



30574023



08250.000012/2025-61



Ministério da Justiça e Segurança Pública  
Secretaria de Direitos Digitais

**NOTA TÉCNICA Nº 4/2025/SEDIGI/MJ**

**PROCESSO ADMINISTRATIVO Nº 08250.000012/2025-61**

**INTERESSADOS: Secretaria de Direitos Digitais, Secretaria Nacional do Consumidor e Autoridade Nacional de Proteção de Dados**

**1. SUMÁRIO EXECUTIVO**

1.1. A ação de aperfeiçoamento das sistemáticas de verificação etária por parte de serviços digitais que são acessados por crianças e adolescentes no Brasil é uma das ações prioritárias da Estratégia de eliminação da violência contra crianças e adolescentes, decorrente de acordo entre o Ministério da Justiça e Segurança Pública (MJSP) e o Escritório das Nações Unidas sobre Drogas e Crime (UNODC). Nesse sentido, para dar início à sua execução, foi aberto o presente processo.

1.2. Esta Nota Técnica delinea os termos desse debate, aponta caminhos com base na discussão internacional recente, e sugere o início dessa ação com a formação de um comitê consultivo de especialistas.

**2. CONTEXTUALIZAÇÃO**

2.1. A construção de um ambiente digital mais seguro para usuários de Internet é uma das prioridades da Secretaria de Direitos Digitais do MJSP. O cenário é especialmente desafiador no Brasil, país que tende a adotar com entusiasmo inovações tecnológicas, com uma das maiores presenças de consumidores em mercados e serviços digitais.

2.2. Segundo os resultados da pesquisa TIC Kids Online Brasil, entre 2015 e 2024, houve crescimento de doze pontos percentuais de usuários de Internet de 9 a 17 anos de idade que relataram que o seu primeiro acesso aconteceu antes dos 6 anos – eram 23% em 2024, frente a 11% em 2015. Em 2015, 9% das crianças de 0 a 2 anos, 26% das de 3 a 5 anos e 41% das de 6 a 8 anos eram usuárias de Internet, conforme a declaração de moradores adultos do mesmo domicílio. Em 2024, esses indicadores alcançaram 44%, 71% e 82%, respectivamente (CETIC, 2025). Observa-se, assim, que se está diante de um cenário de uso cada vez mais precoce e intensivo da Internet na infância.

2.3. A necessidade de compatibilizar as inegáveis oportunidades de comunicação, acesso à informação, entretenimento e livre expressão, de um lado; e de outro, mitigar riscos decorrentes de ameaças emergentes, vem fazendo com que diversos países e organismos internacionais tenham uma

postura mais atenta de medidas de proteção dos usuários, especialmente os mais vulneráveis, como é inegavelmente o caso das crianças e adolescentes. Embora a questão da inclusão no ambiente digital e da conectividade significativa sejam demandas urgentes e ainda mal resolvidas especialmente no Sul Global, o acesso de crianças e adolescentes a serviços digitais e sites de Internet com conteúdos impróprios tem se dado de forma cada vez mais precoce e com escassos controles por parte de familiares e responsáveis.

2.4. Ao lado de muitas dessas aplicações e dispositivos serem desenhados com o propósito de favorecer o uso excessivo e pouco saudável, é necessário destacar os riscos a que estão expostas crianças e adolescentes presentes de forma massiva em sites, aplicativos e serviços digitais. A disseminação do anonimato, aliada à possibilidade de comunicação direta de adultos com crianças as tornam vítimas em potencial de *grooming*, sextorsão, exploração e aliciamento sexual. O uso de imagens criadas artificialmente por inteligência artificial – “*deepfakes*” – como meio para a prática de *cyberbullying* e sextorsão está em expansão exponencial. Ademais, frequentemente essas violências se conectam com violências cometidas no ambiente físico.

2.5. As estatísticas globais são estarrecedoras e servem de termômetro para um país do tamanho do Brasil: segundo [estimativas do Instiuto Childlight](#), no período de 12 meses, mais de **300 milhões** de crianças e adolescentes em todo o mundo foram afetadas pela exploração e abuso sexual infantil *online*, sendo que **1 em cada 8 crianças ou adolescentes** é submetida a conversas sexuais indesejadas, bem como é vítima de compartilhamento ou exposição não consensual a imagens e vídeos sexuais.

2.6. O NCMEC (Centro Nacional para Crianças Desaparecidas e Exploradas), que recebe denúncias de abuso e exploração sexual de plataformas norte-americanas, recebeu **32 milhões** de relatórios de denúncia só em 2023, ao passo que no mesmo ano, a rede INHOPE, que congrega canais de denúncia em dezenas de países, processou 785 mil relatórios de denúncia. Segundo a organização We Protect, em seu [relatório global de 2023](#), 45 minutos é o tempo médio para uma criança ou adolescente ser vítima de aliciamento *online* num ambiente de jogo digital – sendo que há exemplos extremos de aliciamento em 19 segundos.

2.7. A Força-Tarefa Global Virtual, uma rede de organizações policiais dedicadas ao tema, recentemente mostrou, na Conferência da Aliança Global *We Protect* de 2024, que a idade dos perpetradores de violência sexual contra crianças e adolescentes decresce ano após ano, e que a maioria deles já tem menos de 18 anos de idade, sugerindo uma tendência de piora desse cenário.

2.8. A Internet foi criada, desenvolvida e pensada por adultos, num mundo onde então a maioria dos usuários era de pessoas com mais de 18 anos. Essa, porém, não é mais a sua realidade. Hoje, segundo estimativa da UNICEF (2019), 1/3 dos usuários de Internet é de crianças ou adolescentes. A conclusão a que tantas organizações e governos tem chegado é que não há razoabilidade em continuar desenhando produtos e serviços que não levem essa realidade em conta, admitindo que produtos e serviços não seguros para crianças e adolescentes sejam posicionados no mercado e costumeiramente acessados por esse público.

2.9. Ora, o Direito do Consumidor brasileiro exige numerosos critérios de segurança sejam cumpridos e que haja padrões mínimos de segurança para a circulação no mercado de brinquedos, alimentos ou

automóveis, e no caso das tecnologias, não há motivo para ser diferente.

2.10. Cada vez mais, se debate a necessidade da "segurança por design", ou a necessidade de que serviços digitais sejam desenhados, desde a concepção, com as necessárias salvaguardas e os mecanismos de segurança para que sejam adequadamente utilizados por crianças ou adolescentes, algo que nem sempre ocorre.

2.11. Diante desse cenário, diferentes abordagens têm sido adotadas. Como um exemplo extremo, o Parlamento australiano proibiu, em novembro de 2024, que adolescentes com menos de 16 anos criem perfis em redes sociais.

2.12. No Brasil, o debate também tem sido intenso, e perpassou a aprovação da [Lei Federal nº 15.100, de 13 de janeiro de 2025](#), que criou restrições para utilização, por estudantes, de aparelhos eletrônicos portáteis pessoais nos estabelecimentos públicos e privados de ensino da educação básica, visando a inibir usos não pedagógicos das tecnologias nos ambientes educacionais. Ainda no âmbito do Poder Legislativo, muitas propostas normativas foram apreciadas por Comissões temáticas e pelo plenário das Casas legislativas, a exemplo do Projeto de Lei de proteção de crianças e adolescentes no ambiente digital (PL nº 2.628/2022), aprovado em 27/11/2024 pelo Senado Federal, que contém medidas de proteção da infância.

2.13. Por sua vez, o Supremo Tribunal Federal debate a temática da segurança e garantia de direitos online, no bojo do julgamento dos Recursos Extraordinários (RE) nº 1037396 e nº 1057258 (Temas 987 e 533 da repercussão geral, respectivamente), para julgar o regime de responsabilidade de serviços digitais por conteúdos postados por terceiros previsto no art. 19 do Marco Civil da Internet ([Lei nº 12.965, de 2014](#)).

2.14. No âmbito do Poder Executivo, entre as medidas tomadas, cita-se a criação de novas estruturas de política pública no âmbito digital, a exemplo desta Secretaria de Direitos Digitais, criada em novembro de 2023; e a adoção de políticas como a Estratégia Brasileira de Educação Midiática, além da construção, por meio do Grupo de Trabalho constituído entre 7 Ministérios e sociedade civil, do documento [“Crianças, Adolescentes e Telas: Guia de Usos sobre Dispositivos Digitais”, lançado em 11/03/2025](#). Em paralelo a isso, em 2024, o Conselho Nacional dos Direitos da Criança e do Adolescente (CONANDA) aprovou as Resoluções nº 245 e 257, que dispõem respectivamente sobre a proteção dos direitos desses sujeitos no ambiente digital e sobre a necessidade de instituição de uma política nacional dedicada a essa temática.

2.15. Muitas dos principais serviços digitais utilizados por crianças e adolescentes no Brasil deixam claro, em seus termos e políticas de uso, não serem recomendáveis para uso por menores de 13 anos. Esse peculiar corte etário, ausente de qualquer legislação brasileira, trata-se de um limite estabelecido em lei norte americana (*Children's Online Privacy Protection Rule* ou "[COPPA](#)", de 1998), Essa definição, não só está em desacordo com as faixas etárias previstas na política pública de Classificação Indicativa – 10, 12, 14, 16 e 18 anos, nas quais estão classificados esses serviços – como também não basta para evitar que tais serviços sejam acessados por esse público.

2.16. Segundo a pesquisa TIC Kids Brasil (CETIC, 2024), 52% dos usuários de Internet de 9 e 10 anos acessam o WhatsApp “várias vezes ao dia” ou “todos os dias”, percentual que é de 60% no YouTube, 26% no Instagram e 35% no Tiktok - todos serviços digitais com termos de uso com a linha de corte

de 13 anos. Ainda mais preocupante, a referida pesquisa mostra que 40% dos responsáveis por crianças e adolescentes com 12 anos ou menos permitem que elas utilizem redes sociais sem acompanhamento.

2.17. Outro desafio decorrente da negligência em aplicar a legislação pátria por parte dos serviços digitais é que a norma dos Estados Unidos restringe suas salvaguardas aos menores de 13 anos, não trazendo qualquer gradação específica para além desse corte etário. Não há, por exemplo, dispositivos específicos para usuários adolescentes entre 13 e 17 anos - assim como a lei é aplicável somente se esses de serviços digitais *tomarem conhecimento* do fato de o usuário ter menos de 13 anos. Isso desestimula a proatividade em detectar usuários crianças, uma vez que não saber a idade dos usuários se torna uma vantajosa maneira de afastar obrigações legais (5Rights Foundation, 2021, p. 9-10).

2.18. Como pretendemos apontar nesta Nota Técnica, tanto o debate internacional, quanto entidades técnicas, e a própria indústria de tecnologia têm convergido: para proteger adequadamente crianças e adolescentes *online*, uma das ferramentas indispensáveis é ter condições de verificar ou estimar a idade de cada usuário, especialmente em serviços e produtos que possam oferecer risco a esse público. Nesse sentido, a discussão sobre garantia ou verificação etária é um ponto que conecta os direitos fundamentais no ambiente digital às políticas de proteção da infância, como é o caso da política pública de classificação indicativa.

2.19. Por "garantia etária", da qual "verificação etária" é uma das espécies, entende-se o conjunto de ferramentas e métodos utilizados para evitar que crianças e adolescentes tenham contato com produtos e serviços inadequados à sua idade e que possam ser danosos (Livingstone et al., 2024, p. 721). Trata-se de um termo guarda-chuva que designa diferentes processos, sistemáticas e metodologias, que serão explorados adiante.

2.20. O princípio por trás da necessidade e da importância da garantia etária em serviços digitais é o mesmo da Convenção da Criança e do Estatuto da Criança e do Adolescente, o da **autonomia progressiva**. Nesse sentido, é sempre importante lembrar que as proteções que valem no mundo "*offline*" não podem estar ausentes dos ambientes "*online*":

"Reconhecemos que crianças e adolescentes têm necessidades e vulnerabilidades que são específicas da sua idade e fase de desenvolvimento. Uma criança não pode votar; existem faixas de pedestre fora das escolas; uma pista de corrida para crianças ou adolescentes é mais curta do que uma pista para adultos; protegemos instintivamente os olhos de uma criança se algo violento ou perturbador acontece à nossa volta. Isso não se deve às suas circunstâncias específicas, mas porque são crianças.

No mundo digital, crianças e adolescentes são rotineiramente expostas a informações, comportamentos e pressões para as quais não têm capacidade para lidar, seja sendo pressionadas a fazer amizade com adultos desconhecidos em redes sociais, seja sendo incentivadas a fazer compras em jogos, seja sendo alvo de conteúdos sexualizados ou bombardeadas com publicidade e desinformação. A normalização dos serviços concebidos por e para adultos cria um ambiente que está para além da capacidade de desenvolvimento da criança – com exigências difíceis, muitas vezes

prejudiciais e por vezes perigosas" (5Rights Foundation, 2021, p. 14).

2.21. Vale citar a esse respeito também a recente decisão da Autoridade Nacional de Proteção de Dados (ANPD) de [instaurar procedimento administrativo](#) para avaliar a adequação dos termos e políticas de uso de um dos serviços digitais mais populares no Brasil, especificamente mencionando a fragilidade da autodeclaração como modo de verificação etária (Processo nº 00261.004725/2024-81).

2.22. Nesse contexto em que o mundo e o Brasil vêm priorizando formas de mitigar os riscos a crianças e adolescentes no ambiente *online*, o Ministério da Justiça e Segurança Pública, no bojo da Estratégia de enfrentamento à violência contra crianças e adolescentes, em processo de elaboração, elegeu como uma das ações prioritárias para 2025 a elaboração dos requisitos para a adequada verificação etária dos usuários de Internet no Brasil.

### 3. BASE LEGAL

3.1. Compete a esta Secretaria de Direitos Digitais do Ministério da Justiça e Segurança Pública, nos termos do Decreto nº 11.348, de 1º de janeiro de 2023:

"Art. 42-A. À Secretaria de Direitos Digitais compete:

(...)

III - prestar apoio aos órgãos ou às entidades responsáveis por políticas públicas setoriais para o aperfeiçoamento da proteção e da promoção de direitos em ambiente digital;

(...)

V - articular ações do Ministério com órgãos e entidades, públicas e privadas, e organismos internacionais, para a proteção dos direitos e das garantias constitucionais em ambiente digital, em cooperação com os órgãos ou as entidades com competências nas políticas públicas objeto da ação;"

3.2. Nos termos da Constituição da República, da Convenção da Criança, adotada em 1990 pelo Brasil, e do Estatuto da Criança e do Adolescente, todas as políticas públicas devem se pautar pelos princípios da **proteção integral**, da **absoluta prioridade** e do **superior interesse** da criança:

Constituição, art. 227

É dever **da família, da sociedade e do Estado** assegurar à criança, ao adolescente e ao jovem, **com absoluta prioridade**, o direito à vida, à saúde, à alimentação, à educação, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária, além de colocá-los **a salvo de toda forma de**

**negligência, discriminação, exploração, violência, crueldade e opressão.**

Convenção da Criança, internalizada pelo [Decreto nº 99.710, de 1990](#)

Artigo 3º

Todas as ações relativas às crianças, levadas a efeito por instituições públicas ou privadas de bem estar social, tribunais, autoridades administrativas ou órgãos legislativos, devem considerar, primordialmente, o **interesse maior** da criança.

Estatuto da Criança e do Adolescente ([Lei nº 8.069, de 1990](#))

Art. 3º A criança e o adolescente gozam de todos os direitos fundamentais inerentes à pessoa humana, sem prejuízo da **proteção integral** de que trata esta Lei, assegurando-se-lhes, por lei ou por outros meios, todas as oportunidades e facilidades, a fim de lhes facultar o desenvolvimento físico, mental, moral, espiritual e social, em condições de liberdade e de dignidade.

Art. 4º É dever da família, da comunidade, da sociedade em geral e do poder público assegurar, **com absoluta prioridade**, a efetivação dos direitos referentes à vida, à saúde, à alimentação, à educação, ao esporte, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária.

3.3. Além disso, o dispositivo constitucional referido acima – art. 227 – traz a figura da **responsabilidade compartilhada**, isto é, do dever que recai sobre Estado, sociedade, famílias e empresas de proteção das crianças e adolescentes, princípio que também figura no Estatuto da Criança e do Adolescente (Lei nº 8.069, de 1990):

"Art. 18. É dever **de todos** velar pela dignidade da criança e do adolescente, pondo-os a salvo de qualquer tratamento desumano, violento, aterrorizante, vexatório ou constrangedor.

Art. 70. É dever **de todos** prevenir a ocorrência de ameaça ou violação dos direitos da criança e do adolescente".

3.4. Por sua vez, o princípio da **autonomia progressiva** ("evolving capacities"), que leva em conta a condição peculiar de pessoa em desenvolvimento de crianças e adolescentes, é expresso tanto pela Convenção da Criança, quanto pelo Estatuto da Criança e do Adolescente:

Convenção da Criança (Decreto nº 99.710, de 1990)

"Artigo 5

Os Estados Partes respeitarão as responsabilidades, os direitos e os deveres dos pais ou, onde for o caso, dos membros da família ampliada ou da comunidade, conforme determinem os costumes locais, dos tutores ou de outras pessoas legalmente responsáveis, de proporcionar à criança instrução e orientação adequadas e acordes com a **evolução de sua capacidade** no exercício dos direitos reconhecidos na presente convenção."

#### "Artigo 31

Os Estados Partes reconhecem o direito da criança ao descanso e ao lazer, ao divertimento e às **atividades recreativas próprias da idade**, bem como à livre participação na vida cultural e artística."

#### "Estatuto da Criança e do Adolescente (Lei nº 8.069, de 1990)

Art. 71. A criança e o adolescente têm direito a informação, cultura, lazer, esportes, diversões, espetáculos e **produtos e serviços que respeitem sua condição peculiar de pessoa em desenvolvimento.**"

3.5. Por fim, a Convenção da Criança e o Estatuto da Criança e do Adolescente consagram o direito ao respeito e o dever do Estado de proteger crianças e adolescentes de toda forma de violência:

#### Convenção da Criança (Decreto nº 99.710, de 1990)

##### "Artigo 19

1. Os Estados Partes adotarão todas as medidas legislativas, administrativas, sociais e educacionais apropriadas **para proteger a criança contra todas as formas de violência física ou mental**, abuso ou tratamento negligente, maus tratos ou exploração, inclusive abuso sexual, enquanto a criança estiver sob a custódia dos pais, do representante legal ou de qualquer outra pessoa responsável por ela."

#### Estatuto da Criança e do Adolescente (Lei nº 8.069, de 1990)

"Art. 5º Nenhuma criança ou adolescente será objeto de qualquer forma de negligência, discriminação, exploração, violência, crueldade e opressão, punido na forma da lei qualquer atentado, por ação ou omissão, aos seus direitos fundamentais."

"Art. 17. O **direito ao respeito** consiste na inviolabilidade da integridade física, psíquica e moral da criança e do adolescente, abrangendo a preservação da imagem, da identidade, da autonomia, dos valores, ideias e crenças, dos espaços e objetos pessoais."

3.6. Especificamente sobre o modo de implementação desses direitos, Comitê dos Direitos da Criança da ONU, em seu Comentário geral nº 25

(2021) sobre os Direitos das Crianças em relação ao ambiente digital, elenca como Medidas especiais de proteção contra exploração econômica, sexual e outras formas de exploração:

"114. Estados Partes devem assegurar a existência de mecanismos de fiscalização adequados e apoiar crianças, mães, pais e cuidadores no acesso às proteções aplicáveis. Eles devem legislar para assegurar que as crianças sejam protegidas de bens prejudiciais, como armas ou drogas, ou serviços, como jogos de azar. Sistemas robustos de verificação de idade devem ser utilizados para impedir que as crianças adquiram acesso a produtos e serviços que são ilegais para elas possuírem ou usarem. Esses sistemas devem ser consistentes com as exigências de proteção de dados e salvaguardas."

3.7. Ainda nos termos da legislação brasileira, o Código de Defesa do Consumidor ([Lei nº 8.078, de 1990](#)) traz determinações expressas de proteção da criança ou do adolescente num contexto de consumo, especialmente em relação à publicidade abusiva:

Código de Defesa do Consumidor (Lei nº 8.078, de 1990)

"Art. 39. É vedado ao fornecedor de produtos ou serviços, dentre outras práticas abusivas:

(...)

IV - prevalecer-se da fraqueza ou ignorância do consumidor, tendo em vista sua **idade**, saúde, conhecimento ou condição social, para impingir-lhe seus produtos ou serviços;

(...)

Art. 36. A publicidade deve ser veiculada de tal forma que o consumidor, fácil e imediatamente, a identifique como tal.

(...)

§ 2º É abusiva, dentre outras a publicidade discriminatória de qualquer natureza, a que incite à violência, explore o medo ou a superstição, **se aproveite da deficiência de julgamento e experiência da criança**, desrespeite valores ambientais, ou que seja capaz de induzir o consumidor a se comportar de forma prejudicial ou perigosa à sua saúde ou segurança".

3.8. Para tornar viável a implementação dessa previsão, em se tratando de serviços digitais, a verificação etária surge como uma das possibilidades para tornar possível tal controle. Isso não escapou às normas sobre o tema já editadas num contexto de elevada presença de crianças e adolescentes em ambientes digitais. O Conselho Nacional dos Direitos das Crianças e dos Adolescentes recentemente normatizou essa questão, por meio da Resolução CONANDA nº 245, de 2024, que assim estabelece:

"Art. 17. As empresas provedoras de produtos e serviços digitais utilizados por crianças e adolescentes, em funcionamento no Brasil, inclusive aquelas sediadas no exterior, são responsáveis pela



implementação e garantia dos direitos deste público, nos ambientes digitais por elas produzidos e regulados.

(...)

§3º As empresas provedoras devem criar e aprimorar mecanismos que previnam o uso de serviços e ambientes digitais por crianças e adolescentes sempre que seus serviços não sejam adequados e seguros a esse público.

(...)

Art. 19. Mecanismos efetivos de verificação etária nos serviços e ambientes digitais acessíveis a crianças e adolescentes devem ser disponibilizados para impedir que crianças e adolescentes tenham acesso a plataformas, produtos, serviços e conteúdos ilícitos ou incompatíveis com sua idade.

Parágrafo único. Os dados de crianças e adolescentes obtidos pelos mecanismos e sistemas de verificação etária não poderão ser utilizados para quaisquer outros fins, a não ser a verificação etária".

3.9. Ao prever a Política Nacional de Proteção dos Direitos da Criança e do Adolescente no Ambiente Digital, o CONANDA, por meio da Resolução nº 257, de 2024, tratou a verificação etária como um de seus princípios:

"Art. 3º A PNPDCAAD deverá considerar os seguintes princípios:

(...)

X - A garantia dos direitos das crianças e adolescentes desde o design de produtos e serviços em ambientes digitais, prevenindo o uso problemático ou excessivo, viabilizando a verificação etária para acesso a aplicações adequadas à idade, seguindo o princípio da autonomia progressiva, a partir de uma análise de riscos sistêmicos;" (grifos nossos)

3.10. Por fim, vale ressaltar que a Lei Geral de Proteção de Dados Pessoais – LGPD ([Lei nº 13.709, de 2018](#)) traz dispositivos específicos para o tratamento de dados de crianças e adolescentes. Torna-se evidente que para sua plena eficácia, em se tratando do tratamento de dados no ambiente digital, a Lei demanda que se estabeleça que o usuário de fato é criança ou adolescente, algo que depende da implantação de alguma política ou metodologia de garantia etária:

### **"Seção III**

#### **Do Tratamento de Dados Pessoais de Crianças e de Adolescentes**

Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.

§ 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

§ 2º No tratamento de dados de que trata o § 1º deste artigo, os

controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei.

§ 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo.

§ 4º Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.

§ 5º O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis.

§ 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança."

3.11. Tomando-se em conjunto todas as normas mencionadas nesta Seção, conclui-se que tratados internacionais e diversos marcos normativos vigentes no direito brasileiro já fundamentam a necessidade de se implementar uma política pública de garantia etária em serviços digitais acessados por crianças e adolescentes, como parte de uma política de proteção de direitos desses sujeitos.

#### 4. VERIFICAÇÃO ETÁRIA: PANORAMA INTERNACIONAL

4.1. A exigência de medidas de verificação etária também vem se generalizando na legislação internacional como forma de proteção dos direitos de crianças e adolescentes.

4.2. A [Lei de Serviços Digitais](#) aprovada pela União Europeia em 2022 trouxe como medida geral de "atenuação de riscos", em seu art. 35:

"Os fornecedores de plataformas em linha de muito grande dimensão e de motores de pesquisa em linha de muito grande dimensão adotam medidas de atenuação razoáveis, proporcionadas e eficazes, adaptadas aos riscos sistêmicos específicos identificados nos termos do artigo 34, tendo especialmente em conta o impacto de tais medidas nos direitos fundamentais. Estas medidas podem incluir, quando aplicável:

j) A adoção de medidas específicas para proteger os

direitos das crianças, **nomeadamente instrumentos de verificação da idade** e de controlo parental, instrumentos destinados a ajudar os menores a sinalizar abusos ou a obter apoio, conforme adequado" (grifos nossos)

4.3. A União Europeia mantém a estratégia "[Better Internet for Kids](#)", voltada para um ambiente *online* mais seguro para crianças e adolescentes. Além disso, a Comissão Europeia atualmente financia o [projeto euCONSENT](#), organização da sociedade civil que está testando em 3 países, padrões de verificação etária, que poderão eventualmente ser generalizados. O desafio do projeto é mostrar que é possível uma solução de verificação etária aplicável a múltiplos serviços digitais, de fácil uso, e que ao mesmo tempo preserve a privacidade ou anonimato dos usuários de Internet.

4.4. No Reino Unido, o [Online Safety Act](#) trouxe previsões específicas sobre verificação etária em seu art. 12, voltado para deveres de proteção de crianças e adolescentes:

"(3) Dever de operar um serviço utilizando sistemas e processos proporcionais, projetados para:

(a) impedir que crianças e adolescentes de qualquer idade tenham acesso, por meio do serviço, a conteúdo de prioridade primária que lhes seja prejudicial;

(b) proteger crianças e adolescentes em faixas etárias consideradas em risco de danos contra outros conteúdos prejudiciais para elas (ou contra um tipo específico desse conteúdo), impedindo que tenham acesso a eles por meio do serviço.

(4) O dever estabelecido na subseção (3)(a) **exige que um provedor utilize verificação de idade** ou estimativa de idade (ou ambas) para impedir que crianças e adolescentes de qualquer idade tenham acesso a conteúdo de prioridade primária prejudicial a elas que o provedor identificar no serviço.

(5) Esse requisito se aplica a um provedor em relação a um tipo específico de conteúdo de prioridade primária prejudicial a crianças e adolescentes em todos os casos, exceto quando:

(a) um termo de serviço indicar (independentemente das palavras utilizadas) que a presença desse tipo de conteúdo de prioridade primária prejudicial a crianças e adolescentes é proibida no serviço, e

(b) essa política se aplicar a todos os usuários do serviço.

(6) Se um provedor for obrigado, nos termos da subseção (4), a utilizar verificação de idade ou estimativa de idade para cumprir o dever estabelecido na subseção (3)(a), a verificação de idade ou a estimativa de idade deve ser de tal natureza, e utilizada de tal forma, que seja altamente eficaz em determinar corretamente se um usuário específico é ou não uma criança ou adolescente". (tradução livre, grifos nossos)

4.5. Naquele país, diretrizes e balizas referentes à verificação etária são emanadas tanto da entidade reguladora da proteção de dados, o ICO (*Information Commissioner's Office*), como também do regulador encarregado de serviços de comunicação em geral e da implementação da Lei de Segurança Online, o Ofcom (*Office of Communications*). O Reino Unido elegeu como foco da verificação etária os sites pornográficos, numa visão de que por oferecerem o maior risco potencial, a implementação da verificação etária deveria se iniciar por esse setor (OFCOM, 2024).

4.6. Na Índia, o [Digital Personal Data Protection Act \(DPDP\)](#), de 2023, em seu art. 9º, proíbe a coleta de dados de crianças e adolescentes sem autorização do responsável, assim como o monitoramento comportamental ou o direcionamento de publicidade a esse público. Para tanto, algum nível de verificação etária se faz necessário. Porém, como naquele país a identidade digital (Aadhaar) alcança boa parte da população, sendo inclusive publicizada como uma das bases de seu projeto de infraestrutura pública digital, os [debates mais recentes](#) em torno da operacionalização da garantia etária giram em torno do uso de tokens etários conforme a metodologia de "provas de conhecimento zero" - ou uma forma de transmitir a informação sobre a idade do usuário entre duas partes sem necessariamente fornecer outros dados pessoais.

4.7. Na Austrália, conforme já mencionado, a [Online Safety Act](#) de 2021 designou o eSafety como a entidade responsável pela implementação das medidas de segurança digital. A Lei, em seu art. 63C, restringiu o acesso a sites com conteúdos de terceiros, e nos quais um usuário pudesse contatar diretamente outro, a exemplo das redes sociais. Em novembro de 2024, a lei foi emendada para definir essa idade mínima como sendo de 16 anos, previsão essa que demandará até dezembro de 2025 um ambicioso plano de implementação.

4.8. Como decorrência dessa convergência em torno da operacionalização da garantia etária, a International Standards Organization (ISO) está desenvolvendo a [norma técnica de padronização ISO/IEC 27566](#), especificamente voltada para sistemas de verificação etária.

## 5. GARANTIA ETÁRIA COMO MECANISMO DE MITIGAÇÃO DE RISCOS

5.1. A garantia etária não é uma panaceia para a eliminação de todos os riscos que crianças e adolescentes encontram online, mas pode ser um componente importante para mitigá-los, ou mesmo elevar a idade média na qual esse público entra em contato com conteúdos inadequados para sua fase de desenvolvimento (eSafety, 2023, p. 7). Quanto mais robustos os sistemas de garantia etária em ambientes *online*, onde esses riscos estão presentes, espera-se que menor seja a incidência de danos a crianças e adolescentes.

5.2. Mecanismos de verificação etária podem e frequentemente são associados aos assim chamados "controles parentais", ou a ferramentas de mediação parental. Sendo assim, é possível que o acesso a um determinado serviço - por exemplo, a um aplicativo cuja Classificação Indicativa seja de 14 anos - não seja simplesmente proibido, mas possa se dar mediante a autorização de mães, pais ou responsáveis. Trata-se, nesse caso, de uma forma inclusive de empoderamento das famílias, e não uma mera restrição de

acesso. Cada vez mais, reconhece-se a importância dos controles parentais oferecidos pela indústria, mas também o fato de que eles precisam ser reforçados e utilizados de forma combinada com ferramentas de garantia etária (eSafety, 2023, p. 11).

5.3. A tipologia para os riscos *online* desenvolvida por Sonia Livingstone, aceita internacionalmente, adota os chamados 4Cs, resumida no quadro da sequência (Livingstone & Stoilova, 2021; tradução e adaptação do CETIC.br/NIC.br e SaferNet) para detalhar como pode ocorrer a exposição a riscos:

- **conteúdo:** riscos decorrentes da relação com informações prejudiciais;
- **contato:** emergem da interação com atores de risco que integram a mesma rede;
- **conduta:** condutas potencialmente danosas que podem ser observadas ou experimentadas pela criança ou adolescente;
- **contrato:** riscos que envolvem a exploração dos usuários por uma relação contratual, e que costumam ser desconhecidas destes.

| Classificação de Riscos on-line CO:RE |  |  |  |  |
|---------------------------------------|--|--|--|--|
| Tipos de riscos                       | CONTEÚDO<br>criança / adolescente se envolve ou é exposto a conteúdos potencialmente danosos | CONTATO<br>criança / adolescente vivencia ou é alvo de contatos potencialmente danosos de ou por adultos | CONDUTA<br>criança / adolescente testemunha, participa ou é vítima de condutas potencialmente danosas entre pares  | CONTRATO<br>criança / adolescente é parte ou é explorado por um contrato potencialmente danoso                         |
| Agressivo                             | Violento, sangrento, explícito, racista, odioso ou informação e comunicação extremista       | Assédio, perseguição ( <i>stalking</i> ), ataques de ódio, vigilância indesejada ou excessiva            | <i>Cyberbullying</i> , comunicação ou atividade de ódio ou hostil entre pares, como trollagem, exclusão, ato com o intuito de causar constrangimento público | Roubo de identidade, fraude, <i>phishing</i> , golpe, invasão e roubo de dados, chantagem, riscos envolvendo segurança |
| Sexual                                | Pornografia (danosa ou ilegal) cultura da sexualização, normas opressivas para               | Assédio sexual, aliciamento sexual, sextorsão, produção ou compartilhamento de imagens de abuso sexual   | Assédio sexual, troca não consensual de mensagens sexuais, pressões sexuais adversas   | Tráfico para fins de exploração sexual, transmissão de conteúdo pago de abuso sexual infantil                          |

|              |   |  |  |   |
|--------------|---|--|--|---|
|              | a imagem corporal   | infantil   |  |   |
| Valores      | Informação incorreta/desinformação, publicidade imprópria para idade ou conteúdo gerado pelos usuários  | Persuasão ou manipulação ideológica, radicalização e recrutamento extremista | Comunidades de usuários potencialmente danosas, como automutilação, antivacinação, pressões entre pares adversas | Jogos de azar, filtro bolha (filtro de seleção de conteúdos por semelhanças), microsegmentação, padrões ocultos de design modelando a persuasão ou a compra |
| Transversais | Violações de privacidade (interpessoal, institucional e comercial)<br>Riscos para a saúde física e mental (como sedentarismo, estilo de vida, uso excessivo das telas, isolamento, ansiedade)<br>Desigualdades e discriminação (inclusão/exclusão, exploração de vulnerabilidades, vies dos algoritmos/análise preditiva) |  |  |   |

5.4. A tabela acima exemplifica os múltiplos riscos a que crianças e adolescentes estão expostos. Além disso, é importante observar que alguns riscos se apresentam como transversais, ou seja, atravessam as várias experiências conectadas. Diante desse cenário complexo, em que é preciso assegurar tanto a participação e a livre expressão de crianças e adolescentes, sem descuidar da sua proteção e da exposição a conteúdos adequados à sua idade, uma abordagem holística é recomendável (eSafety, 2023, p. 11). Nesse sentido, medidas como o desenho seguro de serviços digitais desde a concepção ("*safety by design*"), a adoção de controles parentais pelos responsáveis, configurações mais protetivas de coleta de dados e que previnam o uso excessivo ou problemático (OECD, 2022), mecanismos efetivos de denúncia de violações, promoção de ações e políticas de Educação Midiática e o uso de ferramentas de verificação etária no acesso aos ambientes digitais podem todos se combinar para tornar a experiência desses sujeitos mais segura.

## 6. VERIFICAÇÃO ETÁRIA: LIMITAÇÕES E DESAFIOS

6.1. No mundo analógico, quando se cumprem dispositivos da legislação de proteção de criança e adolescente referentes à limitação de acesso a determinados produtos ou conteúdos, a exemplo da necessária autorização para ingresso em locais de diversões e espetáculos públicos (art. 75 do ECA), a vedação do acesso a casas de jogos (art. 80 do ECA) ou a proibição de hospedagem em hotel ou motel sem autorização ou presença dos pais e responsáveis (art. 82 do ECA), o controle é presencial e face a face. Na esfera digital, porém, não é aparente ao fornecedor de serviços digitais qual a idade do usuário na outra ponta. Salvo exceções, o acesso a sites, aplicativos e jogos digitais não exige comprovação prévia de idade. Como o anonimato sempre foi regra no desenvolvimento da Internet, só nos últimos anos que se passou a debater formas de levar em conta a idade de usuários

de serviços digitais.

6.2. Como já mencionado acima, costuma-se utilizar o termo guarda-chuva "garantia etária" ("*age assurance*") para o conjunto de ferramentas e metodologias visando a assegurar que usuários crianças e adolescentes não acessem conteúdo inadequado ou potencialmente danoso. Esse gênero pode ser dividido em:

- Verificação etária – permite a verificar a idade exata do usuário;
- Estimativa ou inferência etária – estima a idade aproximada do usuário, às vezes com o uso de tecnologias e/ou de perfilamento do usuário.

6.3. Na definição técnica da norma ISO/IEC WD 27566-1, "*Garantia de idade é o processo de estabelecimento, determinação e/ou confirmação de um atributo de garantia de idade, incluindo-se aí a verificação de idade, estimativa de idade e inferência de idade*".

6.4. A verificação etária, assim, em termos gerais, **não se confunde com a verificação de identidade**, que exige a identificação inequívoca de um sujeito específico, referindo-se, em vez disso, à apuração da idade de um sujeito, não necessariamente identificado.

6.5. A verificação ou estimativa etária podem ser realizadas pelo próprio provedor de serviços digitais, ou por terceiros confiáveis. Há hoje no mercado todo um ecossistema de empresas que oferecem esse serviço e são contratadas pelos provedores, a exemplo dos serviços digitais de redes sociais.

6.6. Em termos principiológicos, toda metodologia de verificação ou estimativa etária deveria ter em vista alguns valores (5Rights Foundation, 2021, p. 8):

- Preservação da privacidade dos usuários;
- Proporcionalidade ao risco ou finalidade;
- Facilidade no uso, especialmente por crianças e adolescentes;
- Possibilidade de aperfeiçoamento das experiências *online* de crianças e adolescentes, e não apenas restrição de acesso ao ambiente digital.

6.7. Nesse sentido, um dos maiores focos de resistência à implementação de soluções de verificação etária refere-se ao direito à **privacidade**, e o receio de que elas representem uma coleta adicional de dados inclusive dos próprios adultos, que precisariam fazer prova da idade para seus usos rotineiros de serviços digitais. Além disso, várias das soluções encontram a limitação de depender do fornecimento de dados pessoais por crianças e adolescentes, o que contraria o espírito da minimização da coleta de dados – especialmente desse público – contida na Lei Geral de Proteção de Dados Pessoais. Sendo assim, para que haja adesão, é essencial que soluções de verificação etária respeitem o direito à privacidade - e que serviços digitais que hospedam conteúdos inadequados a crianças e adolescentes não sejam obrigados a armazenar dados pessoais dos adultos que os acessam (Arcom, 2024, p 15-16).

6.8. Em 11/2/2025, o European Data Protection Board [publicou uma manifestação](#) sobre verificação etária na qual alertou o seguinte: para que a

garantia etária seja feita de forma respeitosa ao direito à privacidade, devem-se observar princípios como proporcionalidade ao risco, minimização da coleta de dados, transparência e segurança de dados.

6.9. O princípio da **proporcionalidade** é crucial nesse debate. Há um entendimento disseminado (Livingstone, 2024, p. 725; 5Rights Foundation, 2021, p. 19) de que aqueles serviços digitais que ofereçam maior risco - por exemplo, conteúdo sexual explícito, de violência extrema, ou publicidade de álcool, jogos e apostas, *vapes* e outros produtos ilegais para crianças e adolescentes - precisam adotar um maior rigor nas medidas de verificação etária. Nesse sentido, seriam exemplos aplicativos de bets, de encontros amorosos ou de acesso a profissionais do sexo. Por sua vez, um portal de jornalismo, um aplicativo de acesso a serviços públicos ou uma enciclopédia virtual de conhecimentos gerais, em princípio, não seriam o foco dessas medidas.

6.10. Há, no entanto, uma série de casos limítrofes em que essa avaliação de riscos e sua proporcionalidade às medidas de verificação etária se faz de forma mais complexa. Qual o nível dessa exigência, por exemplo, num aplicativo de entregas por meio do qual se possa adquirir bebida alcoólica; num serviço de transmissão de conteúdos audiovisuais ou jogo eletrônico com conteúdos de violência; ou de uma rede social em que adultos possam enviar mensagens diretas a adolescentes? Um serviço digital que traga a possibilidade de compra online deveria promover mecanismos etária para comprovar que o usuário tem a idade para a capacidade civil (ou autorização dos responsáveis) firmar para contratos? São questões como essas que vêm sendo debatidas por órgãos reguladores e formuladores de políticas públicas nos últimos anos.

6.11. Outro aspecto que merece consideração é o de que, diante dos princípios da provisão, participação e proteção previstos na Convenção da Criança, e em respeito ao **direito à liberdade de expressão e de pensamento**, de associação e o direito à privacidade (previstos na Constituição e nos arts. 13 a 16 da Convenção da Criança), as ferramentas de verificação etária não signifiquem privar esses sujeitos de direitos do acesso a informações, serviços, possibilidades de expressão e interação compatíveis com sua autonomia progressiva, e mesmo o acesso a canais de denúncia de violações de direitos disponíveis online. Nesse sentido, a verificação etária idealmente seria uma forma de aperfeiçoar as experiências digitais de crianças e adolescentes, e não de limitá-las indevidamente - dado que hoje a presença no ambiente digital é uma imposição da realidade (Livingstone et al., 2024).

6.12. A implementação dessas medidas também tangencia uma discussão sobre a **responsabilidade** pela verificação etária (AEPD, 2024, p. 15-17). A quem cabe a obrigação de verificar a idade? Em que momento esta deve ser efetuada? No acesso ao dispositivo digital? No ato de se realizar o *download* de uma aplicação numa loja de aplicativos? Ou ao se acessar cada serviço, jogo, site ou aplicativo específico? Longe de ser uma tecnicidade, essa questão pode envolver obrigações e investimentos em diferentes pontos da cadeia de serviços digitais.

6.13. Além disso, um ponto de alta relevância se refere ao **momento** em que a verificação etária é realizada (AEPD, 2024, p. 15-17). Ou seja, deveria ser feita uma só vez, ao se criar um perfil? Ou a cada acesso? Quanto mais se exige cumprir etapas, maior a segurança, mas inferior a experiência ou usabilidade do serviço digital - diz-se que "maior a fricção" para o usuário. Ao mesmo tempo, quando se tem o uso compartilhado de dispositivos por mais



de uma pessoa na mesma família, como um adulto responsável e a criança ou adolescente, talvez seja necessário que essa comprovação se faça com maior frequência (Arcom, 2024, p. 7).

6.14. Os métodos ou soluções de verificação ou estimativa etária podem ser usados separadamente ou de forma combinada, cada qual com suas forças e limitações. A tabela abaixo exemplifica alguns deles:

| Solução de Estimação ou Verificação etária   | Requisitos  | Vantagens  | Desafios  |
|--|---|--|---|
| Autodeclaração                               | Preenchimento da data de nascimento, sem fornecimento de nenhum outro dado adicional                            | Simplicidade, rapidez e mínima fricção para o usuário. Pode ser adequado para serviços digitais de mínimo risco.               | Não é considerado método de verificação, mas apenas um ponto de partida. Posiciona a responsabilidade pela garantia etária na própria criança ou adolescente. Pode ser facilmente burlado, não devendo ser utilizado em aplicações com maior risco.                             |
| Análise biométrica por reconhecimento facial | Fornecimento de imagem da face, com o uso de tecnologia de estimativa etária                                    | Facilidade de uso ou baixa fricção para o usuário, que se limita a tirar uma foto da própria face.                             | É um método de estimação (idade aproximada) e não de verificação. Pode trazer riscos como vieses raciais, de privacidade, de proteção de dados pessoais sensíveis e de segurança de dados, ao gerar uma base de dados centralizada.   |
| Análise comportamental                       | Solução de inteligência artificial que identifica padrões de uso do serviço digital para estimar idade provável | Baixa fricção para o usuário. Não exige o fornecimento de dados de identificação. É mais precisa quanto mais se usa o serviço. | É um método de estimação (idade aproximada) e não de verificação. É maximalista na coleta de dados por exigir perfilamento. Exige transparência – usuários devem ser informados de que seus padrões comportamentais estão sendo analisados. Dados não devem ser utilizados para |

|                          |   |  |  |
|--------------------------|---|--|--|
|                          |   |  | outras finalidades que não estimação etária, nem serem fornecidos a terceiros para outros fins. Traz riscos ampliados de privacidade, proteção de dados sensíveis e segurança de dados.  |
| Teste de capacidade      | Exige a solução de algum problema ou execução de alguma tarefa de habilidade que é solucionável a partir de certa idade                   | Não exige o fornecimento de dados de identificação, minimizando a coleta de dados pessoais.  | É um método de estimação (idade aproximada) e não de verificação, não servindo para determinar com precisão, por exemplo, a maioridade. Crianças e adolescentes de idades semelhantes podem ter habilidades distintas. Pode ser uma barreira à acessibilidade de crianças ou adolescentes com deficiência. |
| "Token" etário           | Credencial fornecida por terceiro confiável que atesta a idade do usuário - via OTP (One-Time Password ou senha descartável), por exemplo | Pode transmitir ao serviço apenas a informação essencial sobre a idade do usuário, sem necessidade de demais dados pessoais. Não exige a manutenção de uma base de dados centralizada com os dados pessoais dos usuários, minimizando o risco de vazamentos. | Necessário deixar bem claros os termos do serviço. Dados não devem ser utilizados para outras finalidades que não verificação etária, nem fornecidos a terceiros.  |
| Uso de cartão de crédito | Submissão de número válido de cartão de crédito,  | De fácil aplicação e compreensão,  | Depende do acesso a serviços bancários e da titularidade de cartão de crédito;   |

|                                     |  |   |   |
|-------------------------------------|--|---|---|
|                                     | eventualmente com a exigência de pagamento em pequeno valor para confirmação   | pois usuários estão acostumados a fornecer esses dados ao efetuarem compras <i>online</i> .   | pode deixar de fora também pessoas inadimplentes, excluindo, assim, porção considerável dos usuários de serviços digitais. Não resolve a questão de faixas etárias específicas (ex: distinção entre crianças e adolescentes).   |
| Fornecimento de identificação civil | Envio de cópia ou imagem de documento oficial, como carteira de identidade, passaporte, etc., com o uso de tecnologia OCR e batimento da fotografia; ou batimento com identidade digital | Baseia-se não somente na verificação etária, mas na verificação <b>de identidade</b> .  | Pode representar um impacto desproporcional para usuários adultos do serviço. Necessidade de fornecimento de dados pessoais sensíveis (para além da idade) ao provedor de serviços digitais, que passa a gerir base de dados centralizada, com riscos à privacidade e de segurança de dados; além disso, a subdocumentação é uma questão, especialmente entre crianças e adolescentes, que não necessariamente possuem identificação civil. |
| Emprego de cartão SIM               | Uso de cartão SIM no smartphone que contenha dado sobre a idade do usuário, para trava de aplicativos não adequados à idade  | Mínima fricção para o usuário, já que as restrições de acesso ficam embutidas no próprio dispositivo digital. Permite proteções adicionais (ex: restrição a chamadas por números desconhecidos) | Exige o fornecimento dos dados quando da aquisição do cartão SIM, necessitando do fornecimento de dados nesse momento. Não aplicável em acessos que não sejam efetuados via <i>smartphone</i> .   |

Fonte: elaboração própria  
(referências consultadas ao final)

6.15. Vale ressaltar que mesmo aqueles métodos que parecem ser mais exigentes - como a necessidade de fornecer documento de identificação ou cartão de crédito - podem em alguma medida ser burlados, com o uso de documentos dos pais ou responsáveis pelas crianças e adolescentes. Não se considera, de toda forma, que haja uma solução infalível para a verificação etária. Por sua vez, métodos que se baseiam na criação de bases de dados biográficos e biométricos sempre trazem o risco da criação de bases de dados centralizadas, que impõem riscos à segurança de dados, como os de ciberataques e vazamentos (European Commission, 2024, p. 41).

6.16. Além disso, todos os métodos que empregam a coleta de dados pessoais têm como desafio respeitar o princípio da finalidade - isto é, não utilizar os dados coletados para fins de verificação etária para outros fins, tais como análise de emoções ou direcionamento de publicidade. Ademais, e ainda seguindo os princípios da LGPD, esses dados tampouco devem ser fornecidos a terceiros para outros fins.

6.17. Verifica-se, assim, que todas as metodologias têm limitações e nem sempre consideram a proporcionalidade ao risco. Os documentos consultados tendem a salientar que um caminho promissor é a combinação de diferentes metodologias, conforme o caso (5Rights Foundation, 2021, p. 7).

6.18. Uma solução particularmente interessante para esses percalços é a adoção de "age tokens" (credenciais etárias), conforme a tabela acima. A ideia é que o fornecimento de dados referentes à idade do usuário não se confunda nem com sua plena identificação, nem redunde no fornecimento excessivo de dados pessoais para os serviços digitais. Nesse sentido, a proposta do documento da *European Data Protection Board*, citado acima, é a seguinte:

"Consequentemente, o EDPB recomenda que, com base no estado da arte em termos de garantia de idade no momento em que este documento foi elaborado, seja dada a devida atenção às tecnologias e arquiteturas que favorecem a retenção dos dados pelos usuários e o processamento local seguro (baseado em dispositivos), permitindo propriedades como a não-lincagem (do ponto de vista de diferentes partes e mesmo no caso de vazamentos de dados) e a divulgação seletiva de dados pessoais sob o controle do titular dos dados. Além disso, a utilização de abordagens como as que dependem da emissão em lote de credenciais de utilização única ou de protocolos criptográficos, **como provas de conhecimento zero**, devem ser disponibilizadas aos titulares dos dados nos casos em que a garantia de idade possa envolver riscos elevados para a sua privacidade". (tradução livre)

6.19. Um dos maiores desafios das ferramentas de verificação etária disponíveis, assim como as ferramentas de controle parental oferecidas pelas empresas, é sua **adoção efetiva por famílias**. Segundo a última pesquisa TIC Kids Brasil (CETIC, 2024), apenas cerca de 1/3 dos responsáveis por crianças e adolescentes entre 9 e 17 anos usa a maioria dos controles parentais disponibilizados pela indústria.

6.20. Por fim, é essencial que o encaminhamento de propostas e políticas referentes à verificação etária levem em conta os **padrões de normalização internacional**. A adoção de soluções já consagradas em outros países e já disponíveis no mercado tende a facilitar a adesão do setor privado, ao passo que a adoção de parâmetros que fujam desses consensos tende a dificultar a generalização dessas ferramentas.

6.21. A recomendação da Organização para a Cooperação e Desenvolvimento Econômico é a de que a busca de soluções seja feita via cooperação internacional (OECD, 2024, p. 32). Nesse sentido, no *Communiqué* final da 1ª Cúpula Global de Padrões de Verificação Etária, organizada em abril de 2024 em Manchester, Reino Unido, pelas empresas que oferecem esses serviços ao mercado, constam como consensos do setor:

A garantia etária pode ser feita.

A garantia etária pode ser implantada, com os processos certos para os casos de uso certos, de maneira que preserve a privacidade, seja segura, eficaz e eficiente.

A garantia etária pode ser uma ferramenta valiosa entre uma série de medidas implementadas para proteger as crianças no ambiente digital.

Isso seria facilitado pelo estabelecimento de Padrões Internacionais, implementados e respeitados pelos prestadores de serviços, obrigados a tomar decisões de elegibilidade relacionadas com a idade.

Leis e os regulamentos podem criar o marco jurídico com procedimentos para o cumprimento robusto dessa exigência para garantir a proteção das crianças contra danos.

Se for implementada de forma proporcional e eficaz, a Garantia Etária representa uma oportunidade para reforçar os direitos fundamentais das crianças na era digital, além de proteger o anonimato e a liberdade dos adultos de usufruir de bens, conteúdos e serviços *online*.

6.22. Ainda, segundo o *Communiqué*, as soluções de garantia etária devem ser baseadas a) no melhor interesse dos sujeitos; b) no princípio da minimização da coleta de dados; c) serem transparentes e *accountable*; e d) devem ser construídas de forma cooperativa e participativa.

6.23. Tendo em vista os pontos e princípios supra, sugere-se, a seguir, encaminhamento para a questão.

## 7. CONCLUSÃO: ENCAMINHAMENTOS SUGERIDOS

7.1. Em novembro de 2024, o Brasil participou da 1ª Conferência Ministerial Global para o Fim da Violência contra a Criança, em Bogotá, Colômbia. Naquela oportunidade, o governo brasileiro assumiu oito compromissos, dentre os quais destaca-se: "*Desenvolver, até dezembro de 2026, solução para aperfeiçoamento da sistemática de verificação etária em ambientes digitais, de modo a limitar o acesso de crianças e adolescentes a conteúdos inadequados à idade, ao mesmo tempo garantindo o direito à*

*proteção de dados desses sujeitos".*

7.2. Nesse sentido, para dar início a essa ação prioritária da "Estratégia para eliminação da violência contra crianças e adolescentes", em formulação no âmbito deste MJSP, sugere-se como passo inicial a constituição de Comitê Consultivo específico, contando com as áreas envolvidas desta Pasta, bem como com especialistas e organizações da sociedade civil de reconhecida atuação na temática, sem prejuízo do convite de representantes de outros órgãos de governo ou de entidades empresariais para participação na discussão. Com base nessas discussões, relatório a ser submetido ao Sr. Ministro da Justiça e Segurança Pública poderá subsidiar as políticas públicas que se seguirão.

7.3. Para tanto, junta-se ao presente processo Minuta de Portaria de instituição de colegiado (30574026), a ser submetida aos trâmites de praxe.

7.4. Por fim, sugere-se que eventual solução que venha a ser formulada ou implementada o seja valendo-se de mecanismo de consulta aos próprios afetados, quais sejam, crianças e adolescentes, que têm, pela Convenção da Criança, direito à participação nessas decisões.

À consideração superior.

Ricardo Lins Horta  
Gerente de Projeto

Aprovo. Encaminhe-se à CONJUR/MJSP, para fins de análise da Minuta de Portaria destes autos.

Lílian Cintra de Melo  
Secretária de Direitos Digitais  
Ministério da Justiça e Segurança Pública



Documento assinado eletronicamente por **Ricardo de Lins e Horta, Gerente de Projeto**, em 24/03/2025, às 10:21, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



Documento assinado eletronicamente por **Lilian Manoela Monteiro Cintra de Melo, Secretário(a) de Direitos Digitais**, em 24/03/2025, às 13:24, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade do documento pode ser conferida no site <http://sei.autentica.mj.gov.br> informando o código verificador **30574023** e o código CRC **738E58C6**.  
O documento pode ser acompanhado pelo site <http://sei.consulta.mj.gov.br/> e tem validade de prova de registro de protocolo no Ministério da Justiça e Segurança Pública.

## ANEXO: REFERÊNCIAS

5Rights Foundation. (2021). *But how do they know it is a child? Age Assurance in the Digital World*. Disponível em: [https://5rightsfoundation.com/wp-content/uploads/2024/09/But\\_How\\_Do\\_They\\_Know\\_It\\_is\\_a\\_Child-1.pdf](https://5rightsfoundation.com/wp-content/uploads/2024/09/But_How_Do_They_Know_It_is_a_Child-1.pdf)

AEPD - Agencia Española de Protección Datos, E. (2024). *Nota Técnica: Internet Seguro por Defecto para la Infancia y el Papel de la Verificación de Edad*. Disponível em: <https://www.aepd.es/guias/nota-tecnica-internet-seguro-por-defecto-para-la-infancia.pdf>

Arcom - Autorité de régulation de la communication audiovisuelle et numérique (2024). *Référentiel déterminant les exigences techniques minimales applicables aux systèmes de vérification de l'âge mis en place pour l'accès à certains services de communication au public en ligne et aux plateformes de partage de vidéos qui mettent à disposition du public des contenus pornographiques*. Disponível em: <https://www.arcom.fr/sites/default/files/2024-04/Arcom-Consultation-publique-projet-referentiel-determinant-exigences-techniques-minimales-applicables-aux-systemes-verification-age-acces-contenus-pornographiques-en-ligne.pdf>

Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (CETIC) (2025). *Estatísticas TIC - para crianças de 0 a 8 anos de idade*. Fevereiro de 2025. Disponível em: <https://cetic.br/pt/publicacao/estatisticas-tic-para-criancas-de-0-a-8-anos-de-idade/>.

Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (CETIC). *TIC Kids Online Brasil 2024* Disponível em: [https://cetic.br/media/analises/tic\\_kids\\_online\\_brasil\\_2024\\_principais\\_resultados.pdf](https://cetic.br/media/analises/tic_kids_online_brasil_2024_principais_resultados.pdf).

eSafety Commissioner (2023). *Roadmap for age verification and complementary measures to prevent and mitigate harms to children from online pornography*. Disponível em: [https://www.esafety.gov.au/sites/default/files/2023-08/Roadmap-for-age-verification\\_2.pdf](https://www.esafety.gov.au/sites/default/files/2023-08/Roadmap-for-age-verification_2.pdf)

European Commission (2024). *Mapping age assurance typologies and requirements: Research report*. Directorate General for Communications Networks, Content and Technology., LLM., & Center for Law and Digital Technologies (eLaw). Publications Office. Disponível em: <https://data.europa.eu/doi/10.2759/455338B>

European Data Protection Board (2025). *Statement 1/2025 on Age Assurance*. Disponível em: [https://www.edpb.europa.eu/system/files/2025-02/edpb\\_statement\\_20250211ageassurance\\_en.pdf](https://www.edpb.europa.eu/system/files/2025-02/edpb_statement_20250211ageassurance_en.pdf)

European Union (2024). *Self-assessment tool on age assurance: Manual*. Disponível em: <https://better-internet-for-kids.europa.eu/en/news/new-launch-bik-age-assurance-self-assessment-tool-digital-service-providers>

Global Age Assurance Standards Summit (2024). *Communiqué*. Disponível em: <https://safeonline.global/wp-content/uploads/2024/05/Global-Age-Assurance-Standards-Summit-Communique-Final.pdf>

IEEE Consumer Technology Society (2021). *IEEE Standard for an Age Appropriate Digital Services Framework Based on the 5Rights Principles for Children*. Disponível em: <https://doi.org/10.1109/IEEESTD.2021.9627644>

Information Commissioner's Office (2020). *Age appropriate design: a code of practice for online services*. Disponível em: <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/>

Livingstone, S., Nair, A., Stoilova, M., Van Der Hof, S., & Caglar, C. (2024). Children's Rights and Online Age Assurance Systems: The Way Forward. *The International Journal of Children's Rights*, 32(3), 721–747. <https://doi.org/10.1163/15718182-32030001>

Livingstone, S., & Stoilova, M. (2021). The 4Cs: Classifying Online Risk to Children. *CO:RE Short Report Series on Key Topics* <https://doi.org/10.21241/SSOAR.71817>

OECD. (2022). *Dark commercial patterns*. OECD Digital Economy Papers. Disponível em: [https://www.oecd.org/en/publications/dark-commercial-patterns\\_44f5e846-en.html](https://www.oecd.org/en/publications/dark-commercial-patterns_44f5e846-en.html)

OECD. (2024). Towards digital safety by design for children. *OECD Digital Economy Papers*. Disponível em: [https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/06/towards-digital-safety-by-design-for-children\\_f1c86498/c167b650-en.pdf](https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/06/towards-digital-safety-by-design-for-children_f1c86498/c167b650-en.pdf)

OFCOM. (2024). *Guidance on age assurance and other Part 5 duties for service providers publishing pornographic content on online services*. Disponível em: <https://www.ofcom.org.uk/online-safety/protecting-children/guidance-service-providers-pornographic-content/>