Legal Fronts
Institute

Nota Técnica em defesa do PL 2.628/22

Contribuição aos temas de moderação de conteúdo, verificação etária e educação digital

Direção institucional:
Ricardo Campos

Autoria:
Alana Barreto
Luciana Cabral Doneda
Matheus de Souza Silva
Natália Ribeiro

Gestão executiva:
Francisco Cavalcante

Revisão:
Samuel Oliveira

contato@legalfronts.org **legalfronts**.org

RESUMO EXECUTIVO

O Legal Fronts Institute participou ativamente da construção do PL 2.628/2022 no Senado Federal, a convite do autor Senador Alessandro Vieira, com base em pesquisa jurídica ancorada em boas práticas internacionais e cuja redação foi incorporada substancialmente ao texto final do projeto, e na Câmara dos Deputados. A atuação do Instituto ao longo do processo legislativo inclui, ainda, a publicação de notas técnicas, eventos públicos de escuta qualificada e produção de conhecimento voltado ao aperfeiçoamento das políticas públicas digitais para a infância e adolescência.

Em continuidade ao debate sobre o tema, esta Nota Técnica apoia o referido projeto de lei em tramitação na Câmara dos Deputados e apresenta as contribuições do Núcleo Proteção de Crianças On-line do Legal Fronts Institute aos debates acadêmicos e legislativos atuais em torno dos temas de i) moderação de conteúdo, ii) verificação etária e iii) educação digital. O documento resulta de análise normativa, revisão comparada e articulação multissetorial para formulação de diretrizes regulatórias que garantam a proteção integral de crianças e adolescentes no ambiente digital.

A presente Nota propõe aprimoramentos específicos ao texto legislativo em discussão na Câmara dos Deputados, visando à qualificação dos mecanismos de verificação etária no acesso a plataformas digitais, à definição de parâmetros para políticas de moderação de conteúdo com foco no interesse da criança, e ao fortalecimento da educação digital como política estruturante no enfrentamento das desigualdades informacionais que afetam esse público.

Como citar este documento

LEGAL FRONTS INSTITUTE. **Nota Técnica ao PL 2.628/2022:** Contribuição aos temas de moderação de conteúdo, verificação etária e educação digital. Núcleo Proteção de Crianças On-line. Brasília: Legal Fronts Institute, 2025. Disponível em: www.legalfronts.org. Acesso em: [inserir data de acesso].

1 MODERAÇÃO DE CONTEÚDO NO PL N. 2628/22

1.1 Fundamentação internacional

No Reino Unido, o *Online Safety Bill*, ao propor um novo marco regulatório para proteger a segurança dos cidadãos britânicos na Internet e combater diferentes categorias de online harms - como conteúdos de cunho terrorista, campanhas de desinformação, conteúdos que violem direitos de crianças, etc. - adota como um de seus pilares o desenvolvimento de uma cultura de transparência, confiança e prestação de contas (*accountability*). Um dos instrumentos que garantiria este desenvolvimento seria a publicação de "relatórios de transparência" (*transparency reports*), nos quais as empresas que estejam dentro do escopo da nova regulamentação deveriam prestar contas sobre os tipos de online harms que estão enfrentando e quais foram as medidas implementadas para combatê-los.

O *Online Safety Bill* foca em dois tipos de danos genericamente definidos em suas seções 45 e 46 como, respectivamente, "conteúdo danoso para crianças" e "conteúdo danoso para adultos". Isso inclui, portanto, as mais variadas categorias de danos que podem ocorrer no ambiente digital, como exploração e abuso de crianças, conteúdo e atividade terrorista, pornografia não consensual, crimes de ódio, *cyberbullying*, desinformação, dentre outros.

O objetivo do relatório anual não é apenas a prestação de contas entre a empresa e o governo do Reino Unido, mas também a construção de uma relação de confiança entre a empresa e seus usuários. A aposta do novo marco regulatório é que, ao saber quais são os online harms que prevalecem num dado serviço e quais são os passos concretos tomados para neutralizá-los, os clientes se sentirão mais seguros ao longo de suas interações online e terão mais confiança no trabalho desenvolvido por uma determinada plataforma digital, além, é claro, de contarem com mais informações para poderem cobrar soluções e monitorar seu desempenho. O centro gravitacional desse novo esquema regulatório é a criação de um dever de cuidado (*duty of care*) que deverá guiar as ações de plataformas digitais.

A Lei dos Serviços Digitais (Digital Services Act - DSA) proíbe anúncios direcionados a menores em plataformas online. As Plataformas Online Muito Grandes (Very Large Online Platforms - VLOPs) - tomaram medidas para cumprir essas proibições. Por exemplo, o *Snapchat*, o *Google* e o *YouTube*, da *Alphabet*, e o *Instagram* e o *Facebook*, da *Meta* , não permitem mais que anunciantes exibam anúncios direcionados a usuários menores de idade. O *TikTok* e o *YouTube* agora também definem as contas de usuários menores de 16 anos como privadas por padrão.

A publicidade direcionada em plataformas online também é proibida quando a criação de perfil usa categorias especiais de dados pessoais, como etnia, opiniões políticas e orientação sexual.

De acordo com as novas regras, as plataformas online acessíveis a crianças devem proteger a privacidade e a segurança desses usuários, bem como seu bem-estar mental e físico, por exemplo, adotando configurações especiais de privacidade e segurança por padrão. As plataformas online podem implementar medidas de verificação de idade para controlar quem pode acessar seus serviços, controles parentais para que pais e responsáveis possam ajudar a proteger seus filhos contra o risco de exposição a conteúdo nocivo e ferramentas onde os usuários podem denunciar abusos ou obter apoio. Alguns primeiros passos estão sendo dados.

Por exemplo, o TikTok e o YouTube, além de proibir anúncios direcionados a menores, definiram os perfis de menores automaticamente como privados, o que significa que os vídeos que eles carregam só podem ser vistos pelas pessoas que eles aprovam.

Na Europa, a moderação de conteúdo sensível para crianças e adolescentes é regulada principalmente pela DSA que estabelece um quadro rigoroso para plataformas digitais, com foco na transparência, responsabilização e proteção dos direitos fundamentais dos usuários, especialmente dos menores de idade.

Os artigos da Lei de Serviços Digitais (DSA) da União Europeia que tratam diretamente de conteúdos extremistas, de ódio ou incitação à violência estão relacionados à obrigação das plataformas digitais de detectar, moderar e remover conteúdos ilegais, incluindo discurso de ódio e incitação à violência, conforme definido pelo direito da UE e dos Estados-membros.

Embora a DSA não defina exaustivamente esses termos no texto principal, ela se apoia em definições legais existentes, como a do *Framework Decision* de 2008 da UE, que caracteriza discurso de ódio como incitação à violência ou ao ódio contra grupos protegidos (raça, religião, etnia, gênero, entre outros):

- Art. 3 (Definições e âmbito de aplicação): Define “conteúdo ilegal” como aquele que viola a legislação da UE ou dos Estados-membros, incluindo discurso de ódio e incitação à violência.
- Art. 14 (Obrigações dos prestadores de serviços intermediários): Estabelece que as plataformas devem agir rapidamente para remover ou desabilitar o acesso a conteúdos ilegais após notificação, ou detecção, incluindo conteúdos extremistas e de ódio.
- Arts. 26-32 (relacionados à mitigação de riscos e transparência): Exigem que plataformas muito grandes (VLOPs) implementem medidas para mitigar a disseminação de conteúdos ilegais, como o discurso de ódio e incitação à violência, e reportem essas ações publicamente.

A DSA incorporou o Código de Conduta Revisado sobre o Combate ao Discurso de Ódio Ilegal Online (*Code of Conduct+*), que fortalece as obrigações das plataformas para identificar, moderar e remover rapidamente conteúdos ilegais, incluindo discurso de ódio e extremismo.

Além disso, o DSA cria a figura dos “sinalizadores de confiança” (Art. 22), que são organizações independentes ou autoridades com competência para identificar e notificar conteúdos ilegais, incluindo extremismo, para que as plataformas possam agir rapidamente.

As plataformas devem garantir mecanismos eficazes para que usuários possam apresentar queixas e solicitar revisão de decisões de moderação, assegurando transparência e tratamento justo.

Como funciona a moderação de conteúdo sensível para crianças e adolescentes na Europa:

A. Consentimento parental e verificação de idade
A DSA exige que plataformas digitais obtenham consentimento dos pais para processar dados pessoais de crianças menores de 16 anos, embora os países da União Europeia possam reduzir esse limite até 13 anos, mas não abaixo disso. A lei também prevê a implementação de instrumentos de verificação etária e controle parental para proteger os menores de conteúdos inadequados.

B. Proibição de publicidade direcionada a menores
A legislação proíbe explicitamente o direcionamento de anúncios personalizados a menores com base em dados pessoais, bem como a qualquer usuário com base em informações sensíveis, como preferências sexuais e crenças religiosas. Isso visa reduzir a exposição dos jovens a conteúdos comerciais e sensíveis que possam ser prejudiciais.

C. Proteção contra conteúdos ilegais e nocivos
As plataformas devem agir rapidamente para remover conteúdos ilegais e nocivos que possam afetar crianças e adolescentes, incluindo abuso, assédio e exploração. A DSA também prevê mecanismos para que os menores possam sinalizar abusos e obter apoio adequado.

D. Transparência e contestação
As plataformas são obrigadas a informar claramente os usuários sobre os motivos da moderação de conteúdo ou suspensão de contas, além de oferecer meios para contestar essas decisões, garantindo maior transparência e justiça no processo.

E. Estratégia da União Europeia para uma internet melhor para crianças
Além da DSA, a Comissão Europeia adotou uma estratégia específica para promover experiências digitais seguras, que inclui a criação de um código de conduta para conteúdos adequados à idade e a padronização da verificação da

idade online até 2024. Também está prevista a utilização da carteira europeia de identidade digital para esse fim.

F. Medidas adicionais em países membros

- ***França:*** debate uma lei para proteger a privacidade de menores de 16 anos nas redes sociais, com possibilidade de punições severas para pais que violem a dignidade dos filhos na internet. A França exige consentimento dos pais para menores de 15 anos criarem contas em redes sociais.
- ***Alemanha:*** permite uso de redes sociais para menores entre 13 e 16 anos somente com consentimento dos pais.
- ***Bélgica:*** idade mínima de 13 anos para criar contas sem permissão dos pais.
- ***Itália:*** menores de 14 anos precisam de consentimento parental para redes sociais.
- ***Holanda:*** proíbe dispositivos móveis em salas de aula para reduzir distrações, sem lei específica sobre idade mínima para redes sociais.
- ***Reino Unido:*** aprovou a Lei de Segurança Online com restrições de idade apropriadas para proteger menores.

G. Combate à dependência digital

A legislação também aborda o impacto dos algoritmos viciantes, especialmente para menores, com propostas para proibir algoritmos que incentivem o uso excessivo e para limitar notificações em horários noturnos, buscando proteger a saúde mental dos jovens usuários.

1.2 Contribuições ao PL 2628/22 no tema de moderação de conteúdo

O Projeto de Lei n. 2628/2022, de autoria do Sen. Alessandro Vieira (MDB/SE), reforça parâmetros importantes para a proteção integral das crianças e dos adolescentes, como: a noção do dever de cuidado das plataformas, a obrigação de que seus direitos sejam respeitados desde a concepção e durante todo o fornecimento de tecnologias (direitos das crianças e dos adolescentes por design), a necessidade de avaliação, mitigação, prestação de contas e de transparência sobre os riscos de produtos ou serviços, a responsabilidade por garantir que produtos ou serviços não propaguem conteúdos que violem direitos, a obrigação de disponibilização de configurações padrões de proteção, diretrizes para mecanismos de acompanhamento parental e a proibição do perfilamento para fins comerciais.

Apresenta, também, o importante debate sobre a possibilidade de acesso de crianças às redes sociais. Sobre o acesso de crianças às redes sociais, neste momento, destaca-se a importância de discutir acerca da moderação de conteúdo não adequado para usuários

na infância e na adolescência. Nesse sentido, é necessário abordar algumas especificidades.

Ausente no PL 2628, o PL 2630 faz a necessária diferenciação entre redes sociais e mensageria instantânea, que reconhece as especificidades desta última modalidade de serviço digital, assim diferenciando:

PL 2630/22	
Serviço de mensageria privada: aplicação de internet cuja principal finalidade seja o envio de mensagens instantâneas para destinatários certos e determinados, incluindo a oferta ou venda de produtos, ou serviços e aquelas protegidas por criptografia de ponta-a-ponta, com exceção dos serviços de correio eletrônico.	**Rede social:** aplicação de internet que se destina a realizar a conexão de usuários entre si, permitindo e tendo como centro da atividade a comunicação, o compartilhamento e a disseminação de conteúdo em um mesmo sistema de informação, através de contas conectadas ou acessíveis entre si de forma articulada.

Essa diferenciação importa, pois as obrigações impostas às redes sociais não podem ser as mesmas impostas aos serviços de mensageria, sob o risco de prejudicar a privacidade e a capacidade das pessoas se comunicarem. Por exemplo, no artigo 13 do PL 2628, temos que:

PL 2628/22	SUGESTÃO
Art. 13. Os produtos ou serviços de monitoramento infantil deverão conter mecanismos e soluções de tecnologia da informação e comunicação vigentes para garantir a inviolabilidade das imagens, dos sons e das outras informações captadas, armazenadas e transmitidas aos pais ou responsáveis. § 1º Os produtos e serviços devem conter mecanismos que informem as crianças e os adolescentes, em linguagem apropriada, acerca da realização do monitoramento. § 2º O desenvolvimento e o uso de mecanismos de monitoramento infantil devem ser orientados pelo melhor interesse da criança e do adolescente e pelo pleno desenvolvimento de suas capacidades.	**Art. 13.** Os produtos ou serviços de monitoramento infantil deverão conter mecanismos e soluções de tecnologia da informação e comunicação vigentes para garantir a inviolabilidade das imagens, dos sons e das outras informações captadas, armazenadas e transmitidas aos pais ou responsáveis. § 1º Os produtos e serviços devem conter mecanismos que informem as crianças e os adolescentes, em linguagem apropriada, acerca da realização do monitoramento. § 2º O desenvolvimento e o uso de mecanismos de monitoramento infantil devem ser orientados pelo melhor interesse da criança e do adolescente e pelo pleno desenvolvimento de suas capacidades. **§ 3º A aplicação do artigo não se estende aos serviços de mensageria.**

Assim, se serviços de mensageria, como o *Whatsapp*, *Telegram* ou *Signal* forem entendidos como redes sociais, cria-se a obrigação de monitoramento de conteúdos sensíveis. Além disso, é importante ressaltar que essa possibilidade é inconstitucional,

pois viola o art. 5º, XII da Constituição Federal de 1988, que assegura a inviolabilidade de comunicações privadas.

Neste ponto, merece ser destacado que este projeto de lei deve ter por finalidade proteger esses sujeitos em condição peculiar de desenvolvimento dos perigos existentes na internet e não coibir a utilização desse espaço. Isso quer dizer, de outro modo, que deve existir um cuidado para que a regulação não culminar em uma violação do livre desenvolvimento e da liberdade de expressão de criança e adolescentes.

PL 2628/22	SUGESTÃO
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 no desenho e na operação de produtos e serviços para prevenir e mitigar: I – exploração e abuso sexual de crianças e adolescentes; II – violência física, intimidação sistemática (bullying) virtual e assédio a crianças e adolescentes; III – padrões de uso que indiquem ou incentivem comportamentos semelhantes ao vício ou transtornos de saúde mental a exemplo de ansiedade, depressão, transtornos alimentares, transtornos relacionados ao uso de substâncias e comportamentos suicidas em relação a crianças e adolescentes; IV – promoção e comercialização de narcóticos, produtos de tabaco, jogos de azar ou bebidas alcoólicas em relação a crianças e adolescentes; V – práticas publicitárias predatórias, injustas ou enganosas, ou que possam causar outros danos financeiros a crianças e adolescentes	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 no desenho e na operação de produtos e serviços para prevenir e mitigar: I – exploração e abuso sexual de crianças e adolescentes; II – violência física, intimidação sistemática (bullying) virtual e assédio a crianças e adolescentes; III – padrões de uso que indiquem ou incentivem comportamentos semelhantes ao vício ou transtornos de saúde mental a exemplo de ansiedade, depressão, transtornos alimentares, transtornos relacionados ao uso de substâncias e comportamentos suicidas em relação a crianças e adolescentes; IV – promoção e comercialização de narcóticos, produtos de tabaco, jogos de azar ou bebidas alcoólicas em relação a crianças e adolescentes; V – práticas publicitárias predatórias, injustas ou enganosas, ou que possam causar outros danos financeiros a crianças e adolescentes; e **VI - conteúdos manifestamente ilegais, incluindo materiais discriminatórios, discurso de ódio ou com incitação à violência contra grupos vulnerabilizados; e** **VII - incitação à conduta criminosa ou de ato violento e constrangedor contra crianças e adolescentes.**

As redes sociais passaram a ser os espaços públicos determinantes para a sociabilização na contemporaneidade, principalmente no que diz respeito à população mais jovem, que já nasceu nessa nova realidade em que tudo está conectado. A problemática reside em identificar o acesso de crianças e adolescentes para aquelas páginas com conteúdos inadequados para a faixa etária.

As próprias plataformas desenvolvem sistema de autorregulação, mas que ainda são insuficientes, seja para encontrar esses materiais, ou seja perante a velocidade em removê-los - a rapidez com que esses conteúdos ilegais são espalhados torna relevante que a remoção seja o mais breve possível. É essa realidade, com a facilidade de influenciar crianças e adolescentes, que torna complexa a difusão de mensagens de ódio que reúnem questões como misoginia, racismo, homofobia, entre outros materiais discriminatórios.

Ocorrências recentes demonstram que não se trata somente de atos que culminam em violação de outras pessoas em processo de vulnerabilização, pois o que se identifica é, na verdade, uma estrutura mais complexa com disseminação de ódio. Sendo assim, as crianças e adolescentes também têm sido vítimas com os chamados desafios que incluem, por exemplo, a automutilação ou violência contra animais.

A presença de uma regulamentação em torno desse conteúdo é importante para combater essa cultura digital de ódio, principalmente envolvendo populações historicamente estigmatizadas. Não há, entretanto, uma inovação legislativa, já que trata-se apenas de ratificar, no ambiente digital, o arcabouço normativo anti-discriminatório existente na ordem jurídica brasileira, conduzido a partir do texto constitucional, que põe, no art. 3, inciso III, a promoção do bem de todos sem preconceito como um objetivo fundamental da República.

PL 2628/22	SUGESTÃO

Art. 8º Os fornecedores de produtos ou serviços de tecnologia da informação direcionados ou que possam ser utilizados por crianças e adolescentes deverão: I – realizar avaliação de riscos de seus recursos, funcionalidades e sistemas e seus impactos voltados para a segurança e saúde das crianças e adolescentes; II – realizar avaliação do conteúdo disponibilizado para as crianças e adolescentes de acordo com a faixa etária, para que sejam compatíveis com a respectiva classificação indicativa; e III – oferecer sistemas e processos projetados para impedir que crianças encontrem, por meio do produto ou serviço, conteúdo ilegal, nocivo ou danoso e em desacordo com sua classificação etária.	Art. 8º Os fornecedores de produtos ou serviços de tecnologia da informação direcionados ou que possam ser utilizados por crianças e adolescentes deverão: I – realizar avaliação de riscos de seus recursos, funcionalidades e sistemas e seus impactos voltados para a segurança e saúde das crianças e adolescentes; II – realizar avaliação do conteúdo disponibilizado para as crianças e adolescentes de acordo com a faixa etária, para que sejam compatíveis com a respectiva classificação indicativa; e III – oferecer sistemas e processos projetados para impedir que crianças encontrem, por meio do produto ou serviço, conteúdo ilegal, **odioso,** nocivo ou danoso e em desacordo com sua classificação etária.

A proliferação de conteúdos com caráter extremista nas redes sociais é facilitada pelo funcionamento dos algoritmos das plataformas digitais, que potencializam a circulação desses conteúdos ao mobilizar afetos como medos e fantasias, criando bolhas de autoidentificação e favorecendo a disseminação de discursos polarizadores, inclusive de extrema-direita. Esses algoritmos operam a partir da coleta massiva de dados e da modulação da atenção dos usuários, o que pode amplificar o alcance de discursos de ódio e extremistas, tornando-os um dos maiores desafios contemporâneos na internet.

Quanto à definição legal de conteúdos ilegais, odiosos, nocivos ou danosos, a sugestão de incluir um parágrafo único que delimite esses conceitos visa garantir maior segurança jurídica e evitar o uso indevido da norma para restringir a liberdade de expressão dos usuários. Essa definição precisa ser inclusiva e respeitar a liberdade de expressão, distinguindo claramente o que configura discurso de ódio e seus limites, para que a legislação seja efetiva e justa.

No Brasil, a indefinição jurídica sobre o que são discursos de ódio e a dificuldade de distinguir esses crimes de outros, como os crimes contra a honra, representam um problema prático que prejudica o acolhimento das vítimas. Existem leis específicas que punem crimes de discriminação e preconceito, como racismo, xenofobia e intolerância religiosa, mas a tipificação e a aplicação ainda enfrentam desafios.

O discurso de ódio, segundo definições consolidadas, consiste em expressões que inferiorizam indivíduos ou grupos por características como raça, etnia, religião, orientação sexual, entre outras, e que podem incitar violência, ódio ou discriminação. Ele é considerado um abuso da liberdade de expressão quando atinge direitos fundamentais e rebaixa grupos sociais, configurando uma manifestação que deve ser combatida para proteger a dignidade e os direitos humanos.

Assim, é necessário haver uma remoção rápida e imediata do conteúdo de ódio ou de apologia à violência antes da publicação/conteúdo ser devidamente postada para crianças e adolescentes. Isso porque as plataformas digitais possuem mecanismos de identificação de conteúdos que envolvem categorias específicas de discurso de ódio, como racismo, homofobia, misoginia, xenofobia, insultos e obscenidades, e podem realizar classificações binárias (presença ou ausência de discurso de ódio) e multirrótulo (tipos específicos de ódio)[1].

PL 2628/22	SUGESTÃO
Art. 21. Para atender ao princípio da proteção integral, é dever dos fornecedores de produtos	**Art. 21.** Para atender ao princípio da proteção integral, é dever dos fornecedores de produtos

[1] Muitas redes sociais utilizam técnicas avançadas de Processamento de Linguagem Natural (PLN) e modelos de inteligência artificial, como o BERT e algoritmos de aprendizado de máquina (Naive Bayes, Regressão Logística, SVM), para detectar e classificar discursos de ódio em textos, especialmente em postagens como tweets.

ou serviços de tecnologia da informação direcionados ou que possam ser utilizados por crianças e adolescentes proceder à retirada de conteúdo que viola direitos de crianças e adolescentes assim que forem comunicados do caráter ofensivo da publicação, independentemente de ordem judicial. Parágrafo único. Notificados acerca de violações aos direitos de crianças e adolescentes no âmbito dos seus serviços destinados a esse público, os fornecedores deverão oficiar às autoridades competentes para instauração de investigação, nos termos de regulamento.	ou serviços de tecnologia da informação direcionados ou que possam ser utilizados por crianças e adolescentes proceder à retirada **imediata através dos mecanismos de identificação** de conteúdo que viola direitos de crianças e adolescentes assim **ou que** forem comunicados do caráter ofensivo da publicação, independentemente de ordem judicial. **I - Os fornecedores de produtos ou serviços de tecnologia da informação direcionados ou que possam ser utilizados por crianças e adolescentes devem criar um canal de denúncias acessível dentro da própria plataforma que seja vinculada ao Ministério da Justiça e Segurança Pública.** **II - Notificados acerca de violações aos direitos de crianças e adolescentes no âmbito dos seus serviços destinados a esse público, os fornecedores deverão oficiar às autoridades competentes para instauração de investigação, nos termos de regulamento.** **III - Os usuários têm o direito de apelar das decisões das plataformas.** **IV - Devem disponibilizar um mecanismo de reclamação para contestar decisões de moderação e publicar relatórios anuais detalhando seus procedimentos de moderação.**

A União Europeia adota a regra do “notice and take down” (notificar e remover), que obriga as plataformas a criarem meios para que os usuários denunciem conteúdos ilegais, como pornografia infantil, discurso de ódio, fake news e violações à honra. Após a notificação, a plataforma é responsável por avaliar e decidir sobre a remoção do conteúdo denunciado e deve registrar esse processo em um banco de dados público, garantindo transparência.

Os usuários têm o direito de apelar das decisões das plataformas. Assim, as plataformas devem disponibilizar um mecanismo de reclamação para contestar decisões de moderação e publicar relatórios anuais detalhando seus procedimentos de moderação. Também é exigido um ponto de contato designado para autoridades e usuários e termos de uso transparentes.

Por sua vez, a *Online Safety Act* impõe regras rigorosas para que plataformas como *Facebook*, *TikTok* e outras adotem medidas para prevenir e remover rapidamente conteúdos prejudiciais, incluindo abuso sexual infantil, discurso de ódio e desinformação. Assim, as plataformas também devem oferecer processos eficientes de denúncia e contestação, garantindo que os usuários possam apelar da remoção de conteúdo e que conteúdos removidos injustamente sejam restabelecidos.

Além disso, o órgão regulador *Ofcom* supervisiona o cumprimento da lei, podendo aplicar multas pesadas (até 18 milhões de libras esterlinas ou 10% da receita global) e até bloquear serviços que não se adequem.

2 VERIFICAÇÃO ETÁRIA NO PL 2.628/22 E OS DESAFIOS PARA PROTEÇÃO ON-LINE DE CRIANÇAS E ADOLESCENTES

O Projeto de Lei nº 2.628/2022 visa garantir um ambiente online mais seguro e alinhado aos direitos fundamentais da criança e do adolescente, conforme garantido na Constituição Federal de 1988 e no Estatuto da Criança e do Adolescente (ECA).

Dentre os vários instrumentos previstos, destaca-se a verificação etária como um componente instrumental essencial. Trata-se de um mecanismo cuja finalidade não é apenas restringir acesso, mas habilitar a aplicação de todas as demais medidas de proteção ao público infanto-juvenil – desde o controle de acesso a conteúdos sensíveis e adultos até a limitação da coleta de dados pessoais e a personalização de publicidade. Assim, sem uma verificação de idade eficaz, todas as outras obrigações do projeto tornam-se praticamente inexequíveis, já que, sem identificar corretamente quem são os usuários menores de idade, não é possível ajustar as medidas de proteção para seus perfis no ambiente online.

Apesar das intenções positivas expressas no texto legal e da adoção de iniciativas por parte de plataformas digitais, os mecanismos atualmente utilizados para verificar a idade de perfis criados, a maioria baseados na autodeclaração de idade por usuários, demonstram eficácia limitada e são amplamente contornáveis na prática.

Algumas das plataformas mais utilizadas pelo público infanto-juvenil têm implementado produtos e funcionalidades voltadas a usuários menores de idade, como o YouTube Kids, com conteúdos moderados e interface simplificada; o Family Center do Snapchat, que permite a supervisão remota das interações do adolescente por pais ou responsáveis; o modo restrito do TikTok e a configuração de contas para adolescentes no Instagram, que limita sugestões de conteúdo e interações com desconhecidos.

Atualmente, as plataformas digitais mais usadas por crianças e adolescentes adotam como idade mínima para a criação de contas os 13 anos, em decorrência direta da legislação norte-americana COPPA (*Children's Online Privacy Protection Act*), que proíbe a coleta de dados pessoais de menores de 13 anos sem consentimento verificável dos pais. Contudo, para adolescentes entre 13 e 17 anos, o cenário é marcado por recomendações genéricas de controle parental, sem exigência efetiva de verificação ou autenticação do responsável legal.

Essa lógica, ao ser reproduzida no Brasil, entra em tensão com o marco legal doméstico. O ECA define como criança a pessoa de até 12 anos incompletos e como adolescente aquela entre 12 e 18 anos. O PL 2628/2022, ao "importar" a referência dos 13 anos como limiar crítico, ignora a segmentação etária prevista na legislação brasileira, e não justifica por que esse marco se tornaria juridicamente relevante no contexto nacional.

Além disso, a eficácia prática dos mecanismos atuais é amplamente contestável. Em geral, a verificação de idade ocorre apenas por autodeclaração da data de nascimento: um procedimento que pode ser facilmente burlado por crianças e adolescentes. Segundo a pesquisa TIC Kids Online Brasil 2024, parcela expressiva de crianças entre 9 e 17 anos possui contas próprias em plataformas digitais como Instagram, tiktok e youtube[2], muitas vezes criadas com idades inautênticas.

O texto atual do PL trata da verificação etária em dois principais contextos: para provedores de conteúdo pornográfico ou adulto, há a exigência de "mecanismos confiáveis de verificação de idade e identidade", limitando o uso dos dados à finalidade específica de impedir o acesso por menores de 18 anos. Para redes sociais e demais aplicações acessadas por crianças e adolescentes, o projeto determina o "aprimoramento contínuo" desses mecanismos, desde que respeitados os princípios de privacidade e proteção de dados pessoais.

Embora a previsão legal avance ao reconhecer a importância da verificação etária, faltam diretrizes mais claras quanto: à diferenciação entre faixas etárias para a permissão de uso e dos respectivos serviços – como crianças (pessoas de 0 a 12 anos) e adolescentes (pessoas de 12 a 18 anos); à definição de critérios técnicos mínimos para validar essa verificação etária; à aplicação proporcional das exigências conforme o porte do serviço e o risco envolvido para os menores.

Do ponto de vista técnico, a ausência de consenso internacional sobre métodos eficazes e não invasivos é um desafio real. O Parlamento australiano reconheceu formalmente, em sua exposição de motivos sobre o *Social Media Minimum Age Bill 2024*[3], que não há ainda um modelo técnico eficaz padronizado globalmente para a verificação etária para acessar serviços digitais.

Mesmo assim, do ponto de vista técnico, soluções vêm sendo implementadas em algumas plataformas. De forma exemplificativa, o Instagram utiliza em alguns países uma ferramenta de terceiros baseada em inteligência artificial para inferência de idade por análise biométrica facial em vídeo[4]. Para verificar a identidade, a tecnologia solicita

[2] CGI.br – COMITÊ GESTOR DA INTERNET NO BRASIL. **Pesquisa sobre o uso da Internet por crianças e adolescentes no Brasil: TIC Kids Online Brasil 2024**. São Paulo: CGI.br, 2025. Disponível em: https://cetic.br/pt/pesquisa/kids-online/

[3] Australia: Online Safety Amendment (Social Media Minimum Age) Bill 2024. Ver sobre em: https://parlinfo.aph.gov.au:443/parlInfo/search/display/display.w3p;page=0;query=Id%3A%22legislation%2Fems%2Fr7284_ems_b9c134ac-a19a-47b2-9879-b03dda6e3c1a%22.

[4] Instagram blog. Apresentamos novas formas de verificação de idade no Instagram. 2022

que usuários carreguem um documento oficial, solicitar a confirmação de amigos ou gravar uma selfie em vídeo. A estimativa de idade é realizada sem identificação nominal e com descarte automático do material após a verificação, respeitando os princípios de privacidade e minimização de dados.

Outro exemplo mais recente é o da plataforma Reddit, que passou a adotar, no Reino Unido, um sistema obrigatório de verificação de idade para usuários britânicos[5]. A medida antecipa as exigências previstas no Protection of Children Code of Practice for User-to-User Services, como instrumento de implementação do Online Safety Act[6]. Para atender a esses requisitos, o Reddit firmou parceria com a empresa Persona, responsável pela verificação de idade por meio do envio de foto facial ou documento oficial de identidade. A plataforma informa que os dados fornecidos são usados exclusivamente para esse fim e descartados após a verificação, mantendo apenas o status de conformidade e a data de nascimento do usuário. A Ofcom, autoridade reguladora britânica, reforçou que plataformas que não adotarem mecanismos de verificação de idade eficazes poderão ser alvo de sanções legais, como ordens de bloqueio e remoção de serviços no Reino Unido.

No entanto, o uso de tecnologias como inferência biométrica, escaneamento de documentos ou autenticação parental exige uma governança de dados extremamente responsável para ser implementada. A coleta e o tratamento de dados sensíveis de crianças e adolescentes devem seguir as disposições previstas na Lei Geral de Proteção de Dados Pessoais (LGPD), respeitando os princípios de finalidade, minimização, segurança e descarte adequado. É importante, ainda, ressaltar a proibição expressa de qualquer uso secundário, comercial ou indevido dos dados utilizados para a verificação etária.

Por fim, é fundamental que o Projeto de Lei estabeleça critérios técnicos mínimos e obrigações escalonadas, por exemplo, proporcionais ao grau de risco oferecido pela plataforma às crianças e adolescentes, ao volume de usuários e ao potencial de atração do serviço para crianças e adolescentes. Essa lógica de proporcionalidade regulatória, já presente em experiências normativas da União Europeia e do Reino Unido, permite alinhar a proteção da infância à inovação tecnológica, garantindo segurança jurídica e eficácia prática.

---

https://about.instagram.com/pt-br/blog/announcements/new-ways-to-verify-age-on-instagram

[5] Reddit. Why is Reddit asking for my age? https://support.reddithelp.com/hc/en-us/articles/36429514849428-Why-is-Reddit-asking-for-my-age.

[6] Ofcom (Reino Unido) Protection of Children Code of Practice for User-to-User Services. London: UK Government, 2024. https://www.gov.uk/government/publications/protection-of-children-code-of-practice-for-user-to-user-services

Diante disso, a presente contribuição e comentário ao PL analisará a abordagem adotada por diferentes países quanto à verificação etária no ambiente digital, identificando boas práticas e lacunas relevantes. Em seguida, serão propostas sugestões de aprimoramento normativo ao texto atualmente aprovado pelo Senado, com o objetivo de contribuir para uma implementação mais efetiva das garantias previstas no PL 2.628/2022.

2.1 Comparativo internacional no tema de verificação etária

Na Comunidade Europeia, o Digital Services Act (DSA) foi aprovado pelo Regulamento UE 2022/2065 com a proposta de tornar o ambiente on-line mais seguro, previsível e confiável. No sistem

O desafio de implementar mecanismos eficazes de verificação etária como etapa essencial para a proteção de crianças e adolescentes no ambiente digital não se restringe ao contexto brasileiro. Diante desse cenário, esta seção busca reunir experiências regulatórias e iniciativas internacionais que podem oferecer lições relevantes para o Brasil, tanto em termos de viabilidade técnica quanto de desenho normativo. A comparação visa identificar boas práticas, contribuindo para o aprimoramento do Projeto de Lei nº 2.628/2022 e para a construção de um modelo nacional que seja eficaz e alinhado com os direitos fundamentais de crianças e adolescentes no ambiente digital.

2.1.1 União Europeia

A União Europeia tem avançado de forma coordenada para estabelecer uma abordagem regulatória robusta e tecnicamente viável à verificação etária, sempre em consonância com os princípios do Regulamento Geral de Proteção de Dados (GDPR).

Em fevereiro de 2025, o European Data Protection Board (EDPB) publicou o **Statement 1/2025 on Age Assurance**[7], que estabelece princípios orientadores para a implementação de mecanismos de verificação etária. O documento reforça que qualquer método deve respeitar o princípio da proporcionalidade, ser tecnicamente necessário e voltado ao melhor interesse da criança.

Entre os destaques, o documento traz que a robustez da verificação deve ser proporcional ao risco do serviço – plataformas que podem conter conteúdo sensível para crianças ou adolescentes (pornografia, discurso de ódio, automutilação), coleta de dados comportamentais ou algoritmos de decisão automatizada devem adotar métodos mais robustos para verificação etária; a minimização de dados é mandatória: deve-se evitar

[7] European Data Protection Board. Statement 1/2025 on Age Assurance. https://www.edpb.europa.eu/our-work-tools/our-documents/statements/statement-12025-age-assurance_en.

qualquer coleta de informações desnecessárias — muitas vezes bastando saber se o usuário é “acima de 13” ou “menor de 16”, por exemplo;

O documento também ressalta a preferência por soluções tecnológicas que preservem a privacidade, como:

- i. *Tokens de idade*: um terceiro atesta apenas a elegibilidade etária sem revelar mais dados;
- ii. *Zero-knowledge proofs*: prova de que a idade mínima foi atingida sem expor a idade real;
- iii. *Credenciais digitais de uso único*, armazenadas localmente no dispositivo do usuário;
- iv. Acessibilidade e inclusão: os métodos devem funcionar mesmo para crianças sem documentos formais, dispositivos próprios ou com deficiência;
- v. Governança e transparência: sistemas devem ter “no log policy”, segurança de dados e possibilidade de contestação por usuários.

Complementando essa diretriz, em 14 de julho de 2025, a Comissão Europeia lançou a primeira versão do modelo técnico de verificação de idade white label[8], voltado a promover uma solução padronizada, interoperável e centrada na proteção da privacidade. O projeto é parte da implementação do **Artigo 28(1) do Digital Services Act (DSA)**, que exige que plataformas online garantam um alto nível de segurança para crianças e adolescentes.

Esse modelo, apelidado de "minicarteira", é baseado em código aberto e pensado para operar junto às futuras Carteiras Europeias de Identidade Digital. Ele permite que o usuário prove sua maioridade sem revelar dados pessoais adicionais, com verificação descentralizada, uso único e sem rastreamento entre serviços. A fase piloto já envolve países como Dinamarca, França, Grécia, Itália e Espanha. A Comissão Europeia pretende ampliar a adesão a todos os Estados-Membros até 2026.

2.1.2 Reino Unido

O Reino Unido foi um dos primeiros países a adotar uma abordagem regulatória específica para a proteção digital de crianças e adolescentes. O **Age Appropriate Design Code**[9], em vigor desde 2021, exige que todos os serviços digitais acessíveis a menores de 18 anos implementem políticas que levem em consideração a faixa etária do usuário.

---

[8] European Commission. Commission makes available an age-verification blueprint. https://digital-strategy.ec.europa.eu/en/news/commission-makes-available-age-verification-blueprint.

[9] ICO (Information Commissioner's Office). Reino Unido. Age appropriate design: a code of practice for online services: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/

Mais recentemente, em 2025, como parte da implementação da Online Safety Act, o país deu um passo ainda mais concreto com a publicação, pela Ofcom, de dois Códigos de Prática obrigatórios para serviços digitais que podem ser acessados por crianças e adolescentes: o *Protection of Children Code of Practice for User-to-User Services* e o *Code of Practice for Search Services*[10].

Esses códigos estabelecem medidas técnicas e organizacionais que devem ser adotadas pelas plataformas para evitar que crianças acessem conteúdos prejudiciais, incluindo pornografia, apologia à automutilação, distúrbios alimentares, discurso de ódio e violência. Um dos pilares dessas novas diretrizes é a exigência de verificação de idade altamente eficaz (highly effective age assurance), que vá além da autodeclaração e seja proporcional ao risco apresentado pelo serviço. As plataformas deverão implementar mecanismos robustos de verificação sempre que o risco de acesso a conteúdos inadequados for significativo, podendo recorrer a tecnologias como análise documental automatizada ou verificação biométrica por terceiros. As obrigações incluem, ainda, revisão contínua da eficácia dos métodos adotados, governança transparente e proteção de dados por design, com supervisão direta da Ofcom, que poderá aplicar medidas sancionatórias, como multas ou bloqueio do serviço no Reino Unido, em caso de não conformidade.

2.1.3 Austrália

A eSafety Commissioner, autoridade australiana sobre segurança online, tem promovido ativamente uma agenda de proteção infantil online. Em sua Age Verification Roadmap, reconhece que não há consenso técnico internacional sobre o modelo ideal de verificação etária[11], mas defende o desenvolvimento nacional de soluções.

Uma das iniciativas em andamento é o projeto MyID[12], uma identidade digital federal que poderá incluir atributos de idade verificáveis. Essa solução visa garantir segurança, respeitar a privacidade e evitar a coleta direta por plataformas.

Além disso, na Austrália está em tramitação um projeto de lei que restringe o acesso de menores de 16 anos a determinadas plataformas, como redes sociais[13], exigindo métodos verificáveis para que menores de 16 anos não tenham perfis nessas redes.

---

[10] Reino Unido. Ofcom. Statement: Protecting children from harms online. https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/statement-protecting-children-from-harms-online.

[11] eSafety Commissioner (eSafety). Australia Roadmap for age verification and complementary measures to prevent and mitigate harms to children from online pornography. 2023. https://www.esafety.gov.au/sites/default/files/2023-08/Roadmap-for-age-verification_2.pdf

[12] Austrália. O aplicativo de identificação digital do governo australiano. myID é uma maneira segura de provar quem você é online. https://www.myid.gov.au/.

[13] Australia: Online Safety Amendment (Social Media Minimum Age) Bill 2024. Ver sobre em: https://parlinfo.aph.gov.au:443/parlInfo/search/display/display.w3p;page=0;query=Id%3A%22legislation%2Fems%2Fr7284_ems_b9c134ac-a19a-47b2-9879-b03dda6e3c1a%22.

2.1.5 Espanha

Em 2024, a Espanha lançou, por meio do Ministério da Transformação Digital, um sistema público de verificação de idade baseado em credenciais digitais temporárias e anônimas[14]. Após autenticação via identidade eletrônica (como o DNIe), o usuário recebe credenciais com validade limitada, armazenadas em app móvel e protegidas por identificadores descentralizados. Ao acessar o conteúdo, o usuário valida o provedor de conteúdo e apresenta uma credencial, garantindo anonimato e segurança.

Embora represente um avanço tecnológico importante, o sistema apresenta desafios: exige alto grau de digitalização da população; Pode ser contornado se um adulto autenticar a credencial e permitir o uso por um menor de idade, pois a conta é vinculada ao aparelho digital.

Esse panorama demonstra que não há solução única adotada globalmente, mas sim diretrizes recorrentes: proporcionalidade, minimização de dados, foco em privacidade, preocupação com a proteção de crianças e adolescentes online e incentivo à interoperabilidade. A experiência europeia, em particular, oferece lições valiosas para o Brasil ao vincular direitos digitais infantis a medidas técnicas viáveis e auditáveis, sob controle público ou transparente.

Ainda que as experiências internacionais aqui analisadas ofereçam bons insumos para o debate normativo brasileiro, é importante reconhecer que a maioria delas parte de contextos de alto grau de desenvolvimento digital e maior acesso à conectividade significativa. No caso brasileiro, os desafios relacionados à inclusão digital, à desigualdade de acesso e à fragmentação dos sistemas de identidade e cidadania digital ainda representam entraves estruturais à aplicação direta de alguns desses modelos. Isso significa que a regulação deve levar em conta as capacidades tecnológicas brasileiras atuais, promovendo uma escala progressiva de exigências, conforme o grau de risco do serviço, o porte da plataforma e o avanço do governo digital no país.

2.2 Contribuições ao PL 2628/22 no tema de verificação etária

Esse tópico tem como objetivo sugerir contribuições no texto do PL 2.628/22 para garantir maior efetividade na adoção das medidas de proteção direcionadas a crianças e adolescentes no ambiente online, voltado à verificação etária. A análise do PL 2628/2022 evidencia um esforço normativo importante, mas ainda genérico, em relação à verificação etária. A ausência de diretrizes técnicas mínimas e critérios diferenciados

[14] Espanha. Ministerio para la Transformación Digital y de la Función Pública. Especificaciones técnicas para la herramienta de verificación de edad. https://digital.gob.es/especificaciones_tecnicas.html .

por tipo de serviço digital, faixa etária ou risco associado pode comprometer a efetividade da proteção pretendida. Nesse sentido, propõe-se:

2.2.1 Adição de um capítulo específico sobre verificação etária

Sugere-se a inclusão, ao final do PL, **anterior** ao capítulo X ("Da Governança"), de um novo Capítulo – “Da Verificação Etária”, com redação inspirada em boas práticas internacionais, especialmente o modelo britânico.

SUGESTÃO AO PL 2628/22

CAPÍTULO X - DA VERIFICAÇÃO ETÁRIA

Art. XX. Os serviços digitais a que se aplica esta Lei deverão adotar mecanismos robustos, auditáveis e proporcionais de verificação etária, de forma a garantir o acesso seguro e adequado de crianças e adolescentes, considerando o grau de risco da plataforma, o volume de usuários e o potencial de atração infantojuvenil.

§ 1º Os mecanismos de verificação etária devem observar critérios de:

I – precisão técnica, mediante testes em ambientes controlados que comprovem a capacidade de distinguir com acurácia entre usuários adultos e infantojuvenis;

II – robustez, com medidas para impedir e mitigar tentativas de contorno, inclusive com reavaliação periódica de eficácia;

III – confiabilidade, especialmente no uso de tecnologias baseadas em inteligência artificial, com testes contínuos para garantir resultados consistentes;

IV – equidade, mediante treinamento e validação de modelos com dados diversos, evitando viés e discriminação.

§ 2º Os serviços deverão aplicar o mais alto padrão de verificação etária sempre que houver probabilidade significativa de acesso por crianças e adolescentes, mesmo que não sejam o público-alvo principal do serviço.

§ 3º As tecnologias utilizadas deverão priorizar métodos que preservem a privacidade do usuário, como credenciais digitais binárias (“entre 13 e 16 anos”, “acima de 16 anos”) ou inferência de idade com minimização de dados.

§ 4º Os dados eventualmente coletados para fins de verificação etária não poderão ser reutilizados para qualquer outra finalidade, sendo vedada sua monetização, compartilhamento ou reutilização para outros propósitos;

§ 5º Os serviços classificados como de alto risco deverão implementar, de forma progressiva e auditável, mecanismos de verificação etária mais robustos e tecnicamente eficazes, garantindo a preservação da privacidade e dos direitos do usuário.

§ 6º Os serviços de pequeno porte, ou que apresentem baixo risco de uso por crianças e adolescentes, poderão adotar mecanismos menos intrusivos de verificação etária, desde que justificados por meio de avaliação de impacto e sujeitos à aprovação da autoridade competente.

§ 7º A autoridade competente poderá estabelecer diretrizes complementares para definição do grau de risco dos serviços, bem como parâmetros técnicos e metodológicos para os mecanismos de verificação etária, respeitando o princípio da proteção integral da criança e do adolescente.

2.2.2 Revisão e redistribuição de artigos do texto atual

Sugere-se aprimorar as definições do Art. 2º, com base no PL 2630/2020, incluindo:a

- **Serviço de rede social:** plataforma cuja funcionalidade principal é permitir interação entre usuários via perfis, publicações, comentários e compartilhamento de conteúdo.
- **Serviço de mensageria privada:** aplicações cujo objetivo principal é a troca direta de mensagens entre usuários.

Como já mencionado na contribuição sobre moderação de conteúdo por pesquisadores deste Núcleo, a definição e diferenciação são importantes, pois as obrigações impostas às redes sociais não podem ser as mesmas impostas aos serviços de mensageria, sob o risco de prejudicar a privacidade e a capacidade das pessoas se comunicarem.

- **Serviços digitais de alto risco para crianças e adolescentes**: serviço digital cuja arquitetura, funcionalidades ou conteúdos apresentam elevado potencial de exposição de crianças e adolescentes a danos, incluindo, mas não se limitando a:

  I – facilitação de interações com usuários desconhecidos, sem filtros ou mediação adequada;

  II – oferta ou disseminação de conteúdo impróprio, como violência, discurso de ódio, pornografia, promoção de distúrbios alimentares, automutilação ou suicídio;

  III – utilização de sistemas de perfilamento comportamental voltados à monetização, como publicidade personalizada baseada em coleta de dados de navegação;

  IV – mecanismos de recomendação automatizada que amplifiquem conteúdos sensíveis ou inadequados à faixa etária.

A classificação de serviços digitais de "alto risco" se inspira no Digital Services Act (DSA) da União Europeia[15], que estabelece um modelo escalonado de obrigações regulatórias com base no porte do serviço e no grau de risco sistêmico. O DSA introduz, por exemplo, a categoria de Very Large Online Platforms (VLOPs) e Very Large Online Search Engines (VLOSEs), com mais de 45 milhões de usuários mensais na UE, sujeitas a obrigações especiais de mitigação de riscos e auditorias independentes.

Esses parágrafos tratam da obrigatoriedade da verificação etária e uso exclusivo dos dados para essa finalidade . **Propõe-se realocá-los para o novo capítulo específico de verificação etária**, com o objetivo de permitir detalhamento técnico e harmonização com princípios da LGPD e com práticas internacionais como o estabelecimento de critérios de proporcionalidade e escalonamento conforme risco do serviço; Tecnologias mínimas

[15] Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho de 19 de outubro de 2022 relativo a um mercado único para os serviços digitais e que altera a Diretiva 2000/31/CE (Regulamento dos Serviços Digitais) (Texto relevante para efeitos do EEE). https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32022R2065

aceitáveis; Governança e auditoria dos dados; Proibição expressa de monetização ou reaproveitamento dos dados coletados.

Sugere-se que o texto defina critérios mais objetivos para "diferentes idades, capacidades e necessidades", referenciando, por exemplo, faixas etárias progressivas (ex.: entre 13 e 16 anos, de 13 a 17), como fazem códigos internacionais de design apropriado por idade.

Para evitar que a definição de faixas etárias e níveis de proteção recaia exclusivamente sobre as plataformas digitais, o que poderia gerar assimetrias e riscos à consistência normativa, recomenda-se que a lei preveja a participação de instâncias especializadas, como o Conanda (Conselho Nacional dos Direitos da Criança e do Adolescente), na elaboração de diretrizes técnicas sobre necessidades de desenvolvimento por faixa etária. Essas diretrizes poderiam orientar a regulamentação infralegal e os próprios provedores, garantindo base científica, participação social qualificada e proteção integral. Alternativamente, a lei poderia remeter à autoridade competente essa atribuição, com base em consulta a especialistas e organismos reconhecidos.

O § 3º do Art. 17 e os §§ 1º e 2º do Art. 19 já trazem previsões sobre verificação etária, mas são vagas. Recomenda-se sua reestruturação dentro do novo capítulo (Da verificação etária) como mencionado acima, com exigências concretas sobre o tipo de tecnologia a ser adotado e padrão mínimo de eficácia (ex: sistema de verificação com terceiros, credenciais binárias, reavaliação periódica).

A partir da análise comparativa internacional e da avaliação do texto aprovado no Senado, observa-se que a proteção de crianças e adolescentes em ambientes digitais exige medidas específicas, proporcionais e tecnicamente fundamentadas para a verificação etária. A proposta de consolidação de um capítulo próprio sobre o tema visa conferir maior efetividade e segurança jurídica ao PL 2628/2022, além de alinhar a legislação brasileira às melhores práticas internacionais. Ao incorporar definições normativas mais precisas, critérios técnicos mínimos e diferenciação conforme o risco das plataformas, busca-se garantir um equilíbrio entre proteção infanto-juvenil, inovação tecnológica e respeito à privacidade. Espera-se, com isso, contribuir para o aprimoramento do marco regulatório, assegurando que crianças e adolescentes possam exercer seus direitos digitais com respeito ao seu estágio de desenvolvimento.

3 EDUCAÇÃO DIGITAL NO PL 2628/22: ESTRATÉGIAS DE EDUCAÇÃO PARA A PROTEÇÃO ON-LINE DE CRIANÇAS E ADOLESCENTES

A proteção on-line das crianças exige políticas públicas que visam a formação de pais, educadores, e das próprias crianças, ao mesmo tempo que solicita órgãos reguladores que monitorem as grandes empresas que atuam na Internet. A Política Brasileira de

Educação Digital (PNED) propõe o desenvolvimento de uma estratégia nacional para fornecer proteção às crianças no mundo virtual. Considerando que as novas tecnologias estão integradas às vidas das crianças e jovens, assim como dos adultos, constata-se que o mundo real e o virtual estão cada vez mais interligados e interdependentes.

A legislação brasileira pode e deve se inspirar em experiências que promovam um alto nível de proteção à infância e adolescência.

3.1 Estratégias de educação digital no direito comparado

Na Comunidade Europeia, o Digital Services Act (DSA) foi aprovado pelo Regulamento UE 2022/2065 com a proposta de tornar o ambiente on-line mais seguro, previsível e confiável. No sistema de governança do DAS tem sido essencial a cooperação entre a Comissão Europeia e as autoridades nacionais para garantir a aplicação, a monitoração e a vigilância das obrigações. O coordenador de serviços digitais atua nacionalmente nos países da União Europeia para a aplicação do regulamento.

Além da regulamentação na oferta de serviços digitais, a União Europeia investe também em programas educativos para o mundo digital. Os programas formativos têm como fundamentos o DAS, a privacidade, a violência on-line e a inteligência artificial.

A Comissão Europeia promove a divulgação de conteúdos educativos sobre os riscos e as oportunidades para os menores no mundo on-line. Uma rede, formada pelos centros para uma internet mais segura (SIC) dos estados membros da União Europeia (EU), desenvolve campanhas de sensibilização e fornece recursos e melhores práticas em todas as línguas oficiais da EU para dar suporte às crianças, pais e professores na vida on-line.

Ao longo do ano, são criados e divulgados projetos em campanhas de comunicação para orientar professores, pais, jovens e crianças. As propostas são alimentadas com o ePolicy, um documento programático produzido pelas escolas, com base nos índices apresentados na plataforma on-line para descrever a visão do fenômeno, as normas comportamentais e os procedimentos para a utilização de tecnologias no ambiente escolar, com medidas de prevenção, de detecção e de gestão dos problemas para um uso mais consciente das tecnologias digitais. O objetivo é promover as competências digitais e o uso positivo, crítico e consciente das tecnologias digitais tanto por parte dos jovens quanto dos adultos envolvidos no processo educativo.

A Comissão Europeia instituiu, no dia 11 de fevereiro, o Safer Internet Day, o Dia Mundial pela Segurança na Internet, com objetivo de estimular a reflexão para fazer com que os jovens reflitam sobre o uso consciente da Internet, considerando também o papel ativo e responsável que cada um deve assumir para que a Internet seja um lugar que possa ser considerado positivo e seguro. Em maio de 2024 a Comissão Europeia publicou um compêndio da nova estratégia “Internet melhor para os jovens” com os textos formais da

EU sobre os menores no mundo digital com as diversas leis de proteção aos menores, as estratégias e as regulamentações recentes.

Todas essas iniciativas demonstram o quanto é preocupante a falta de regulamentação na Internet e a importância de uma educação digital sólida para a construção da cidadania no mundo atual.

3.2 Arcabouço jurídico-normativo brasileiro e arranjos institucionais

No Brasil, várias legislações (PNED, Marco Civil da Internet e LGPD) e vários órgãos públicos e organizações não governamentais tratam da proteção on-line infantil, como o Ministério dos Direitos Humanos e da Cidadania, a SaferNet Brasil, a Polícia Federal, o Ministério Público Federal (MPF) e o Comitê Gestor da Internet (CGI.br), entre outros. A Agência Nacional de Telecomunicações (Anatel) disponibiliza um conjunto de cartilhas com orientações para os diversos atores envolvidos na proteção on-line das crianças: pais, educadores, formuladores de políticas e indústria. Os materiais foram produzidos pela União Internacional de Telecomunicações (UIT) e publicados no Brasil em parceria com a Anatel, a Embaixada do Reino Unido e o CGI.br.

3.2.1 Política Nacional de Educação Digital (Lei nº 14.533/2023)

Em 11 de janeiro de 2023, foi sancionada a Lei nº 14.533, que instituiu a Política Nacional de Educação Digital (PNED). O objetivo da lei é aprimorar o acesso da população brasileira aos recursos e ferramentas digitais, incentivando as boas práticas no ambiente digital. A PNED foi estruturada em quatro eixos: inclusão digital; educação digital escolar; capacitação e especialização digital; e pesquisa e desenvolvimento em Tecnologias da Informação e Comunicação (TICs).

3.2.2 Marco Civil da Internet (Lei nº 12.965/2014)

O Marco Civil da Internet (Lei nº 12.965/2014) estabeleceu, no artigo 26, o dever constitucional do Estado brasileiro de incluir a capacitação para o "uso seguro, consciente e responsável da internet como ferramenta para o exercício da cidadania, a promoção da cultura e o desenvolvimento tecnológico". A Lei Geral de Proteção de Dados (Lei n. 13.709/2018), no artigo 14, dispõe sobre o tratamento de dados pessoais de crianças e adolescentes, considerados vulneráveis.

3.2.3 Constituição Federal de 1988 e Código Civil de 2002

A Constituição Federal de 1988 e o Código Civil de 2002 consideraram o direito à privacidade como direito básico para se concretizar a personalidade humana ao adotar o paradigma da dignidade da pessoa humana como princípio e valor central do ordenamento jurídico brasileiro.

A proteção on-line das crianças e jovens faz parte da transformação social, econômica, política e tecnológica da qual o direito deve procurar respostas para cumprir seu papel de racionalizar às necessidades das sociedades. Além do nosso corpo físico, com a Internet passamos também a ter um corpo eletrônico, que deve ser protegido e respeitado da mesma forma. O direito das crianças e adolescentes à privacidade deve conter também o direito de manter o controle sobre as próprias informações, configurando a subjetividade do direito fundamental da proteção de dados.

A implantação de educação midiática como parte da formação acadêmica se torna cada vez mais necessária diante do crescimento da importância do fenômeno da vida digital entre as crianças e adolescentes. O controle parental sobre o que os filhos fazem no mundo virtual e a responsabilização das plataformas, através de legislação específica e canais de denúncia vinculados, são parte do processo de proteção da vida infantil e juvenil on-line. Mas é extremamente necessário que as crianças cresçam recebendo educação adequada sobre os perigos e benefícios da internet.

3.2.4 Resolução nº 245/2024 do Conselho Nacional dos Direitos da Criança e do Adolescente (CONANDA)

Em abril de 2024, o Conselho Nacional dos Direitos da Criança e do Adolescente (CONANDA) propôs a Resolução nº 245, que dispõe sobre os direitos das crianças e adolescentes em ambiente digital e que estabelece que empresas e Poder Público devem promover ações de sensibilização sobre os direitos e riscos que se colocam para crianças e adolescentes na sua relação com o ambiente digital, bem como benefícios e riscos associados a produtos e serviços digitais.

Os formuladores de políticas públicas deveriam assim considerar o contexto jurídico, social e político do país para moldar uma política de proteção on-line eficaz e sustentável. A estratégia deve se basear em uma visão total que incorpore governo, indústria e sociedade, respeitando os direitos fundamentais das crianças definidos pela Convenção das Nações Unidas sobre os Direitos da Criança e de outras convenções e leis internacionais importantes.O respeito e adequação às leis e estratégias nacionais existentes, semelhantes ou relacionadas, devem ser seguidas, como, por exemplo, as leis de abuso infantil ou estratégias de segurança infantil

Outro aspecto importante a ser considerado é o respeito aos direitos civis e às liberdades das crianças. O projeto deve contar com a participação ativa de todas as partes interessadas, incluindo crianças, abordando suas necessidades e responsabilidades e atendendo também às necessidades de grupos minoritários e marginalizados. A proteção on-line deve estar alinhada com planos governamentais considerando a prosperidade econômica e social e maximizando a contribuição das TICs para o desenvolvimento sustentável e a inclusão social, considerando os instrumentos de política disponíveis mais adequados e as circunstâncias específicas do país. É essencial prever como serão alocados os recursos humanos e financeiros para construir um

ambiente digital em que crianças, pais/responsáveis e partes interessadas possam confiar.

Os profissionais envolvidos no processo devem receber orientação adequada sobre como capacitar e educar as crianças para a alfabetização digital e a proteção on-line. Os formuladores de políticas e profissionais devem educar as crianças e jovens para o pleno conhecimento dos seus direitos e cuidados que devem ser tomados para a prevenção de abusos. Um dos problemas notáveis, por exemplo, é como os serviços de verificação de idade são geralmente fracos ou inexistentes, o que faz com que os riscos que as crianças enfrentam possam ser intensificados.

3.3 Sugestões técnicas para o PL 2628/22 no tema de educação digital

SUGESTÃO AO PL 2628/22
Art. 5º Será assegurado o direito à educação voltado para o uso seguro e saudável dos produtos e serviços de tecnologia da informação. §1º Cabe ao poder público, em conjunto com os fornecedores de produtos ou serviços de tecnologia da informação e a sociedade civil, promover a educação e fornecer informações sobre o uso dos produtos ou serviços de tecnologia da informação, bem como definir boas práticas para a inclusão digital de crianças e adolescentes. §2º O Estado, por seus órgãos competentes, estabelecerá diretrizes básicas de educação digital a serem incorporadas na grade curricular escolar da rede pública e privada de ensino, de acordo com a faixa etária e o grau de amadurecimento de cada série letiva, **conforme previsto na Política Nacional de Educação Digital (PNED)**; §3º A educação digital de crianças e adolescentes será estimulada e implementada mediante a criação de programas de aperfeiçoamento e atualização contínua de professores da educação infantil, básica e de nível médio; **§4º Os programas de aperfeiçoamento e atualização serão ministrados preferencialmente na modalidade virtual, com destinação preferencial de vagas a docentes da rede pública das esferas municipal e estadual);** §5º Os docentes receberão instruções claras e atualizadas para que possam transmitir aos seus alunos conteúdos sobre cuidados básicos no uso de tecnologias da informação, **seguindo os eixos previstos na PNED: inclusão digital, educação digital escolar, capacitação e especialização digital, Pesquisa e Desenvolvimento (P&D) em Tecnologias da Informação e Comunicação (TICs), que deverão conter:** I – Medidas de segurança para acesso a páginas na internet e criação de senhas de acesso;

II – Medidas de segurança e precaução no envio de dados pessoais, sobretudo mídias audiovisuais, para outros usuários por meio de mensagens de texto, áudio ou vídeo, de forma síncrona ou assíncrona;

III – Realização de pesquisas em fontes de informação online confiáveis;

IV – Uso responsável e crítico de redes sociais e demais produtos ou serviços de tecnologia da informação.

Legal Fronts *Institute*

As posições expressas neste documento resultam de pesquisa jurídica abrangente, que inclui a análise minuciosa da legislação vigente, doutrina e jurisprudência relevantes, tanto em âmbito nacional como internacional, quando aplicável. Foram consideradas as possíveis contraposições aos entendimentos propostos, a fim de apresentar uma visão ponderada sobre o tema. A aplicação destes argumentos deve ser considerada à luz das circunstâncias particulares apresentadas. Devido à subjetividade do assunto, pode haver divergências de entendimento por parte de outros agentes, incluindo autoridades competentes, que podem interpretar essas questões de maneira diferente.

Legal Fronts
Institute

www.legalfronts.org