

# PL 2628/2022

## Ambientes Digitais e Saúde Mental de crianças e adolescentes

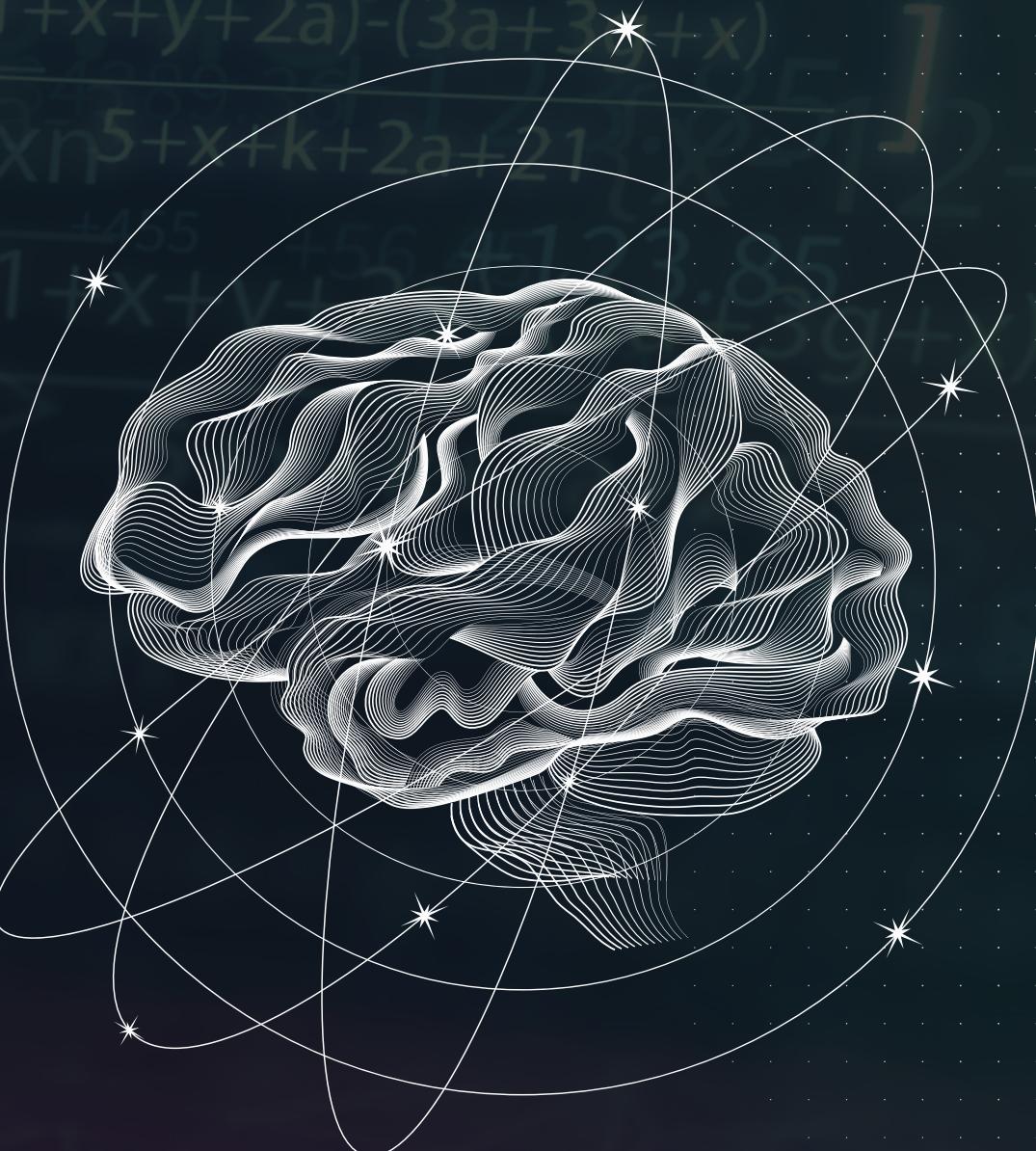
07.05.2025

**Karina Queiroz**

Especialista em Segurança Cibernética  
Diretora Executiva do Instituto Teckids

*Teckids - Instituto de Pesquisa e Educação em  
Proteção de Criança e Adolescente On-line*

 teckids



# O Silêncio Digital

## Uma Epidemia Oculta de Violência

1 em cada 3 usuários da internet no mundo é uma criança.

Fonte: UNICEF, 2023

A cada 7 minutos, uma criança é vítima de abuso online.

Fonte: Interpol, 2022

Ataques cibernéticos contra crianças aumentaram em 30% durante a pandemia.

Fonte: Europol, 2021

O cyber crime global cresceu mais de 300% na última década.

Fonte: Cybersecurity Ventures, 2023

# A Facilidade da Violência na Era Digital

## Anonimato & Desinibição

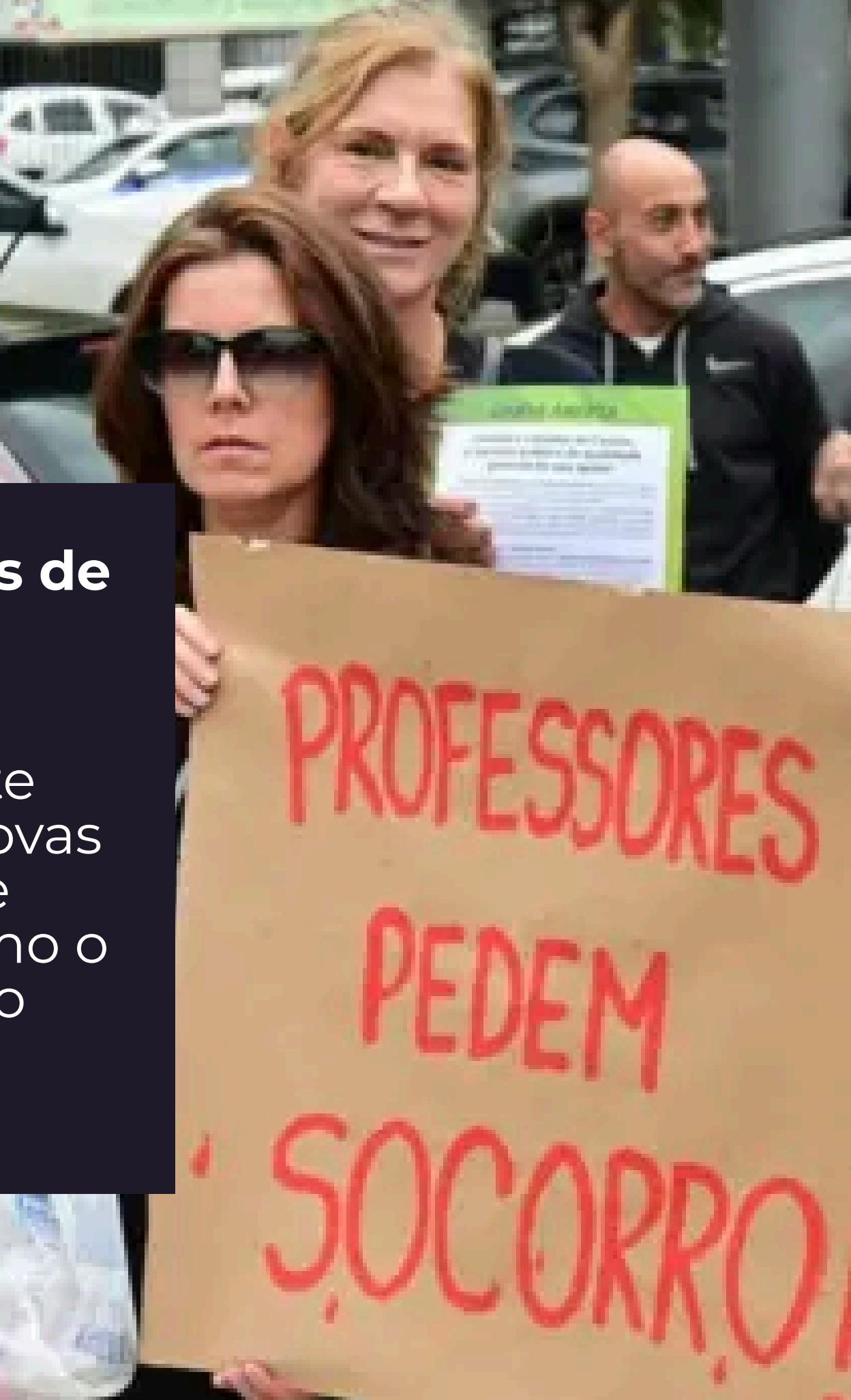
A falsa sensação de anonimato online facilita comportamentos agressivos e abusivos

## Agilidade e Viralização

Conteúdo violento e abusivo pode se espalhar em segundos, causando danos irreparáveis

## Novas formas de Abuso

O ambiente digital cria novas formas de violência, como o 'doxing' e o 'deepfake'



# Material sexual “autogerado” & armadilhas

aliciamento online **aumentou** 80% nos últimos quatro anos.

45 minutos é o tempo médio **para aliciar uma criança** em jogos

Transmissão ao vivo de abuso sexual infantil é um **desafio**, não é gravada e nem monitorada adequadamente

Apesar da maioria do tráfego de abuso estar em website público, plataformas que criptografam os dados são as mais usadas por predadores

*a busca pela Aceitação*

Fonte: Global Threat Assessment 2023

# Tendências (2030)

Prevê-se que o mercado mundial da XR ultrapasse 1,1 bilhões de dólares até 2030

a utilização de tecnologias integradas, tais como a háptica, que simulam sensações reais como movimentos, vibrações e força.

Aumento de Abuso &Estupro Virtual

Aumento de mais e 50%/ano dos ataques cibernéticos devido ao uso de IA

haverá aumento de tráfego automatizado superando atividades humanas, a simulação aperfeiçoada de voz e vídeos

Aumento de golpes e deepfakes

Aumento de regulação específica por tecnologia e/ou serviços

A diversidade de serviços e tecnologias que impulsionam o crime cibernético deverão ser balisadores de políticas públicas

Aumento de educação e controle

# PL 2628/2022



*“Esta Lei aplica-se a todo produto ou serviço de tecnologia da informação **direcionado ou que possa ser utilizado** por crianças e adolescentes”*

# Notas - I



*Atenção na redação onde utiliza-se palavras e diretivas que não estabelecem de fato o controle e com isso deixa em aberto, para o fornecedor, a escolha sobre o que fazer. Como: “medidas razoáveis disponíveis”, “modelo disponível”. Sugestão: definir os controles necessários, Padrões e Melhores práticas já reconhecidas.*



*Atenção na redação, onde destaca-se a necessidade da privacidade, da proteção de dados ou da segurança em diversos contextos porém em todos os casos ambos são necessários. Ex.: Art.3 , Art.5, Art.6, Art.7, Art.9 , e outros. Sugestão: Sempre buscar “proteção dos dados e segurança” e mencionar a LGPD para dados pessoais.*

# Notas - II



*Atenção ao Art. 6º - Os fornecedores de produtos ou serviços de tecnologia da informação direcionados ou que possam ser utilizados por crianças e adolescentes **deverão tomar medidas razoáveis em seu desenho e operação para prevenir e mitigar o acesso e a exposição a conteúdos que retratem os seguintes aspectos:***

*Sugestão: Reescrita para incluir riscos, esclarecer medidas e padrões de controle e sumarizar neste artigo, o Art.7.*

# Notas - II



Art. 6. Os fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e adolescentes deverão adotar mecanismos eficazes para **prevenir, identificar e mitigar riscos associados ao uso de suas plataformas**, em conformidade com as diretrizes deste Capítulo.

**§ 1º. São considerados riscos:**

- I. *Discurso de ódio e intolerância, incluindo conteúdos que promovam discriminação racial, religiosa, de gênero ou outras formas de preconceito;*
- II. *Aliciamento e grooming, caracterizado por ações que visem manipular ou explorar crianças e adolescentes para fins ilegais ou abusivos;*
- III. *Práticas criminosas, como indução à prática de crimes, tráfico de substâncias ilícitas ou participação em atividades ilegais;*

# Notas - II



- .III. Práticas criminosas, como indução à prática de crimes, tráfico de substâncias ilícitas ou participação em atividades ilegais;
- IV. Práticas perigosas, incluindo a promoção de desafios prejudiciais à saúde e segurança, bem como fóruns e comunidades que incentivem comportamentos autodestrutivos ou danosos.

§ 2º. As medidas de proteção deverão incluir, no mínimo:

- I. Ferramentas de monitoramento e filtragem de conteúdos ilegais ou prejudiciais;
- II. Sistemas de denúncia acessíveis e anônimos para reportar comportamentos ou conteúdos suspeitos;
- III. Processos para a remoção imediata de conteúdos que representem risco iminente à segurança de crianças e adolescentes;

# Notas - II



IV. Adoção de práticas de design que impeçam a exposição inadvertida a conteúdos nocivos.

§ 3º. Os fornecedores deverão apresentar relatórios periódicos às autoridades competentes, demonstrando as ações realizadas para mitigar os riscos descritos, em conformidade com o princípio da transparência.

§ 4º. A inobservância das disposições deste Capítulo sujeitará o fornecedor às penalidades previstas nesta Lei, proporcionalmente à gravidade da infração e ao impacto causado.

Este capítulo consolida a necessidade de proteção ampla contra riscos emergentes e práticas prejudiciais no ambiente digital, assegurando que os direitos e a segurança de crianças e adolescentes sejam priorizados.

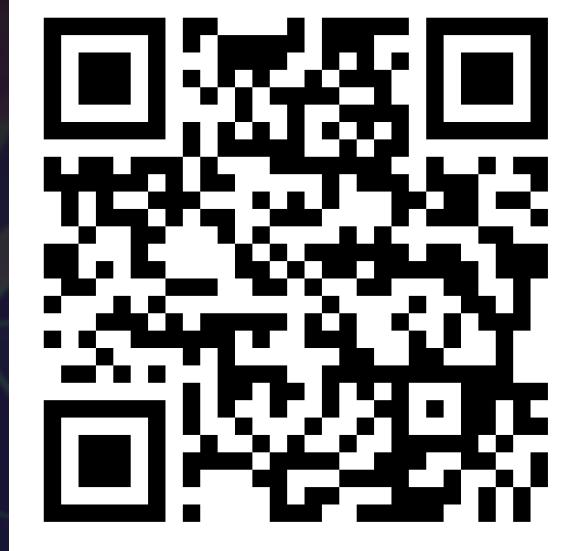


# Notas - III (Final)

- *Esclarecer objetivamente riscos que se busca controlar: Aliciamento, discurso de ódio, doxing, deepfake, uso excessivo de tela, etc. Ainda que a lista possua itens mais genéricos como “crime cibernético contra criança e adolescente”.*
- *Escopo: Evitar desenvolver novos escopos de ação utilizar o escopo definido no Art.1.*
- *Definir prazos e sanções graduados para “implementação de controles”, por meio de uma tabela de impacto com prazos ajustados. (Prática em segurança e proteção porque trata-se de mitigação de riscos.*
- *Ressaltar em Artigo de Conscientização, a necessidade das plataformas de promover conscientização e comunicação sobre os riscos e o uso seguro de seus produtos e serviços.*



**"Estamos certos de que, juntos, podemos promover transformações significativas e garantir proteção."**



**Como  
impulsionar  
ações!**

Siga nossas redes e promova a educação



@teckidsbr



[www.teckids.com.br](http://www.teckids.com.br)

**Instituto Teckids - Proteção da Criança e do  
Adolescente no Ambiente Digital.  
[parcerias@teckids.com.br](mailto:parcerias@teckids.com.br)**