é fundamental para a intimidação, mas pode manifestar-se de forma diferente em linha. Na intimidação tradicional, o desequilíbrio de poder decorre frequentemente da força física, do estatuto social ou das normas do grupo. Na ciberintimidação, decorre também de níveis desiguais de influência digital, competências digitais, acesso à tecnologia ou controlo sobre os conteúdos.

A ciberintimidação é cada vez mais difícil de combater, uma vez que pode ocorrer em dispositivos privados a qualquer momento, em qualquer lugar, sem a presença física do autor do crime. Além disso, ocorre também em canais não acessíveis ao público.

As formas mais comuns de ciberintimidação incluem tecer comentários maldosos ou ofensivos, difundir rumores em linha ou partilhar publicações embaraçosas ou humilhantes.

O anonimato, o vasto alcance do público e a capacidade de enviar mensagens privadas às pessoas a qualquer momento amplificam os danos causados pela intimidação tradicional. Além disso, os ambientes digitais promovem a desvinculação moral, a diminuição da empatia e a desinibição em linha, reduzindo os obstáculos à agressão em linha.

Os conteúdos nocivos podem permanecer em linha indefinidamente. Podem ser continuamente acedidos e partilhados novamente, ou tornados virais, o que amplifica os danos, causa revitimização e dificulta a recuperação. Estes fatores têm de ser tidos em conta na prestação de um apoio eficaz. Esta situação alarga o público potencial, permitindo uma agressão contínua entre espaços físicos e em linha ou vice-versa.

A rápida evolução digital em curso significa que os ambientes e as ferramentas utilizados para infligir danos estão em constante mudança. Para assegurar flexibilidade, devem ser utilizadas as tecnologias mais recentes para os detetar e combater.

Em especial, embora a IA possa ajudar a detetar a ciberintimidação, a adoção crescente da IA, especificamente da IA generativa, e a sua integração em aplicações e serviços em linha aumentam os riscos de ciberintimidação e as ferramentas utilizadas para praticar atos de ciberintimidação ou até criam novos riscos e ferramentas. Por exemplo, as falsificações profundas têm vindo a aumentar e conduzem cada vez mais a abusos de falsificações profundas sexualmente explícitas, que visam maioritariamente mulheres e raparigas, incluindo em casos de ciberintimidação, e que passam de comportamentos nocivos a infrações penais quando se trata da criação de imagens que constituem abuso sexual de crianças ou ciberviolência baseada no género. Tal introduz uma dimensão adicional dos danos que não só prejudica a reputação, mas também, tal como outros comportamentos de ciberintimidação, pode conduzir a traumas psicológicos, sublinhando a urgência de acompanhar e combater estes riscos emergentes a nível da UE.

A ciberintimidação e os crimes de ódio podem sobrepor-se quando a ciberintimidação é motivada pelo ódio ou incita à violência e ao ódio e visa pessoas por referência a determinadas características protegidas. A Decisão-Quadro 2008/913/JAI do Conselho exige que os Estados-Membros criminalizem a incitação pública à violência ou ao ódio contra um grupo de pessoas ou os seus membros, definido por referência à raça, cor, religião, ascendência ou origem étnica. Exige igualmente que os Estados-Membros assegurem a aplicação de sanções adicionais por infrações penais cometidas com motivação racista ou xenófoba.

A ciberintimidação pode sobrepor-se ao abuso sexual de crianças na aceção da Diretiva 93/2011 relativa à luta contra o abuso sexual e a exploração sexual de crianças e a pornografia infantil.

A Diretiva (UE) 2024/1385 relativa ao combate à violência contra as mulheres e à violência doméstica exige que os Estados-Membros assegurem que a incitação à violência ou ao ódio em linha com base no género seja punível como crime. Além disso, criminaliza outros crimes de ciberviolência que ocorrem frequentemente no contexto da ciberintimidação: a partilha não consensual de material íntimo ou manipulado, a ciberperseguição e o ciberassédio. A diretiva inclui igualmente disposições que permitem a supressão imediata de material ilegal relacionado com a ciberviolência.

2.2 Grupos em risco de ciberintimidação

A ciberintimidação é particularmente prevalecente entre **as crianças e os adolescentes em idade escolar**, especialmente à medida que a sua atividade em linha aumenta.

As raparigas e as mulheres jovens estão expostas à intimidação de natureza sexista e misógina, sendo desproporcionadamente afetadas, por exemplo, pela partilha não consensual de imagens íntimas e falsificações profundas sexualmente explícitas.

Os grupos vulneráveis estão desproporcionadamente expostos à ciberintimidação, uma vez que esta pode ser dirigida a uma pessoa com base na presunção da sua pertença a esses grupos.

As crianças de agregados familiares com baixos rendimentos estão mais expostas à ciberintimidação do que os seus pares.

As crianças e os jovens com deficiência sofrem níveis mais elevados de vitimização em linha, incluindo violência sexual e de género. Alguns chegam mesmo a afastar-se dos espaços digitais devido a abusos constantes.

As minorias étnicas e religiosas, os migrantes e os refugiados enfrentam riscos elevados de intimidação racista ou discriminatória. Por exemplo, os ciganos e outras minorias raciais ou étnicas estão particularmente expostos ao assédio em linha e ao discurso ilegal de incitação ao ódio associado à exclusão sistémica, e 90 % dos europeus judeus afirmaram ter sido vítimas de antissemitismo em linha no último ano.

Entre as **pessoas LGBTIQ+,** 63 % já se depararam frequentemente com conteúdos violentos em linha contra a comunidade LGBTIQ+. Além disso, 11 % afirmaram que alguém publicou comentários ofensivos ou ameaçadores sobre elas na Internet no último ano, e dois terços foram vítimas de ridicularização ou assédio durante o seu período escolar.

As ações apresentadas no presente plano de ação contribuirão para combater a ciberintimidação de qualquer vítima. As considerações em matéria de igualdade acima descritas serão tidas em conta na execução, a fim de reforçar o impacto das ações.

2.3 O impacto da ciberintimidação

As consequências da ciberintimidação podem ser graves e duradouras, tanto para as pessoas como para a sociedade em geral. A curto prazo, a ciberintimidação pode ser um primeiro passo para a prática de crimes ou abusos mais graves, incluindo o abuso sexual.

As vítimas de ciberintimidação enfrentam um risco acrescido de ansiedade, depressão, solidão, automutilação e comportamento suicida, sendo igualmente mais propensas a problemas comportamentais, incluindo comportamentos de resposta nocivos. Além disso, as pessoas que são vítimas de ciberintimidação podem tornar-se, elas próprias, autoras de atos de ciberintimidação, quanto mais não seja numa tentativa de escapar ao seu papel de vítimas. Tal exige uma resposta cuidadosa e adaptada às crianças.

A ciberintimidação pode também prejudicar o desempenho académico, o bem-estar dos alunos e o ambiente escolar. Esta situação pode ter consequências a longo prazo para os percursos educativos e profissionais, bem como para o bem-estar geral e a satisfação com a vida dos estudantes.

Por conseguinte, o impacto nas crianças e nos jovens pode ter consequências de grande alcance para a sociedade, agravando as desigualdades existentes.

3. O caminho a seguir

É necessária uma resposta mais sólida, coerente e coordenada da UE à ciberintimidação, que reforce os esforços envidados em matéria de prevenção e literacia digital e melhore e simplifique a denúncia e o apoio às vítimas em toda a União. A nossa visão é a de uma Europa em que todas as crianças e jovens possam crescer sem ser vítimas de ciberintimidação, protegidos na sua dignidade e capacitados para prosperar num mundo digital que respeite os valores europeus. Para o efeito, o presente plano de ação assenta em três pilares interligados: uma abordagem coordenada a nível da UE, prevenção e sensibilização, e denúncia e apoio.

Este apelo à ação é apoiado pela opinião pública: mais de nove em cada 10 europeus afirmam que é urgente que as autoridades públicas tomem medidas para proteger as crianças da ciberintimidação. A consulta pública que apoia o presente plano revelou um forte apoio aos programas de literacia digital e de criação de empatia nas escolas e na formação de professores, bem como à melhoria das ferramentas de denúncia e dos serviços de apoio às vítimas.

3.1 Pilar I: Uma abordagem coordenada a nível da UE em matéria de proteção

A Comissão fará pleno uso dos instrumentos políticos e jurídicos existentes e identificará oportunidades para combater a ciberintimidação no âmbito de iniciativas futuras. Além disso, **os Estados-Membros são convidados a traduzir objetivos comuns em medidas nacionais eficazes e a criar um ecossistema integrado e funcional para combater a ciberintimidação**.

O RSD continua a ser fundamental para os esforços de aplicação da lei, exigindo que os fornecedores de plataformas em linha acessíveis a menores assegurem um elevado nível de privacidade, segurança e proteção dos menores no seu serviço.

Além disso, as orientações no âmbito do RSD sobre a proteção dos menores em linha estabelecem medidas que os fornecedores de plataformas em linha devem adotar para cumprir essa obrigação, incluindo medidas adequadas destinadas a reduzir o risco de os menores serem expostos a conteúdos nocivos, como a conceção de sistemas de recomendação no interesse

superior dos menores, ou a comportamentos nocivos, incluindo riscos relacionados com o contacto decorrentes de interações com os pares. Para proteger as vítimas de ciberintimidação, as orientações incluem ainda medidas de controlo e capacitação dos utilizadores, mecanismos de denúncia adaptados às crianças e ferramentas de reclamação, bem como a moderação de conteúdos nas línguas oficiais do Estado-Membro em que o serviço é prestado. O RSD exige igualmente que os fornecedores de plataformas em linha criem mecanismos de fácil acesso e utilização que permitam a todos os utilizadores, incluindo menores, denunciar conteúdos ilegais, por exemplo, determinadas formas de discurso ilegal de incitação ao ódio ou material com imagens de abusos sexuais de crianças. Dependendo da legislação nacional, determinadas formas de ciberintimidação também podem ser ilegais. Os prestadores têm de tomar decisões imediatas após a receção de tais notificações.

O presente plano de ação servirá de base à próxima revisão e atualização das orientações no âmbito do RSD sobre a proteção dos menores em linha. Em especial, as orientações poderão ajudar os fornecedores de plataformas em linha a conceber ferramentas de denúncia mais eficientes, por exemplo, no que diz respeito à sua visibilidade, acessibilidade técnica e regime linguístico, e a utilizar tecnologias eficazes para prevenir a exposição à ciberintimidação. As orientações poderão também ajudar os fornecedores a conceber medidas adequadas para reagir às notificações dos menores, por exemplo, apoiando os utilizadores no armazenamento de informações que possam servir de elementos de prova.

O RSD prevê igualmente a possibilidade de recorrer a «sinalizadores de confiança», entidades especializadas cujas notificações têm de ser tratadas com prioridade. Estas disposições podem ser utilizadas para combater a ciberintimidação, contribuindo os sinalizadores de confiança para combater a difusão de conteúdos ilegais relacionados com ciberintimidação. A Comissão emitirá orientações sobre sinalizadores de confiança que ajudarão a clarificar o papel dos mesmos no combate aos conteúdos ilegais, incluindo a ciberintimidação ilegal. Essas orientações ajudarão igualmente a clarificar as obrigações dos fornecedores de plataformas em linha no que diz respeito às notificações apresentadas por sinalizadores de confiança.

A ciberintimidação também pode ocorrer através de conteúdos audiovisuais em linha. A Diretiva Serviços de Comunicação Social Audiovisual estabelece requisitos gerais para proteger os menores, em especial em linha, de conteúdos nocivos suscetíveis de prejudicar o seu desenvolvimento físico, mental ou moral. Tal inclui conteúdos que constituem ciberintimidação. A Diretiva Serviços de Comunicação Social Audiovisual exige que as plataformas de partilha de vídeos tomem medidas adequadas para evitar que os menores acedam a conteúdos nocivos, através da inclusão de normas relativas aos conteúdos dos meios de comunicação social nos termos e condições ou de sistemas de controlo parental e de classificação de conteúdos. Além disso, os Estados-Membros têm a obrigação de proteger a dignidade humana aquando da aplicação da Diretiva Serviços de Comunicação Social Audiovisual. A avaliação e a revisão em curso da diretiva avaliarão a eficácia com que as plataformas de partilha de vídeos aplicaram estas regras e se é necessário fazer mais para proteger os menores de conteúdos nocivos em linha, nomeadamente no que diz respeito à ciberintimidação, e em consonância com o RSD.

O Regulamento da Inteligência Artificial (Regulamento IA) proíbe os sistemas de IA que manipulam ou enganam pessoas explorando vulnerabilidades associadas à sua idade, a fim de

distorcer o seu comportamento causando danos significativos. Estas proibições podem prevenir a ciberintimidação. A Comissão adotou orientações sobre as práticas de IA proibidas, a fim de facilitar a aplicação coerente e eficaz em toda a União. O Regulamento IA estabelece igualmente requisitos de transparência, incluindo a obrigação de informar os utilizadores quando estes interagem com a IA e de identificar claramente os conteúdos gerados ou manipulados por IA, como as falsificações profundas, a fim de evitar o engano.

Além disso, estas políticas devem ser complementadas pela recolha de dados sobre a ciberintimidação, que é atualmente incoerente, dificultando uma compreensão abrangente das tendências em todos os Estados-Membros. Em resposta ao apelo decorrente da consulta pública, a Comissão facilitará a recolha de dados comparáveis e coerentes sobre a ciberintimidação em toda a UE, por exemplo, fornecendo orientações, como um quadro comum para a recolha de dados e indicadores, e lançando inquéritos à escala da UE através da plataforma Internet Melhor para as Crianças, em cooperação com outros mecanismos de participação das crianças e dos jovens. Serão disponibilizados recursos adequados para permitir que a rede de Centros Internet Segura assuma estas tarefas adicionais e assegure a continuidade a longo prazo deste trabalho.

A Comissão irá:

1. Aumentar a tónica colocada no combate à ciberintimidação na **revisão das orientações no âmbito do RSD sobre a proteção dos menores**, em especial no que diz respeito a medidas destinadas a prevenir ainda mais a exposição a conteúdos nocivos e a melhorar os sistemas de denúncia das plataformas em linha — previsto para **2026**;

2. **Adotar orientações no âmbito do RSD sobre sinalizadores de confiança**, que ajudarão a clarificar o papel dos mesmos no combate aos conteúdos ilegais, como a ciberintimidação ilegal — **até ao segundo trimestre de 2026**;

3. Avaliar formas de combater a ciberintimidação em plataformas de partilha de vídeos na **avaliação em curso da Diretiva Serviços de Comunicação Social Audiovisual e na sua revisão — até ao terceiro trimestre de 2026**;

4. **Apoiar a aplicação efetiva das disposições do Regulamento IA relativas às práticas de IA proibidas**, nomeadamente quando são utilizadas para efeitos de ciberintimidação, através da coordenação no âmbito do Comité para a Inteligência Artificial e das indicações fornecidas nas orientações da Comissão sobre as práticas de IA proibidas — **a partir do terceiro trimestre de 2026**;

5. **Facilitar a aplicação efetiva das obrigações de transparência do Regulamento IA, nomeadamente através de um código de práticas sobre a marcação e rotulagem de conteúdos gerados por IA**, que visa apoiar o cumprimento das obrigações de transparência do Regulamento IA relacionadas com a marcação e rotulagem de conteúdos gerados por IA, incluindo os utilizados para efeitos de ciberintimidação — **a partir do terceiro trimestre de 2026**.

Os Estados-Membros são convidados a:

1. Elaborar **planos nacionais abrangentes de luta contra a intimidação, incluindo a ciberintimidação**, beneficiando do apoio da Rede Europeia dos Direitos da Criança, em consonância com a Comunicação e a Recomendação da Comissão sobre sistemas integrados de proteção das crianças;

2. Utilizar o entendimento comum da ciberintimidação apresentado no presente plano de ação para **recolher dados coerentes e comparáveis sobre a ciberintimidação**, objetivo facilitado pelo apoio prestado pela Comissão através da rede de Centros Internet Segura e da plataforma Internet Melhor para as Crianças, e trabalhar em conjunto no sentido de estabelecer normas comuns para combater a ciberintimidação em toda a UE.

3.2 Pilar II: Prevenção e sensibilização

A melhor forma de combater a ciberintimidação é agir antes da ocorrência de incidentes nocivos. A prevenção da ciberintimidação exige práticas digitais saudáveis desde tenra idade. Significa dotar as crianças, os jovens e os adultos das competências e da confiança necessárias que lhes permitam falar sobre os riscos em linha e reconhecê-los. É igualmente importante abordar as atitudes subjacentes que podem conduzir a comportamentos nocivos em linha.

Para serem eficazes, os esforços de prevenção têm de envolver as testemunhas, os pares, os autores dos crimes, os progenitores, os cuidadores, os educadores e a comunidade escolar em geral, com o apoio de todos os intervenientes pertinentes, em especial das organizações da sociedade civil. Este argumento foi apoiado por 62 % dos inquiridos na consulta pública, que salientaram a necessidade de apoiar a formação profissional dos educadores, das autoridades responsáveis pela aplicação da lei e dos assistentes sociais.

As iniciativas de prevenção e sensibilização devem também ter lugar em ambientes de aprendizagem informal e não formal, como centros de juventude, clubes desportivos e contextos comunitários, onde as crianças e os jovens passam grande parte do seu tempo. Essas iniciativas devem também integrar a prevenção e o combate a todas as formas de discriminação, em sinergia com as estratégias da UE para a igualdade.

A educação digital e a literacia digital são cada vez mais necessárias para navegar no mundo em linha de forma segura e responsável. Informar as crianças e os jovens sobre a importância de serem respeitadores e responsáveis nos ambientes digitais pode reduzir os casos de danos intencionais ou não intencionais. Esta é também uma medida preventiva prevista na Diretiva Combate à Violência contra as Mulheres e à Violência Doméstica.

As crianças e os jovens, incluindo aqueles com necessidades especiais, com deficiência ou em situações vulneráveis, devem participar ativamente na conceção e realização de atividades de sensibilização que capacitem, sejam inclusivas e acessíveis e quebrem o silêncio em torno da ciberintimidação.

A Comissão disponibilizará uma série de instrumentos de prevenção e sensibilização a nível da UE, desenvolvidos em parceria com crianças e jovens, progenitores, educadores, profissionais de saúde mental e Estados-Membros, bem como organizações da sociedade civil.

No âmbito do Plano de Ação para a Educação Digital (2021-2027), a Comissão Europeia atualizará as suas Orientações para professores e educadores sobre o combate à desinformação e a promoção da literacia digital através da educação e da formação. Além disso, tal como anunciado na Comunicação sobre o Escudo Europeu da Democracia, as atualizações refletirão a evolução da IA e das redes sociais e incluirão material didático e atividades sobre a ciberintimidação, prestando atenção à inclusão e à diversidade. A Comissão Europeia desenvolverá igualmente um quadro de competências em matéria de cidadania da UE, juntamente com orientações para reforçar a educação para a cidadania nas escolas.

Além disso, a literacia digital, a prevenção da ciberintimidação e o bem-estar digital serão domínios prioritários no Roteiro sobre o Futuro da Educação e das Competências Digitais 2030. O roteiro para 2030 terá por objetivo assegurar que os jovens sejam apoiados na criação de hábitos em linha saudáveis e informados sobre a utilização responsável de dispositivos digitais, tanto dentro como fora da sala de aula.

Este trabalho em matéria de literacia digital baseia-se em iniciativas que a Comissão está a executar através do programa Erasmus+ e do Corpo Europeu de Solidariedade, da Plataforma de Educação Escolar Europeia e da geminação eletrónica. No contexto da Plataforma de Educação Escolar Europeia, a Comissão garantirá uma melhor e permanente visibilidade de todos os materiais úteis para as escolas sobre intimidação, incluindo a ciberintimidação. A partir do convite à apresentação de propostas Erasmus+ de 2026, o bem-estar na escola será reforçado para melhor apoiar, acompanhar e incentivar projetos que abordem a intimidação e a ciberintimidação.

A rede da UE de prevenção do abuso sexual de crianças ajudará a promover a educação e a sensibilização das crianças para o abuso sexual de crianças, incluindo a ponderação de iniciativas destinadas a ajudar a evitar que os casos de ciberintimidação evoluam para comportamentos criminosos (por exemplo, difusão de material com imagens de abusos sexuais de crianças). Além disso, a prevenção da ciberintimidação será igualmente tida em conta no próximo plano de ação da UE para a proteção das crianças contra a criminalidade. O plano de ação procurará dar uma resposta coerente e abrangente aos vários riscos que as crianças enfrentam em relação à criminalidade, tanto em linha como fora de linha.

A plataforma Internet Melhor para as Crianças e a sua rede de Centros Internet Segura fornecem ferramentas de apoio às crianças, aos progenitores, aos educadores e aos profissionais a nível da UE (plataforma Internet Melhor para as Crianças) e nacional (Centros Internet Segura). Estes recursos serão alargados para reforçar as capacidades, chegar a mais partes interessadas e responder aos novos desafios da ciberintimidação.

Uma vez que as escolas desempenham um papel fundamental na prevenção da ciberintimidação, serão realizadas atividades de sensibilização com o apoio dos Centros Internet Segura e da plataforma Internet Melhor para as Crianças, a começar pela campanha anual «Regresso à Escola» no início de cada novo ano letivo, a fim de dotar os professores e

as crianças de materiais de formação, ferramentas e informações sobre como prevenir e denunciar a ciberintimidação.

Os recursos e a formação em matéria de ciberintimidação para a educação não formal e informal serão reforçados através de plataformas europeias. Entre estas incluem-se o Portal Europeu da Juventude, o balcão único para sensibilizar e promover oportunidades para os jovens, a Plataforma de Educação Escolar Europeia, o ponto de encontro para a comunidade educativa escolar, e o Espaço de Aprendizagem, que disponibiliza aos professores e profissionais da educação recursos e conjuntos de ferramentas sobre as iniciativas da UE.

Eventos como a Semana Europeia da Juventude e a Semana Europeia do Desporto facilitam o envolvimento numa série de temas, incluindo o combate à ciberintimidação. O grupo do método aberto de coordenação para o combate ao discurso de ódio no desporto, criado no contexto do plano de trabalho da UE para o desporto, está a elaborar recomendações para os Estados-Membros e as partes interessadas para o ambiente desportivo em geral, incluindo em linha. O seu relatório está previsto para o final de 2026 e incluirá recomendações para combater a ciberintimidação.

A Comissão irá:

6. **Abordar a ciberintimidação** na **atualização das Orientações para professores e educadores sobre o combate à desinformação e a promoção da literacia digital** através da educação e da formação — **até ao segundo trimestre de 2026**;

7. **Reforçar a educação para a cidadania nas escolas** através de um quadro de competências e orientações em matéria de cidadania da UE — **em 2027**;

8. **Reforçar** as competências digitais, **a prevenção da ciberintimidação** e o bem-estar digital através do **Roteiro sobre o Futuro da Educação e das Competências Digitais 2030 — até ao terceiro trimestre de 2026**;

9. Contribuir para a **prevenção da ciberintimidação** no próximo **plano de ação da UE para a proteção das crianças contra a criminalidade — até ao terceiro trimestre de 2026**;

10. **Alargar os recursos e a formação em matéria de ciberintimidação** às escolas e à educação não formal e informal, acessíveis às pessoas com deficiência, através da plataforma Internet Melhor para as Crianças, dos Centros Internet Segura, do Portal Europeu da Juventude e da Plataforma de Educação Escolar Europeia — **a partir do segundo trimestre de 2026**;

11. Apoiar o grupo do método aberto de coordenação para o combate ao discurso de ódio no desporto no seu trabalho sobre **recomendações para combater a ciberintimidação no ambiente desportivo** — relatório a apresentar até ao **quarto trimestre de 2026**.

Os Estados-Membros são convidados a:

3. Reforçar a prevenção e a identificação precoce da ciberintimidação com **orientações claras e formação para as partes interessadas**, como educadores, cuidadores e profissionais que trabalham com crianças em diferentes domínios (por exemplo, saúde, desporto, justiça, aplicação da lei);

4. **Reforçar a participação das crianças** na conceção de políticas e na aplicação de medidas para o bem-estar das crianças.

3.3 Pilar III: Denúncia e apoio abrangente

As vítimas de ciberintimidação têm de dispor de canais claros, fiáveis e acessíveis para denunciar abusos e obter ajuda, incluindo para ciberintimidação através de mensagens privadas. Para serem eficazes, os esforços de apoio têm de ir além da prestação de ajuda apenas às vítimas de ciberintimidação e chegar também às testemunhas, aos autores dos crimes, aos progenitores, aos cuidadores, aos educadores e à comunidade escolar em geral.

A Comissão promoverá possibilidades coerentes de denúncia e apoio às vítimas à escala da UE. A denúncia deve conduzir rapidamente a um apoio multidisciplinar, tanto em linha como fora de linha. Deve envolver todas as autoridades competentes a todos os níveis, intervenientes privados, organizações da sociedade civil, bem como os progenitores, os cuidadores, e as próprias crianças e jovens.

Com base nas informações recolhidas através de várias consultas específicas, **a Comissão apoiará a implantação de uma aplicação de segurança em linha em todos os Estados-Membros**, com base em modelos nacionais de práticas bem-sucedidas já existentes, como a aplicação francesa 3018. A aplicação proporcionará uma ferramenta segura, convivial e confidencial que permitirá às crianças e aos jovens:

i. **denunciar facilmente a ciberintimidação** a uma **linha de apoio**,

ii. **armazenar e transmitir provas de forma segura**, em consonância com os quadros jurídicos nacionais e

iii. receber **assistência personalizada através de encaminhamentos coordenados**, por exemplo, para as autoridades responsáveis pela aplicação da lei, os serviços de educação e os serviços de proteção de menores.

A Comissão apoiará os Estados-Membros, sempre que necessário e pertinente:

i. na **adaptação da aplicação ao contexto e às necessidades nacionais** (por exemplo, tradução, questões relacionadas com a marca, ligação aos serviços nacionais pertinentes de apoio e plataformas de denúncia) e na disponibilização de funcionalidades como a denúncia segura, a preservação de provas em consonância com o direito nacional e a garantia da confidencialidade,

ii. na **garantia da interoperabilidade** com as infraestruturas e os sistemas de apoio existentes e

iii. no **apoio à promoção** da adoção da aplicação entre os Estados-Membros, os utilizadores e as plataformas em linha.

As plataformas em linha continuarão a ser responsáveis pela criação de mecanismos de denúncia eficazes. Tal pode corresponder a uma das medidas adotadas para assegurar o cumprimento das obrigações decorrentes do RSD em matéria de proteção de menores. Em complemento destes esforços, a aplicação será disponibilizada às plataformas em linha para integração nas suas ferramentas de denúncia e de apoio aos utilizadores, nomeadamente através de interfaces de programação de aplicações (IPA), tornando a denúncia e a resposta eficientes em termos de recursos e eficazes.

O êxito da aplicação depende da disponibilidade do apoio e do acompanhamento por parte das autoridades nacionais. Os Estados-Membros desempenharão um papel importante para garantir que a denúncia através da aplicação seja apoiada por um apoio fora de linha coordenado (por exemplo, apoio jurídico, social, psicológico e educativo), bem como na comunicação dos benefícios da aplicação. A aplicação visará criar sinergias com mecanismos de denúncia bem estabelecidos nos Estados-Membros para denunciar material com imagens de abusos sexuais de crianças e violência contra as mulheres em linha, bem como com linhas de apoio nacionais, internacionais e da UE, nomeadamente linhas de apoio às crianças (116 111) e linhas diretas para crianças desaparecidas (116 000).

A Comissão adotará a próxima Estratégia da UE sobre os Direitos das Vítimas em 2026, a fim de complementar as regras da UE com medidas não legislativas. A estratégia promoverá estruturas de apoio específico (por exemplo, exames médicos e apoio emocional e psicológico) e serviços de proteção dirigidos às crianças vítimas, incluindo as vítimas de crimes em linha. Estas medidas visarão igualmente as vítimas de ciberintimidação nos Estados-Membros em que tais atos são criminalizados ao abrigo do direito nacional.

Nos termos do Regulamento Geral sobre a Proteção de Dados, o direito ao apagamento dos dados pessoais assume particular importância quando o titular dos dados deu o seu consentimento quando era criança e pode não ter estado totalmente ciente dos riscos inerentes, nomeadamente no contexto da ciberintimidação. A Comissão continuará a apoiar as autoridades de proteção de dados no desenvolvimento de ferramentas centradas nas crianças para proteger os dados das redes sociais, prevenir o roubo de dados ou de contas e permitir o exercício dos seus direitos.

A Comissão irá:

12. **Apoiar a implantação, em todos os Estados-Membros, de uma aplicação de segurança em linha acessível** para facilitar a denúncia da ciberintimidação, adaptada aos contextos nacionais, em sinergia com os mecanismos de denúncia existentes, incluindo linhas de apoio e linhas diretas, promovendo o apoio multidisciplinar em linha e fora de linha — **a partir do terceiro trimestre de 2026;**

13. Abordar a questão das crianças vítimas e da vitimização em linha, que pode incluir a ciberintimidação, na próxima **Estratégia da UE sobre os Direitos das Vítimas — 2026**.

Os Estados-Membros são convidados a:

5. Analisar o seu contexto nacional com vista a disponibilizar uma **aplicação nacional de segurança em linha** com apoio personalizado e, com base em modelos nacionais de práticas bem-sucedidas já existentes, **adaptar esse modelo ao contexto nacional**, incluindo, por exemplo, a tradução, questões relacionadas com a marca, a ligação aos serviços nacionais pertinentes de apoio e as plataformas de denúncia, assegurando simultaneamente funcionalidades essenciais como a denúncia segura, a preservação de provas em consonância com o direito nacional e a garantia da confidencialidade;

6. Assegurar que a denúncia através da aplicação nacional de segurança em linha seja integrada num **ecossistema holístico e funcional para a gestão de processos e apoio**, incluindo apoio coordenado fora de linha (por exemplo, serviços de apoio jurídico, policial, social, psicológico e educativo);

7. **Disponibilizar a aplicação nacional de segurança em linha às plataformas em linha para integração nas suas ferramentas de denúncia e de apoio aos utilizadores**, nomeadamente através de interfaces de programação de aplicações (IPA), tornando a denúncia e a resposta eficientes em termos de recursos e eficazes;

8. **Promover a ampla adoção e utilização da aplicação nacional de segurança por todas as partes interessadas pertinentes;**

9. **Promover ferramentas desenvolvidas pelas autoridades de proteção de dados** nas suas línguas nacionais para que as crianças se protejam dos riscos em linha, como a ciberintimidação, o roubo de dados ou de contas, as tentativas de burla e a chantagem sexual.

4. Alcance internacional e cooperação multilateral

A UE visa salvaguardar o bem-estar e os direitos das crianças dentro das suas fronteiras, mas também contribuir significativamente para promover um ambiente digital mais seguro e inclusivo em todo o mundo. O Dia por uma Internet mais segura é agora uma campanha mundial que apela às partes interessadas para que tomem medidas conjuntas para tornar a Internet um lugar mais seguro e melhor para todos, especialmente para as crianças e os jovens, sensibilizando para os principais desafios em linha e para as preocupações e tendências emergentes.

A proteção e a capacitação dos menores em linha representam uma prioridade global. Tal reflete-se na Estratégia Digital Internacional para a União Europeia. A rede de linhas diretas cofinanciada pela UE nos Estados-Membros para combater a difusão de material com imagens de abusos sexuais de crianças em linha faz parte da rede INHOPE (Associação Internacional das Linhas Diretas para a Internet), que conta atualmente com 57 linhas diretas a funcionar em todo o mundo.

A Comissão continuará a colaborar com entidades reguladoras que partilham as mesmas ideias em matéria de segurança em linha, incluindo a prevenção e o combate à ciberintimidação, ao abrigo de acordos administrativos (por exemplo, atualmente com a Ofcom no Reino Unido e o comissário para a segurança eletrónica na Austrália) e de parcerias digitais (por exemplo, com o Canadá, Singapura e a Índia).

A UE promoverá a cooperação contra a ciberintimidação em fóruns internacionais, em consonância com o Pacto Digital Global. As organizações das Nações Unidas elaboraram orientações e desenvolveram instrumentos que podem ser utilizados como boas práticas e parâmetros de referência, nomeadamente o Fundo das Nações Unidas para a Infância (UNICEF) (sítio Web e IPA de código fonte aberto), a União Internacional das Telecomunicações (orientações sobre a proteção das crianças em linha), bem como o Representante Especial do Secretário-Geral das Nações Unidas para a violência contra as crianças. A UE apoia as atividades de sensibilização da Organização das Nações Unidas para a Educação, Ciência e Cultura (UNESCO) junto das entidades reguladoras para que estas apliquem as orientações da UNESCO sobre a governação das plataformas em linha.

A UE financia programas específicos de sensibilização e apoio à proteção das crianças em países terceiros, em especial nos países candidatos e nos países vizinhos, em linha e fora de linha, através do instrumento IVCDCI — Europa Global (Instrumento de Vizinhança, de Cooperação para o Desenvolvimento e de Cooperação Internacional — Europa Global). A UE apoia igualmente o alinhamento pelas regras da UE no âmbito do processo de adesão dos países candidatos e potenciais candidatos e promove a segurança em linha das crianças e dos jovens nos países vizinhos através do intercâmbio de conhecimentos e de boas práticas no âmbito do programa Centro Internet Segura+.

5. Próximas etapas

A Comissão acompanhará a execução do plano de ação nos três pilares, trabalhando em estreita colaboração com os Estados-Membros, os Centros Internet Segura e outras partes interessadas. Os progressos, os desafios e as boas práticas serão acompanhados através das ferramentas existentes, como o mapa anual de políticas da Internet Melhor para as Crianças, os relatórios dos Centros Internet Segura e os intercâmbios regulares através de fóruns de peritos, assegurando um acompanhamento transparente e participativo.

A Comissão trabalhará com os Estados-Membros para integrar quadros de acompanhamento nas estratégias ou políticas nacionais de combate à ciberintimidação, avaliando a execução, a acessibilidade, a inclusividade e a adaptabilidade a contextos digitais em evolução, com a participação das crianças e dos jovens. As conclusões serão partilhadas a nível da UE para apoiar a aprendizagem mútua e o alinhamento das políticas, contribuindo para atualizações das iniciativas no âmbito da Estratégia para uma Internet Melhor para as Crianças e do RSD.

A Comissão fará um balanço do presente plano de ação em 2029, nomeadamente através de consultas com as crianças e os jovens.

6. Conclusões

> «Queremos um espaço em linha seguro para as crianças, os jovens e a próxima geração, mas ainda não o temos. Temos alguns problemas. E estes problemas não afetam apenas esta geração. Por conseguinte, precisamos da ajuda da UE para tornar os nossos espaços em linha seguros. É preciso começar por algum lado. Temos de o fazer agora. Pelo futuro.»
>
> Citação de crianças que são membros da Plataforma Europeia para a Participação das Crianças.

As crianças e os jovens pedem-nos ajuda para tornar os espaços em linha seguros para si, para os seus pares e para as gerações futuras. Temos de estar à altura do desafio em toda a nossa União, uma vez que a proteção e a capacitação das nossas crianças e jovens não devem depender de um código postal.

Com base num conjunto já sólido de medidas jurídicas e políticas da UE contra os danos em linha e nos contributos de um vasto leque de partes interessadas, o presente plano de ação ajudará a construir um ambiente digital seguro, inclusivo e capacitante para as crianças e os jovens na Europa. Complementará e inspirará as iniciativas em curso da UE em matéria de Internet mais segura, responsabilidade das plataformas, competências digitais e educação, capacitação das crianças e dos jovens, recolha de dados e cooperação internacional.

A Comissão convida o Parlamento Europeu e o Conselho a aprovarem o presente plano de ação e a unirem esforços para a sua execução. A Comissão apela ao Comité das Regiões e ao Comité Económico e Social Europeu para que promovam o diálogo com as autoridades locais e regionais, os parceiros económicos e sociais e a sociedade civil.

ANEXO: Ações-chave e calendário

Pilar I: Abordagem coordenada a nível da UE em matéria de proteção

A Comissão irá:	
Aumentar a tónica colocada no combate à ciberintimidação na revisão das **orientações no âmbito do RSD sobre a proteção dos menores;**	2026
Adotar **orientações no âmbito do RSD sobre sinalizadores de confiança**, que ajudarão a clarificar o seu papel no combate aos conteúdos ilegais, como a ciberintimidação ilegal;	até ao segundo trimestre de 2026
Avaliar formas de combater a ciberintimidação em plataformas de partilha de vídeos durante a **avaliação em curso da Diretiva Serviços de Comunicação Social Audiovisual** e a sua revisão;	até ao terceiro trimestre de 2026
Apoiar a **aplicação efetiva das disposições do Regulamento IA relativas às práticas de IA proibidas**, nomeadamente quando utilizadas para efeitos de ciberintimidação;	a partir do terceiro trimestre de 2026
Facilitar a **aplicação efetiva das obrigações de transparência do Regulamento IA relacionadas com a marcação e rotulagem de conteúdos gerados por IA**, incluindo os utilizados para efeitos de ciberintimidação.	a partir do terceiro trimestre de 2026

Os Estados-Membros são convidados a:
Elaborar **planos nacionais abrangentes de luta contra a intimidação, incluindo a ciberintimidação**, nomeadamente com o apoio da Rede Europeia dos Direitos da Criança;
Recolher dados coerentes e comparáveis sobre a ciberintimidação, objetivo facilitado pela rede de Centros Internet Segura e pela plataforma Internet Melhor para as Crianças.

Pilar II: Prevenção e sensibilização

A Comissão irá:	
Abordar a ciberintimidação na **atualização das Orientações para professores e educadores sobre o combate à desinformação e a promoção da literacia digital**;	até ao segundo trimestre de 2026
Reforçar a educação para a cidadania nas escolas através de um quadro de competências e orientações em matéria de cidadania da UE;	2027

Reforçar as competências digitais, a prevenção da ciberintimidação e o bem-estar digital através do **Roteiro sobre o Futuro da Educação e das Competências Digitais 2030**;	até ao terceiro trimestre de 2026
Contribuir para a prevenção da ciberintimidação no próximo **plano de ação da UE para a proteção das crianças contra a criminalidade**;	até ao terceiro trimestre de 2026
Alargar **os recursos e a formação em matéria de ciberintimidação** às escolas e à educação não formal e informal, acessíveis às pessoas com deficiência, através da plataforma Internet Melhor para as Crianças, dos Centros Internet Segura e do Portal Europeu da Juventude;	a partir do segundo trimestre de 2026
Apoiar o grupo do método aberto de coordenação para o combate ao discurso de ódio no desporto no seu trabalho sobre **recomendações para combater a ciberintimidação no ambiente desportivo**.	até ao quarto trimestre de 2026

Os Estados-Membros são convidados a:
Reforçar a prevenção e a identificação precoce da ciberintimidação com **orientações e formação para as partes interessadas**, como educadores, cuidadores e profissionais que trabalham com crianças em diferentes domínios;
Reforçar a participação das crianças na conceção de políticas e na aplicação de medidas para o bem-estar das crianças.

Pilar III: Denúncia e apoio abrangente

A Comissão irá:	
Apoiar a implantação de **uma aplicação de segurança em linha acessível** em todos os Estados-Membros;	a partir do terceiro trimestre de 2026
Abordar a questão das crianças vítimas e da vitimização em linha, que pode incluir a ciberintimidação, na **Estratégia da UE sobre os Direitos das Vítimas**.	2026

Os Estados-Membros são convidados a:
Analisar o seu contexto nacional com vista a disponibilizar **uma aplicação nacional de segurança em linha** e, com base em modelos nacionais de práticas bem-sucedidas já existentes, adaptar esse modelo ao contexto nacional;
Assegurar que a denúncia através da aplicação nacional de segurança em linha seja integrada num **ecossistema de apoio holístico e funcional**;
Disponibilizar a aplicação nacional de segurança em linha às plataformas em linha para integração nas suas ferramentas de denúncia e de apoio aos utilizadores;
Promover a aplicação nacional de segurança em linha junto das partes interessadas pertinentes;
Promover ferramentas desenvolvidas pelas autoridades de proteção de dados nas suas línguas nacionais para que as crianças se protejam dos riscos em linha, como a ciberintimidação.