

Sede | Head Office

Rua José Estêvão, 135-A | Piso 1  
1150-201 Lisboa | Portugal

T. + 351 21 358 79 00 | apav.sede@apav.pt



## **Parecer sobre o Projeto de Lei n.º 398/XVII/1.ª**

### **Estabelece medidas de proteção de crianças em ambientes digitais**

O presente parecer incide sobre o Projeto de Lei n.º 398/XVII/1.ª, apresentado pelo Grupo Parlamentar do Partido Social Democrata, já aprovado na generalidade, que visa estabelecer medidas de proteção de crianças em ambientes digitais.

A iniciativa legislativa procura responder a um contexto de crescente exposição e risco de crianças e jovens a riscos associados à utilização de plataformas em linha, redes sociais, serviços de partilha de conteúdos, aplicações de comunicação, jogos e outros serviços online.

Em termos gerais, o projeto propõe a fixação da maioridade digital aos 16 anos, prevenindo mecanismos de consentimento parental entre os 13 e os 16 anos, a implementação de sistemas de verificação de idade, a adoção de configurações de segurança por defeito, limitações a funcionalidades de design aditivo e deveres acrescidos de proteção relativamente a conteúdos e serviços de risco elevado.

A APAV reconhece a relevância da presente iniciativa legislativa e considera que a proteção de crianças e jovens em ambientes digitais constitui hoje uma matéria prioritária de política pública, diretamente relacionada com os direitos fundamentais da criança, a prevenção da violência, a proteção da saúde mental e a segurança digital.

A experiência operacional da APAV, nomeadamente através da Linha Internet Segura, demonstra de forma consistente que o ambiente digital constitui atualmente um espaço relevante de vitimação de crianças e jovens, incluindo situações de cyberbullying, extorsão sexual, aliciamento para fins sexuais, partilha não consentida de imagens íntimas, exposição a conteúdos violentos ou sexualizados, assédio, perseguição online e outras formas de violência digital.

Neste contexto, a APAV considera que o Projeto de Lei n.º 398/XVII/1.ª constitui uma iniciativa tendencialmente positiva e alinhada com a evolução recente do direito europeu e internacional em matéria de proteção de menores na utilização de plataformas online, embora entenda que o diploma beneficiará de aperfeiçoamentos técnicos relevantes em sede de especialidade.

#### **I. Enquadramento estatístico e realidade nacional**

A necessidade de reforço da proteção de crianças e jovens em ambientes digitais encontra confirmação nos dados nacionais mais recentes.

A Linha Internet Segura, serviço coordenado pela APAV no âmbito do Centro Internet Segura<sup>1</sup>, integra uma componente Helpline, destinada ao apoio de vítimas de cibercrime e violência digital,

<sup>1</sup> O Centro Internet Segura, coordenado pelo Centro Nacional de Cibersegurança, resulta de um Consórcio que envolve o EduQA – Instituto de Educação, Qualidade e Avaliação, o IPDJ – Instituto Português do Desporto e Juventude, a FCT – Fundação para a Ciência e a Tecnologia, a APAV – Associação Portuguesa de Apoio à Vítima e a Microsoft Portugal.



aconselhamento e esclarecimento confidencial, bem como uma componente Hotline, dedicada à análise e remoção de denúncias de conteúdos ilegais online, incluindo conteúdos de abuso sexual de crianças, incitamento ao ódio e à violência e outras formas de cibercriminalidade.

Em 2025, a Linha Internet Segura registou 949 novos processos relacionados com situações de cibercrime e violência online, correspondendo a um aumento de 39% face ao ano anterior. No mesmo período, foram apoiadas 119 crianças vítimas de cibercrime e violência online, comparativamente a 74 apoiadas em 2024.

Entre os casos envolvendo crianças e jovens, registaram-se 75 situações relacionadas com crimes sexuais online contra menores, incluindo pornografia de menores, aliciamento para fins sexuais, importunação sexual e extorsão sexual, traduzindo um aumento de 92% relativamente ao ano anterior.

Na dimensão Hotline da Linha Internet Segura, em 2025 foram recebidas 1 747 denúncias de conteúdos ilegais online, registando-se um aumento de cerca de 70% face a 2024. Do total de denúncias recebidas em 2025, 61,6% dizem respeito a conteúdos de abuso sexual de menores online (1 076), o que representa um aumento de cerca de 41% face a 2024 (761)<sup>2</sup>.

Os dados recolhidos pela APAV demonstram igualmente que uma parte significativa destas situações tem origem em plataformas de redes sociais e serviços de comunicação, sendo frequente a deslocação posterior das interações para aplicações de comunicação privada ou encriptada.

Também os dados globais da APAV relativos à vitimação de crianças e jovens revelam um crescimento consistente deste fenómeno. Entre 2022 e 2025, a APAV apoiou 13039 crianças e jovens vítimas de crime e violência, tendo o número anual de vítimas apoiadas aumentado de 2595 para 3954.

No mesmo período, os crimes sexuais reportados à APAV passaram de 390 para 864 situações anuais, incluindo casos de abuso sexual de crianças, pornografia de menores, coação sexual, partilha de conteúdos íntimos, importunação sexual e aliciamento online.

Por sua vez, o Relatório Anual de Segurança Interna de 2025 confirmou o crescimento da criminalidade informática e dos fenómenos de violência digital, assinalando um aumento significativo de crimes relacionados com acesso ilegítimo, falsidade informática, fraude digital e utilização abusiva de plataformas de comunicação.

A leitura conjugada destes dados demonstra que a violência contra crianças e jovens ocorre hoje de forma cada vez mais integrada entre os espaços físicos e digitais, sendo as plataformas online frequentemente utilizadas como instrumentos de aproximação, manipulação, intimidação, exploração e revitimação.

Neste contexto, a intervenção legislativa não pode limitar-se a uma lógica exclusivamente repressiva ou penal. A proteção efetiva de crianças e jovens exige mecanismos preventivos, proporcionais e estruturais, incluindo deveres específicos para os prestadores de serviços digitais.

<sup>2</sup> Estatísticas Linha Internet Segura 2025, [https://apavdata.blob.core.windows.net/publico/estatisticas/Estatisticas%202025\\_Linha\\_Internet\\_Segura.pdf](https://apavdata.blob.core.windows.net/publico/estatisticas/Estatisticas%202025_Linha_Internet_Segura.pdf)



## II. Enquadramento internacional e europeu

A iniciativa legislativa encontra enquadramento nos instrumentos internacionais e europeus de proteção dos direitos da criança.

A Convenção sobre os Direitos da Criança, bem como o Comentário Geral n.º 25 do Comité dos Direitos da Criança das Nações Unidas, relativo aos direitos das crianças em ambiente digital, reconhecem que os Estados têm o dever de assegurar que os direitos das crianças sejam respeitados, protegidos e realizados também no espaço digital.

O Comentário Geral n.º 25 sublinha que os Estados devem adotar medidas legislativas e regulamentares destinadas a prevenir riscos digitais, proteger a privacidade e a segurança das crianças, assegurar mecanismos de proteção adequados à idade e responsabilizar os prestadores de serviços digitais.

Ao nível europeu, o Regulamento (UE) 2022/2065, relativo a um mercado único para os serviços digitais — Regulamento dos Serviços Digitais (Digital Services Act – DSA) — estabelece um quadro europeu harmonizado de deveres de diligência aplicáveis a plataformas digitais e serviços intermediários.

O artigo 28.º do DSA assume especial relevância nesta matéria, ao impor aos fornecedores de plataformas acessíveis a menores a obrigação de assegurar um elevado nível de privacidade, proteção e segurança das crianças. O referido artigo estabelece igualmente limitações à publicidade direcionada, com base na definição de perfis de menores, e consagra o princípio segundo o qual a proteção das crianças deve ser integrada ao próprio desenho e funcionamento dos serviços digitais.

As orientações, publicadas em outubro de 2025<sup>3</sup>, constituem um instrumento particularmente relevante para a interpretação e concretização das obrigações previstas no DSA.

As orientações recomendam a adoção de medidas concretas de mitigação destinadas a concretizar uma lógica de proteção por defeito e de *safety by design*, incluindo contas privadas por defeito, limitação de funcionalidades suscetíveis de potenciar comportamentos aditivos, adaptação dos sistemas de recomendação, mecanismos proporcionais de verificação de idade, avaliações de risco específicas na utilização destas plataformas por crianças, ferramentas de denúncia acessíveis e adaptadas à idade, mecanismos de proteção contra contactos suspeitos e reforço da transparência e do controlo exercido pelos próprios utilizadores menores sobre a sua experiência digital.

Embora estas orientações não sejam juridicamente vinculativas, a sua relevância normativa e interpretativa é significativa, constituindo, atualmente, o principal referencial europeu para a concretização do artigo 28.º do DSA.

Neste sentido, a APAV considera que a densificação destas orientações através de legislação

<sup>3</sup> Guidelines on measures to ensure a high level of privacy, safety and security for minors online, pursuant to Article 28(4) of Regulation (EU) 2022/2065, <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-protection-minors>



nacional pode constituir um instrumento importante para garantir uma aplicação mais uniforme, previsível e eficaz das obrigações de proteção de menores.

A iniciativa legislativa portuguesa surge igualmente num contexto europeu de crescente preocupação institucional relativamente à proteção de menores online.

Em novembro de 2025, o Parlamento Europeu aprovou uma *Resolução sobre a proteção de menores online*<sup>4</sup>, na qual apelou ao reforço da aplicação efetiva do Regulamento dos Serviços Digitais, manifestou preocupação com os efeitos das práticas de design aditivo e dos sistemas de recomendação assentes na maximização de *engagement*, recomendou limitações reforçadas relativamente a funcionalidades suscetíveis de potenciar comportamentos aditivos em crianças e defendeu uma abordagem europeia mais harmonizada em matéria de idade digital e proteção reforçada relativamente a plataformas de risco elevado.

A resolução identificou igualmente riscos associados a funcionalidades como rolagem infinita (infinite scroll), reprodução automática (autoplay), sistemas de recompensa variável, caixas de recompensa (loot boxes), dark patterns e mecanismos de monetização dirigidos a crianças.

Paralelamente, a Declaração da Jutlândia, subscrita por 25 Estados-Membros da União Europeia, incluindo Portugal, reforçou a necessidade de desenvolver mecanismos robustos de proteção de crianças e jovens, incluindo medidas de verificação de idade, proteção por defeito e reforço das obrigações das plataformas.

### III. Apreciação do Projeto de Lei

A APAV considera que o projeto concretiza, de forma globalmente positiva, o dever de proteção especial das crianças previsto no artigo 69.º da Constituição da República Portuguesa, respondendo a riscos reais, atuais e documentados. A iniciativa revela-se igualmente coerente com a Convenção sobre os Direitos da Criança, com o Comentário Geral n.º 25 do Comité dos Direitos da Criança das Nações Unidas, com o Regulamento dos Serviços Digitais e com a evolução recente do debate europeu relativo à proteção de menores online.

O projeto reconhece corretamente que a proteção de crianças em ambientes digitais não pode depender exclusivamente da autorregulação das plataformas, nem de mecanismos meramente declarativos. Nesse sentido, assume particular relevância o reforço das obrigações impostas às plataformas digitais, designadamente através das medidas previstas nos artigos 10.º, 11.º e 12.º, relativas às configurações seguras por defeito, limitação de funcionalidades suscetíveis de gerar comportamentos aditivos, mecanismos de denúncia e configurações seguras por defeito.

A APAV acompanha igualmente a preocupação do legislador relativamente à necessidade de abandonar mecanismos de verificação de idade assentes exclusivamente na autodeclaração dos utilizadores, conforme resulta dos artigos 7.º e 8.º do projeto, reconhecendo que a eficácia das medidas de proteção depende da existência de sistemas fiáveis de verificação de idade.

<sup>4</sup> European Parliament resolution of 26 November 2025 on the protection of minors online (2025/2060(INI)), [https://www.europarl.europa.eu/doceo/document/TA-10-2025-0299\\_EN.html](https://www.europarl.europa.eu/doceo/document/TA-10-2025-0299_EN.html)



Ao mesmo tempo, importa reconhecer que o Regulamento dos Serviços Digitais já prevê diversas obrigações relevantes nesta matéria, nomeadamente avaliações de risco relativas à segurança de menores realizadas por plataformas em linha de muito grande dimensão e motores de pesquisa em linha de muito grande dimensão. Contudo, a experiência europeia tem demonstrado que essas avaliações nem sempre têm sido suficientemente robustas ou eficazes.

Acresce que as orientações publicadas ao abrigo do artigo 28.º do DSA, supramencionado, embora altamente relevantes, não possuem natureza juridicamente vinculativa. Neste contexto, a APAV considera que a densificação destas orientações através de legislação nacional poderá contribuir para uma aplicação mais uniforme e efetiva das medidas de proteção de menores, incluindo relativamente a prestadores de serviços digitais que não integrem a categoria de plataformas de muito grande dimensão.

Importa igualmente ter presente que a ausência de uma abordagem harmonizada relativamente a mecanismos fiáveis de verificação de idade e de proteção de menores tem contribuído para uma fragmentação regulatória que enfraquece a proteção das crianças no espaço digital europeu.

Neste contexto, a iniciativa legislativa portuguesa poderá desempenhar um papel relevante na concretização prática das obrigações de proteção previstas no DSA, reforçando mecanismos de prevenção e clarificando expectativas regulatórias dirigidas às plataformas.

Ainda assim, a APAV entende que o diploma beneficiará de aperfeiçoamentos técnicos relevantes em sede de especialidade, nomeadamente no que respeita à definição de conceitos, à proporcionalidade das medidas, à diferenciação entre categorias de risco, à operacionalização do consentimento parental e à proteção da privacidade.

#### IV. A necessidade de um modelo baseado no risco

A APAV considera que a proteção de crianças em ambientes digitais deve assentar numa lógica graduada e baseada no risco do serviço.

Mais do que estabelecer uma idade abstrata de maturidade digital aplicável indistintamente a todos os serviços, importa reconhecer que o risco depende sobretudo da natureza da plataforma, das funcionalidades disponibilizadas, da intensidade dos sistemas algorítmicos, da existência de contacto entre utilizadores, da exposição a conteúdos nocivos e da presença de mecanismos de monetização ou recompensa.

Neste sentido, a APAV considera adequada a fixação da maioridade digital aos 16 anos prevista no artigo 5.º enquanto princípio orientador geral. Contudo, entende igualmente que **determinados serviços de risco elevado devem permanecer inacessíveis a menores**, mesmo quando exista consentimento parental entre os 13 e os 16 anos. **Essa proibição em muitos casos deve estender-se até à maioridade.**

Tal deverá aplicar-se, designadamente, a plataformas de apostas, plataformas predominantemente assentes em conteúdos sexuais, serviços com elevado risco de contacto com adultos desconhecidos, plataformas de chat aleatório, serviços assentes em recomendação algorítmica intensiva de conteúdos violentos ou sexualizados.



A APAV entende, por isso, que o artigo 9.º do projeto deverá densificar melhor:

- o tipo de plataformas abrangidas;
- os critérios de avaliação do risco;
- as idades relevantes para acesso;
- as obrigações concretas aplicáveis aos prestadores.

A necessidade de maior precisão conceptual verifica-se igualmente relativamente às definições constantes dos artigos 2.º e 4.º do diploma. Expressões como “jogos em linha”, “serviços de partilha de imagens e vídeos”, “conteúdos suscetíveis de prejudicar o desenvolvimento físico ou mental das crianças” ou “jogos em linha com carácter informativo ou pedagógico especialmente desenhados para crianças” apresentam atualmente **um grau elevado de indeterminação**. Expressões como “recomendações algorítmicas não aditivas” ou “gamificação destinada a prolongar o uso” também apresentam um elevado grau de abstração.

Essa indeterminação poderá gerar **dificuldades interpretativas e problemas de aplicação prática**, sobretudo tendo em conta que o próprio diploma prevê simultaneamente exclusões de determinados serviços e a aplicação transversal de obrigações relacionadas com proteção desde a conceção, verificação de idade, entre outras.

No que respeita especificamente ao artigo 6.º, a APAV considera importante assegurar **um equilíbrio adequado entre proteção, acompanhamento parental, respeito pela privacidade e autonomia progressiva das crianças e jovens**. Embora seja positiva a previsão de ferramentas de controlo e supervisão parental, entende-se que **modelos de monitorização permanente ou de supervisão relacional total poderão revelar-se excessivamente intrusivos e potencialmente contraproducentes**.

Neste contexto, a APAV considera mais adequado privilegiar mecanismos proporcionais e orientados para a mitigação de risco, designadamente através de alertas de segurança, definição de limites temporais de utilização, reforço das configurações de privacidade e maior transparência relativamente ao funcionamento dos serviços e às interações de risco.

Importa também clarificar que a exclusão de determinados serviços do âmbito principal da lei não deverá significar ausência total de obrigações de proteção quando esses serviços sejam efetivamente acessíveis a menores.

## V. Verificação de idade e proteção da privacidade

A APAV considera que a verificação de idade constitui um elemento essencial para a eficácia de qualquer regime de proteção de menores online.

Sem mecanismos fiáveis de verificação de idade, os limites etários tornam-se essencialmente declarativos e de reduzida eficácia prática. Neste contexto, considera positiva a opção prevista no artigo 7.º, n.º 2, relativa à **proibição da simples autoidentificação como mecanismo exclusivo de verificação etária**.



Todavia, a implementação destes mecanismos deve respeitar plenamente o princípio da minimização de dados, a proteção da privacidade, o RGPD, o DSA e os princípios da proporcionalidade e necessidade.

A APAV considera particularmente relevante privilegiar mecanismos de prova de idade, que permitam confirmar apenas que o utilizador ultrapassa determinado limiar etário ou está abaixo dele, **sem necessidade de revelar identidade civil, data de nascimento completa ou outros dados desnecessários.**

Neste domínio, a carteira europeia de identidade digital poderá constituir uma solução relevante para assegurar mecanismos interoperáveis, seguros e compatíveis com a proteção de dados.

A APAV considera igualmente importante que a verificação de idade seja integrada numa estratégia de proteção mais ampla e multinível<sup>5</sup>.

## VI. Configurações seguras por defeito

A APAV acompanha de forma globalmente positiva a lógica de *safety by design* subjacente ao projeto.

A proteção das crianças não pode depender exclusivamente do comportamento individual dos utilizadores ou da supervisão parental posterior. As próprias plataformas devem ser concebidas de forma a reduzir estruturalmente os riscos para menores.

Neste sentido, assumem particular relevância as medidas previstas nos artigos 10.º e 11.º relativas a contas privadas por defeito, limitação do contacto com desconhecidos, **restrição de funcionalidades aditivas e adaptação dos sistemas de recomendação.**

A experiência das organizações que trabalham diariamente com vítimas de violência online demonstra que muitos conteúdos inicialmente publicados por menores são posteriormente reutilizados, sexualizados ou instrumentalizados por terceiros.

Neste contexto, a APAV considera especialmente importante reforçar mecanismos destinados a limitar a circulação não autorizada de conteúdos produzidos por menores, dificultar a reutilização abusiva de imagens e reduzir o acesso de adultos desconhecidos a perfis de menores.

Seria recomendável circunscrever estas categorias a práticas concretas de cibercrime, nomeadamente conteúdo sexual de crianças online e conteúdo de exploração sexual de crianças online, tanto na tentativa de obtenção do mesmo em processos de aliciamento, como na partilha efetiva do conteúdo.

Lembramos que, à data da publicação deste parecer, as plataformas em causa não podem, no Espaço Europeu, de forma voluntária, detetar e denunciar material de abuso sexual de crianças ao abrigo da Diretiva ePrivacy<sup>6</sup>. Esta falha na renovação da base legal representa um recuo grave na

<sup>5</sup> Ver infra, pp. 8-9

<sup>6</sup> Ver *Child sexual abuse online: voluntary detection measures will not be extended*, <https://www.europarl.europa.eu/news/en/press-room/20260325IPR39207/child-sexual-abuse-online-voluntary-detection-measures-will-not-be-extended>



proteção das crianças.

A deteção destes conteúdos é essencial para identificar vítimas, apoiar investigações e remover material ilegal, permitindo, todos os anos, que milhares de crianças sejam protegidas e que milhões de ficheiros abusivos sejam retirados de circulação. Assim, sabendo que esta capacidade é de extrema relevância, é igualmente importante perceber de que forma esta previsão no âmbito deste projeto é **compatível com a diretiva ePrivacy**.

## VII. Serviços de comunicação interpessoal

A exclusão generalizada dos serviços de comunicações eletrónicas interpessoais prevista no artigo 2.º, n.º 3, suscita reservas.

Uma parte significativa das situações de violência digital reportadas à APAV e à Linha Internet Segura ocorre precisamente através de aplicações de comunicação privada ou encriptada.

Embora a proteção da privacidade e o respeito pelas comunicações privadas devam ser plenamente assegurados, **a exclusão absoluta destes serviços pode criar lacunas relevantes na proteção de menores**.

Neste sentido, a APAV considera recomendável prever obrigações proporcionais e compatíveis com os limites impostos pelo direito europeu, designadamente no que respeita:

- a mecanismos de denúncia;
- a ferramentas de bloqueio;
- a canais de resposta prioritária;
- a medidas de prevenção de contacto abusivo;
- a mecanismos de apoio e encaminhamento.

## VIII. Mecanismos de denúncia e apoio às vítimas

A APAV considera particularmente positiva a previsão de mecanismos de denúncia rápidos e prioritários constante do artigo 12.º do projeto.

Todavia, estes mecanismos **devem ser especificamente adaptados a menores**, assegurando: linguagem acessível, rapidez de resposta, acessibilidade e encaminhamento para estruturas de apoio especializadas.

A APAV entende igualmente que se deve prever **mecanismos de cooperação institucional** com entidades com experiência operacional no domínio do apoio a vítimas, nomeadamente crianças, e da denúncia de conteúdos ilegais, designadamente aos **Sinalizadores de Confiança**.

A proteção efetiva de menores exige uma abordagem multinível e integrada.

Tal como a APAV defendeu no âmbito da consulta pública europeia relativa às orientações do artigo 28.º do DSA<sup>7</sup>, a verificação de idade deve constituir apenas um dos elementos de uma estratégia

<sup>7</sup> *Comments and recommendations on the guidelines on measures to ensure a high level of privacy, safety and security*



mais ampla de proteção, articulada com: moderação adequada, mecanismos eficazes de denúncia e resposta, apoio às vítimas na referenciação para serviços especializados, literacia digital e desenho seguro das plataformas.

## IX. Observações adicionais

A APAV considera igualmente positiva a previsão, artigos, 17.º e 18.º de mecanismos de acompanhamento institucional, campanhas públicas, selo de boas práticas e avaliação de execução.

Todavia, entende que a proteção efetiva de crianças e jovens em ambientes digitais exige uma abordagem mais ampla e continuada, que **não se limite a ações pontuais de sensibilização**. Neste sentido, considera importante **reforçar estruturalmente as medidas de prevenção e literacia digital**, assegurar mecanismos periódicos de avaliação da eficácia e clarificar a articulação entre as diferentes autoridades competentes, garantindo uma **resposta coordenada, operacional e sustentável**.

## X. Conclusão

Em suma, a APAV considera que o Projeto de Lei n.º 398/XVII/1.ª constitui uma iniciativa globalmente positiva e necessária, respondendo a riscos reais e crescentes associados à utilização de plataformas e serviços digitais por crianças e jovens.

O diploma revela-se alinhado com a evolução recente do direito europeu em matéria de proteção de menores online, nomeadamente com o Regulamento dos Serviços Digitais, com as orientações relativas ao artigo 28.º do DSA e com as recomendações recentes do Parlamento Europeu.

A APAV entende, contudo, que o diploma beneficiará de aperfeiçoamentos técnicos em sede de especialidade, designadamente quanto à **clarificação de conceitos jurídicos indeterminados**, à **diferenciação das obrigações em função do risco** efetivamente associado aos serviços digitais, à **proteção reforçada de menores relativamente a plataformas de risco elevado**, ao equilíbrio entre **mecanismos de supervisão parental, privacidade e autonomia progressiva das crianças**, bem como à implementação de **mecanismos proporcionais e seguros de verificação de idade**.

A APAV considera igualmente importante reforçar estruturalmente as **medidas de prevenção e literacia digital**, bem como a articulação entre entidades competentes, **estruturas de apoio à vítima e mecanismos de denúncia de conteúdos ilegais**, contribuindo para uma abordagem mais integrada e sustentável de proteção de crianças e jovens em ambientes digitais. O que contribuirá para a aplicação dos três eixos do *Action Plan against Cyberbullying*<sup>8</sup> e colocará Portugal em linha com a *European strategy for a better internet for kids - BIK+*<sup>9</sup>.

for minors online pursuant to Article 28 of Regulation (EU) 2022/2065, [https://apav.pt/wp-content/uploads/2025/08/2025\\_06-DSA-art.-28-Guidelines-Review.pdf](https://apav.pt/wp-content/uploads/2025/08/2025_06-DSA-art.-28-Guidelines-Review.pdf)

<sup>8</sup> <https://digital-strategy.ec.europa.eu/en/policies/cyberbullying>

<sup>9</sup> [European strategy for a better internet for kids - BIK+ | Shaping Europe's digital future](https://digital-strategy.ec.europa.eu/en/policies/bik)



Com os ajustamentos identificados, o projeto poderá contribuir de forma relevante para o reforço da proteção de crianças e jovens em ambientes digitais.

APAV ©, 13 de maio de 2026