

O RSD explica

**o que as plataformas em
linha devem fazer para
manter as crianças e os
jovens seguros em linha**



O que é o Regulamento dos Serviços Digitais (Digital Services Act — DSA)?

As plataformas em linha fazem parte da vida quotidiana das crianças e dos jovens, seja para encontrar amigos, ver vídeos, jogar ou para aprender algo novo. No entanto, estar em linha também acarreta sérios riscos. As crianças e os jovens podem:

- ▶ *ser vítimas de perseguição no ambiente em linha (cyberbullying)*
- ▶ *ser contactados por estranhos com más intenções*
- ▶ *ver conteúdos prejudiciais ou perturbadores, suscetíveis de os incomodar, transtornar ou assustar*
- ▶ *sentir-se pressionados a comprar produtos*
- ▶ *participar em desafios perigosos*
- ▶ *ter dificuldade em largar o telemóvel ou desligar a consola.*



Com vista a tornar a internet mais segura, a União Europeia (UE) criou o Regulamento dos Serviços Digitais (RSD) em 2022. Este regulamento aplica-se às plataformas em linha (europeias ou não) disponíveis na UE e tem como objetivo ajudar a manter todos os utilizadores da Internet, incluindo as crianças e os jovens, a salvo destes e de outros riscos, bem como proteger os seus direitos fundamentais em linha.

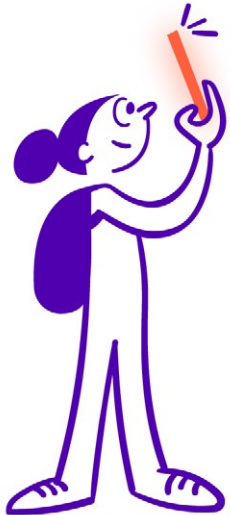
Todas as plataformas em linha devem respeitar este regulamento e ajudar a manter os utilizadores seguros na UE.



De que forma é que o RSD mantém as crianças e os jovens seguros em linha?

O RSD estabelece que as **plataformas em linha acessíveis a menores têm de garantir que os seus serviços oferecem um elevado nível de privacidade, proteção e segurança aos jovens utilizadores**. Isto significa que estes se devem sentir protegidos e seguros ao utilizar as aplicações, as redes sociais e os jogos abrangidos pelo regulamento. As plataformas em linha de muito grande dimensão — as quais têm mais de 45 milhões de utilizadores na UE —, como o TikTok, o Instagram e o Snapchat, também têm de identificar e avaliar outros potenciais riscos a que estão expostos as crianças e os jovens que utilizam os seus serviços.

Em julho de 2025, a Comissão Europeia publicou as orientações sobre proteção de menores com o objetivo de ajudar todas as plataformas a compreender o que devem fazer para manter as crianças e os jovens seguros em linha. Esta brochura explica o funcionamento dessas orientações.



As orientações contêm as seguintes informações

1. Quem tem de cumprir as diretrizes relativas à proteção de menores?	4
2. Quais são os princípios fundamentais das diretrizes?	5
3. Recomendações	6
a. Avaliação dos riscos: cada plataforma acarreta riscos diferentes	6
b. Verificação da idade: como é que as plataformas verificam a idade dos utilizadores	6
c. Registo: informação e capacitação desde o início	10
d. Configurações da conta: privacidade e segurança que o utilizador pode controlar	11
e. Interfaces: desenvolver plataformas fáceis e seguras de utilizar	13
f. Sistemas de recomendação e funcionalidades de pesquisa: ajudar as crianças a manter o controlo	14
g. Práticas comerciais: ajudar as crianças e os jovens a compreender o que está a ser promovido e vendido	15
h. Moderação: manter as plataformas seguras e respeitadoras	16
i. Denúncia: ajudar as crianças e os jovens a denunciar abusos ou a obter apoio	17
j. Ferramentas para pais e encarregados de educação	18
4. Quem garante o cumprimento das regras do RSD?	19
5. O que acontece a seguir?	19
Onde se pode obter mais informações e ajuda?	24

Esta publicação destina-se apenas a fins informativos e não constitui um documento legal.

1. Quem tem de cumprir as diretrizes relativas à proteção de menores?

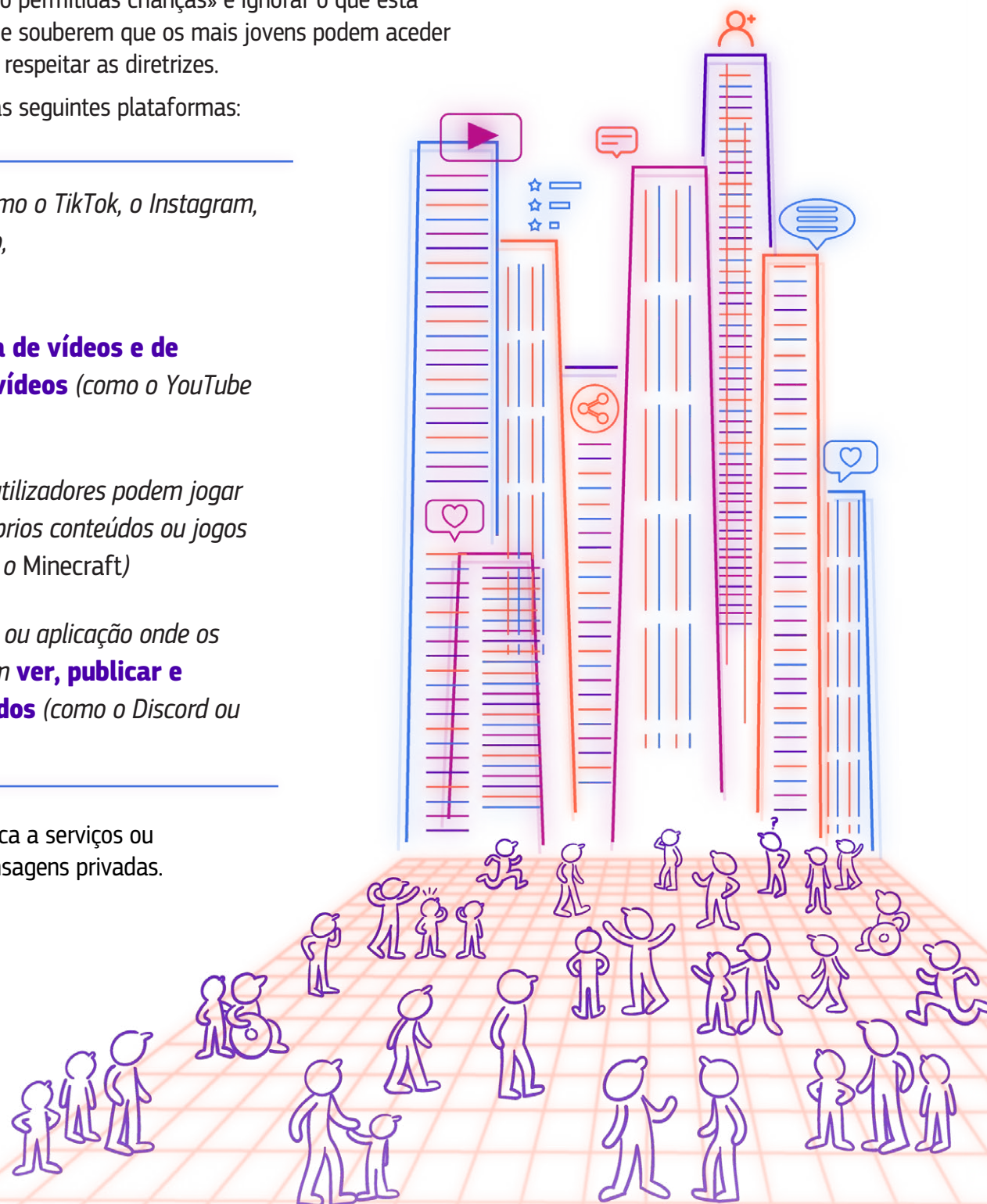
Se uma plataforma for utilizada por crianças e jovens, ou se estes tiverem acesso a ela, então a plataforma **tem de** cumprir as regras do RSD e as diretrizes relativas à proteção de menores.

Os sítios Web criados para adultos não se podem limitar a indicar, nas suas regras, que «não são permitidas crianças» e ignorar o que está realmente a acontecer. Se souberem que os mais jovens podem aceder ao seu conteúdo, têm de respeitar as diretrizes.

As diretrizes abrangem as seguintes plataformas:

- ▶ **redes sociais** (como o TikTok, o Instagram, o Snapchat, o Yubo, o BeReal, etc.)
- ▶ **sítios de partilha de vídeos e de transmissão de vídeos** (como o YouTube ou o Twitch)
- ▶ **jogos** em que os utilizadores podem jogar e criar os seus próprios conteúdos ou jogos (como o Roblox ou o Minecraft)
- ▶ **qualquer sítio Web ou aplicação onde os utilizadores possam ver, publicar e partilhar conteúdos** (como o Discord ou o Reddit).

Nota: o RSD não se aplica a serviços ou funcionalidades de mensagens privadas.



2. Quais são os princípios fundamentais das diretrizes?

As diretrizes assentam em três pontos essenciais:

1. Os direitos das crianças são uma prioridade

As plataformas devem respeitar os direitos das crianças e agir sempre segundo o princípio do superior interesse da criança. Estes direitos incluem:

- ▶ o direito à proteção
- ▶ o direito à não discriminação
- ▶ o direito à inclusão
- ▶ o direito à privacidade
- ▶ o direito de acesso à informação e à educação
- ▶ o direito à liberdade de expressão
- ▶ o direito à participação.

Isto significa conceber, desenvolver e gerir serviços em linha que sejam sempre *seguros, privados e protegidos*.

2. Segurança desde a conceção

As plataformas não devem esperar que surjam problemas—devem integrar a privacidade, a segurança e a proteção nos seus serviços desde o início. As funcionalidades devem ser adequadas às diferentes faixas etárias e fases de desenvolvimento das crianças.

3. Compreender as necessidades dos utilizadores

As plataformas devem ter em particular consideração a forma como os seus serviços são utilizados por crianças e jovens, bem como os riscos que estes podem enfrentar, nomeadamente:

- ▶ *perseguição em linha*
- ▶ *conteúdos nocivos*
- ▶ *utilização excessiva.*

Em seguida, devem procurar soluções para reduzir esses riscos.



3. Recomendações

Vejamos quais são as recomendações que as plataformas em linha devem seguir para proteger as crianças e os jovens.

a. Avaliação dos riscos: cada plataforma acarreta riscos diferentes

As diretrizes recomendam que as plataformas **verifiquem regularmente** se os seus serviços representam um **risco para crianças e jovens** e que compreendam como e porquê isso acontece. Devem encontrar um ponto de equilíbrio entre:

- ▶ permitir que as crianças e os jovens partilhem os seus conteúdos, ideias e opiniões
- ▶ dar-lhes a oportunidade de explorar, jogar e aprender coisas novas em linha...

... enquanto os mantêm seguros!

Uma vez identificados os riscos, as plataformas devem responder com soluções eficazes, sem limitar as importantes oportunidades e os benefícios de que as crianças podem usufruir em linha.

b. Verificação da idade: como é que as plataformas verificam a idade dos utilizadores

Para tornar as plataformas mais seguras e evitar que as crianças e os jovens utilizem serviços que não lhes são destinados, é importante saber se os utilizadores **têm idade suficiente** para aceder a determinados conteúdos. A **verificação da idade** é essencial neste contexto. A verificação da idade significa utilizar ferramentas que permitam:

- ▶ saber ou estimar a idade de um utilizador, ou
- ▶ confirmar se alguém tem idade superior ou inferior a um limite específico.

Sabia que...

tem de se ter pelo menos 13 anos para utilizar o TikTok, o Snapchat, o Instagram, o BeReal e o Steam?



Modalidades de verificação da idade

Existem três formas principais de as plataformas verificarem a idade de um utilizador:

1. Autodeclaração

O utilizador deve introduzir a sua data de nascimento ou clicar em «Sim, tenho mais de 13 anos» ou «Sim, tenho mais de 18 anos». Embora seja rápido, este método é fácil de ludibriar, pelo que **não é muito eficaz nem fiável**.

2. Estimativa da idade

A tecnologia estima a idade do utilizador com base em vários métodos, nomeadamente:

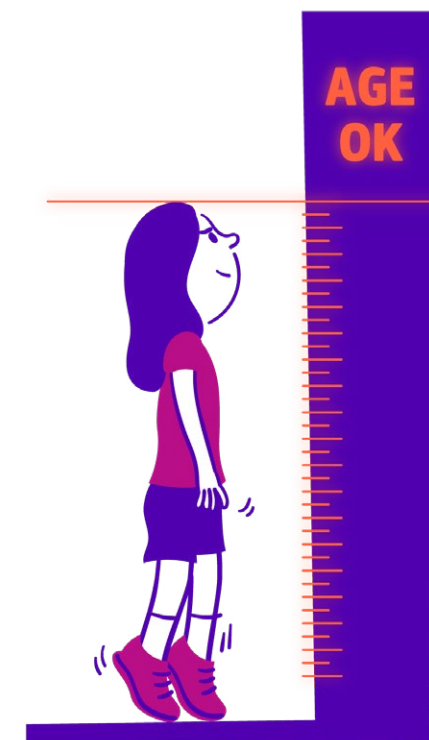
- > deteção de rosto
- > estilo de digitação
- > os interesses pessoais.

No entanto, não se trata de um método perfeito, uma vez que não permite determinar a idade exata e pode constituir uma **intrusão** na privacidade do utilizador.

3. Verificação da idade

Este é o método **mais preciso**. A idade é confirmada com recurso a:

- > documentos oficiais, como um passaporte
- > identificações digitais fiáveis, como um documento de identificação emitido pelo governo ou a carteira de identidade digital da UE (EU Digital Identity Wallet). Este último método **protege a privacidade** dos utilizadores, uma vez que estes podem comprovar a sua idade sem ter de revelar quaisquer outros dados pessoais.



O que é a carteira de identidade digital da UE? Trata-se de uma aplicação gratuita (disponível em 2026) que ajuda as pessoas na Europa a:

- ▶ manter os documentos importantes seguros num único local
- ▶ provar quem são, em linha e na vida real.

É como se fosse uma mochila digital para a identificação e os documentos importantes.



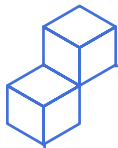
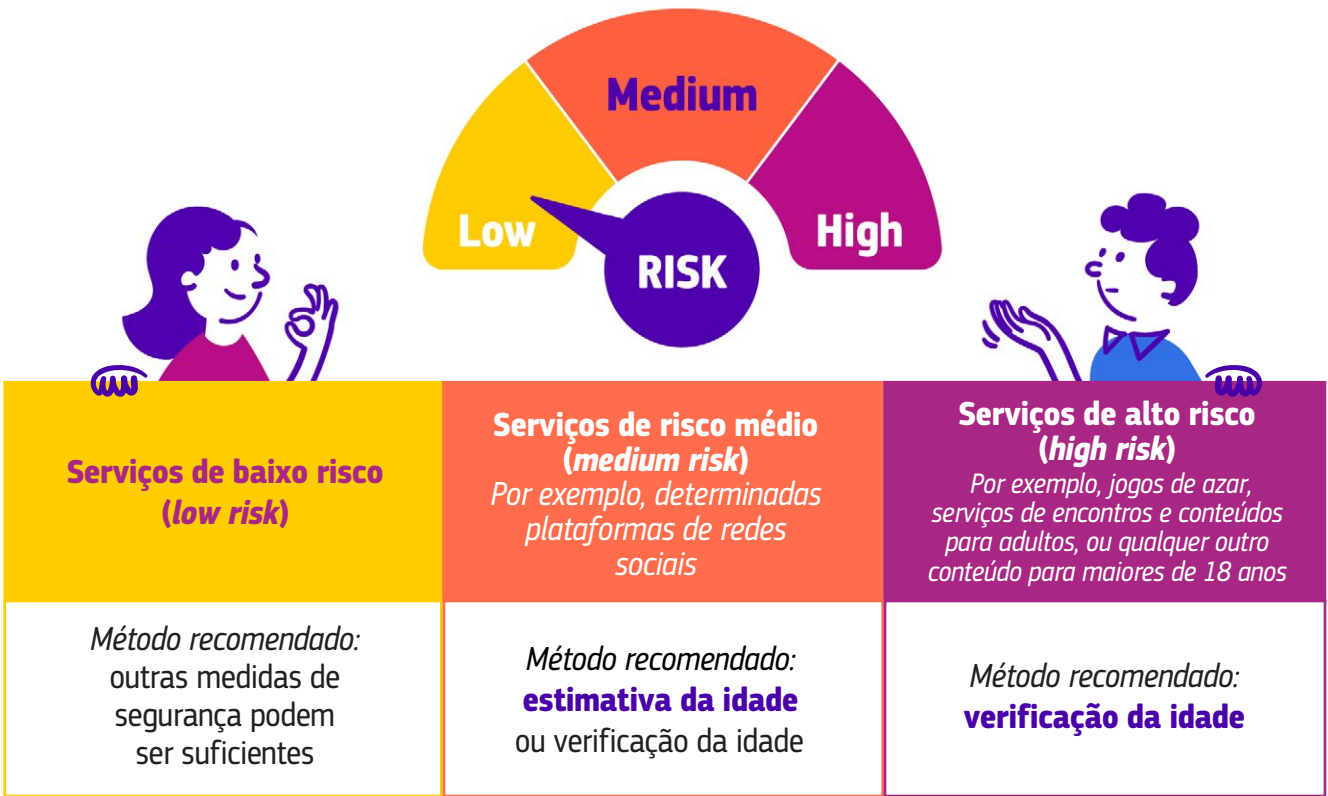
3. Recomendações

As plataformas em linha devem:

- ▶ explicar as verificações de idade de forma **fácil e compreensível** para crianças e jovens
- ▶ questionar sobre a idade apenas quando for **realmente necessário** para ajudar a manter os utilizadores seguros
- ▶ utilizar o **método mais simples** que funcione bem, sem solicitar mais informações do que as necessárias
- ▶ garantir que todos os métodos de verificação da idade são **precisos, justos e difíceis de contornar**
- ▶ disponibilizar **mais do que uma opção**, para que ninguém seja excluído
- ▶ permitir que os utilizadores possam **reclamar** caso a sua idade não seja estimada corretamente.



Que método devem as plataformas utilizar?



A verificação da idade parece um pouco complicada, não é? Este guia sobre o processo de verificação da idade pode ajudá-lo a compreender este método de segurança!



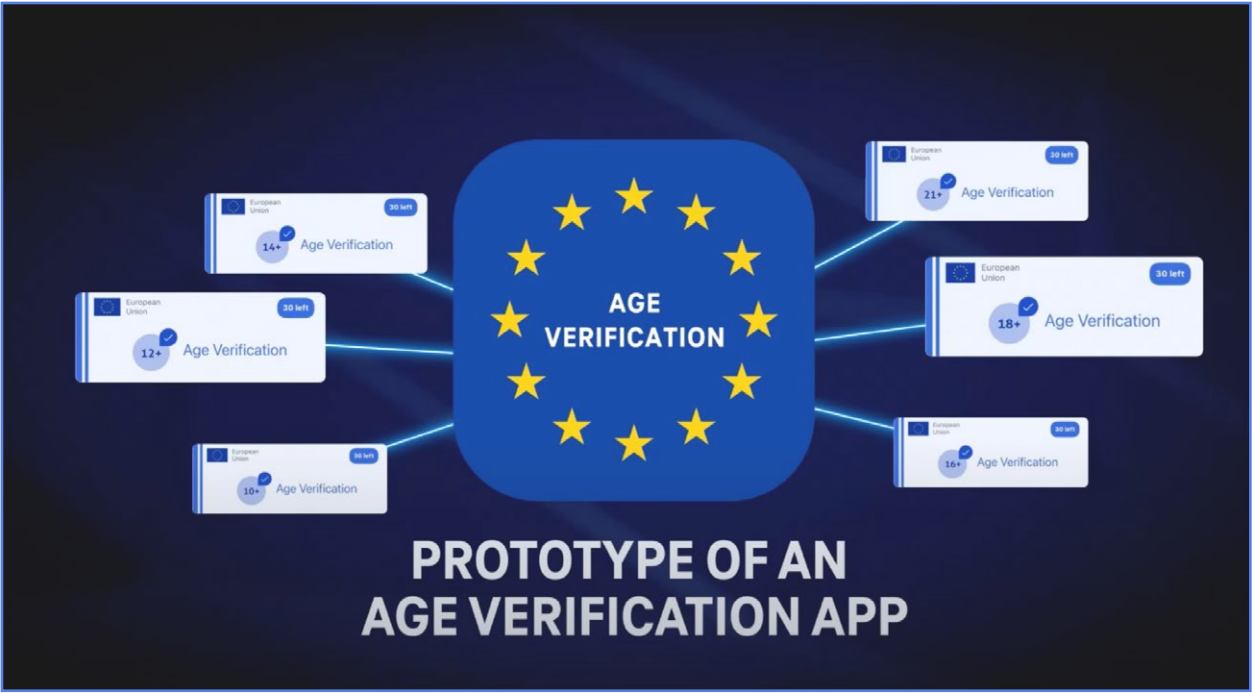
Será que uma aplicação consegue realmente verificar a idade?

Sim! A Comissão Europeia está a trabalhar numa solução para si! Em julho de 2025, foi lançado um **projeto para uma aplicação de verificação da idade**.

Esta aplicação está a ser desenvolvida para:

- ▶ ser fácil de utilizar
- ▶ permitir aos utilizadores provar que têm mais de 18 anos
- ▶ evitar a partilha de quaisquer outros dados pessoais.

Desta forma, é possível garantir que o acesso a determinados conteúdos é **seguro e adequado à idade** do utilizador.



Tem curiosidade em conhecer a abordagem da UE em matéria de verificação da idade? Leia o código QR para ficar a saber mais!



3. Recomendações

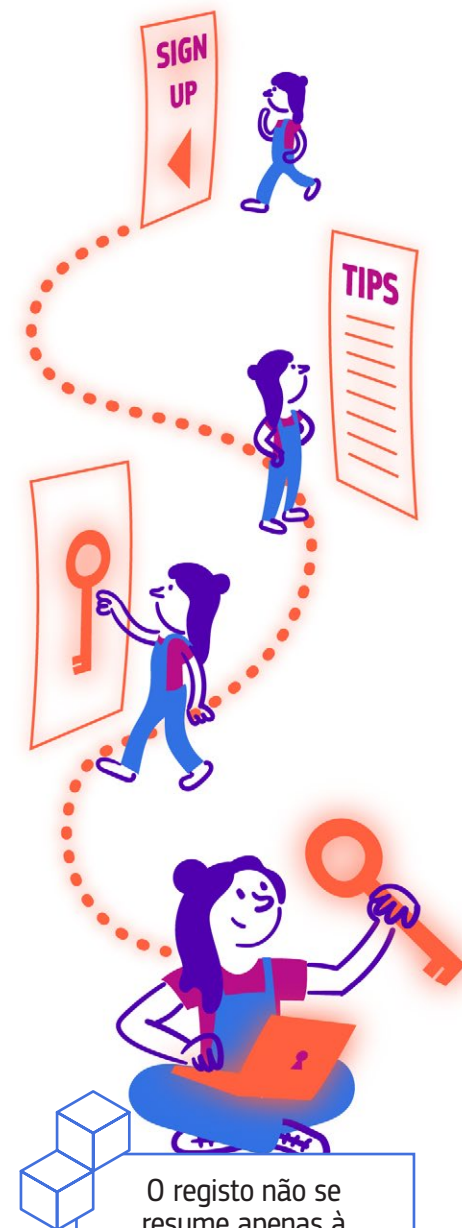
c. Registo: informação e capacitação desde o início

Quando uma plataforma pede aos utilizadores para se registarem, trata-se muitas vezes de uma boa oportunidade para:

- ▶ **partilhar informações de segurança importantes**
- ▶ **fornecer sugestões educativas**
- ▶ **garantir que o utilizador tem idade suficiente para aceder aos conteúdos.**

Para isto ser bem feito, as plataformas têm de:

- ▶ **explicar claramente** por que razão é necessário efetuar o registo e quais são os benefícios
- ▶ **manter o processo simples e acessível**, sobretudo para crianças e jovens com necessidades adicionais ou deficiências
- ▶ **evitar incentivar os utilizadores com idade inferior à legalmente estabelecida a registarem-se**
- ▶ **facilitar às crianças o encerramento da sessão ou a eliminação das suas contas** em qualquer altura
- ▶ **utilizar o registo para apresentar e explicar as principais características de segurança**, nomeadamente:
 - > as definições de privacidade
 - > as proteções predefinidas
 - > as ferramentas de denúncia
- ▶ **ajudar as crianças e os jovens a compreender:**
 - > que **ferramentas de segurança estão disponíveis**
 - > como **obter ajuda**, se necessário.



O registo não se resume apenas à criação de uma conta. É também uma oportunidade para a plataforma garantir que os jovens utilizadores iniciam a sua experiência de forma **segura, informada e controlada**.

d. Configurações da conta: privacidade e segurança que o utilizador pode controlar

As definições da conta podem ajudar as crianças, os jovens e os seus pais a gerir a sua presença em linha, por exemplo controlando a quantidade de dados pessoais visíveis para outrem ou a facilidade com que podem ser contactados. Uma vez que a maioria dos utilizadores não altera as configurações predefinidas, as plataformas devem certificar-se de que estas são **privadas, seguras e protegidas desde o início**.

As configurações predefinidas devem incluir:

- ▶ **contacto limitado:** controlar quem pode seguir ou enviar mensagens à criança ou jovem
- ▶ **desativação de funcionalidades de risco** predefinida, nomeadamente em relação a:
 - > geolocalização
 - > reprodução automática de vídeos
 - > microfone e câmara
 - > sincronização de contactos
 - > rastreamento
- ▶ **impedir que estranhos** vejam ou descarreguem conteúdos
- ▶ **partilhar informações de contacto** (como o endereço de correio eletrónico e o número de telefone) **apenas com autorização explícita**
- ▶ **gerir as notificações:** **desativar notificações automáticas ou alertas** de determinados utilizadores ou aplicações, ou durante as horas de sono
- ▶ **reduzir a utilização excessiva** desativando funcionalidades como:
 - > contadores de «gostos» e reações
 - > funcionalidades do tipo «... está a escrever»
 - > confirmação de leitura
- ▶ **proteger a saúde mental:** desativar filtros de imagem que possam afetar negativamente a imagem corporal ou a autoestima.



3. Recomendações

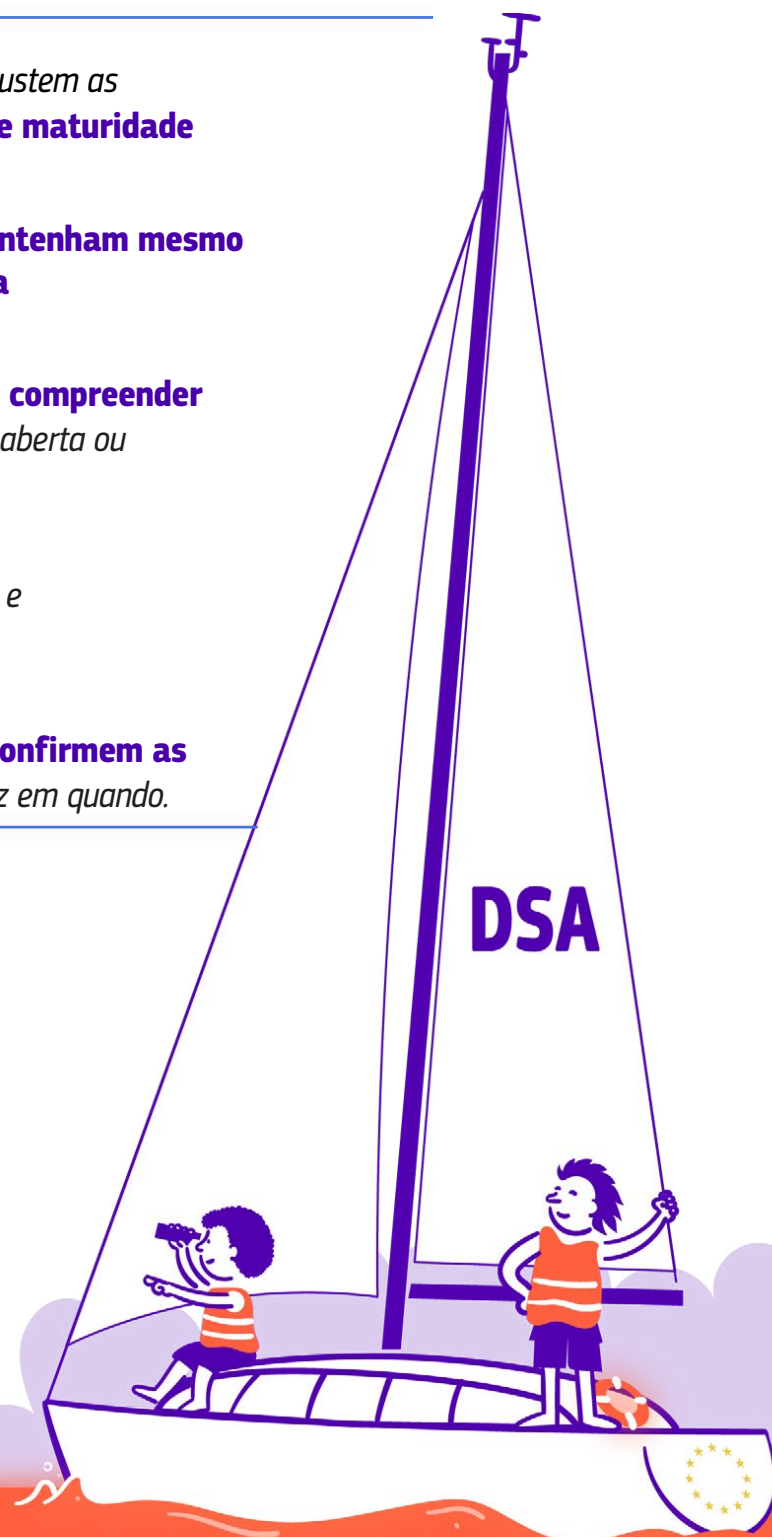
Atribuir responsabilidades às crianças e aos jovens, orientando-os

Nunca se deve encorajar as crianças e os jovens a reduzir as suas definições de privacidade, segurança e proteção. No entanto, se eles quiserem **personalizar a sua experiência**, devem poder fazê-lo de forma segura e adequada à sua idade.

As plataformas devem:

- ▶ permitir que os jovens utilizadores ajustem as configurações segundo a sua **idade e maturidade**
- ▶ garantir que as suas escolhas se **mantenham mesmo após atualizações da plataforma**
- ▶ fornecer **avisos claros e fáceis de compreender** antes de tornarem a sua conta mais aberta ou vulnerável
- ▶ permitir **alterações temporárias** e não apenas permanentes
- ▶ pedir aos jovens utilizadores que **reconfirmem as suas escolhas importantes** de vez em quando.

Porque é que isto é importante?
Porque as predefinições ajudam as crianças e os jovens a manterem-se **seguros e em controlo**, sem se sentirem sob pressão ou expostos a riscos desnecessários.



e. Interfaces: desenvolver plataformas fáceis e seguras de utilizar

Uma **interface** é descrita como o aspeto e o funcionamento de uma plataforma em linha, ou seja, o que se vê no ecrã e como se interage com isso. Uma interface bem concebida pode ajudar as crianças e os jovens a **manterem-se seguros, a sentirem-se confiantes e a desfrutarem o tempo que passam em linha**.

Com vista a evitar a utilização excessiva e os comportamentos viciantes, bem como a facilitar o encerramento da sessão, as plataformas devem evitar funcionalidades como:

- ▶ deslocamento infinito (quando a página chega ao fim, é automaticamente atualizada com novos conteúdos)
- ▶ deslizar para atualizar
- ▶ notificações constantes
- ▶ reprodução automática de vídeos
- ▶ recompensas diárias virtuais, séries ou pontos que exijam que as crianças abram a aplicação ou o jogo todos os dias.



As plataformas devem disponibilizar:

- ▶ ferramentas que ajudem as crianças e os jovens a **gerir o seu tempo em linha**, por exemplo lembretes amigáveis para fazerem pausas
- ▶ configurações de segurança, bem como ferramentas de comunicação e de feedback, **fáceis de encontrar, compreender e utilizar**
- ▶ **acessibilidade** para todos, incluindo crianças e jovens com deficiência ou necessidades adicionais
- ▶ avisos claros sempre que as crianças e os jovens estejam a interagir com **funcionalidades de inteligência artificial (IA)**.



3. Recomendações

f. Sistemas de recomendação e funcionalidades de pesquisa: ajudar as crianças a manter o controlo

Já se perguntou como é que as aplicações das redes sociais ou as plataformas dos seus programas de televisão sabem sempre o que lhe devem mostrar a seguir?

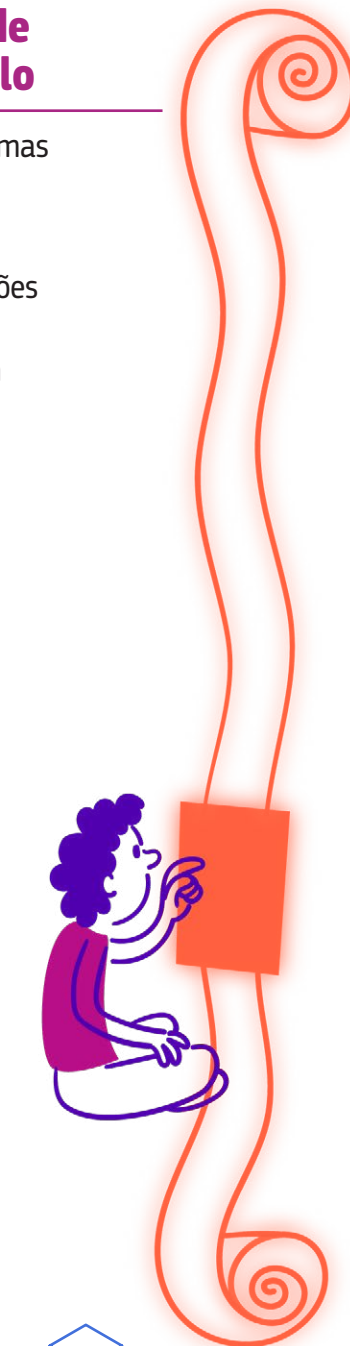
Os sistemas de recomendação decidem que tipo de conteúdo ou sugestões de contacto aparecem nos *feeds* dos utilizadores, incluindo páginas de exploração, com base no que estes gostaram, viram, clicaram ou decidiram seguir anteriormente. Embora isto possa ser útil, também pode expor as crianças e os jovens a imagens, vídeos ou produtos comerciais nocivos ou inadequados.

As plataformas devem:

- ▶ **mostrar apenas conteúdos adequados à idade**
- ▶ **limitar a quantidade de dados recolhidos e utilizados** para fazer recomendações
- ▶ **dar prioridade às escolhas ativas e ao feedback dos utilizadores, por exemplo:**
 - > «Mostra-me menos/mais disto»
 - > «Não quero ver isto»
 - > «Não estou interessado nisto»
- ▶ **evitar confiar demasiado no feedback passivo, como o tempo que os utilizadores passam a ver ou a navegar**
- ▶ **explicar por que razão algo foi recomendado e como os utilizadores o podem alterar**
- ▶ **permitir que os utilizadores reiniciem o seu feed de forma completa e permanente**
- ▶ **facilitar a denúncia de conteúdos indesejados e garantir que o feedback altera efetivamente o que é apresentado**
- ▶ **tornar todas as configurações dos sistemas de recomendação adequadas e acessíveis às crianças.**

As funcionalidades de pesquisa devem:

- ▶ **bloquear palavras ou hashtags não seguras**
- ▶ **ajudar as crianças e os jovens a escolher o que mais lhes interessa.**



Os sistemas de recomendação devem capacitar as crianças e os jovens, não deixá-los sob pressão. Dar aos jovens utilizadores controlo sobre o que veem ajuda a criar experiências em linha **mais seguras e positivas.**

g. Práticas comerciais: ajudar as crianças e os jovens a compreender o que está a ser promovido e vendido

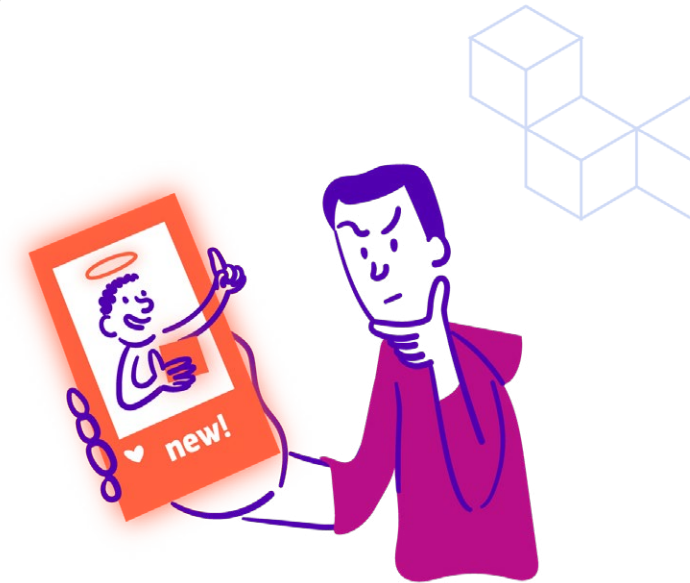
Tal como os adultos, as crianças e os jovens nem sempre se apercebem de quando algo em linha é:

- ▶ um anúncio publicitário
- ▶ uma promoção oculta
- ▶ uma publicação paga por um influenciador.

Também pode ser difícil descortinar como as aplicações, os jogos ou os sítios Web nos tentam convencer a gastar mais tempo ou dinheiro. Tal pode conduzir a compras desnecessárias, a gastos excessivos ou a hábitos difíceis de perder. As plataformas devem:

- ▶ **identificar claramente toda a publicidade e os conteúdos patrocinados, incluindo a colocação de produtos por influenciadores**
- ▶ **rever regularmente a forma como os anúncios são identificados, garantindo que esta identificação é clara e eficaz para as crianças e os cuidadores**
- ▶ **evitar a publicidade de produtos e serviços dirigidos a crianças e jovens suscetível de prejudicar a sua privacidade, segurança e/ou proteção**
- ▶ **ser transparentes quanto aos custos e consequências de:**
 - > **compras feitas na aplicação**
 - > **moedas «virtuais» ou tokens**
 - > outras **transações**
- ▶ **evitar estratégias de pressão como:**
 - > **temporizadores de contagem decrescente**
 - > mensagens que incentivam a compra imediata, como **«compre agora»**
- ▶ **bloquear o acesso a qualquer funcionalidade que se assemelhe a jogos de azar, como as loot boxes (caixas com prémios)**
- ▶ **garantir que os produtos e serviços «gratuitos» não incluem compras ocultas**
- ▶ **assegurar que a publicidade é adequada à idade**
- ▶ **adaptar os algoritmos de publicidade por forma a proteger as crianças de uma exposição excessiva ou frequente a anúncios.**

Porque é que isto é importante? Porque estas medidas podem ajudar a proteger as crianças e os jovens de serem **enganados ou pressionados** a gastar dinheiro contra a sua vontade.



Qual o significado destes termos?

A **colocação de um produto** ocorre quando uma marca ou artigo é apresentado num vídeo ou publicação como parte de uma promoção paga.

Uma **loot box** refere-se a um artigo digital que oferece recompensas aleatórias, sendo frequentemente utilizada em jogos.

Uma **compra feita na aplicação** refere-se a algo adquirido dentro da própria aplicação, como funcionalidades adicionais, novas vidas, novas *skins* (aparências) ou moedas virtuais.

3. Recomendações

h. Moderação: manter as plataformas seguras e respeitadoras

Moderação consiste em **verificar e remover conteúdos ou utilizadores** que possam pôr em risco a privacidade, a segurança e a proteção das crianças e dos jovens, incluindo o seu bem-estar físico e mental.

Esta ferramenta é crucial para proteger os utilizadores e evitar riscos graves, como a perseguição em linha, a exposição a conteúdos nocivos ou o aliciamento (quando alguém tenta fazer amizade com uma criança ou um jovem para o enganar ou fazer com que se sinta desconfortável).

As plataformas devem:

- ▶ **definir claramente o que se entende por conteúdos e comportamentos nocivos**
- ▶ **utilizar um processo eficaz para remover rapidamente conteúdos e contas nocivos ou ilegais**
- ▶ **formar moderadores aptos a detetar ameaças a crianças e jovens, como o aliciamento ou desafios perigosos**
- ▶ **remover conteúdos ilegais ou nocivos de forma imediata**
- ▶ **utilizar ferramentas para impedir os utilizadores de criarem ou partilharem conteúdos nocivos gerados por IA**
- ▶ **rever e melhorar regularmente o funcionamento dos sistemas de moderação.**



A moderação não se resume à remoção de conteúdos. Trata-se de criar um espaço em linha mais seguro e mais respeitoso para todos.

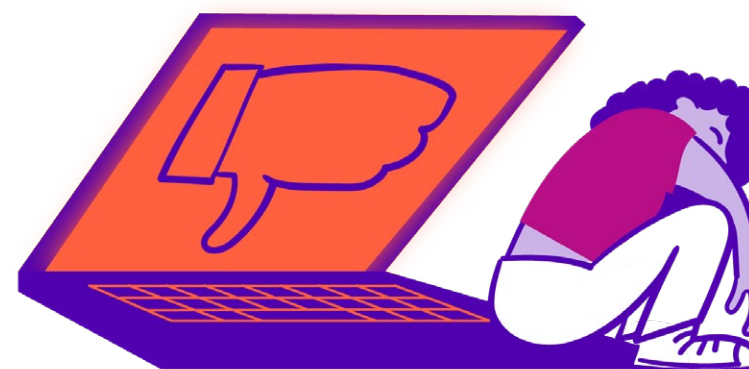
Uma boa moderação ajuda a criar um espaço onde as crianças e os jovens se sintam **seguros, respeitados e apoiados**.

i. Denúncia: ajudar as crianças e os jovens a denunciar abusos ou a obter apoio

Por vezes, as coisas não correm bem em linha. Podemos assistir a algo perturbador, ser vítimas de perseguição em linha ou sentir-nos inseguros. É por isso que é importante que as plataformas **facilitem a comunicação de problemas e a obtenção de ajuda**.

As plataformas devem:

- ▶ **disponibilizar formas simples e claras** que permitam a qualquer utilizador, incluindo pessoas com deficiência, denunciar abusos, perseguição em linha ou conteúdos nocivos
- ▶ **permitir aos utilizadores bloquear, silenciar ou restringir** comentários e interações com outros utilizadores
- ▶ **assegurar que os utilizadores não são automaticamente adicionados a grupos** — a adesão só deve ocorrer após a aceitação de um convite
- ▶ **dar respostas rápidas e úteis** quando os utilizadores comunicam um problema e dar feedback sobre o que aconteceu.



Necessita de ajuda para denunciar conteúdos perturbadores?

A rede de Centros para uma Internet mais Segura em toda a Europa pode ajudá-lo! Independentemente do assunto, os centros estão disponíveis para oferecer apoio, ajuda prática e orientação, bem como alguém para o ou a ouvir.

3. Recomendações

j. Ferramentas para pais e encarregados de educação

Os pais e os encarregados de educação podem ajudar as crianças e os jovens a manterem-se seguros em linha. As plataformas podem disponibilizar ferramentas que apoiem este papel **sem comprometer os direitos ou a autonomia dos jovens**.

Se as plataformas escolherem ferramentas de controlo parental para complementar as suas funcionalidades de segurança obrigatórias, essas ferramentas devem:

- ▶ **basear-se na comunicação e na capacitação**, não no controlo
- ▶ **respeitar a privacidade das crianças e dos jovens** e informá-los sempre que um dos pais ou um cuidador ativar essas ferramentas
- ▶ **funcionar em todos os dispositivos e versões de software**
- ▶ **ser compatíveis com as ferramentas parentais existentes**, como as incorporadas nos telemóveis ou nas aplicações.



As ferramentas de controlo parental podem ajudar as famílias a criar laços de confiança e apoio mútuo, mas nunca **devem ser utilizadas** para fins de vigilância ou para retirar os direitos às crianças. Além disso, não devem substituir as funcionalidades de segurança incorporadas na plataforma.



Precisa de apoio como pai ou encarregado de educação? O BIK Parent Corner oferece sugestões que lhe podem ser úteis para fomentar o desenvolvimento de hábitos digitais saudáveis nos seus filhos, assim como para potenciar uma navegação mais segura no mundo em linha.

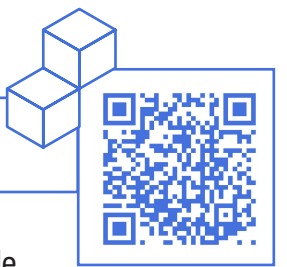


4. Quem garante o cumprimento das regras do RSD?

Cada país da UE tem um **coordenador dos serviços digitais (CSD)**, que colabora com a Comissão Europeia para supervisionar e acompanhar a forma como as plataformas aplicam o RSD.



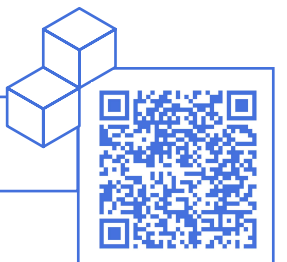
Leia o código QR para saber quem é o coordenador dos serviços digitais no seu país



Cada CSD pode nomear organizações especializadas na identificação e sinalização de conteúdos ilegais e nocivos. São os chamados **«trusted flaggers»** (sinalizadores de confiança) e, quando manifestam preocupações, as plataformas devem agir rapidamente! Pense neles como árbitros que assinalam os problemas assim que os detetam.



Leia o código QR para saber quem são os trusted flaggers no seu país.



5. O que acontece a seguir?

A Comissão Europeia e os Estados-Membros da UE continuarão a assegurar que as plataformas cumprem o RSD e mantêm as crianças e os jovens seguros em linha. Em conjunto, estão a:

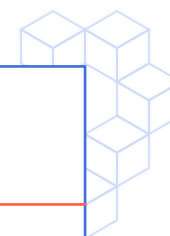
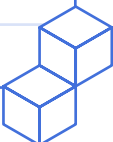
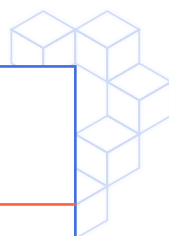
- ▶ **verificar se as plataformas cumprem as orientações sobre a proteção de menores ao abrigo do RSD e a instaurar processos judiciais caso tal não aconteça**
- ▶ **testar e lançar a aplicação de verificação da idade da UE**
- ▶ **desenvolver um plano de ação europeu contra a perseguição em linha**
- ▶ **analisar o impacto da utilização das redes sociais na saúde mental das crianças e dos jovens.**

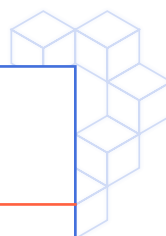


Maioridade digital

A maioridade digital corresponde à idade a partir da qual se pode começar a utilizar serviços em linha de forma autónoma, sem necessidade de autorização dos pais. Geralmente, esta idade é de 13 ou 18 anos, consoante as regras do país em questão e o tipo de serviço.







Onde se pode obter mais informações e ajuda?

Texto integral das orientações do RSD sobre a proteção de menores



Portal «Melhor Internet para as Crianças»



Seja qual for a sua idade, se é pai, cuidador ou educador, pode contactar o Centro para uma Internet mais Segura do seu país para obter apoio ou informações sobre qualquer questão relacionada com a Internet.

A ajuda está sempre disponível, seja por **telefone**, **correio eletrónico** ou **chat em linha**, e é **gratuita!**



Este opúsculo, dirigido às famílias, explica de forma simples as orientações da Comissão Europeia sobre a proteção dos menores, em conformidade com a Lei dos Serviços Digitais. Mostra como as plataformas em linha devem proteger as crianças e os jovens, dando prioridade aos seus direitos, integrando a privacidade e a segurança no *design* da plataforma, verificando a idade, tomando as definições privadas, projetando interfaces seguras, moderando conteúdos prejudiciais, facilitando a denúncia e apoiando os pais — para que os mais jovens possam desfrutar da Internet com confiança e segurança.

Comissão Europeia
Direção-Geral das Redes de Comunicação,
Conteúdos e Tecnologias
Manuscrito terminado em outubro de 2025

Esta publicação destina-se apenas a fins informativos e não constitui um documento legal.

Luxemburgo: Serviço das Publicações da União Europeia, 2025

© União Europeia, 2025



Descarregue este folheto em:
<https://link.europa.eu/cgyKch>



A política de reutilização da Comissão é estabelecida nos termos da Decisão 2011/833/UE da Comissão, de 12 de dezembro de 2011, relativa à reutilização de documentos da Comissão (JO L 330 de, 14.12.2011, p. 39, ELI: <http://data.europa.eu/eli/dec/2011/833/oj>). Salvo indicação em contrário, a reutilização do presente documento é autorizada ao abrigo da licença «Atribuição 4.0 Internacional (CC BY 4.0)» da Creative Commons (<https://creativecommons.org/licenses/by/4.0/>). Tal significa que a reutilização é autorizada desde que seja feita uma menção adequada da origem do documento e que sejam indicadas eventuais alterações.

PDF ISBN 978-92-68-31237-7 KK-01-25-130-PT-N doi:10.2759/7702114

Print ISBN 978-92-68-31238-4 KK-01-25-130-PT-C doi:10.2759/0136252



Serviço das Publicações
da União Europeia

DSA for YOUTH