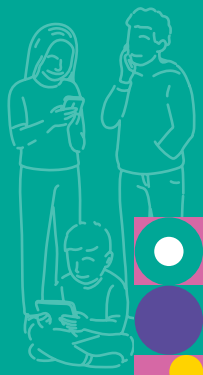


GLOSSÁRIO SOBRE PROTEÇÃO DE CRIANÇAS E ADOLESCENTES EM AMBIENTES DIGITAIS

André Freire
Filipe Medon

edições câmara

Câmara dos Deputados
57ª Legislatura | 2023 — 2027

Presidente
Hugo Motta

1º Vice-Presidente
Altineu Côrtes

2º Vice-Presidente
Elmar Nascimento

1º Secretário
Carlos Veras

2º Secretário
Lula da Fonte

3ª Secretária
Delegada Katarina

4º Secretário
Sergio Souza

Suplentes de secretários

1º Suplente
Antonio Carlos Rodrigues

2º Suplente
Paulo Folletto

3º Suplente
Dr. Victor Linhalis

4º Suplente
Paulo Alexandre Barbosa

Secretário-Geral da Mesa
Lucas Ribeiro Almeida Júnior

Diretor-Geral
Guilherme Barbosa Brandão

Câmara dos Deputados

GLOSSÁRIO SOBRE PROTEÇÃO DE CRIANÇAS E ADOLESCENTES EM AMBIENTES DIGITAIS

André Freire

Filipe Medon

Brasília, 2025

edições câmara

Câmara dos Deputados
Diretoria-Geral: Guilherme Barbosa Brandão
Centro de Documentação e Informação: Sergio Sampaio Contreiras de Almeida
Coordenação Edições Câmara: Ana Lígia Mendes

Edição: Ana Viana e Rachel De Vico
Preparação de originais: Ana Viana
Revisão: Mariana Moura
Projeto gráfico e diagramação: Patrícia Weiss

Linha Cidadania.

Dados Internacionais de Catalogação-na-publicação (CIP)
Coordenação de Biblioteca. Seção de Catalogação.
Bibliotecária: Débora Machado de Toledo – CRB1: 1303

Freire, André.
Glossário sobre proteção de crianças e adolescentes em ambientes digitais [recurso eletrônico] / André Freire, Filipe Medon. -- Brasília : Câmara dos Deputados, Edições Câmara, 2025.

Versão e-book
Modo de acesso: livraria.camara.leg.br
Disponível, também, em formato impresso.
ISBN 978-85-402-1171-1

1. Direitos da criança, vocabulários, glossários etc. 2. Proteção de menor, vocabulários, glossários etc. 3. Segurança de dados. 4. Proteção de dados pessoais. 5. Internet. I. Medon, Filipe. II. Título.

CDU 342.726-053.2:004(03)

ISBN 978-85-402-1170-4 (papel) ISBN 978-85-402-1171-1 (e-book)

Câmara dos Deputados
Centro de Documentação e Informação — Cedi
Coordenação Edições Câmara — Coedi
Palácio do Congresso Nacional — Anexo 2 — Térreo
Praça dos Três Poderes — Brasília (DF) — CEP 70160-900
Telefone: (61) 3216-5833
livraria.camara.leg.br

Sumário

Apresentação

Traduzindo a lei em proteção real

É com profunda satisfação que celebro com vocês o lançamento deste *Glossário sobre proteção de crianças e adolescentes em ambientes digitais*, resultado do trabalho dedicado e incansável do Grupo de Trabalho de Proteção de Crianças e Adolescentes em Ambientes Digitais, coordenado pela deputada Rogéria Santos.

A Câmara dos Deputados é a Casa do povo brasileiro, e não há missão mais nobre para um Parlamento do que zelar pelo futuro de uma nação — e esse futuro tem nome: são nossas crianças e nossos adolescentes. Quando o ECA Digital (Lei 15.211/2025) foi aprovado e sancionado, demos um passo histórico para que o Brasil se tornasse referência mundial na proteção de meninos e meninas no ambiente digital. Mas sabemos que leis, por mais bem elaboradas que sejam, só ganham vida quando chegam às pessoas, quando são compreendidas, apropriadas e praticadas no dia a dia.

Este glossário é a prova de que legislar vai além de aprovar textos legais. É preciso traduzi-los, explicá-los, torná-los acessíveis a quem mais precisa dessa informação. É fundamental que falemos a mesma língua — que famílias entendam o que seus filhos vivenciam *online*, que educadores saibam identificar

sinais de risco, que crianças e adolescentes conheçam seus direitos e saibam como se proteger.

Vivemos tempos de transformação. A internet deixou de ser apenas uma ferramenta e se tornou um espaço de convivência, aprendizado, trabalho e lazer. Nossas crianças já nascem conectadas, crescem explorando aplicativos e plataformas, e constroem suas identidades também no mundo virtual. Essa realidade é repleta de oportunidades extraordinárias, mas também nos apresenta responsabilidades inadiáveis — e a primeira delas é garantir que todos tenham condições de compreender os riscos e as ferramentas de proteção disponíveis.

Expressões como "*cyberbullying*", "*grooming*", "*deepfake*", "sextorsão" e "conta vinculada" deixaram de ser jargões técnicos para se tornarem parte do cotidiano de milhões de famílias. Este glossário oferece a cada uma dessas famílias, a cada escola, a cada criança e adolescente a chave para decifrar essa linguagem e transformá-la em ação protetiva. Mais do que definições, vocês encontrarão aqui orientações práticas, canais de denúncia e caminhos concretos para enfrentar situações de risco.

Quero deixar um recado especial para as crianças e adolescentes que lerão estas páginas: vocês são incríveis. Sua geração domina tecnologias que nossos avós nem sonhavam existir. Vocês criam, inovam, conectam-se com o mundo inteiro com apenas alguns toques na tela. Contudo, lembrem-se sempre: por trás de cada tela, há um ser humano; por trás de cada perfil, há dignidade que merece respeito; por trás de cada clique, há consequências reais. Este glossário está aqui para ajudá-los a navegar com segurança e consciência.

E para os familiares, educadores e todos os adultos que zelam por essas vidas preciosas: vocês não estão sozinhos nessa jornada. O Parlamento brasileiro está ao lado de vocês, trabalhando todos os dias para criar um ambiente digital mais seguro, ético e educativo. Usem este material, conversem com seus filhos, façam perguntas, ouçam com atenção, estabeleçam combinados. A proteção digital começa em casa, mas conta com o apoio das instituições.

Agradeço imensamente à deputada Rogéria Santos e a todos os membros do GT pela dedicação exemplar. Agradeço também aos técnicos, consultores, especialistas e representantes da sociedade civil que contribuíram para a construção deste material. O trabalho de vocês transforma complexidade em clareza, transforma lei em proteção real e planta sementes que florescerão em gerações mais conscientes e preparadas.

A Câmara dos Deputados renova seu compromisso: continuaremos legislando, fiscalizando, educando e dialogando para que o Brasil seja, cada vez mais, um país onde todas as crianças e adolescentes possam desenvolver plenamente seu potencial, seja nas ruas, nas escolas ou no vasto universo digital.

Que este glossário seja uma bússola para famílias, uma ferramenta para educadores e um escudo para nossas crianças e adolescentes.

Boa leitura e boas conversas em família!

Hugo Motta
Presidente da Câmara dos Deputados

Prefácio

Uma linguagem comum para proteger nossas crianças e adolescentes

É com imensa alegria e senso de responsabilidade que apresento a vocês este *Glossário sobre proteção de crianças e adolescentes em ambientes digitais*, fruto de um trabalho coletivo, dedicado e apaixonado do Grupo de Trabalho de Proteção de Crianças e Adolescentes em Ambientes Digitais, que tenho a honra de coordenar na Câmara dos Deputados.

A internet transformou o mundo e abriu portas inimagináveis para o aprendizado, a criatividade e a conexão entre pessoas. Nossos meninos e meninas merecem crescer em um ambiente digital seguro, educativo e repleto de oportunidades. Mas, como toda grande transformação, o mundo digital também trouxe desafios que precisamos enfrentar juntos — e o primeiro passo para enfrentar qualquer desafio é compreendê-lo.

Por isso, criamos este glossário: para que falemos a mesma língua. Para que famílias e escolas compreendam os termos usados por crianças, adolescentes e

jovens na internet. Para que crianças e adolescentes entendam as palavras, siglas, serviços e leis criados para sua proteção. Para que ninguém se sinta perdido diante de expressões como "*cyberbullying*", "*grooming*", "*deepfake*", "sextorsão" ou "conta vinculada".

Ao longo desta jornada, conquistamos avanços históricos. Aprovamos e vimos sancionado o ECA Digital (Lei 15.211/2025), uma legislação pioneira que atualiza o Estatuto da Criança e do Adolescente para a era digital. Trabalhamos incansavelmente em cinco frentes fundamentais:

- **Educação e letramento digital:** porque conhecimento é proteção. Crianças e adolescentes que compreendem como funcionam as tecnologias digitais, que sabem identificar riscos e usar a internet de forma crítica e responsável estão mais preparados para aproveitar tudo de bom que o mundo digital oferece.
- **Proteção de dados pessoais:** porque a privacidade de nossas crianças e adolescentes não estão à venda. Defendemos regras claras para que empresas respeitem a infância e a adolescência e não explorem dados de meninos e meninas para fins comerciais.
- **Regulamentação do trabalho artístico infantojuvenil em ambientes digitais:** porque talentos mirins que brilham nas telas e plataformas digitais merecem proteção trabalhista, dignidade e respeito aos seus direitos fundamentais.

- **Reforço da legislação penal contra crimes virtuais:** porque deve-se ter tolerância zero com quem ameaça a segurança de nossas crianças. Aprimoramos as leis para punir com rigor crimes como abuso, exploração sexual, *cyberbullying* e aliciamento *online*.
- **Regulação da inteligência artificial (IA) voltada ao público infanto-juvenil:** porque as tecnologias do futuro precisam ser construídas com ética, transparência e o bem-estar das crianças no centro das decisões.

Mas nossa missão não termina aqui. Mesmo após a aprovação do ECA Digital, este GT segue firme, vigilante e comprometido. A proteção da infância e adolescência no ambiente digital é um trabalho contínuo, que exige atualização constante, diálogo permanente com a sociedade e coragem para enfrentar novos desafios.

Este glossário que você tem em mãos é mais do que um dicionário técnico: é um instrumento de cidadania digital. É uma ponte entre o Parlamento e as famílias brasileiras. É um convite ao diálogo em casa e na escola. É uma ferramenta de empoderamento que transforma linguagem complexa em conhecimento acessível, permitindo que cada pessoa se torne protagonista da proteção digital.

Queremos que cada criança e adolescente se sinta seguro para explorar o mundo digital, que cada familiar tenha recursos para orientar e proteger, que cada educador disponha de instrumentos para ensinar e prevenir. Sem materiais claros e acessíveis, os comandos legais permanecem distantes do coti-

diano. Por isso, este glossário materializa nosso compromisso de fazer o ECA Digital sair do papel e entrar na vida real.

Juntos, estamos construindo um Brasil onde o digital e o humano caminham lado a lado, onde a tecnologia serve às pessoas e não o contrário, onde cada criança pode explorar, aprender, criar e sonhar em segurança.

Que esta leitura inspire conversas, desperte reflexões e fortaleça os laços de cuidado e proteção que tecem nossa sociedade.

Com carinho e compromisso,

Deputada Rogéria Santos
Coordenadora do Grupo de Trabalho de Proteção de Crianças e Adolescentes em Ambientes Digitais

Nota dos autores

O uso de internet entre crianças e jovens entre 9 e 17 anos é praticamente universal e começa cada vez mais cedo. Redes sociais, jogos e serviços de vídeo curto passaram a mediar amizades, autoexpressão, consumo cultural e estão inseridos em atividades de lazer, estudo, trabalhos escolares, etc. Esse cenário traz oportunidades (aprendizagem, criatividade, participação cívica), mas também expõe crianças e jovens a inúmeros riscos (exposição sexual, assédio, *bullying*, desafios perigosos, golpes, publicidade predatória e coleta de dados excessiva). Por essa razão, a proteção integral — princípio estruturante do Estatuto da Criança e do Adolescente (ECA) — precisou se atualizar para o contexto digital.

A sanção do ECA Digital (Lei 15.211/2025) organiza deveres concretos para plataformas, lojas de aplicativos, jogos e demais serviços com provável acesso por menores, e atribui responsabilidades compartilhadas a famílias, escolas e poder público.

O debate extrapola a técnica jurídica: trata de governança de dados e desenho algorítmico, saúde mental, educação midiática, integridade física e dignidade sexual dessas pessoas em desenvolvimento. O ECA Digital responde a riscos que deixaram de ser marginais — *grooming*, sextorsão, hiperexposição, publi-

cidade predatória e práticas de perfilamento — e busca harmonizar inovação com o melhor interesse da criança e do adolescente. Nesse cenário, a comunicação qualificada é condição de eficácia normativa, pois, sem materiais claros e acessíveis para famílias, escolas e rede de proteção, os comandos legais permanecem distantes do cotidiano. É fundamental que falemos a mesma língua, que família e escola compreendam os termos usados por crianças e jovens na internet, e que crianças e jovens saibam mais sobre termos, siglas, serviços e leis cunhados para sua proteção.

Este glossário foi pensado como um instrumento para quem educa, protege e decide em meio a telas. Com uma linguagem clara e com base em exemplos reais, esta publicação tem o intuito de auxiliar famílias, escolas e a sociedade, como um todo, para que o ECA Digital e demais normas que cuidam da proteção de crianças e adolescentes em ambientes digitais se transformem em atitudes cotidianas que realmente protejam.

André Freire

Analista legislativo, coordenador de comissões
da liderança do Republicanos

Filipe Medon

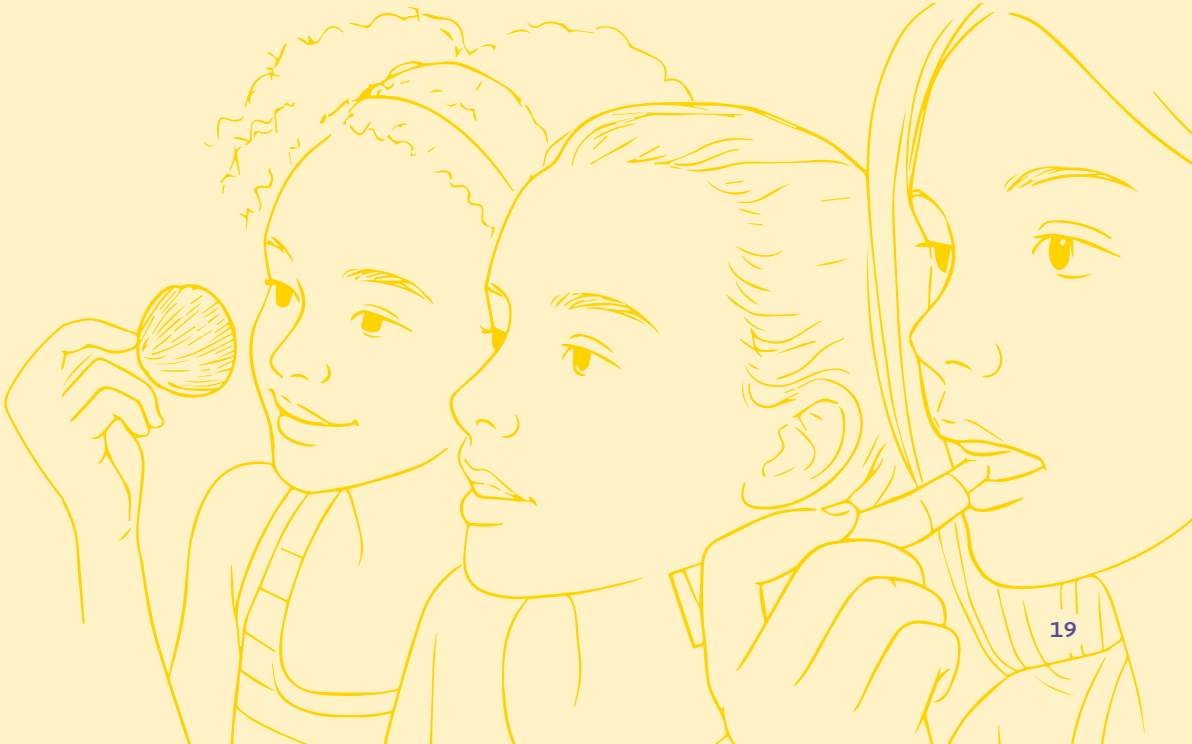
Professor de Direito Civil na FGV Direito Rio.
Doutor e Mestre em Direito Civil pela UERJ

Glossário

Adultização

Termo usado para definir exposição precoce de crianças a conteúdos ou padrões adultos (sexualização, estética, responsabilidades).

Esse tipo de exposição pode causar ansiedade, distorção de autoimagem e aumento de riscos *online*.



Aliciamento *online*

Quando um adulto se aproxima de uma criança pela internet para fins sexuais.

Também conhecido no ambiente digital pelo termo de língua inglesa "*grooming*".

Para esse tipo de aproximação, os criminosos usam estratégias como fingir ter a mesma idade e interesses, oferecer presentes como jogos, dinheiro, etc.; demonstrar compreensão especial e empatia, por meio de expressões como "só eu te entendo". Com o tempo, vão normalizando conversas sobre sexo e induzem a criança a não contar para os familiares, depois começam a pedir fotos cada vez mais íntimas, até evoluir para a marcação de encontros presenciais.

Pesquisas como a TIC Kids Online Brasil[1] e diversas pesquisas internacionais indicam um risco maior quando há contato com desconhecidos em redes sociais e jogos *online*.

1 A pesquisa TIC Kids Online Brasil tem como objetivo gerar evidências sobre o uso da internet por crianças e adolescentes no Brasil. Realizada desde 2012, produz indicadores sobre oportunidades e riscos relacionados à participação *online* da população de 9 a 17 anos no Brasil. Disponível em: https://cetic.br/pesquisa/kids-online/. Acesso em: 10 dez. 2025.

Em geral, o *grooming* pode evoluir para abuso sexual virtual ou presencial, sextorsão, chegando ao limite de tráfico de pessoas.

Família

- Converse abertamente sobre riscos de interagir com desconhecidos em ambiente digital.
- Ofereça um canal de confiança. Deixe claro que, se acontecer algo estranho e a criança te contar, você não vai brigar ou tirar o celular, mas que você está ali para proteger.

Criança e adolescente

- Nem todo mundo na internet é quem diz ser. Adultos podem fingir ser adolescentes.
- Nunca compartilhe fotos íntimas, documentos, endereço ou informações pessoais, como a escola em que você estuda.
- Caso alguém peça que você guarde segredo dos familiares ou te convide para um encontro escondido, bloqueie e conte imediatamente para um adulto.

Escola

- Explique em linguagem acessível e adaptada a cada idade o que é *grooming* e como pedir ajuda.
- Oriente sobre canais oficiais de denúncia.
- Treine profissionais para identificar mudanças comportamentais (isolamento, segredos excessivos, presentes sem explicação).
- Promova educação sobre consentimento, limites corporais e relações saudáveis.

Algoritmo de recomendação

São *softwares* que se conectam ao banco de dados de uma página *online* e avaliam as interações dos usuários para entregar as recomendações mais alinhadas ao seu perfil com base em determinados critérios.

Atrelados a sistemas de inteligência artificial, os algoritmos de recomendação podem amplificar riscos se forem otimizados apenas para engajamento em, por exemplo, *sites*, plataformas, redes sociais, jogos ou aplicativos que sugerem vídeos ou conteúdo com base em comportamento. Isso pode prender crianças em bolhas de conteúdo inadequado ou viciante.

Ambiente digital

Local onde ocorrem interações, transações e comunicações por meio da internet. Como o ambiente digital abrange uma vasta gama de plataformas (redes sociais, *sites*, aplicativos e serviços *online*, que permitem que indivíduos e empresas se conectem e compartilhem informações), é acessado constantemente também por crianças e adolescentes.

ANPD

Agência Nacional de Proteção de Dados (ANPD). É o órgão do governo brasileiro que atua como o guardião dos dados pessoais de todos os cidadãos. Sua função principal é fiscalizar se empresas, *sites* e aplicativos estão respeitando a privacidade e protegendo corretamente as informações dos usuários, aplicar multas e atender a denúncias de vazamento de dados quando necessário. Essa fiscalização garante que a Lei Geral de Proteção de Dados Pessoais (LGPD) seja cumprida, assegurando que os usuários, incluindo crianças e adolescentes, possam navegar na internet com mais segurança e ter seus direitos de privacidade respeitados. Com a sanção do ECA Digital, a ANPD ganhou poderes especiais para reforçar a proteção infantojuvenil no ambiente *online*. O órgão é responsável por exigir que as plataformas digitais implementem mecanismos de verificação de idade, garantam que as configurações de privacidade sejam seguras por padrão para os menores e fiscalizem os algoritmos que recomendam conteúdo, evitando a exposição a riscos. Em casos de descumprimento das regras de proteção, a ANPD tem o poder de aplicar sanções rigorosas, como multas e até mesmo o bloqueio de plataformas, garantindo que o melhor interesse da criança e do adolescente prevaleça no ambiente digital.

Avaliação de impacto (AIPD/AIR)

Avaliação de Impacto à Proteção de Dados (AIPD) e Avaliação de Impacto aos Direitos da Criança e do Adolescente (AIR) são estudos obrigatórios que empresas, plataformas digitais e desenvolvedores de aplicativos devem fazer antes de lançar produtos ou serviços voltados para crianças e adolescentes, ou que possam coletar dados desses públicos.

Esses documentos avaliam quais riscos o produto pode trazer à privacidade, segurança, desenvolvimento e bem-estar de menores de idade, e descrevem as medidas de proteção adotadas para evitar ou reduzir esses riscos. Por exemplo: um novo aplicativo de rede social deve analisar riscos como exposição a conteúdo impróprio, contato com predadores sexuais, *cyberbullying*, coleta excessiva de dados pessoais e vício digital, além de demonstrar como vai proteger crianças e adolescentes através de verificação de idade, moderação de conteúdo, ferramentas de denúncia, controles parentais e configurações de privacidade reforçadas.

A ANPD pode exigir essas avaliações e aplicar sanções caso empresas não as realizem ou descumpram as medidas de proteção propostas, conforme previsto no ECA Digital (Lei 14.811/2024) e na LGPD (Lei 13.709/2018).

Boas práticas (*by design/by default*)

Princípios de ***design*** e implementação que garantem que sistemas, produtos ou processos sejam seguros, eficientes e éticos desde o início, sem a necessidade de medidas adicionais por parte do usuário final.

Consentimento digital

Autorização clara, informada e voluntária para que suas informações, fotos, vídeos ou outros conteúdos pessoais sejam usados ou compartilhados no ambiente digital.

No caso de crianças e adolescentes, o consentimento deve sempre ser visto com muito cuidado, porque há assimetria de poder, imaturidade e possibilidade de pressão ou manipulação.

Menores de 18 anos não podem “consentir” com conteúdo sexual. Produzir, enviar, receber, armazenar ou compartilhar imagens íntimas de pessoas menores de 18 anos é crime, mesmo que a própria pessoa tenha “autorizado”.

Família e escola

- Trabalhe o conceito de autonomia corporal, limites pessoais e intimidade também no ambiente digital.
- Reforce que a responsabilidade nunca é da criança ou do adolescente quando há exploração, manipulação ou crime.
- Explique, em linguagem acessível, que consentimento não é definitivo, pode ser retirado, e que o adulto tem dever de cuidado e proteção — inclusive ao orientar sobre envio de imagens, exposição em redes sociais e tratamento de dados pessoais.

Adolescente

- Você tem o direito de dizer “não”. Ninguém pode exigir que você compartilhe fotos, vídeos ou dados pessoais.
- Você pode mudar de ideia e retirar o consentimento (por exemplo, pedir para apagar uma foto).
- Pressão, chantagem, insistência ou ameaça anulam o consentimento, pois quando há medo, culpa ou constrangimento, não há escolha livre.
- Argumento do tipo “mas você aceitou” não é desculpa para abuso, violência, exposição ou chantagem.
- Você não é obrigado(a) a enviar foto, vídeo ou qualquer conteúdo íntimo porque alguém pediu, ameaçou terminar o namoro, zombou ou pressionou.
- Consentimento para ver uma foto não é consentimento para salvar, reenviar ou postar essa foto.
- Se algo te deixar desconfortável, com medo ou com vergonha, procure um adulto de confiança, a escola ou a rede de proteção.

Conta vinculada

O ECA Digital determina que as contas de redes sociais para menores de 16 anos devem estar vinculadas ao CPF de um responsável legal. Essa medida exige que as plataformas digitais implementem ferramentas de supervisão e verificação de idade para proteger crianças e adolescentes de conteúdos inadequados.

Conteúdo limítrofe

Conteúdo que quase viola as regras da plataforma, como *posts* sexualmente sugestivos, violentos, notícias falsas distribuídas para menos pessoas, exposição de informações privadas ou inadequadas para menores (linguagem adulta, violência sutil).

Em geral, esse tipo de conteúdo não é removido pelas plataformas, mas é rebaixado pelo algoritmo para não viralizar.

Controle parental

Conjunto de ferramentas, configurações e combinações de regras que ajudam familiares e responsáveis a acompanhar e organizar o uso de celulares, computadores, televisões conectadas, consoles, aplicativos, jogos e redes sociais por crianças e adolescentes. O objetivo principal é proteger e educar, e não vigiar ou punir: apoiar o uso seguro da tecnologia, respeitando a idade, a maturidade e o direito à privacidade em desenvolvimento.

Em geral, os principais recursos do controle parental permitem: limitar tempo de uso de aplicativos, jogos e telas; restringir conteúdos e aplicativos impróprios para a idade (classificação indicativa, filtros de busca); filtrar *sites* com conteúdo violento, sexual ou inadequado; definir horários de uso (por exemplo, bloquear à noite ou em horário de estudo); restringir quem pode entrar em contato com a criança ou adolescente em determinados serviços; receber relatórios gerais de atividade, quando disponíveis (tempo de tela, tipos de aplicativos usados etc.). O ideal é que esses recursos sejam utilizados de forma transparente e que a criança ou o adolescente seja informado das regras de supervisão.

Controle parental não substitui diálogo, afeto e presença. Use as ferramentas como apoio educativo, não apenas como forma de vigilância ou castigo. Evite monitoramento secreto: isso quebra a confiança e dificulta que a criança peça ajuda quando realmente precisar.

Para configurar o controle parental

1. Acesse as configurações de segurança, privacidade ou “controle parental” do dispositivo ou serviço. Crie, se possível, perfis separados para adultos e para crianças/adolescentes. Ajuste limites de tempo de tela, classificação indicativa de conteúdo, filtros e horários de uso.
2. Revise periodicamente as regras, de acordo com a idade, a maturidade e as necessidades da criança ou adolescente. Sempre explique o que está sendo feito e por que está sendo feito.

Família e escola

- Estabeleça regras em conjunto, em linguagem acessível, explicando o porquê de cada limite (sono, estudo, segurança, bem-estar emocional).
- Combine controle parental com conversas sobre: privacidade, intimidade e compartilhamento de fotos, vídeos e dados pessoais; como reagir a conteúdos violentos, sexuais, preconceituosos ou perturbadores; como pedir ajuda em situações de medo, vergonha, ameaça ou exposição.
- Com adolescentes mais velhos, envolva-os na definição de limites razoáveis. Isso fortalece confiança, senso de responsabilidade e o uso crítico e seguro das tecnologias digitais.

Cyberbullying

Termo de língua inglesa usado para descrever a prática de agressão sistemática e perseguição no ambiente virtual.

Segundo diversos estudos, parcela significativa de crianças e adolescentes relata experiências de ofensa e constrangimento *online*, com impacto na saúde mental e desempenho escolar. O *cyberbullying* se diferencia do *bullying* tradicional porque tem alcance massivo (viralização); maior permanência, pois o conteúdo fica *online*; e anonimato facilitado, em razão da possibilidade de criação de perfis falsos. As consequências para a vítima vão de queda no rendimento escolar, recusa de ir à escola, transtornos de sono e alimentação, isolamento social, ansiedade, depressão, chegando até mesmo a ideação suicida.

Cyberbullying é crime previsto em lei!

(Lei 14.811/2024, sobre intimidação sistemática virtual).

Família

- Peça para ver como são as conversas em grupos.
- Ajude a criança a registrar ofensas (*prints* com data/hora), bloquear e denunciar.
- Se seu filho é vítima, acredite, acolha e não minimize.
- Se seu filho for o agressor, não ignore. Busque entender o porquê e responsabilize educativamente. Acione a escola e, se necessário, o Conselho Tutelar ou a polícia.

Escola

- Estabeleça políticas claras de combate ao *bullying* e ao *cyberbullying*, incluindo consequências pedagógicas, e não apenas punitivas, que trabalhem empatia, respeito e cidadania digital.
- Deixe claro que o *bullying* e o *cyberbullying* não serão tratados como "brincadeira" ou "conflito entre alunos".
- Integre as famílias no enfrentamento.
- Crie um canal seguro para denúncias e uma política de acolhimento para quem sofre e para quem testemunha.

Criança e adolescente

- Se não é engraçado para todo mundo, é *bullying*.
- Se está acontecendo com você, não é frescura e não é culpa sua: conte para um adulto de confiança.
- Se você está "zoando" com alguém, mesmo que "só *online*", pare! Isso pode causar sofrimento real e pode ser considerado crime.
- Se você vê que está acontecendo com outra pessoa, não compartilhe e apoie quem está sofrendo.

Deep web

Termo de língua inglesa usado para descrever a maior parte da internet, que não é indexada por buscadores comuns (como Google ou Bing).

A *deep web* inclui páginas que exigem *login* e senha (como e-mail pessoal ou conta bancária) e que, por essa razão, não são perigosas por si só.

Entretanto, o acesso a uma pequena parte da *deep web* exige o uso de programas especiais (como o navegador Tor). Essa parte se chama *dark web*, um ambiente anônimo e altamente perigoso porque possibilita atividades ilegais graves, como crimes sexuais, pornografia infantil e exploração sexual, tráfico, venda de drogas, de armas, de documentos falsos, além de crimes financeiros, fraudes, roubo de dados e contratação de crimes.

Família e escola

- A presença de navegadores como Tor, I2P ou Freenet no dispositivo de uma criança ou adolescente é um sinal de alerta grave. Caso os encontre, converse imediatamente com seu filho ou aluno e busque orientação profissional

Criança e adolescente

- Não tente acessar a *dark web* nem mesmo por curiosidade. Acessar certos conteúdos é crime, mesmo que seja "só para ver". Você corre o risco de se deparar com conteúdos traumáticos e perturbadores. Existe o risco de rastreamento por criminosos e de infecção por vírus e *malware*.

Deepfake

Termo de língua inglesa usado para descrever uma técnica de manipulação de mídia que utiliza inteligência artificial para criar vídeos, áudios e imagens falsos com um realismo impressionante. A tecnologia permite substituir rostos, clonar vozes e simular ações de forma que pareçam autênticas, dificultando a distinção entre conteúdo real e sintético.

As *deepfakes* podem ser usadas de maneira maliciosa para desinformação política e social (*fake news* sofisticadas), aplicação de golpes financeiros (como vídeos falsos de familiares pedindo dinheiro) e possibilitam que se coloque o rosto de pessoas — inclusive de crianças e adolescentes — em cenas íntimas e situações vexatórias. Isso acarreta inúmeros problemas como perda de confiança na realidade (“nada mais é verdade”) e danos irreparáveis à reputação e à saúde mental.

Crianças e adolescentes são especialmente vulneráveis, tanto a acreditar e compartilhar quanto a se tornar vítimas de *deepfake*. Por isso, é importante que a família e a escola invistam em educação midiática, a fim de alfabetizar crianças e adolescentes para que possam se defender de informações falsas.

Família

- Se seu filho for vítima de *deepfake*, preserve as evidências (baixe o vídeo, faça *prints*), denuncie à polícia, às plataformas e busque a SaferNet. Apoio psicológico e jurídico é essencial.

Escola

- Promover alfabetização midiática: como verificar fontes, identificar sinais de manipulação digital (inconsistências, verificação reversa de imagens), checagem de fatos.
- Propor discussões sobre ética no uso de IA.
- Ter protocolos para casos de *deepfakes* que envolvam estudantes (tratar com urgência e seriedade).
- Convidar checadores de fatos ou jornalistas para oficinas com estudantes.

Criança e adolescente

- Antes de compartilhar qualquer conteúdo chocante, para e pense: será que isso é verdade? Procure a mesma notícia em *sites* confiáveis (grandes jornais, veículos conhecidos). Se receber *deepfake* que mostre você ou colegas em situação constrangedora, denuncie imediatamente.

Desafios perigosos *online*

São desafios virais ou brincadeiras que circulam nas redes sociais e que colocam em risco grave a saúde física e mental, podendo causar lesões permanentes ou, em casos extremos, a morte.

Entre esses riscos, estão desafios que envolvem autolesão ou indução ao suicídio, que causam sufocamento, queimaduras graves ou intoxicação, ou que forçam o envio de *nudes* como "prova de coragem".

Em geral, os jovens participam desses desafios motivados por pressão do grupo ("todo mundo está fazendo"), desejo de aceitação e popularidade, busca por likes, imaturidade para avaliar as consequências, busca por emoções fortes ou manipulação por adultos criminosos (que usam o desafio como isca).

Atenção!

Esses tipos de desafios já causaram mortes no Brasil e no mundo.

Plataformas

O ECA Digital exige que seja prioridade máxima das plataformas digitais a remoção e a redução do alcance de qualquer conteúdo que promova ou incentive a autolesão, o suicídio ou a participação em desafios perigosos.

Família

- Conheça os riscos.
- Busque informações em fontes confiáveis para se manter atualizado.

Escola

- Promova debates sobre pensamento crítico e pressão de grupo, mas evite mencionar os nomes dos desafios para não despertar curiosidade.

Criança e adolescente

- Priorize sua proteção.
- Não participe de desafios *online*. Sua vida e saúde não têm preço, não importa quem está desafiando ou quantos *likes* você pode ganhar.
- Se alguém te desafiar:
  1. Diga NÃO com firmeza.
  2. Bloqueie quem insiste.
  3. Conte imediatamente para um adulto de confiança.
  4. Denuncie à plataforma e às autoridades.

Dependência digital

Uso excessivo e compulsivo da internet, dispositivos móveis e outras tecnologias digitais.

Segundo a pesquisa TIC Kids Online Brasil 2024, crianças entre 5 e 8 anos passam em média três horas por dia em frente a telas, e adolescentes ultrapassam cinco horas. O uso excessivo de dispositivos eletrônicos pode causar ansiedade, estresse, isolamento social, baixa produtividade, medo irracional de ficar sem o celular ou de não estar conectado (nomofobia).

Especialmente no período noturno, o uso excessivo causa privação de sono. Isso afeta o desenvolvimento cognitivo, memória, aprendizado e regulação emocional, além de proporcionar maior exposição a conteúdos inadequados, uma vez que os familiares estão dormindo e a criança fica sem supervisão.

Família

- Estabeleça regras claras de horário: sem celular no quarto à noite e desconexão duas horas antes de dormir.
- Use ferramentas de controle parental para definir limites de tempo.
- Desconecte-se junto com seu filho, pois seu exemplo é essencial.
- Observe sinais de dependência: irritação ao desligar, uso escondido, mentiras sobre tempo de tela. Incentive atividades *offline* (esporte, arte, leitura, tempo em família).

Escola

- Observe sinais de sonolência recorrente, desatenção e queda de rendimento. Converse com a família sobre isso.
- Trabalhe em projetos de bem-estar digital: gestão de tempo de tela, higiene do sono, equilíbrio *online*/*offline*. Promova "desafios de desconexão" ou "semanas sem tela" com prêmios para incentivar.

Discurso de ódio

Qualquer forma de comunicação oral e escrita ou comportamento que ataque ou utilize linguagem depreciativa ou discriminatória contra uma pessoa ou grupo, com base em sua identidade — como raça, religião, gênero, orientação sexual ou deficiência.

DM (mensagem direta)

Abreviação para *direct message*, termo de língua inglesa que significa uma mensagem enviada em um canal de contato privado nas redes sociais.

Nas contas para menores, recomenda-se que esses canais estejam desabilitados por padrão e que o acesso seja mediado.

ECA

Estatuto da Criança e do Adolescente (Lei 8.069/1990). Principal instrumento normativo do Brasil sobre os direitos da criança e do adolescente.

ECA Digital

Lei 15.211/25. Conjunto de novas regras que amplia os direitos fundamentais já previstos pelo ECA para proteger crianças e adolescentes no ambiente ***online***, estabelecendo obrigações para plataformas digitais, empresas, Estado, família e sociedade.

Educação midiática

Desenvolvimento de competências para analisar, avaliar e produzir conteúdo de forma crítica e responsável na internet. Capacita as pessoas a entender como as mídias funcionam, identificar desinformação e participar do ambiente informacional de maneira consciente e ética.

Estupro virtual

Agressão sexual perpetrada por meio de tecnologias digitais. Esse tipo de abuso envolve coerção, chantagem, manipulação emocional para convencer a vítima a participar de atividades sexuais *online* (como enviar fotos ou vídeos), criação de perfis falsos nas redes sociais ou em plataformas de relacionamento para enganar a vítima e induzi-la a compartilhar informações ou conteúdo íntimo.

Garantia de idade (*age assurance*)

Conjunto de técnicas usadas para confirmar a idade de um usuário, como documentos ou padrões de uso, que garante que menores de idade não acessem conteúdos impróprios.

Influenciador mirim

Criança ou adolescente que produz conteúdo em ambiente digital.

Jogos *online*

Jogos eletrônicos que funcionam pela internet e permitem que várias pessoas joguem juntas ao mesmo tempo, conversem por mensagem de texto ou voz e usem dinheiro real para fazer compras no jogo.

Os principais riscos dos jogos *online* incluem contato com desconhecidos (possível aliciamento), *cyberbullying*, gastos não autorizados e dependência digital.

O ECA Digital estabelece regras importantes: proíbe *loot boxes* (caixas-surpresa que funcionam como jogo de azar) para menores de 18 anos, exige que as *odds* sejam visíveis (ou seja, os jogos devem mostrar claramente a probabilidade real de ganhar cada item; por exemplo: "Espada Lendária: 0,5% de chance, ou seja, 1 em 200 tentativas"), estabelece limites claros de gastos e proíbe publicidade abusiva que pressione crianças a comprar. Para um uso seguro, é essencial verificar a classificação indicativa, configurar controles parentais, desabilitar ou limitar o chat, nunca compartilhar dados pessoais, estabelecer limites de tempo e dinheiro, e os familiares devem jogar junto com os filhos para conhecer o ambiente.

Denuncie jogos que descumprem essas regras à ANPD (www.gov.br/anpd), à plataforma de *download* ou ao Programa de Proteção e Defesa do Consumidor (Procon).

LGPD

Lei Geral de Proteção de Dados (Lei 13.709/2018). Tem como principal objetivo garantir a proteção aos dados pessoais, respeitados os direitos fundamentais de liberdade e de privacidade. Traz segurança jurídica ao tratamento dos dados pessoais e privacidade. Estabelece a transparência como um princípio orientador, garantindo que os dados pertencem ao titular, não à empresa.

Loot box (caixa de recompensa)

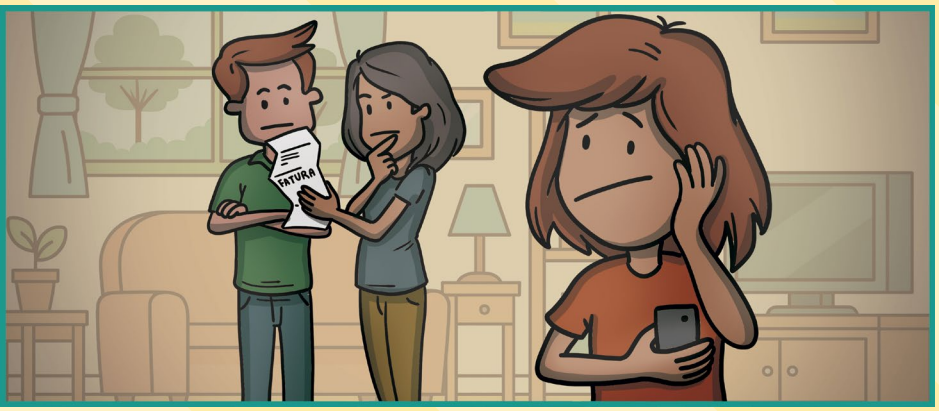
Itens virtuais em jogos eletrônicos que, ao serem abertos, liberam uma seleção aleatória de recompensas, como itens de personalização ou melhorias de equipamentos. As *loot boxes* podem ser compradas com dinheiro real ou moedas do jogo. Em razão de sua mecânica criar expectativa de recompensa, pode incentivar o vício e gastos compulsivos. Por essa razão, no Brasil, as *loot boxes* são proibidas para menores de 18 anos.

Mediação parental

Conjunto de atos que permitem aos familiares e responsáveis monitorar as atividades de uma criança. Pode envolver desde o acompanhamento presencial até o uso de ferramentas digitais para gerenciar o tempo de tela e o acesso a aplicativos e conteúdos *online*, com o objetivo de proteger crianças e adolescentes de perigos *online*, estabelecer limites e promover o bem-estar.

Melhor interesse da criança

Princípio jurídico que determina que todas as decisões sobre crianças e adolescentes — legais, políticas ou pessoais — devem priorizar seu bem-estar físico, psicológico e social. Isso significa que os interesses da criança devem prevalecer sobre os de qualquer outro adulto ou instituição, como em casos de guarda e adoção. O princípio orienta políticas públicas e decisões judiciais para proteger crianças de negligência, violência e exploração, garantindo seus direitos fundamentais como vida, saúde e educação.



Monetização

Estratégia de geração de receita a partir de cliques, visualizações, serviços pagos, cursos *online* via *sites*, aplicativos, canal de YouTube, etc.

Quando envolve crianças e adolescentes, a monetização requer limites rigorosos — porque crianças e adolescentes têm mais dificuldade de distinguir conteúdo orgânico de propaganda, ficando mais vulneráveis a riscos como consumismo precoce, golpes financeiros por *sites* falsos e *links* maliciosos, compras por impulso (já que crianças ainda não têm compreensão do valor do dinheiro), exposição de dados pessoais e bancários.

Em geral, crianças e jovens que caem em golpes têm vergonha e medo de contar para a família, o que pode perpetuar o golpe e causar até mesmo endividamento familiar.

No Brasil publicidade direcionada a menores de 12 anos é considerada abusiva e é ilegal (Código de Defesa do Consumidor, ECA, Resolução Conanda 163/2014).

A publicidade para adolescentes deve ser claramente identificada com #publi, “publicidade”, etc.

Família

- Desative compras sem senha nos dispositivos.
- Ensine a identificar anúncios e golpes, por meio da observação de sinais como erros de português, urgência, promessas exageradas.
- Combine regras claras para uso de cartão de crédito, PIX e compras *online*.
- Converse sobre valor do dinheiro e consumo consciente.
- Denuncie publicidade infantil abusiva ao Procon, Conselho Nacional de Autorregulamentação Publicitária (Conar) ou Ministério Público (MP).

Escola

- Promova atividades que ensinem a identificar publicidade, inclusive em conteúdo de influenciadores.
- Inclua a educação financeira em sua grade de conteúdos.
- Converse sobre golpes digitais comuns envolvendo crianças/adolescentes, como *links* falsos do tipo “você foi sorteado” ou “ajude seu influencer favorito”.
- Convide especialistas em educação financeira para palestras

Criança e adolescente

- Nem tudo que o influenciador indica é “dica de amigo”. Muitas vezes é propaganda paga e ele não deixa claro.
- Desconfie de *links* que prometem “brindes”, “moedas infinitas” ou “descontos exclusivos”, pois pode ser golpe. Antes de clicar em qualquer *link* ou comprar algo, converse com um adulto.

Nudes

Fotos ou vídeos de uma pessoa sem roupa ou com pouca roupa, focados em partes íntimas ou com intenção sexual/erótica, enviados ou produzidos para alguém em conversas privadas, redes sociais ou aplicativos de mensagem, por exemplo.

Quando envolvem crianças e adolescentes menores de 18 anos, imagens íntimas passam a ser tratadas como material de abuso ou exploração sexual de crianças e adolescentes.

É crime produzir, armazenar, receber, enviar ou compartilhar imagens de nudez ou de ato sexual envolvendo menores de 18 anos. Isso vale mesmo entre namorados ou parceiros da mesma idade, quando alguém “pede”, “insiste” ou promete que “ninguém vai ver” ou que “vai apagar depois”. Essas regras existem para proteger crianças e adolescentes de abuso, exploração, chantagem e exposição, e não para culpá-los moralmente. A responsabilização deve recair, principalmente, sobre quem explora, pressiona, guarda, compartilha, difunde ou lucra com esse tipo de imagem — e sobre os adultos que se valem da vulnerabilidade de crianças e adolescentes, inclusive no ambiente digital.

Família

- Converse sobre *nudes*, com linguagem clara e sem ameaças, antes de o problema acontecer.
- Explique que imagens podem se espalhar rapidamente e gerar sofrimento profundo, que pressionar alguém por *nude* é uma forma de violência e que compartilhar *nude* de outra pessoa, especialmente menor, é uma conduta que pode ter consequências legais sérias.
- Caso descubra que seu filho ou filha enviou ou recebeu *nudes*, evite julgamentos e gritos — o que aumenta a culpa e o silêncio — e acolha. Ajude a interromper o compartilhamento e busque orientação na escola, rede de proteção ou serviços especializados. Deixe claro que o foco é cuidar e proteger, não apenas punir.
- A mensagem central para crianças e adolescentes deve ser: você merece respeito, não é culpado ou culpada pela violência que alguém cometeu contra você. Pedir ajuda é sempre um direito.

Adolescente

- Não envie imagens ou vídeos de *nudes*. Depois que a imagem ou vídeo são enviados, você perde o controle e esse material pode ser copiado, salvo, repassado e repostado inúmeras vezes.
- Uma imagem ou vídeo de *nude* compartilhado pode ser usado para ameaçar, humilhar, pedir mais fotos ou vídeos, dinheiro ou favores. O conteúdo pode ser exposto em *sites* ou grupos, páginas pornográficas, grupos de troca de *nudes* ou ambientes criminosos.
- Se você já enviou uma imagem íntima, não se culpe: a responsabilidade maior é de quem se aproveita, pressiona, chantageia ou compartilha sem autorização.
- Caso se sinta seguro, peça para a pessoa apagar a imagem. Se alguém ameaçar divulgar (“se não mandar mais”, “se não fizer tal coisa”), não ceda: guarde provas (*prints*, *links*, mensagens) e procure ajuda imediatamente com um adulto de confiança, escola, Conselho Tutelar, serviços da rede de proteção ou canais de denúncia.
- Denuncie: é seu direito pedir ajuda e proteção — você não está sozinho(a).
- Se você receber um *nude* de outra pessoa, não repasse: compartilhar imagem íntima de alguém, especialmente se for menor de idade, pode ser crime grave e causa enorme sofrimento. Apague a imagem. Bloqueie quem enviou, se for o caso.
- Se a imagem for de criança ou adolescente, denuncie em canais oficiais (escola, rede de proteção, canais de direitos humanos, polícia especializada).

Oversharenting

Prática na qual familiares e responsáveis compartilham fotos, vídeos e informações sobre crianças e adolescentes nas redes sociais de forma excessiva. Essa prática pode expor crianças a riscos como roubo de identidade, uso indevido de imagens e até contato com pessoas mal-intencionadas.

Antes de postar, pergunte-se se aquela imagem pode constranger seu filho no futuro.

Perfilamento

Processo de coletar, examinar e sumarizar informações sobre um usuário para construir um perfil comportamental e de preferências, em geral para direcionar publicidade segmentada.

Privacidade dos dados pessoais

É o direito de cada pessoa controlar como suas informações são coletadas, usadas, compartilhadas e guardadas, evitando exposição indevida e usos abusivos. Os dados pessoais são informações que permitem identificar quem você é ou traçar um perfil da sua vida (*online* e *offline*). Por exemplo: nome, apelido, foto, voz, CPF, RG, data de nascimento, endereço, telefone, e-mail, localização (onde você está ou aonde costuma ir), histórico de navegação, buscas, curtidas e tempo de uso, dados de saúde, religião, escola em que estuda, situação familiar, imagens e vídeos postados ou marcados com o seu nome. Alguns são dados pessoais sensíveis, que merecem cuidado extra, como saúde, religião, orientação sexual, dados biométricos, geolocalização precisa.

A LGPD garante que você não é um produto e que tem direitos sobre seus dados e sobre a forma como são usados por empresas, plataformas, escolas, órgãos públicos e outros "controladores" de dados.

Entre esses direitos, estão:

- Saber quem coleta seus dados, quais dados estão sendo usados e para qual finalidade.
- Pedir acesso aos seus dados pessoais guardados por um serviço ou empresa.
- Pedir correção de dados errados, desatualizados ou incompletos.

- Pedir exclusão de dados que não sejam mais necessários ou que estejam sendo usados de forma abusiva.
- Retirar o consentimento, quando você tiver autorizado o uso dos dados (por exemplo, para receber mensagens de *marketing*).
- Questionar decisões automatizadas, como perfis criados por algoritmos que podem afetar você (por exemplo, bloqueios, restrições, recomendações).

Crianças e adolescentes têm direitos reforçados na LGPD

Os dados de crianças (até 12 anos incompletos) só podem ser usados com autorização específica de pelo menos um dos familiares ou responsáveis, com explicações claras, em linguagem que a criança consiga entender.

No caso de adolescentes, o tratamento de dados deve sempre considerar o melhor interesse do adolescente, com proteção extra e incentivo à participação nas decisões sobre sua própria privacidade.

Aplicativos, jogos, redes sociais, escolas e empresas devem coletar o mínimo necessário de dados, guardar com segurança e não transformar crianças e adolescentes em alvo fácil de publicidade, vigilância ou exploração comercial.

Adolescente

As principais responsabilidades são de adultos, plataformas, empresas e instituições. Ainda assim, algumas atitudes podem ajudar você a se proteger no dia a dia digital:

- Sempre que possível, leia (ou peça para um adulto ler) as políticas de privacidade e termos de uso — desconfie quando nada é explicado.
- Pense antes de clicar em “aceitar tudo”: se houver opção, escolha “somente o necessário” para *cookies* e coleta de dados.
- Prefira manter seus perfis fechados/privados, principalmente se você for criança ou adolescente.
- Evite compartilhar localização em tempo real e rotinas (por exemplo, horário e trajeto da escola).
- Use senhas fortes, não repita a mesma senha em todos os *apps* e não as compartilhe com amigos.
- Ative, quando disponível, a autenticação em duas etapas (um código extra além da senha).
- Se algo parecer invasivo demais (“muitos dados pedidos”, “muitas permissões estranhas”), converse com um adulto de confiança e questione se aquilo é realmente necessário.
- Privacidade não é “segredo bobo”: é direito fundamental e parte da proteção contra violências, discriminação, vigilância abusiva e exploração de crianças e adolescentes no ambiente digital.

Privacidade por padrão

Configuração de privacidade de um produto ou serviço automaticamente definida com o mais alto nível de proteção, sem a necessidade de o usuário interagir com as configurações. Isso garante que a coleta, o uso, a retenção e a divulgação de dados sejam limitados ao mínimo necessário e que as opções mais restritivas já venham habilitadas por padrão, como no caso do uso de *cookies* que devem estar desativados até a permissão do usuário.

Rede de proteção

Conjunto articulado de órgãos, serviços e profissionais que atuam de forma integrada para garantir os direitos de crianças e adolescentes, prevenir violências e responder a situações de risco, inclusive no ambiente digital. É composta, entre outros, pelos serviços de assistência social — Centro de Referência de Assistência Social (Cras) e Centro de Referência Especializado de Assistência Social (Creas) —, de saúde — hospitais, Centro de Atenção Psicossocial (Caps), Unidade Básica de Saúde (UBS) —, de educação (escolas e equipes multiprofissionais), de segurança pública (polícias e delegacias especializadas), além do Ministério Público, Defensoria Pública, Poder Judiciário (Vara da Infância e Juventude), Conselho Tutelar e órgãos de direitos humanos. No contexto digital, essa rede também inclui autoridades e estruturas responsáveis pela aplicação do ECA Digital, da LGPD e de normas específicas sobre crimes e violações contra crianças e adolescentes no ambiente digital, incluindo a ANPD.

Qualquer pessoa pode acionar a Rede de Proteção pelos canais de denúncia, e todos os órgãos devem agir rapidamente, de forma coordenada e sem burocracias, garantindo proteção integral e prioridade absoluta a crianças e adolescentes.

Relatório de transparência

Documento periódico que plataformas digitais, redes sociais, aplicativos e jogos *online* são obrigados a publicar, apresentando dados detalhados sobre moderação de conteúdo e proteção de crianças e adolescentes, incluindo: número de denúncias recebidas (violência, abuso sexual infantil, *cyberbullying*, discurso de ódio), quantidade de conteúdos removidos e contas bloqueadas, tempo médio de resposta e resolução, ações de verificação de idade, medidas de proteção de dados de menores, investimentos em segurança digital, treinamento de equipes de moderação e planos de melhoria contínua.

Previsto no ECA Digital (Lei 14.811/2024) e regulamentado pela ANPD, o relatório deve ser público, acessível e apresentado em linguagem clara, permitindo que a sociedade civil, as autoridades e as famílias avaliem se as empresas estão cumprindo suas obrigações legais de proteger crianças e adolescentes no ambiente digital. Caso apresentem dados insuficientes, omitam informações ou demonstrem negligência sistemática na proteção infanto-juvenil, as empresas podem receber sanções, como multas, suspensão ou bloqueio da plataforma.

Risco por *design* ou riscos estruturais

São os perigos à segurança, privacidade e bem-estar de crianças e adolescentes criados pelas regras e pela estrutura de uma plataforma, aplicativo, jogo ou rede social. Ou seja, o risco não está apenas no que o usuário faz, mas na maneira como o ambiente digital foi construído.

Exemplos de riscos de *design*:

- **Configurações de privacidade abertas por padrão:** expor o perfil de um menor publicamente sem que ele ou o responsável precise mudar a configuração.
- **Algoritmos otimizados para engajamento:** recomendar conteúdos nocivos ou extremos apenas para manter o usuário mais tempo *online*.
- **Mecânicas viciantes:** uso de *loot boxes* ou notificações constantes que incentivam o uso excessivo e a dependência digital.

Pelo ECA Digital, as plataformas têm a obrigação de aplicar o princípio das boas práticas (*by design*/*by default*) para eliminar esses riscos desde a fase de criação, garantindo que a segurança e o bem-estar sejam priorizados sobre o lucro ou o engajamento.

Safety by design (segurança por desenho)

Abordagem de projeto que exige que a segurança, a proteção de dados e o bem-estar — especialmente de crianças e adolescentes — sejam considerados desde a concepção de uma plataforma, aplicativo, jogo ou rede social, e não apenas como um recurso opcional ou posterior. No contexto da proteção de crianças e adolescentes em ambientes digitais, isso significa que as plataformas devem ser planejadas para prevenir riscos e violações antes que aconteçam, reduzindo a exposição a contatos abusivos, conteúdos inadequados, coleta excessiva de dados e práticas comerciais exploratórias.

O *safety by design* implica em medidas como:

- **Desenho de funcionalidades seguras por padrão:** perfis fechados para menores, limitação de contato por desconhecidos e restrições de geolocalização.
- **Proteção de dados:** limitar a coleta e o uso de dados pessoais ao mínimo necessário, com proteção reforçada para dados de crianças e adolescentes.
- **Acessibilidade:** oferecer mecanismos de denúncia, bloqueio e apoio que sejam facilmente acessíveis, compreensíveis e adaptados à idade.
- **Transparência:** informar claramente como a plataforma funciona, incluindo algoritmos de recomendação e publicidade, e como os dados são tratados.

Sexting

Envio de mensagens, fotos ou vídeos com conteúdo sexual ou sensual, geralmente pelo celular. Entre adolescentes da mesma idade, pode ser uma forma de explorar a sexualidade, mas traz riscos: o conteúdo pode ser compartilhado sem permissão, gerando constrangimento e violência.

Atenção!

Compartilhar ou divulgar imagens íntimas de outra pessoa sem consentimento é crime! (Lei 13.772/2018 — divulgar conteúdo íntimo sem consentimento, mesmo entre adultos).

Sextorsion ou sextorsão

Expressão derivada de termo da língua inglesa que significa ameaça de divulgar imagens íntimas de uma pessoa para obter proveitos econômicos e/ou sexuais.

A prática de *sexting*, principalmente entre adolescentes, pode evoluir para vazamento (compartilhamento não autorizado), pornografia de vingança (divulgação após o término de um namoro) e sextorsão. Trata-se de situações que ocasionam danos psicológicos profundos, como vergonha, humilhação pública, ideação suicida, *bullying* intensificado. Além disso, o conteúdo pode permanecer na internet e afetar a imagem da vítima no futuro.

É importante deixar claro para jovens e adolescentes que a prática de sextorsão é crime, e quem compartilha está sujeito a processo criminal, medidas socioeducativas e registro de antecedentes.

Sextorção é crime previsto em lei!

(Lei 11.829/2008 — divulgar cena de sexo/nudez envolvendo adolescente).

Família

- Converse desde cedo sobre intimidade, consentimento, permanência de arquivos e mensagens no ambiente digital e responsabilidade.
- Evite respostas apenas punitivas, como “a culpa é sua”, “eu avisei”.
- Acolha. Neste momento, a vítima precisa de apoio.
- Preserve evidências (*prints*, mensagens). Caso tenha acontecido em ambiente escolar, acione a escola e, se necessário, órgãos de proteção, como Conselho Tutelar, delegacias especializadas, SaferNet.
- Oriente-se sobre remoção de conteúdo nas plataformas.
- Busque apoio psicológico.

Escolas

- Crie protocolos para casos de vazamento de imagens envolvendo estudantes.
- Não trate esse tipo de situação como fofoca ou assunto privado.
- Promova ações educativas sobre respeito ao corpo, consentimento, crime de compartilhamento de *nudes* de menores, masculinidades e cultura do estupro.
- Acolha a vítima, evite julgamentos do tipo “por que você compartilhou?”.

Adolescente

- Lembre-se: depois que a foto íntima sai do seu celular, você perde o controle. O conteúdo pode ser copiado, editado e espalhado para sempre.
- Caso alguém pressione você a compartilhar esse tipo de informação, saiba que o erro é de quem está exigindo. Se você enviou e vazou, a culpa é de quem divulgou, não sua. Procure ajuda imediatamente.
- Se você recebeu foto íntima de algum colega, apague! Não compartilhe — isso é crime!

Shorts (vídeos curtos)

Vídeos verticais e curtos (com até 3 minutos de duração) para assistir e interagir no aplicativo do YouTube. Existem formatos semelhantes em outras plataformas, como Instagram e TikTok.

Por terem formato de alto engajamento, é preciso atentar-se para que não causem dependência digital e para que crianças e adolescentes não sejam expostos a conteúdo impróprio.

Transparência do uso de dados

Prática de fornecer informações claras, abertas e acessíveis sobre como dados pessoais são coletados, usados, armazenados e compartilhados. É um princípio fundamental da LGPD no Brasil, o que garante ao titular o controle e o conhecimento sobre suas informações. Isso envolve disponibilizar políticas de privacidade detalhadas, mecanismos para o titular gerenciar suas autorizações e o histórico de acesso aos seus dados, promovendo a responsabilização e a proteção da privacidade individual

Vulnerabilidade explorada

Prática em que plataformas digitais, aplicativos, jogos ou anunciantes identificam e exploram propositalmente as fragilidades naturais do desenvolvimento infantojuvenil para aumentar engajamento, lucro ou tempo de uso, desconsiderando os riscos ao bem-estar de crianças e adolescentes. Diferentemente de falhas técnicas de segurança, refere-se à exploração de características próprias dessa fase da vida, como:

- **Impulsividade:** oferta de compras por impulso com um clique, *loot boxes* e ofertas "por tempo limitado".
- **Busca por aceitação social:** exibição de quantos "amigos" já compraram algo ou alcançaram determinado nível no jogo.
- **Vulnerabilidade à pressão estética:** bombardeamento de propagandas de produtos de beleza, filtros que distorcem a autoimagem, comparações com padrões corporais irreais.
- **Imaturidade para avaliar riscos:** normalização de comportamentos perigosos através de desafios virais.
- **Necessidade de pertencimento:** medo de ficar de fora (FOMO) ou exclusão de quem não tem determinado item virtual.
- **Sensibilidade emocional aumentada:** notificações manipulativas como "seu amigo está triste porque você não jogou hoje".
- **Menor capacidade de resistir a recompensas imediatas:** sistemas viciantes de pontos, *badges*, *streaks* que incentivam uso compulsivo.

Dicas de segurança digital para famílias

Checklist para configurar, orientar e monitorar o uso de dispositivos *online* por crianças e adolescentes

Configurações básicas para fazer ANTES de entregar um dispositivo

[ ] Criar conta de e-mail supervisionada (Gmail para crianças/Family Link)

[ ] Instalar antivírus

[ ] Ativar controle parental

[ ] Configurar restrições de conteúdo por idade

[ ] Desabilitar compras sem autorização

[ ] Configurar privacidade em todas as redes sociais

[ ] Ativar autenticação em duas etapas

[ ] Ensinar a criar senhas fortes

Conversas essenciais

[ ] Explicar que as pessoas na internet podem mentir sobre quem são

[ ] Orientar a nunca compartilhar dados pessoais

[ ] Ensinar a dizer NÃO a pedidos inadequados

[ ] Deixar claro que você está disponível para ajudar, sem julgar

[ ] Explicar riscos de *nudes* e sextorsão

[ ] Conversar sobre *cyberbullying* (ser vítima e agressor)

[ ] Alertar sobre desafios perigosos

[ ] Ensinar a identificar e denunciar conteúdo impróprio

Monitoramento (sem invadir)

[ ] Seguir seu filho nas redes sociais

[ ] Revisar histórico de navegação periodicamente

[ ] Conhecer os jogos que ele joga

[ ] Saber quem são os “amigos virtuais”

[ ] Verificar configurações de privacidade regularmente

[ ] Observar mudanças de comportamento

Sinais de alerta

Procure urgentemente a ajuda de um profissional se a criança ou adolescente...

- Fala sobre morte ou suicídio
- Pesquisa na internet sobre “como morrer”
- Postagens de despedida
- Uso de *deep web*
- Participação em desafios perigosos
- Automutilação (cortes, queimaduras)

Fique atento e considere buscar apoio se observar...

- Mudanças bruscas de humor
- Isolamento social crescente
- Queda significativa no rendimento escolar
- Recusa em ir à escola
- Alterações no sono ou apetite
- Uso compulsivo de internet (ver critérios em “Dependência digital”)

- Ansiedade ou pânico ao usar/não usar redes sociais
- Sinais de estar sofrendo *cyberbullying*
- Excesso de tempo em *sites*/grupos sobre emagrecimento extremo
- Sigilo excessivo sobre o que faz *online*

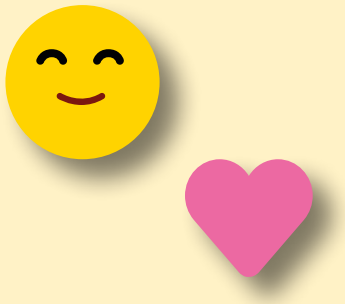
Como configurar senhas seguras

Senhas fracas são a porta de entrada para que outras pessoas acessem suas contas, leiam suas conversas privadas, roubem suas fotos e usem suas informações pessoais.

Proteger sua senha é proteger seus dados e sua privacidade. Sua senha é seu escudo digital

Crie uma senha forte

REGRA	EXEMPLO PRÁTICO
Tamanho: pelo menos 12 caracteres.	
Mistura: letras maiúsculas, minúsculas, números e símbolos (@, #, !, $).	
Frases: use frases fáceis de lembrar, mas difíceis de adivinhar.	"MeuG@t0Tem3Anos!" é muito melhor que "gato123".
Exclusividade: crie senhas DIFERENTES para cada conta.	Se uma conta for invadida, as outras permanecem seguras.
O que NÃO usar: datas de nascimento, nomes de familiares ou sequências óbvias (123456, abcdef).	



Autenticação em duas etapas (2FA), sua camada extra de segurança

A 2FA é essencial. Mesmo que alguém descubra sua senha, precisará de um **código temporário** que chega pelo seu celular para entrar na conta.

Ative a autenticação em duas etapas em todas as suas contas importantes!

Gerenciadores de senhas

Eles guardam todas as suas senhas em um “cofre digital” protegido e geram senhas fortes automaticamente, facilitando sua vida e aumentando sua segurança.

- Exemplos: Bitwarden, Lastpass, 1Password.

Atenção!

- Nunca compartilhe suas senhas (nem com seu melhor amigo ou namorado(a)!).
- Nunca anote em papel ou no bloco de notas do celular.
- Nunca use a mesma senha para tudo.

Administre bem o tempo de tela

O uso equilibrado e consciente de dispositivos digitais (celulares, *tablets*, computadores), respeitando os limites de tempo e conteúdo adequados para cada faixa etária, é fundamental para o desenvolvimento saudável e o bem-estar digital de crianças e adolescentes.

Recomendações da Sociedade Brasileira de Pediatria para tempo de tela, por idade

IDADE	TEMPO MÁXIMO RECOMENDADO	OBSERVAÇÕES ESSENCIAIS
0 a 2 anos	Evite telas	Prejudica o desenvolvimento cerebral, a linguagem e os vínculos afetivos. Priorize brincadeiras e leitura.
2 a 5 anos	Máximo 1 hora/dia	Sempre com supervisão de adulto. Priorize conteúdo educativo e de qualidade.
6 a 10 anos	Máximo 1 a 2 horas/dia	Supervisão frequente. Estabeleça regras claras sobre o que pode acessar.
11 a 18 anos	Máximo 2 a 3 horas/dia	Monitore sem invadir a privacidade. Incentive atividades físicas e sociais.

Regras universais para todas as idades

- Higiene do sono: desligue as telas de uma a duas horas antes de dormir, pois a luz azul emitida pelos dispositivos atrapalha o sono.
- Conexão familiar: nada de telas durante as refeições ou em momentos de conversa em família.
- Uso consciente: nunca use telas como “babá eletrônica” para substituir a interação humana.

Por que o excesso prejudica?

O uso excessivo pode causar problemas de sono, obesidade (sedentarismo), dificuldade de atenção, ansiedade, depressão e atraso no desenvolvimento em crianças pequenas.

Dicas práticas para famílias e escolas

- Seja o exemplo: crianças e adolescentes imitam o comportamento dos adultos.
- Estabeleça limites: use cronômetros e crie “horários livres de tela” para toda a família.
- Recolha aparelhos: crie uma “estação de carga” fora do quarto e desligue o Wi-Fi à noite.
- Incentive alternativas: priorize brincadeiras ao ar livre, esportes, leitura e jogos de tabuleiro.

Juntos somos mais fortes: responsabilidade compartilhada

O ambiente digital faz parte da vida e pode ser incrível quando usado com cuidado, respeito e consciência. Ninguém nasce sabendo navegar com segurança; isso é algo que devemos aprender juntos — família, escola e sociedade.

- **Papel da família e das escolas:** proteger, orientar, acolher e ensinar.
- **Papel das plataformas:**
  - » Implementar proteções por *design*: verificação de idade eficaz, moderação de conteúdo, transparência de algoritmos, configurações de privacidade robustas.
  - » Responder rapidamente a denúncias e remover conteúdo ilegal.
  - » Investir em pesquisa sobre impactos do contato com o ambiente digital no desenvolvimento infantojuvenil.
  - » Colaborar com pesquisadores, sociedade civil e poder público.
  - » Respeitar legislação de proteção de dados e direitos de crianças.

- **Papel do poder público:**
  - » Promover uma legislação protetiva, atualizada e aplicada.
  - » Fiscalizar de forma efetiva as plataformas.
  - » Investir em educação digital nas escolas públicas e em campanhas de conscientização.
  - » Investir em delegacias especializadas em crimes cibernéticos bem equipadas e treinadas, em canais de denúncia acessíveis e eficientes, em políticas intersetoriais (educação + saúde + assistência + justiça) e fomento a pesquisas — como TIC Kids Online Brasil, usada amplamente nesse glossário — para embasar decisões baseadas em evidências.

Juntos, podemos construir um ambiente digital mais seguro, saudável e justo para todas as gerações.

A proteção digital de crianças e adolescentes é responsabilidade compartilhada

(art. 227 da Constituição Federal).

Rede de proteção: canais de denúncia e ajuda

Muitas denúncias podem ser feitas de forma anônima. Se você ou alguém que você conhece está sofrendo violência digital (ameaças, vazamento de *nudes*, discurso de ódio, aliciamento, *bullying*, exposição de dados, etc.), existem canais oficiais e gratuitos para pedir ajuda.

Você não precisa ter certeza absoluta para denunciar; se existe suspeita, já vale buscar ajuda.

Proteção de dados pessoais — ANPD

A ANPD é o órgão federal responsável por fiscalizar o cumprimento da LGPD, inclusive quando há tratamento indevido de dados de crianças e adolescentes.

COMO ACESSAR?

Site: gov.br/anpd

Serviço: “Abrir requerimento relacionado à LGPD” (petição de titular ou denúncia).

Esse canal é especialmente importante quando há:

- Exposição de dados pessoais (nome, foto, localização, contatos) sem autorização.
- Coleta abusiva de dados de crianças e adolescentes em *apps*, jogos, escolas, plataformas.
- Dificuldade em conseguir que um *site* ou serviço atenda a pedidos de exclusão, correção ou esclarecimento previstos na LGPD.

Canais nacionais de denúncia de violência e violação de direitos

Disque 100: Direitos Humanos

Recebe denúncias de violação de direitos humanos, com prioridade para crianças, adolescentes e outros grupos vulneráveis. Atende 24h por dia, todos os dias. A ligação é gratuita e pode ser anônima.

COMO ACESSAR?
Ligue 100

SaferNet Brasil: central de denúncias

Recebe denúncias anônimas de crimes e violências na internet (imagens de abuso sexual contra crianças, racismo, discurso de ódio, etc.) e encaminha às autoridades.

COMO ACESSAR?

Site: new.safernet.org.br/denuncie

SaferNet Brasil: canal de ajuda

Serviço de apoio e assistência para crianças, adolescentes, famílias e educadores com dúvidas ou em situação de risco em ambiente digital (*nudes*, *sextorsão*, *cyberbullying*, medo de alguém na internet, etc.).

COMO ACESSAR?

Site: canaldeajuda.org.br

Conselho Tutelar

Órgão previsto no ECA que zela pelos direitos de crianças e adolescentes. Atua em casos de violência, negligência, exploração, inclusive digital.

COMO ACESSAR?

Procure o Conselho Tutelar do seu município (site da prefeitura, governo estadual ou Ministério dos Direitos Humanos).

Polícia Civil/Delegacia (incluindo Delegacia de Crimes Cibernéticos)

Faz o registro de boletim de ocorrência e investigação de crimes (ameaças, extorsão, vazamento de imagens íntimas, golpes, aliciamento, etc.). Alguns estados têm delegacias especializadas em crimes cibernéticos.

COMO ACESSAR?

Delegacia mais próxima ou delegacia online (quando disponível no seu estado).

Apoio emocional e saúde mental

Centro de Valorização da Vida (CVV)

Apoio emocional e prevenção do suicídio para qualquer pessoa. Atendimento sigiloso, gratuito, 24h por dia.

COMO ACESSAR?
Ligue 188
Site: cvv.org.br

Pode Falar

Canal de ajuda oferecido pelo Fundo das Nações Unidas para a Infância (Unicef), junto com parceiros, em questões de saúde mental para adolescentes e jovens, em geral de 13 a 24 anos, com atendimento virtual, gratuito e anônimo em horários definidos.

COMO ACESSAR?
Site: podefalar.org.br

CAPS/UBS

Serviços do Sistema Único de Saúde (SUS) para atendimento psicológico/psiquiátrico e para situações de violência sexual, autoagressão ou sofrimento intenso.

COMO ACESSAR?

Procure o CAPS ou UBS mais próximo.

Situação de risco imediato

Se houver perigo agora, ligue para os números de emergência nacionais:

- **190 — Polícia Militar:** emergência policial, risco à vida, agressões em andamento.
- **192 — SAMU:** emergência de saúde, risco de morte, tentativa de suicídio, trauma grave.

Busque também ajuda das seguintes instâncias:

- **Escola:** a direção, a coordenação pedagógica, o professor de confiança e a equipe multiprofissional são aliados importantes em casos de *cyberbullying*, violência, discriminação, exposição de imagens, etc.

- **Ministério Público:** atua na defesa dos direitos de crianças e adolescentes e na responsabilização de agressores; cada estado dispõe de canais *online* e presenciais (inclusive ouvidorias e número 127 em muitos MPs).
- **Defensoria Pública:** pode orientar juridicamente e propor ações quando a família não tem condições de pagar por um advogado.

Atenção!

Em muitos casos, é recomendável combinar canais: por exemplo, Conselho Tutelar + Disque 100 + SaferNet + Delegacia.

Denunciar diretamente nas plataformas digitais

Além dos canais oficiais (Disque 100, SaferNet, Conselho Tutelar, polícia, etc.), é importante usar os mecanismos internos das próprias plataformas, porque elas têm o dever de remover conteúdo inapropriado e cooperar com as autoridades.

Dicas gerais

- Procure sempre o botão “Denunciar” ou “Reportar” perto do conteúdo, do comentário, da mensagem ou do perfil.
- Escolha o motivo: “envolve crianças/adolescentes”, “conteúdo sexual”, “violência”, “assédio/*bullying*”, “discurso de ódio” ou similar.
- Depois de denunciar, você pode bloquear o perfil e, se for seguro, guardar provas (*prints*, *links*, datas) para levar ao Conselho Tutelar, Delegacia, SaferNet, Ministério Público ou outro serviço da rede de proteção

A seguir, um passo a passo simplificado para denunciar conteúdos em algumas das plataformas mais populares. Os nomes dos botões podem mudar conforme possíveis atualizações, mas a lógica é parecida.

Meta (Instagram e Facebook)

1. Abra o *post*, *story*, comentário ou perfil.
2. Toque nos três pontinhos (···) ou no menu ao lado do conteúdo.
3. Selecione “Denunciar”.
4. Escolha o motivo, dando preferência a opções relacionadas a crianças/adolescentes, nudez, exploração sexual, discurso de ódio, assédio.
5. Confirme o envio.

WhatsApp

1. Abra a conversa ou o grupo.
2. Toque no nome do contato ou do grupo para abrir as informações.
3. Role até encontrar a opção “Denunciar”.
4. Confirme a denúncia. Em alguns casos, você pode optar por enviar as últimas mensagens para que o app analise o conteúdo.

TikTok

1. Toque em “Compartilhar” ou mantenha o vídeo, comentário, conta ou mensagem pressionada.
2. Toque em “Denunciar”.
3. Escolha o motivo (por exemplo: exploração sexual de menores, nudez, violência, assédio, discurso de ódio).
4. Siga as instruções até enviar a denúncia.

YouTube

1. Abra o vídeo, comentário ou canal.
2. Clique nos três pontinhos (···) abaixo ou ao lado.
3. Selecione “Denunciar”.
4. Escolha a categoria (por exemplo: conteúdo sexual envolvendo menores, violência, discurso de ódio, assédio).
5. Confirme.

Também é possível denunciar comentários e canais:

X (antigo Twitter)

1. Abra o post que você quer denunciar.
2. Clique nos três pontinhos ou na seta de opções ao lado do post.
3. Selecione “Denunciar post” (ou “Reportar”).
4. Siga as etapas, escolhendo motivos ligados a exploração sexual de crianças, nudez, violência, assédio ou outros conteúdos ilegais.
5. Envie a denúncia.

Também é possível denunciar contas inteiras por comportamento abusivo ou por publicação de conteúdo sexual envolvendo menores.

Referências

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Institucional**. Brasília, DF: ANPD, [2024]. Disponível em: https://www.gov.br/anpd/pt-br. Acesso em: 12 dez. 2025.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2016]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 12 dez. 2025.

BRASIL. Conselho Nacional dos Direitos da Criança e do Adolescente (CONANDA). Resolução no 163, de 13 de março de 2014. Dispõe sobre a abusividade do direcionamento de publicidade e de comunicação mercadológica à criança e ao adolescente. **Diário Oficial da União**: seção 1, Brasília, DF, p. 4, 4 abr. 2014. Disponível em: https://www.gov.br/mdh/pt-br/acesso-a-informacao/participacao-social/conselho-nacional-dos-direitos-da-crianca-e-do-adolescente-conanda/resolucoes/resolucao-163-_publicidade-infantil.pdf/view. Acesso em: 12 dez. 2025.

BRASIL. Lei nº 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. **Diário Oficial da União**: seção 1, Brasília, DF, p. 13563, 16 jul. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 12 dez. 2025.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências (Código de Defesa do Consumidor). **Diário Oficial da União**: Brasília, DF, 12 set. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 12 dez. 2025.

BRASIL. Lei nº 11.829, de 25 de novembro de 2008. Altera a Lei nº 8.069, de 13 de julho de 1990 – Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet. **Diário Oficial da União**: seção 1, Brasília, DF, 26 nov. 2008. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11829.htm. Acesso em: 12 dez. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**: seção 1, Brasília, DF, ano 155, n. 157, p. 59-64, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 12 dez. 2025.

BRASIL. Lei nº 13.772, de 19 de dezembro de 2018. Altera a Lei nº 11.340, de 7 de agosto de 2006 (Lei Maria da Penha), e o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para reconhecer que a violação da intimidade da mulher configura violência doméstica e familiar e para criminalizar o registro não autorizado de conteúdo com cena de nudez ou ato sexual ou libidinoso de caráter íntimo e privado. **Diário Oficial da União**: seção 1, Brasília, DF, 20 dez. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13772.htm. Acesso em: 12 dez. 2025.

BRASIL. Lei nº 14.811, de 12 de janeiro de 2024. Institui medidas de proteção à criança e ao adolescente contra a violência nos estabelecimentos educacionais ou similares, prevê a Política Nacional de Prevenção e Combate ao Abuso e Exploração Sexual da Criança e do Adolescente. **Diário Oficial da União**: seção 1, Brasília, DF, 15 jan. 2024. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2023-2026/2024/lei/L14811.htm. Acesso em: 12 dez. 2025.

BRASIL. Lei nº 15.211, de 17 de setembro de 2025. Dispõe sobre a proteção de crianças e adolescentes em ambientes digitais (Estatuto Digital da Criança e do Adolescente).

Diário Oficial da União: Brasília, DF, 17 set. 2025. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/L15211.htm. Acesso em: 12 dez. 2025.

BRASIL. Ministério dos Direitos Humanos e da Cidadania. **Disque 100**: Disque Direitos Humanos. Brasília, DF: MDHC, [2024]. Disponível em: https://www.gov.br/mdh/pt-br/disque100. Acesso em: 12 dez. 2025.

CAVALCANTE, A. P. P. et al. **Crianças, adolescentes e telas**: guia sobre usos de dispositivos digitais. Brasília, DF: Secretaria de Comunicação Social da Presidência da República, 2025. Disponível em: https://www.gov.br/secom/pt-br/assuntos/uso-de-telas-por-criancas-e-adolescentes/guia/guia-de-telas_sobre-usos-de-dispositivos-digitais_versaoweb.pdf1. Acesso em: 12 dez. 223025.

CENTRO DE VALORIZAÇÃO DA VIDA (CVV). **Atendimento 188**. [S. l.]: CVV, [s.d.]. Disponível em: https://www.cvv.org.br/. Acesso em: 12 dez. 2025.

CONSELHO TUTELAR. **Atribuições e competências**. Brasília, DF: Ministério dos Direitos Humanos e da Cidadania, [2024]. Disponível em: https://www.gov.br/mdh/pt-br/navegue-por-temas/crianca-e-adolescente/conselhos-tutelares. Acesso em: 12 dez. 2025.

EDUCA MÍDIA. **Glossário**. [S. l.]: Instituto Palavra Aberta, [s.d.]. Disponível em: https://educamidia.org.br/glossario/. Acesso em: 12 dez. 2025.

FERNANDES, E.; TEFFÉ, C.; BRANCO, S. **Privacidade e Proteção de Dados de Crianças e Adolescentes**. 2. ed. revisada e atualizada. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio (ITS Rio), 2024. Disponível em: https://itsrio.org/pt/publicacoes/privacidade-e-protecao-de-dados-de-criancas-e-adolescentes/. Acesso em: 12 dez. 2025.

FREENET PROJECT. **Freenet**. [S. l.]: Freenet Project, [s.d.]. Disponível em: https://freenetproject.org/. Acesso em: 12 dez. 2025.

FUNDO DAS NAÇÕES UNIDAS PARA A INFÂNCIA (UNICEF). **Pode Falar**: canal de ajuda em saúde mental. [S. l.]: UNICEF, [s.d.]. Disponível em: https://podefalar.org.br/. Acesso em: 12 dez. 2025.

INFÂNCIAS encurtadas – adultização digital e os riscos ao desenvolvimento cognitivo e escolar. **ResearchGate**, 22 set. 2025. Disponível em: https://www.researchgate.net/publication/395682901_Infancias_encurtadas_-_adultizacao_digital_e_os_riscos_ao_desenvolvimento_cognitivo_e_escolar. Acesso em: 12 dez. 2025.

NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR (NIC.br). **Pesquisa sobre o uso da internet por crianças e adolescentes no Brasil**: TIC Kids Online Brasil 2024. São Paulo: Comitê Gestor da Internet no Brasil, 2024. Disponível em: https://cetic.br/pt/pesquisa/kids-online/. Acesso em: 12 dez. 2025.

SAFERNET BRASIL. **Canal de Ajuda**. Salvador: SaferNet, [202-?]. Disponível em: https://new.safernet.org.br/canaldeajuda. Acesso em: 12 dez. 2025.

SAFERNET BRASIL. **Central Nacional de Denúncias de Crimes Cibernéticos**. [S. l.]: SaferNet Brasil, [s.d.]. Disponível em: https://new.safernet.org.br/denuncie. Acesso em: 12 dez. 2025.

SOCIEDADE BRASILEIRA DE PEDIATRIA. **Manual de orientação**: #MenosTelas #MaisSaúde. Atualização 2024. Rio de Janeiro: SBP, 2024. Disponível em: https://www.gov.br/secom/pt-br/arquivos/2024_menostelas-maissaude_atualizado.pdf/view. Acesso em: 12 dez. 2025.

THE INVISIBLE INTERNET PROJECT (I2P). **I2P**: The Invisible Internet Project. [S. l.]: I2P, [s.d.]. Disponível em: https://geti2p.net/. Acesso em: 12 dez. 2025.

THE TOR PROJECT. **Tor Browser**. [S. l.]: The Tor Project, [s.d.]. Disponível em: https://www.torproject.org/. Acesso em: 12 dez. 2025.

edições câmara
CIDADANIA

CÂMARA DOS DEPUTADOS