Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

RELATÓRIO FINAL

Grupo de Trabalho 6 – Implementação da Lei nº 15.211/2025

Estatuto Digital da Criança e do Adolescente - ECA Digital

MEMBROS GT

Ana Paula Bialer (Coordenadora)
Bruno Ricardo Bioni
Cláudio Simão de Lucena Neto
Fernando Antonio Santiago Junior
Gabrielle Bezerra Sales Sarlet
Isabella Vieira Machado Henriques
Myreilla Aloia Triumpho Pereira da Cruz

APOIO AO GT

Adriana Macedo Marques
Emanuella Halfeld
Isabella Miranda Silvério
Paula Belotto André

2026

Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

Sumário

PARTE I – Introdução e Governança do Projeto

O Grupo de Trabalho 6 (GT-6) foi instituído em 5 de novembro de 2025, no âmbito do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD), por meio da Portaria CNPD nº 6/2025[1]. O GT6 foi constituído com o objetivo de realizar análises, estudos e fazer proposições na temática de implementação da Lei nº 15.211/2025 (Estatuto Digital da Criança e do Adolescente – ECA Digital).

Os trabalhos do Grupo estavam inicialmente previstos para durar cento e vinte dias, contados da entrada em vigor da Portaria que instituiu o GT-6, contudo, esse prazo foi prorrogado por igual período, nos termos da Portaria CNPD nº 2/2026[2].

1.1. O Plano de Trabalho e o Mapeamento Preliminar

O Plano de Trabalho (Anexo 1) estruturou as atividades do GT-6 em cinco frentes principais: (i) elaboração do próprio Plano de Trabalho; (ii) mapeamento das questões do ECA Digital dependentes de regulamentação; (iii) benchmarking internacional; (iv) realização de entrevistas com stakeholders; e (v) elaboração de Relatório Final consolidado.

O Plano de Trabalho definiu os objetivos do Grupo, a periodicidade das reuniões, os membros participantes, os entregáveis previstos e o cronograma de execução das atividades. A partir dessa organização metodológica, estabeleceu-se que o primeiro esforço substantivo do GT-6 seria o "Mapeamento das Questões que Dependem de Regulamentação" (Anexo 2), destinado a identificar as atribuições regulatórias conferidas pelo ECA Digital (Lei nº 15.211/2025), bem como a avaliar a quem seria atribuída a competência regulatória correspondente.

O levantamento demonstrou que parcela significativa das competências regulamentares atribuídas pela Lei nº 15.211/2025 ficou concentrada na ANPD. Entre os temas identificados estavam: (i) regulamentação de políticas de prevenção à intimidação sistemática virtual (cyberbullying) e outras formas de assédio; (ii) definição das regras para elaboração e compartilhamento de relatórios de impacto; (iii) estabelecimento de

[1] CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE (CNPD). Portaria CNPD/ANPD GT-06/2025. Brasília, DF: Agência Nacional de Proteção de Dados, 2025. Disponível em: https://www.gov.br/anpd/pt-br/cnpd-2/portarias-gts-2a-formacao/2as-grupos-de-trabalho-da-2a-formacao-do-cnpd/portaria_cnpd_gt06_2025.pdf/@@display-file/file. Acesso em: 19 maio 2026.

[2] CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE (CNPD). Portaria CNPD nº 2/2026. Brasília, DF: Agência Nacional de Proteção de Dados, 2026. Disponível em: https://www.gov.br/anpd/pt-br/cnpd-2/sei_0243177_portaria_cnpd_2_2026-prorrogacao.pdf/@@display-file/file. Acesso em: 19 maio 2026.

diretrizes e padrões mínimos para mecanismos de supervisão parental; (iv) definição de critérios para avaliação da efetividade de mecanismos de aferição de idade e procedimentos de apelação para contas suspensas em redes sociais; (v) regulamentação de obrigações relacionadas à remoção e comunicação de conteúdos envolvendo exploração, abuso sexual, sequestro e aliciamento de crianças e adolescentes; (vi) definição de critérios para compartilhamento de dados com instituições acadêmicas, científicas e jornalísticas para fins de pesquisa; (vii) estabelecimento de requisitos para manutenção de registros relacionados ao uso abusivo de instrumentos de denúncia; (viii) regulamentação de adesivos informativos em embalagens de equipamentos eletrônicos; e (ix) definição de critérios de adequação etária e modulação de obrigações de provedores digitais. Além dessas competências específicas, o levantamento também destacou o poder geral de regulamentação conferido à ANPD pelos artigos 2º, inciso X, e 34 do ECA Digital.

Em adição ao mapeamento das competências expressamente previstas na legislação, o documento também analisou as iniciativas incorporadas à proposta inicial de atualização da Agenda Regulatória da ANPD para 2025–2026 após a sanção do ECA Digital[3]. A análise buscou identificar os temas sinalizados pela Agência como prioritários para futura regulamentação, que incluíam: (i) tratamento de dados pessoais de crianças e adolescentes; (ii) conceitos gerais e definições do ECA Digital; (iii) fiscalização e sanção no âmbito da Lei nº 15.211/2025; e (iv) mecanismos de aferição de idade. A partir desse cruzamento entre as competências regulatórias atribuídas pelo ECA Digital e as prioridades já indicadas pela própria ANPD, buscou-se orientar a definição dos temas prioritários a serem aprofundados pelo GT-6.

Na sequência, o Plano de Trabalho estabeleceu a realização de Benchmarking Internacional voltado à análise comparativa de iniciativas regulatórias estrangeiras relacionadas à proteção de crianças e adolescentes em ambientes digitais, com destaque para a União Europeia, Reino Unido, Austrália e Estados Unidos. O estudo deveria contemplar legislações, códigos e documentos regulatórios relevantes nos temas identificados pelo mapeamento.

Além disso, o Plano previu a realização de entrevistas com representantes da academia, empresas, poder público, reguladores internacionais e sociedade civil, com o objetivo de reunir perspectivas técnicas e institucionais sobre os desafios de implementação do ECA Digital. As entrevistas incluíram a seleção dos participantes, a

[3] AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). ANPD abre tomada de subsídios para revisão da agenda regulatória. Brasília, DF, 20 out. 2025. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-abre-tomada-de-subsidios-para-revisao-da-agenda-regulatoria. Acesso em: 19 maio 2026.

elaboração de roteiros temáticos, a condução das reuniões e a consolidação das contribuições em relatórios. Buscou-se uma escuta ativa multisetorial.

Por fim, o Plano de Trabalho previu a elaboração de um Relatório Final consolidando todas as etapas do projeto, incluindo a descrição das atividades desenvolvidas, os produtos elaborados ao longo do GT-6 e um parecer conclusivo contendo recomendações e proposições relacionadas à implementação do ECA Digital pela ANPD.

1.2. O Desenvolvimento do Benchmarking

Durante as sessões de alinhamento do Grupo, definiu-se que o Benchmarking deveria isolar as variáveis regulatórias de jurisdições maduras, especificamente União Europeia, Reino Unido, Austrália, Estados Unidos, e Índia. Decidiu-se também que seria feito mapeamento na América Latina, a fim de identificar jurisdições com legislações relevantes. Essa seleção e o próprio corte metodológico do estudo foram consolidados na segunda reunião ordinária, quando os conselheiros acordaram que, diante da imensa amplitude do texto legal do ECA Digital, realizar um diagnóstico comparado irrestrito seria inviável no prazo do colegiado. Por isso, o escopo foi deliberadamente restringido às atribuições e disposições da Lei nº 15.211/2025 que dependiam de regulamentação futura pela ANPD - considerando-se curto e médio prazo - e às iniciativas prioritárias propostas na revisão da Agenda Regulatória da ANPD para o biênio 2025–2026.

A partir dessa diretriz, a coordenação do GT-6 estruturou as frentes de análise e, na terceira reunião ordinária, apresentou a primeira proposta de documento. Naquela oportunidade, os membros sugeriram e aprovaram ajustes operacionais. Com essas validações metodológicas, o colegiado determinou que o benchmarking seria estruturado formalmente a partir dos seguintes tópicos, seções e subtópicos:

- **Seção 1: Introdução e Escopo do Benchmarking:** Delimitação do nexo causal entre a versão revisada da Agenda Regulatória da ANPD para o biênio 2025–2026 e as indicações expressas de regulamentação futura contidas no ECA Digital (Lei nº 15.211/2025).

- **Seção 2: Conceitos Gerais e Definições:** Seção dedicada a estabelecer bases conceituais claras, reduzir incertezas interpretativas e subsidiar atividades regulatórias futuras com foco em sete subtópicos estruturantes:
    - *Subtópico 2.1: Acesso Provável:* Critérios para definir o limiar em que um produto ou serviço é considerado suscetível de ser acessado por crianças e adolescentes.

- *Subtópico 2.2: Melhor Interesse da Criança e do Adolescente:* Operacionalização do princípio como consideração primária na concepção do serviço (*safety by design*) e vetor transversal de proteção.
- *Subtópico 2.3: Caixa de Recompensa (Loot Box):* Definições e abordagens sobre caixas de recompensa.
- *Subtópico 2.4: Condição Peculiar de Pessoa em Desenvolvimento:* Incorporação normativa de estágios diferenciados de desenvolvimento cognitivo e autonomia progressiva por meio de faixas etárias.
- *Subtópico 2.5: Conteúdo Pornográfico:* Critérios objetivos para caracterização de material de natureza pornográfica.
- *Subtópico 2.6: Conteúdo Impróprio, Inadequado ou Proibido:* Definições e critérios utilizados para identificar conteúdo impróprio, inadequado e proibido e abordagem dada a cada um dos conteúdos.
- *Subtópico 2.7: Verificação de Idade vs. Aferição de Idade:* Distinção técnico-conceitual entre verificação e aferição.

- **Seção 3: Mecanismos de Aferição de Idade (*Age Assurance*):** Abordagem focada no detalhamento operacional das obrigações dispostas nos artigos 9º a 15 do ECA Digital:
  - *Subtópico 3.1: Fundamentos Regulatórios:* Definições relevantes, objetivos centrais do controle de acesso e escopo de produtos ou serviços sujeitos à obrigatoriedade.
  - *Subtópico 3.2: Atores Relevantes:* Atribuição de responsabilidades a provedores e plataformas, papel regulador e fiscalizatório do Estado, e a governança de auditorias externas ou entidades certificadoras.
  - *Subtópico 3.3: Implementação Prática:* Catálogo de mecanismos admitidos, critérios de seleção, e o momento em que a implementação deve ocorrer.

- **Seção 4: Outros Temas Regulatórios:** Levantamento comparativo focado em dispositivos transversais e adicionais sujeitos à regulamentação pela ANPD:
  - *Subtópico 4.1:* Medidas de prevenção e mitigação de risco de acesso (Art. 6º, § 2º).
  - *Subtópico 4.2:* Mecanismos de supervisão parental (Art. 17, §§ 1º e 3º).
  - *Subtópico 4.3*: Procedimento de apelação para contas suspensas (Art. 24, § 4º).
  - *Subtópico 4.4:* Remoção e comunicação de violações graves (Art. 27 e § 1º).
  - *Subtópico 4.5:* Notificação de violações aos direitos de crianças (Art. 28, Parágrafo único).

- *Subtópico 4.6:* Acesso a dados para pesquisa (Art. 31, Parágrafo único).
- *Subtópico 4.7:* Registros de uso abusivo de denúncias (Art. 33, § 3º).
- *Subtópico 4.8:* Adesivos informativos em embalagens (Art. 38).
- *Subtópico 4.9:* Critérios de adequação etária e modulação (Art. 39, § 1º, I e § 3º).

O GT-6 estabeleceu em suas sessões de planejamento que a análise comparativa de cada um dos subtópicos deveria responder a quatro variáveis de controle, organizadas de forma descritiva e sistemática na matriz: Jurisdição (identificação geográfica do país ou bloco econômico estudado); Instrumento Normativo (isolamento de leis primárias, regulamentos secundários, códigos de conduta, guias técnicos oficiais, dentre outros); Questões Centrais a serem Analisadas no Tópico (abordagem direta do conceito ou comando legal equivalente ao mapeado no ECA Digital); e Observações Relevantes (detalhes técnicos, lições extraídas das experiências estrangeiras, salvaguardas de privacidade, assimetrias regulatórias e eventuais lacunas ou exemplos negativos para fins de modelagem regulatória).

A divisão de trabalho para o preenchimento dessas variáveis foi pactuada formalmente entre os conselheiros nas reuniões ordinárias. A coordenação, sob a responsabilidade de Ana Paula Bialer, assumiu o estudo sobre o ecossistema do Reino Unido e da Índia. A conselheira Isabella Henriques ficou encarregada da análise sobre a Austrália. O monitoramento da União Europeia foi delegado à conselheira Myreilla Aloia, enquanto o mapeamento relativo aos Estados Unidos ficou sob a responsabilidade da conselheira Adriana Marques. Ao longo das discussões, os membros deliberaram expandir a análise para a América Latina, incorporando dados recentes sobre a Colômbia.

1.3. Dinâmica das Reuniões e Entrevistas

A execução do Plano de Trabalho amparou-se em uma rotina de reuniões ordinárias semanais, realizadas virtualmente às quartas-feiras, e em um amplo ciclo de auscultação técnica conduzido entre dezembro de 2025 e março de 2026. Nas primeiras reuniões do grupo, além de debater o Plano de Trabalho, o Mapeamento Preliminar e o Benchmarking, os conselheiros definiram os parâmetros de governança das entrevistas, acordando que a lista de contatos das entidades convidadas seria gerida em documento apartado por razões de privacidade, além de estipularem que cada oitiva deveria contar com a participação e relatoria de, no mínimo, dois membros do GT-6, utilizando roteiros e questionários padronizados previamente validados.

No total, o Grupo de Trabalho realizou 11 entrevistas estratégicas estruturadas de forma multissetorial. O ciclo de escuta englobou a realização de oitivas com representantes do setor de jogos digitais, plataforma de redes sociais, órgãos e comitês da infraestrutura governamental e do Poder Executivo, entidades representativas dos setores de streaming audiovisual e do mercado financeiro e de crédito, e especialistas e pesquisadores independentes do ambiente acadêmico. Optou-se por não chamar para novas entrevistas atores relevantes que foram ouvidos pelo GT2, aproveitando-se a contribuição feita naquela esfera, inclusive por membros da ANPD.

1.4. O Desenvolvimento do Relatório Final

A etapa de consolidação do Relatório Final teve início nas reuniões ordinárias de abril e maio de 2026, quando o colegiado passou a debater de forma estruturada os achados produzidos ao longo dos trabalhos e a definir a arquitetura do documento conclusivo.

Na 9ª Reunião Ordinária, realizada em 24 de março de 2026, foi apresentada pela equipe de apoio ao GT-6 uma primeira proposta de estrutura para o relatório, organizada em seções temáticas que contemplavam: a descrição da dinâmica das reuniões e entrevistas; o plano de trabalho e o mapeamento preliminar; o quadro normativo brasileiro anterior e posterior ao ECA Digital; os resultados do benchmarking internacional; o aprofundamento técnico sobre aferição de idade; e a síntese dos diagnósticos extraídos das entrevistas com stakeholders nacionais. Os membros do GT apresentaram sugestões sobre essa estrutura inicial.

Na 10ª Reunião Ordinária, realizada em 6 de maio de 2026, Ana Paula Bialer apresentou a estrutura revisada do relatório em desenvolvimento, percorrendo o esqueleto do documento e descrevendo o escopo de cada parte. No curso da discussão, foram incorporadas novas sugestões dos membros. Nessa reunião, procedeu-se também à divisão formal das contribuições ao relatório entre os membros, considerando a disponibilidade e a especialização de cada um nas respectivas seções.

Ao final desse processo de consolidação, o GT-6 deliberou que o Relatório Final seria estruturado em cinco partes. A **Parte I** descreve a governança e a metodologia do projeto, incluindo o Plano de Trabalho, o mapeamento preliminar, a dinâmica das reuniões e entrevistas, e a linha do tempo institucional que contextualiza o cenário regulatório em que os trabalhos se desenvolveram. A **Parte II** apresenta a paisagem normativa nacional e comparada, com análise do quadro jurídico brasileiro anterior e posterior ao ECA Digital e o benchmarking internacional elaborado pelo GT-6, organizado por jurisdição e por temas

regulatórios. A **Parte III** aprofunda o desafio técnico da aferição de idade, examinando padrões técnicos internacionais, práticas do setor público e privado, mecanismos de sinais de idade, controvérsias em torno da estimativa facial e reação à implementação dos mecanismos de aferição. A **Parte IV** apresenta o diagnóstico nacional, com a síntese das entrevistas com stakeholders brasileiros, o mapeamento de convergências, desafios e tensões entre atores, e dois elementos adicionais identificados pelos próprios membros do GT-6 ao longo das reuniões. A **Parte V** reúne as considerações finais e as proposições do Grupo dirigidas à ANPD.

Foi justamente nas reuniões finais de consolidação que os membros do GT-6 identificaram dois temas que, embora não derivassem diretamente do benchmarking ou das entrevistas, emergiram como pontos de atenção relevantes para a implementação do ECA Digital, e que, por essa razão, foram incorporados à Parte IV do relatório como elementos adicionais. O primeiro diz respeito ao papel do CNPD no processo de implementação do Estatuto, e à importância de que a Agência utilize de forma contínua e estruturada essa instância multisetorial como espaço privilegiado de subsídio qualificado. O segundo trata da interface com o Poder Judiciário e do sistema de justiça como um todo, cuja capacitação e articulação com a ANPD os membros identificaram como condição para a efetividade do regime protetivo e sancionatório instituído pelo ECA Digital. Esses dois temas são desenvolvidos na Seção 4.3 deste Relatório.

1.5. A Linha do Tempo Institucional

A construção do Relatório Final pelo GT-6 não ocorreu em um vácuo temporal ou regulatório; pelo contrário, deu-se em meio a um cenário de intensa e acelerada produção normativa por parte do Poder Executivo e da própria ANPD . Para compreender o escopo, a oportunidade e o grau de aplicabilidade das recomendações apresentadas neste documento, faz-se necessário analisar o desenvolvimento dos trabalhos do grupo em paralelo com a evolução dos marcos regulatórios externos. Essa contextualização evidencia que o GT-6 operou sob uma dinâmica de "alvo em movimento", exigindo que a leitura deste relatório seja acompanhada por um estrito fator de temporalidade, uma vez que o amadurecimento institucional contínuo alterou o peso e a relevância de diferentes temas ao longo do tempo .

- **O Cenário de Dezembro de 2025 (Início dos Trabalhos):** Quando o GT-6 desenhou o seu Plano de Trabalho, estruturou o Mapeamento Preliminar e iniciou o levantamento do benchmarking internacional, o cenário regulatório nacional apresentava profundas lacunas e incertezas. Naquele momento, não havia um decreto regulamentador publicado, tampouco a versão final da Agenda Regulatória

revisada ou o Mapa de Temas Prioritários de Fiscalização da ANPD. A proposta inicial de atualização da agenda, que balizou os primeiros passos do grupo, difere substancialmente do desenho que veio a ser consolidado pela Agência no final de dezembro. Dessa forma, é preciso considerar que o delineamento inicial dos trabalhos do GT-6, que guiaram sua atuação ao longo dos meses, levou em conta o cenário da época.

- **O Ponto de Inflexão de Março de 2026:** O ciclo de oitivas e a redação do documento de benchmarking foram formalmente encerrados pelo grupo na semana anterior ao Carnaval de 2026. Portanto, todo o diagnóstico comparado foram consolidados antes da entrada em vigor da lei, da edição do Decreto nº 12.880/2026, da publicação das Orientações Preliminares sobre Mecanismos Confiáveis de Aferição de Idade e da abertura da tomada de subsídios sobre o Guia da ANPD. Como consequência direta desse descasamento temporal, determinados aspectos técnicos e operacionais levantados no mapeamento comparativo do grupo podem, em alguma medida, já ter sido endereçados ou respondidos pelas ações posteriores do Executivo e da Agência, inclusive na complexa temática de aferição de idade.
- **O Fator de Temporalidade e Relevância:** Diante desse histórico, este Relatório Final deve ser interpretado à luz das datas em que os insumos foram colhidos e estruturados. Determinadas análises que se mostravam urgentes no início do cronograma perderam parte do ineditismo frente aos guias e normativas supervenientes da ANPD, enquanto outras discussões ganharam ainda maior relevância para balizar as próximas etapas definitivas da Autoridade. O relatório funciona, assim, como uma fotografia técnica de um processo evolutivo, cujo valor reside tanto no registro histórico da construção participativa quanto no fornecimento de subsídios que devem ser filtrados e calibrados de acordo com o estado da arte regulatório do momento de sua leitura.

Para ilustrar de forma clara essa sobreposição de agendas e o dinamismo institucional que acompanhou as atividades do colegiado, apresenta-se a linha do tempo vertical a seguir, detalhando os marcos cronológicos que impactaram diretamente o andamento e o foco dos trabalhos:

- **17 de setembro de 2025:** Sanção da Lei nº 15.211/2025 (Estatuto Digital da Criança e do Adolescente — ECA Digital), estabelecendo o marco legal central e fixando o período de *vacatio legis*.
- **15 de outubro de 2025:** Abertura simultânea de duas consultas públicas na plataforma Brasil Participativo pelo Governo Federal, sendo uma delas voltada especificamente aos mecanismos de aferição de idade (SEDIGI/MJSP).

- **5 de novembro de 2025:** Instituição do Grupo de Trabalho 6 (GT-6) no âmbito do CNPD, por meio da Portaria nº 6/2025, iniciando formalmente o planejamento e o mapeamento das demandas de regulamentação.
- **Dezembro de 2025:** Início do ciclo de oitivas técnicas do GT-6 com os stakeholders do mercado e aprovação do esqueleto metodológico do benchmarking internacional .
- **24 de dezembro de 2025:** Publicação conjunta da Resolução CD/ANPD nº 30/2025 (Mapa de Temas Prioritários para Fiscalização 2026-2027) e da Resolução CD/ANPD nº 31/2025 (Agenda Regulatória 2025-2026), absorvendo e reorganizando as temáticas do ECA Digital em três novas iniciativas regulatórias.
- **Fevereiro de 2026 (Semana anterior ao Carnaval):** Encerramento formal e consolidação definitiva do documento de benchmarking internacional pelo GT-6.
- **17 de março de 2026:** Fim do prazo de *vacatio legis* e entrada em vigor definitiva de todos os dispositivos da Lei nº 15.211/2025 (ECA Digital).
- **18 de março de 2026:** Assinatura do Decreto Presidencial nº 12.880/2026, regulamentando o ECA Digital, instituindo a Política Nacional e atribuindo competências específicas à ANPD. Publicação do documento conjunto de Perguntas e Respostas pelas autoridades públicas.
- **20 de março de 2026:** Publicação das Orientações Preliminares sobre Mecanismos Confiáveis de Aferição de Idade pela ANPD, estruturando os seis eixos de conformidade e o cronograma escalonado de fiscalização.
- **Abril e Maio de 2026:** Últimas entrevistas e reuniões finais ordinárias do GT-6 voltadas à avaliação de todas as frentes desenvolvidas, debate do esqueleto do documento e início da etapa de consolidação dos trabalhos do grupo como um todo .
- **30 de abril de 2026:** Abertura pela ANPD da tomada de subsídios sobre o Guia Orientativo de Fornecedores e Obrigações Gerais do ECA Digital, na plataforma Brasil Participativo.

PARTE II – Paisagem Normativa Nacional e Comparada

A Parte II apresenta a paisagem normativa sobre proteção de crianças e adolescentes em ambientes digitais sob duas perspectivas complementares. A seção 2.1 narra, de forma panorâmica, o quadro normativo e institucional brasileiro anterior ao ECA Digital e o que passou a existir com sua entrada em vigor, sem pretensão de esgotar obrigações ou direitos, mas de situar o leitor no contexto nacional antes do exame comparado. A seção 2.2 apresenta o benchmarking internacional elaborado pelo GT-6.

O benchmarking foi estruturado a partir dos temas que o ECA Digital indicava expressamente como objeto de regulamentação futura pela ANPD, complementados pela proposta de revisão da Agenda Regulatória 2025–2026 então em circulação. A análise comparada abrange dois eixos: conceitos gerais e definições (acesso provável, melhor interesse da criança e do adolescente, caixa de recompensa, condição peculiar de pessoa em desenvolvimento e categorias de conteúdo) e outros dispositivos expressamente sujeitos à regulamentação pela Agência, como supervisão parental, critérios de adequação etária e modulação de obrigações, entre outros. Os mecanismos de aferição de idade, dada sua densidade técnica e centralidade na agenda regulatória imediata, são objeto de tratamento específico na Parte III.

2.1. Proteção de Crianças e Adolescentes no Brasil

A proteção de crianças e adolescentes no ambiente digital passou, nos últimos anos, por um processo de rápida transformação normativa e institucional no Brasil. Antes da edição do ECA Digital, o regime jurídico aplicável ao tema era formado por um conjunto fragmentado de normas constitucionais, disposições do Estatuto da Criança e do Adolescente (ECA), regras de defesa do consumidor, proteção de dados pessoais, classificação indicativa e atos administrativos editados por diferentes órgãos públicos. Embora esse arcabouço já permitisse enfrentar parte dos riscos decorrentes da crescente digitalização da vida infantojuvenil, inexistia um marco regulatório unificado voltado especificamente à responsabilização e aos deveres dos fornecedores de produtos e serviços de tecnologia da informação.

A aprovação da Lei nº 15.211/2025 alterou significativamente esse cenário. O ECA Digital consolidou, em um único diploma, regras voltadas à proteção de crianças e adolescentes em ambientes digitais, estabelecendo deveres específicos relacionados à prevenção de riscos, aferição de idade, supervisão parental, publicidade digital, jogos eletrônicos, transparência, governança e fiscalização regulatória. Paralelamente, sua implementação impulsionou intensa movimentação institucional, envolvendo

regulamentação infralegal, consultas públicas, produção de guias orientativos e reorganização das agendas regulatórias da ANPD e de outros órgãos federais.

Nesse contexto, o presente tópico tem por objetivo apresentar, de forma panorâmica, o quadro normativo e institucional brasileiro anterior e posterior ao ECA Digital, a fim de contextualizar o status quo doméstico antes do exame comparado das experiências internacionais que será desenvolvido nos tópicos seguintes.

2.1.1. Panorama Brasileiro Anterior ao ECA Digital

A proteção da infância e da adolescência no Brasil é estruturada sob o paradigma da proteção integral e prioritária, que rompe com a antiga visão "menorista" para reconhecer crianças e adolescentes como sujeitos de direitos plenos. Durante cerca de um século, vigorou na maioria dos países ocidentais e latino-americanos o modelo das chamadas "legislações de crianças e adolescentes", fundamentado na Doutrina da Situação Irregular. Esse paradigma caracterizava-se pela intervenção estatal discricionária e coercitiva sobre uma categoria específica rotulada como "crianças e adolescentes", tratados estritamente como objetos de proteção a partir de sua incapacidade jurídica, sem que se reconhecesse sua condição de sujeitos de direitos humanos e fundamentais. Os conflitos e deficiências das políticas sociais eram patologizados, criminalizados e convertidos em problemas individuais, com opção prioritária pela institucionalização e pela privação de liberdade por tempo indeterminado. No caso brasileiro, o Juiz de crianças e adolescentes atuava com faculdades ilimitadas, sem vinculação estrita à legalidade ou ao devido processo. Nessa época, crianças e adolescentes em situação de vulnerabilidade socioeconômica eram punidos por vivenciarem tal condição, com a sua institucionalização sem qualquer diferenciação em relação aos adolescentes acusados de atos contrários à lei.

A transição paradigmática global consolidou-se com o advento de uma série de instrumentos internacionais, as Regras de Beijing (1985)[4], as Regras de Tóquio[5] e as Diretrizes de Riad (1990)[6], e, sobretudo, com a Convenção Internacional sobre os Direitos

[4] CONSELHO NACIONAL DE JUSTIÇA; PROGRAMA DAS NAÇÕES UNIDAS PARA O DESENVOLVIMENTO. Regras de Beijing: regras mínimas das Nações Unidas para a administração da justiça juvenil adotada pela Resolução n.º 40/33 da Assembleia Geral, de 29 de novembro de 1985. Brasília: CNJ, 2024. 30 p. Disponível em: https://www.cnj.jus.br/wp-content/uploads/2024/08/regras-beijing.pdf. Acesso em: 21 maio 2026.

[5] CONSELHO NACIONAL DE JUSTIÇA (Brasil). *Regras de Tóquio: regras mínimas padrão das Nações Unidas para a elaboração de medidas não privativas de liberdade*. Brasília: CNJ, 2016. 22 p. (Série Tratados Internacionais de Direitos Humanos). Disponível em: https://www.cnj.jus.br/wp-content/uploads/2019/09/6ab7922434499259ffca0729122b2d38-2.pdf?utm_source=chatgpt.com.. Acesso em: 21 maio 2026.

[6] CONSELHO NACIONAL DE JUSTIÇA; PROGRAMA DAS NAÇÕES UNIDAS PARA O DESENVOLVIMENTO. *Diretrizes de Riad: diretrizes das Nações Unidas para a prevenção da delinquência juvenil*. Brasília: CNJ, 2024. 26 p. Disponível em: https://www.cnj.jus.br/wp-content/uploads/2024/08/diretrizes-riad.pdf. Acesso em: 21 maio 2026.

da Criança da ONU (1989), recepcionada pelo Brasil, com status constitucional, por meio do Decreto 99.710/90. No Brasil, esse movimento se concretizou na positivação do artigo 227 da Constituição Federal de 1988[7], que impõe à família, à sociedade[8] e ao Estado o dever de assegurar à criança e ao adolescente, com prioridade absoluta, o acesso à vida, à saúde, à educação e ao lazer, além de protegê-los de toda forma de negligência, exploração e violência. No plano internacional, a estrutura normativa é complementada pelos Comentários Gerais do Comitê de Direitos da Criança da ONU, instrumentos interpretativos da Convenção que aprofundam suas obrigações em temáticas específicas. Para os fins do presente Relatório, destacam-se, entre outros, o Comentário Geral nº 14[9], sobre o direito da criança a que seu melhor interesse seja considerado como primordial, e o Comentário Geral nº 25[10], que detalha as obrigações dos Estados e dos agentes privados na conformação de ecossistemas digitais que assegurem, de forma prévia e proativa, o pleno desenvolvimento infantojuvenil. No ambiente tecnológico atual, essa força constitucional vincula diretamente os arquitetos de sistemas a estruturarem ecossistemas digitais que protejam esse fluxo de desenvolvimento de forma prévia e proativa.

No plano infraconstitucional, a materialização desses comandos ocorre, em primeiro lugar, por meio do Estatuto da Criança e do Adolescente (ECA — Lei nº 8.069/1990)[11], que reconhece crianças (até doze anos incompletos) e adolescentes (entre doze e dezoito anos) como titulares de direitos fundamentais e atribui à família, à

---

[7] BRASIL. Decreto n.º 99.710, de 21 de novembro de 1990. Promulga a Convenção sobre os Direitos da Criança. Brasília, DF: Presidência da República, 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d99710.htm. Acesso em: 21 maio 2026.

[8] O constituinte, ao incluir a "sociedade" como destinatária autônoma do dever de proteção, abrangeu os agentes privados, inclusive pessoas jurídicas que desenvolvem atividade econômica dirigida ou acessível a crianças e adolescentes. O STF consolidou esse entendimento em casos paradigmáticos, reconhecendo o dever das empresas de assegurar direitos fundamentais infantojuvenis com absoluta prioridade (STF, ADI 5.357, Rel. Min. Edson Fachin, Plenário, DJe 11/11/2016; RE 629.053, Red. acórdão Min. Alexandre de Moraes, Plenário, DJe 27/02/2019, Tema 809; RE 778.889, Rel. Min. Roberto Barroso, Plenário, DJe 01/08/2016, Tema 782). O STJ aplicou o mesmo vetor para impor obrigações a emissoras e editoras privadas com fundamento direto no art. 227 da CF e nos princípios da proteção integral e do superior interesse da criança (STJ, REsp 509.968, Rel. Min. Ricardo Villas Bôas Cueva, Terceira Turma, DJe 17/12/2012; REsp 1.569.814). Sobre o dever das corporações digitais nesse contexto, v. HENRIQUES, Isabella Vieira Machado. Direitos fundamentais da criança no ambiente digital: o dever de garantia da absoluta prioridade. São Paulo: Thomson Reuters Brasil, 2023.

[9] COMITÊ DOS DIREITOS DA CRIANÇA. Comentário Geral n.º 14 (2013) sobre o direito da criança de ter seu interesse superior considerado primordialmente (artigo 3º, parágrafo 1, da Convenção sobre os Direitos da Criança). Genebra: Organização das Nações Unidas, 2013. Documento CRC/C/GC/14. Disponível em: https://www2.ohchr.org/English/bodies/crc/docs/GC/CRC_C_GC_14_ENG.pdf. Acesso em: 31 maio 2026.

[10] COMITÊ DOS DIREITOS DA CRIANÇA. Comentário Geral n.º 25 (2021) sobre os direitos das crianças em relação ao ambiente digital. Genebra: Organização das Nações Unidas, 2021. Documento CRC/C/GC/25. Disponível em: https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation. Acesso em: 31 maio 2026.

[11] BRASIL. Lei n.º 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Brasília, DF: Presidência da República, 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 21 maio 2026.

comunidade, à sociedade em geral e ao poder público o dever de assegurar, com absoluta prioridade, a efetivação desses direitos. O Código de Defesa do Consumidor (CDC — Lei nº 8.078/1990)[12] complementa esse quadro ao classificar como abusiva a publicidade que se aproveita da deficiência de julgamento e da inexperiência da criança (art. 37, § 2º). A Lei Geral de Proteção de Dados Pessoais (LGPD — Lei nº 13.709/2018)[13] dedica o artigo 14 a criança e adolescente, condicionando o tratamento de seus dados ao melhor interesse do titular e estabelecendo, nos parágrafos 1º a 6º, disposições sobre consentimento parental, limites à coleta e obrigações dos controladores. A Lei nº 14.811/2024[14] criminalizou o bullying e o cyberbullying, e a Lei nº 14.852/2024 (Marco Legal dos Jogos Eletrônicos)[15] introduziu regime jurídico próprio para o setor, erigindo a proteção de crianças e adolescentes como princípio orientador e dedicando capítulo específico ao tema. Mais recentemente, a Lei nº 15.100/2025[16] restringiu o uso de celulares nas escolas da educação básica.

No plano institucional, cabe destacar, em primeiro lugar, a classificação indicativa[17]. Com fundamento no artigo 21, XVI, da Constituição Federal, o instituto foi regulamentado pelo ECA, cujos artigos 74 a 80 disciplinam o acesso de crianças e adolescentes a espetáculos e produtos potencialmente prejudiciais. Operado pela Coordenação de Política de Classificação Indicativa (COCIND) da Secretaria Nacional de Justiça, o sistema ClassInd informa às famílias a faixa etária para a qual obras audiovisuais, jogos eletrônicos e aplicativos não se recomendam, resultando em classificações que vão de "livre" a "não

---

[12] BRASIL. Lei n.º 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências (Código de Defesa do Consumidor). Brasília, DF: Presidência da República, 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 21 maio 2026.

[13] BRASIL. Lei n.º 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em:https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 21 maio 2026.

[14] BRASIL. Lei n.º 14.811, de 12 de janeiro de 2024. Institui medidas de proteção à criança e ao adolescente contra a violência nos estabelecimentos educacionais ou similares, prevê a Política Nacional de Prevenção e Combate ao Abuso e Exploração Sexual da Criança e do Adolescente e altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), e as Leis nºs 8.072, de 25 de julho de 1990 (Lei dos Crimes Hediondos), e 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente). Brasília, DF: Presidência da República, 2024. Disponível em: https://www2.camara.leg.br/legin/fed/lei/2024/lei-14811-12-janeiro-2024-795244-publicacaooriginal-170834-pl.html. Acesso em: 21 maio 2026.

[15] BRASIL. Lei n.º 14.852, de 3 de maio de 2024. Cria o marco legal para a indústria de jogos eletrônicos; e altera as Leis nºs 8.313, de 23 de dezembro de 1991, 8.685, de 20 de julho de 1993, e 9.279, de 14 de maio de 1996. Brasília, DF: Presidência da República, 2024. Disponível em: https://www2.camara.leg.br/legin/fed/lei/2024/lei-14852-3-maio-2024-795567-publicacaooriginal-171677-pl.html. Acesso em: 21 maio 2026.

[16] BRASIL. Lei n.º 15.100, de 13 de janeiro de 2025. Dispõe sobre a utilização, por estudantes, de aparelhos eletrônicos portáteis pessoais nos estabelecimentos públicos e privados de ensino da educação básica. Brasília, DF: Presidência da República, 2025. Disponível em: https://www2.camara.leg.br/legin/fed/lei/2025/lei-15100-13-janeiro-2025-796892-publicacaooriginal-174094-pl.html. Acesso em: 21 maio 2026.

[17] BRASIL. Ministério da Justiça e Segurança Pública. Classificação indicativa. Brasília, DF: MJSP, [s.d.]. Disponível em: https://www.gov.br/mj/pt-br/assuntos/seus-direitos/classificacao-1?utm_source=chatgpt.com. Acesso em: 21 maio 2026.

recomendado para crianças e adolescentes de 18 anos". Destaca-se, igualmente, o Conselho Nacional dos Direitos da Criança e do Adolescente (CONANDA)[18], criado pela Lei nº 8.242/1991, que no campo digital editou a Resolução nº 245/2024[19], sobre os direitos de crianças e adolescentes no ambiente digital, e a Resolução nº 257/2024[20], que estabeleceu as diretrizes gerais da Política Nacional sobre o tema. No campo da regulação de dados, a ANPD firmou, por meio do Enunciado CD/ANPD nº 01/2023[21], o entendimento de que o tratamento de dados de crianças e adolescentes pode ser realizado com base em qualquer das hipóteses dos artigos 7º e 11 da LGPD, desde que o melhor interesse do titular prevaleça como critério avaliativo em cada operação, e publicou, em outubro de 2025, a quinta edição do Radar Tecnológico, dedicada aos mecanismos de aferição de idade.

No campo das políticas públicas, o Governo Federal lançou, em março de 2025, o Guia sobre o Uso de Dispositivos Digitais por Crianças e Adolescentes[22], com recomendações de tempo de tela por faixa etária e orientações sobre mediação parental e rotinas digitais saudáveis. O Ministério dos Direitos Humanos e da Cidadania publicou o Diagnóstico da Violência Sexual Online contra Crianças e Adolescentes[23], e o Ministério da Justiça e Segurança Pública lançou a estratégia Crescer em Paz[24], composta por 45 ações, parte delas voltadas ao contexto digital.

---

18 BRASIL. Ministério dos Direitos Humanos e da Cidadania. Conselho Nacional dos Direitos da Criança e do Adolescente (Conanda). Brasília, DF: MDHC, [s.d.]. Disponível em:https://www.gov.br/mdh/pt-br/acesso-a-informacao/participacao-social/conselho-nacional-dos-direitos-da-crianca-e-do-adolescente-conanda/conanda?utm_source=chatgpt.com. Acesso em: 21 maio 2026.

19 CONSELHO NACIONAL DOS DIREITOS DA CRIANÇA E DO ADOLESCENTE (CONANDA). Resolução nº 245, de 5 de abril de 2024. Dispõe sobre os direitos das crianças e adolescentes em ambiente digital. Diário Oficial da União: seção 1, Brasília, DF, ed. 68, p. 42, 9 abr. 2024. Disponível em: https://www.gov.br/participamaisbrasil/blob/baixar/48630. Acesso em: 31 maio 2026.

20 BRASIL. Conselho Nacional dos Direitos da Criança e do Adolescente (CONANDA). Resolução nº 257, de 12 de dezembro de 2024. Estabelece as diretrizes gerais da Política Nacional de Proteção dos Direitos da Criança e do Adolescente no Ambiente Digital. Diário Oficial da União: seção 1, Brasília, DF, 20 dez. 2024. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-n-257-de-12-de-dezembro-de-2024-603297985. Acesso em: 1 jun. 2026.

21 BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). Conselho Diretor. Enunciado CD/ANPD nº 1, de 22 de maio de 2023. Dispõe acerca do tratamento de dados pessoais de crianças e adolescentes. Diário Oficial da União: seção 1, Brasília, DF, 24 maio 2023. Disponível em: https://www.in.gov.br/en/web/dou/-/enunciado-cd/anpd-n-1-de-22-de-maio-de-2023-485306934. Acesso em: 1 jun. 2026.

22 BRASIL. Secretaria de Comunicação Social da Presidência da República (SECOM). Crianças, adolescentes e telas: guia sobre uso de dispositivos digitais. Brasília, DF: Governo Federal, 2024. Disponível em: https://www.gov.br/secom/pt-br/assuntos/uso-de-telas-por-criancas-e-adolescentes/guia/guia-de-telas_sobre-usos-de-dispositivos-digitais_versaoweb.pdf. Acesso em: 1 jun. 2026.

23 BRASIL. Ministério dos Direitos Humanos e da Cidadania (MDHC). MDHC apresenta diagnóstico inédito sobre violência sexual online contra público infantojuvenil no Brasil. Brasília, DF, 2025. Disponível em: https://www.gov.br/mdh/pt-br/assuntos/noticias/2025/setembro/mdhc-apresenta-diagnostico-inedito-sobre-violencia-sexual-online-contra-publico-infantojuvenil-no-brasil. Acesso em: 1 jun. 2026.

24 BRASIL. Ministério da Justiça e Segurança Pública (MJSP). Crescer em Paz. Brasília, DF: MJSP, 2025. Disponível em: https://www.gov.br/mj/pt-br/assuntos/sua-protecao/politicas-sobre-drogas/crescer-em-paz. Acesso em: 1 jun. 2026.

2.1.2. Panorama Brasileiro Posterior ao ECA Digital

O marco legal central de proteção a crianças e adolescentes no ambiente digital é a Lei nº 15.211/2025 (Estatuto Digital da Criança e do Adolescente — ECA Digital)[25], sancionada em 17 de setembro de 2025 e vigente desde 17 de março de 2026, após vacatio legis de seis meses fixada pela Medida Provisória nº 1.319/2025[26]. O diploma dispõe sobre a proteção de crianças e adolescentes no ambiente digital e aplica-se a todo produto ou serviço de tecnologia da informação direcionado a esse público no país ou de acesso provável por ele, independentemente da localização do fornecedor. Estruturado em dezesseis capítulos, disciplina os deveres gerais de prevenção, proteção, informação e segurança dos fornecedores de produtos e serviços de tecnologia da informação; a vedação ao acesso a conteúdos impróprios, inadequados ou proibidos por lei; os mecanismos de aferição de idade; a supervisão parental; os produtos de monitoramento infantil; os jogos eletrônicos, incluindo a proibição de caixas de recompensa; a publicidade em meio digital; as redes sociais; a prevenção e o combate a violações graves contra crianças e adolescentes; o reporte de violações e os procedimentos de remoção de conteúdo; a transparência e a prestação de contas; o uso abusivo dos instrumentos de denúncia; a governança, com atribuição da fiscalização e regulamentação à ANPD; e o regime sancionatório.

No plano participativo que antecedeu e acompanhou a regulamentação, duas consultas públicas foram abertas simultaneamente em 15 de outubro de 2025 na plataforma Brasil Participativo, por iniciativa do Comitê Intersetorial para a Proteção dos Direitos da Criança e do Adolescente no Ambiente Digital, instituído pela Portaria Conjunta nº 1/2025 do Ministério dos Direitos Humanos e da Cidadania, do Ministério da Justiça e Segurança Pública e da Secretaria de Comunicação Social da Presidência da República. A primeira[27] tinha por objeto a construção da Política Nacional de Proteção dos Direitos da Criança e do Adolescente no Ambiente Digital, estabelecida pela Resolução CONANDA nº 257/2024, e a coleta de subsídios para os regulamentos derivados do ECA Digital. A

[25] BRASIL. Lei n.º 15.211, de 17 de setembro de 2026. Dispõe sobre a proteção de crianças e adolescentes em ambientes digitais (Estatuto Digital da Criança e do Adolescente)l. Brasília, DF: Presidência da República, 2025. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/l15211.htm. Acesso em: 21 maio 2026.

[26] BRASIL. Medida Provisória n.º 1.319, de 17 de setembro de 2025. Altera a Lei nº 15.211, de 17 de setembro de 2025, para dispor sobre a vigência do Estatuto Digital da Criança e do Adolescente.. Brasília, DF: Presidência da República, 2025. Disponível em: https://www.in.gov.br/en/web/dou/-/medida-provisoria-n-1.319-de-17-de-setembro-de-2025-656854355. Acesso em: 21 maio 2026.

[27] BRASIL. Secretaria-Geral da Presidência da República. Política Nacional de Proteção dos Direitos da Criança e do Adolescente no Ambiente Digital. Plataforma Brasil Participativo, [s.d.]. Disponível em: https://brasilparticipativo.presidencia.gov.br/processes/criancaeadolescenteambientedigital/f/1626/. Acesso em: 21 maio 2026.

segunda[28], conduzida pela Secretaria Nacional de Direitos Digitais (SEDIGI) do MJSP no âmbito da Estratégia Crescer em Paz, voltou-se especificamente aos mecanismos de aferição de idade, recebendo, entre 15 de outubro e 14 de novembro de 2025, mais de 70 contribuições de entidades, associações empresariais e organizações da sociedade civil. Em 3 de fevereiro de 2026, o MJSP publicou o relatório "Mecanismos de Aferição de Idade: análise das contribuições à consulta pública e subsídios para regulamentação da Lei nº 15.211/2025"[29], elaborado em parceria com a Universidade Federal do Ceará e com apoio da UNESCO, da SENACON e da ANPD.

Em 24 de dezembro de 2025, a ANPD publicou conjuntamente a Resolução CD/ANPD nº 30/2025[30], que aprova o Mapa de Temas Prioritários para Fiscalização e Atuação Regulatória para o biênio 2026-2027, e a Resolução CD/ANPD nº 31/2025[31], que atualiza a Agenda Regulatória para o período 2025-2026. A Agenda Regulatória passou a contemplar três novos temas relacionados à implementação do ECA Digital: mecanismos de aferição de idade; fornecedores de produtos ou serviços de tecnologia da informação, escopo e obrigações gerais do ECA Digital; e fiscalização e sanção do ECA Digital, com revisão das Resoluções nº 1/2021 e nº 4/2023. O item anteriormente previsto sobre tratamento de dados de crianças e adolescentes foi absorvido por essas iniciativas específicas.

Em 18 de março de 2026, no dia seguinte à entrada em vigor do ECA Digital, o Presidente da República assinou o Decreto nº 12.880/2026[32], que regulamenta a Lei nº 15.211/2025 e institui a Política Nacional de Promoção e Proteção dos Direitos da Criança e do Adolescente no Ambiente Digital. O decreto concretiza obrigações da lei, estabelece deveres específicos para fornecedores conforme seu modelo de negócio e nível de risco, e atribui à ANPD a regulamentação dos requisitos mínimos de transparência, segurança e

---

28 BRASIL. Secretaria-Geral da Presidência da República. Consulta pública sobre aferição etária em ambientes digitais. Plataforma Brasil Participativo, [s.d.]. Disponível em: https://brasilparticipativo.presidencia.gov.br/processes/idadeafericao. Acesso em: 21 maio 2026.

29 BRASIL. Ministério da Justiça e Segurança Pública. Secretaria de Direitos Digitais. Relatório da consulta pública sobre aferição de idade em ambientes digitais. Brasília, DF: MJSP, 2025. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/relatorio-sedigi-consulta-de-afericao-de-idade.pdf. Acesso em: 21 maio 2026.

30 BRASIL. Agência Nacional de Proteção de Dados. Resolução CD/ANPD n.º 30, de 23 de dezembro de 2025. Aprova o Mapa de Temas Prioritários para o biênio 2026-2027. Brasília, DF: ANPD, 2025. Disponível em: https://www.in.gov.br/web/dou/-/resolucao-cd/anpd-n-30-de-23-de-dezembro-de-2025-677947163. Acesso em: 21 maio 2026.

31 BRASIL. Agência Nacional de Proteção de Dados. Resolução CD/ANPD n.º 31, de 22 de dezembro de 2025. Altera a Agenda Regulatória para o biênio 2025-2026. Brasília, DF: ANPD, 2025. Disponível em: https://www.in.gov.br/web/dou/-/resolucao-cd/anpd-n-31-de-22-de-dezembro-de-2025-677950080. Acesso em: 21 maio 2026.

32 BRASIL. Decreto n.º 12.880, de 18 de março de 2026. Regulamenta a Lei nº 15.211, de 17 de setembro de 2025, que dispõe sobre a proteção de crianças e adolescentes em ambientes digitais, e institui a Política Nacional de Promoção e Proteção dos Direitos da Criança e do Adolescente no Ambiente Digital. Brasília, DF: Presidência da República, 2026. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/decreto/d12880.htm. Acesso em: 21 maio 2026.

interoperabilidade para os mecanismos de aferição de idade e de supervisão parental. Na mesma data, a ANPD, o MJSP e a Secretaria de Comunicação Social da Presidência da República publicaram conjuntamente documento de Perguntas e Respostas sobre o ECA Digital[33].

Em 20 de março de 2026, a ANPD publicou as Orientações Preliminares sobre Mecanismos Confiáveis de Aferição de Idade[34], apresentando parâmetros iniciais organizados em seis eixos (proporcionalidade; acurácia, robustez e confiabilidade; privacidade e proteção de dados; inclusão e não discriminação; transparência e auditabilidade; e interoperabilidade) para orientar os agentes regulados neste momento inicial de vigência da nova legislação. O documento, de caráter não definitivo, reflete a posição institucional da ANPD e servirá de referência para as atividades de monitoramento até a publicação das orientações definitivas, prevista para agosto de 2026. A ANPD estruturou seu cronograma de fiscalização em etapas: a primeira, já iniciada, prioriza lojas de aplicativos e sistemas operacionais proprietários, por seu papel estruturante na cadeia digital; a segunda, prevista para agosto de 2026, ampliará o monitoramento para outros setores a partir do nível de risco de cada produto ou serviço; a terceira, a partir de janeiro de 2027, dará início às ações de fiscalização efetiva e aplicação de sanções[35].

Em 30 de abril de 2026, a ANPD abriu tomada de subsídios sobre o Guia Orientativo "Fornecedores de Produtos ou Serviços de Tecnologia da Informação: escopo e obrigações gerais do ECA Digital", com prazo de contribuição até 15 de junho de 2026 pela plataforma Brasil Participativo[36]. O guia, de natureza orientativa, tem por objetivo esclarecer a quem a legislação se aplica e o significado dos deveres de prevenção, proteção, informação e segurança impostos aos fornecedores.

2.2. Benchmarking Internacional e Tendências Globais

[33] BRASIL. Agência Nacional de Proteção de Dados.. Perguntas e respostas: Estatuto da Criança e do Adolescente Digital (ECA Digital). Brasília, DF: ANPD, 2026. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/perguntas_respostas_eca_digital_18032026.pdf/@@display-file/file. Acesso em: 1 jun. 2026.

[34] BRASIL. Agência Nacional de Proteção de Dados. Mecanismos confiáveis de aferição de idade: orientações preliminares. Brasília, DF: ANPD, 2026. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/eca-digital/mecanismos-confiaveis-de-afericao-de-idade-orientacoes-preliminares.pdf/@@display-file/file. Acesso em: 21 maio 2026.

[35] BRASIL. Agência Nacional de Proteção de Dados. Fundamentação: mecanismos confiáveis de aferição de idade em ambientes digitais. Brasília, DF: ANPD, 2026. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/eca-digital/fundamentacao.pdf/@@display-file/file. Acesso em: 21 maio 2026.

[36] BRASIL. Secretaria-Geral da Presidência da República. Guia orientativo para fornecedores de produtos ou serviços de tecnologia da informação: escopo e obrigações gerais do ECA Digital. Plataforma Brasil Participativo, [s.d.]. Disponível em: https://brasilparticipativo.presidencia.gov.br/processes/Guia-orientativo-fonecedores-eca-digital. Acesso em: 21 maio 2026.

O benchmarking, constante no Anexo 2 deste Relatório, foi elaborado ao longo de 2025 e início de 2026, período em que o Decreto regulamentador do ECA Digital ainda não havia sido publicado e a versão final da Agenda Regulatória da ANPD para o biênio 2025–2026 ainda não estava disponível. Diante desse cenário, a análise tomou como base os dispositivos do ECA Digital que indicavam expressamente a necessidade de regulamentação futura pela ANPD, bem como a proposta de agenda regulatória revisada então em circulação, devidamente mapeados no Anexo 1 deste Relatório.

Assim, o benchmarking concentrou-se nos temas priorizados pela proposta de revisão à Agenda Regulatória 2025–2026 da ANPD, bem como das disposições do ECA Digital que contavam com indicação expressa de regulamentação futura atribuída à Agência. A partir desse mapeamento, a análise comparativa abordou três eixos principais: (i) conceitos gerais e definições; (ii) mecanismos de aferição de idade; e (iii) outros dispositivos sujeitos à regulamentação pela ANPD.

A Parte II do Relatório trata dos eixos (i) e (iii) do benchmarking. O eixo (ii), relativo aos mecanismos de aferição de idade, é objeto de análise comparativa específica, aprofundada na Parte III do presente documento. No eixo de conceitos gerais e definições, o benchmarking examina cinco temas: acesso provável de crianças e adolescentes a produtos e serviços digitais; melhor interesse da criança e do adolescente; caixa de recompensa (loot box); condição peculiar de pessoa em desenvolvimento; e categorias de conteúdo (pornográfico, impróprio, inadequado e proibido). No eixo de outros dispositivos sujeitos à regulamentação pela ANPD, são analisados nove temas: medidas de prevenção e mitigação de risco de acesso (Art. 6º, §2º); mecanismos de supervisão parental (Art. 17, §§1º e 3º); procedimento de apelação para contas suspensas (Art. 24, §4º); remoção e comunicação de violações graves (Art. 27 e §1º); notificação de violações aos direitos de crianças e adolescentes (Art. 28, parágrafo único); acesso a dados para pesquisa (Art. 31, parágrafo único); registros de uso abusivo de denúncias (Art. 33, §3º); adesivos informativos em embalagens (Art. 38); e critérios de adequação etária e modulação de obrigações (Art. 39, §1º, I e §3º).

As jurisdições selecionadas para a análise, em razão da relevância e maturidade de seus marcos regulatórios de proteção de crianças e adolescentes em ambientes digitais, são apresentadas na seção seguinte.

2.2.1. Síntese por Jurisdição

Esta seção apresenta, por jurisdição, os instrumentos normativos que integram o benchmarking internacional elaborado no âmbito do GT6 do CNPD. O objetivo é descrever

o que cada normativa é (sua natureza, sua autoridade emissora e os temas sobre os quais se debruça), de modo a oferecer uma visão panorâmica do arcabouço regulatório de cada jurisdição antes de qualquer análise comparativa aprofundada. Os instrumentos descritos são exclusivamente aqueles presentes no benchmarking. Os estados norte-americanos são reunidos em uma seção única, dada a fragmentação do modelo regulatório federal dos Estados Unidos e a complementaridade entre as legislações estaduais analisadas.

I. Austrália

O arcabouço normativo australiano é composto por instrumentos de diferentes naturezas (lei federal, norma regulatória, código setorial e instrumento de classificação), articulados em torno de uma autoridade reguladora especializada, a eSafety Commissioner, e do Office of the Australian Information Commissioner (OAIC), responsável pela dimensão de proteção de dados pessoais.

Online Safety Act 2021 (OSA AU)[37]

O Online Safety Act 2021 é a lei federal central de segurança online na Austrália. Aprovado pelo Parlamento federal em junho de 2021 e em vigor desde janeiro de 2022, ele estrutura a proteção de australianos, com ênfase especial em crianças e adolescentes, por meio de um conjunto de arranjos regulatórios específicos, cada um voltado a tipos distintos de risco ou dano online. O OSA AU cria e atribui poderes à eSafety Commissioner, incluindo a emissão de avisos de remoção com prazo de 24 horas para cumprimento, prazo que se aplica ao Cyberbullying Scheme e ao Image-Based Abuse Scheme, podendo a eSafety estipular prazo diverso quando necessário, a requisição de informações e relatórios de conformidade com as Basic Online Safety Expectations, definidas no item abaixo, (cujos intervalos, previstos no BOSE Regulatory Guidance, variam de 6 a 24 meses) e a aplicação de sanções civis por meio dos Tribunais Australianos. O OSA AU estrutura quatro fluxos de reclamação e remoção de conteúdo: o Cyberbullying Scheme (voltado especificamente a crianças), o Adult Cyber Abuse Scheme, o Image-Based Abuse Scheme e o Online Content Scheme. Este último classifica conteúdos em Class 1, subdividida em 1A e 1B, cobrindo os conteúdos ilegais mais graves como material de abuso sexual infantil (CSAM) e conteúdo terrorista, e Class 2, lícito mas restrito, como pornografia adulta classificada R18+ ou X18+, e regula sua remoção ou restrição de acesso. O conteúdo que retrata conduta violenta considerada “abominável” (abhorrent violent conduct) é tratado em regime próprio na lei, que autoriza a eSafety a requisitar o bloqueio de acesso a esse material pelos provedores de serviço de internet. As obrigações de informar pais e responsáveis sobre como

[37] AUSTRALIA. Online Safety Act 2021 (No. 76, 2021). Canberra: Federal Register of Legislation, 2021. Disponível em: https://www.legislation.gov.au/C2021A00076/latest. Acesso em: 1 jun. 2026.

supervisionar e controlar o acesso de crianças a conteúdos decorrem de padrões de indústria desenvolvidos com base na própria lei.

Basic Online Safety Expectations (BOSE) e BOSE Regulatory Guidance

As Basic Online Safety Expectations são um instrumento normativo editado pelo Ministro para Notificações, com base nos poderes conferidos pela Seção 45 do Online Safety Act. A versão original, de janeiro de 2022, foi emendada pela Online Safety (Basic Online Safety Expectations) em 2024. O BOSE Regulatory Guidance, emitido pela eSafety Commissioner e atualizado mais recentemente em fevereiro de 2026, é o documento que operacionaliza as expectativas previstas na atualização de 2024. As BOSE estabelecem expectativas mínimas de conduta para todos os provedores de serviços online com usuários na Austrália. Em relação a crianças, determinam que o melhor interesse da criança deve ser consideração primária no design e na operação de qualquer serviço de provável acesso por esse público, incluindo a obrigação de configurações de privacidade e segurança robustas por padrão, a realização de avaliações de risco à segurança infantil, o funcionamento de mecanismos eficazes de denúncia e a publicação de relatórios periódicos de transparência. O Regulatory Guidance orienta os provedores sobre o que constitui "medidas razoáveis" em cada uma das expectativas previstas e adota a definição de melhor interesse da criança a partir do Comentário Geral nº 14 do Comitê dos Direitos da Criança da ONU.

Online Safety Amendment (Social Media Minimum Age) Act 2024 (SMMA)[38] e Social Media Minimum Age Regulatory Guidance[39]

O Online Safety Amendment (Social Media Minimum Age) Act 2024 é uma lei federal que inseriu a Parte 4A no Online Safety Act 2021, aprovada pelo Parlamento em novembro de 2024 e em vigor desde 10 de dezembro de 2025. Ela estabelece uma idade mínima de 16 anos para o uso de plataformas de redes sociais qualificadas como restritas, assim definidas por critérios estruturais objetivos: propósito único ou significativo de interação social entre usuários, possibilidade de os usuários se conectarem entre si e de postarem material no serviço, e adoção de algoritmos de recomendação ou de funcionalidades específicas como recursos de feedback ou recursos por tempo limitado. Essas plataformas têm o dever de tomar "medidas razoáveis" para impedir que usuários crianças e adolescentes de até 16 anos mantenham contas, sob pena de sanções civis. As exceções

[38] AUSTRALIA. Online Safety Amendment (Social Media Minimum Age) Act 2024 (No. 127, 2024). Canberra: Federal Register of Legislation, 2024. Disponível em: https://www.legislation.gov.au/C2024A00127/latest. Acesso em: 1 jun. 2026.

[39] AUSTRALIA. eSafety Commissioner. Social Media Minimum Age Regulatory Guidance. Canberra: eSafety Commissioner, set. 2025. Disponível em: https://www.esafety.gov.au/sites/default/files/2025-09/eSafety-SMMA-Regulatory-Guidance.pdf. Acesso em: 1 jun. 2026.

ao regime foram definidas pelo Ministro para Comunicações por meio das Normas de Online Safety (Age-Restricted Social Media Platforms) de 2025, editadas em julho de 2025 com base em recomendação da eSafety Commissioner. Estão excluídas do escopo, entre outras, plataformas cujo propósito único ou primário seja mensageria, jogos, networking profissional, educação ou saúde. O complemento operacional da lei é o Social Media Minimum Age Regulatory Guidance, emitido pela eSafety Commissioner em setembro de 2025, que diferencia três categorias de mecanismos de aferição de idade, estimativa de idade, inferência de idade e verificação de idade, lista mecanismos insuficientes como a autodeclaração e estabelece princípios orientadores para a escolha de soluções: confiabilidade, precisão, robustez, preservação da privacidade, acessibilidade, transparência e proporcionalidade. O Guidance orienta ainda que a aferição não se limita ao momento do cadastro, devendo ocorrer também em relação a contas preexistentes e de forma contínua ao longo da jornada do usuário.

Privacy and Other Legislation Amendment Act 2024[40] *e Children's Online Privacy Code*[41]

O Privacy and Other Legislation Amendment Act 2024 é uma lei federal aprovada pelo Parlamento australiano em 29 de novembro de 2024 que, entre outras alterações ao Privacy Act australiano, introduziu o mandato para o OAIC elaborar um Children's Online Privacy Code. O Código foi publicado em 31 de março de 2026 para consulta pública de 60 dias e deve ser registrado até 10 de dezembro de 2026, com data de entrada em vigor ainda a ser determinada. Trata-se de instrumento que especifica como as obrigações das Australian Privacy Principles devem ser aplicadas em relação a dados pessoais de crianças e adolescentes, com exigências adicionais: as entidades abrangidas deverão considerar o melhor interesse da criança e adolescentes antes de coletar, usar ou divulgar seus dados, obter consentimento para publicidade direcionada baseada em dados de crianças e adolescentes e permitir que crianças e adolescentes requisitem a exclusão de suas informações. O Código é aplicável a provedores de serviços de mídia social, serviços eletrônicos relevantes e serviços de Internet designados, conforme definidos no Online Safety Act 2021, cujos serviços sejam de provável acesso por crianças e adolescentes ou sejam primariamente voltados às atividades de crianças e adolescentes. O processo de elaboração envolveu três fases de consulta: fase 1 com crianças, adolescentes, pais e organizações de bem-estar infantil (janeiro a agosto de 2025), fase 2 com indústria,

[40] AUSTRALIA. Privacy and Other Legislation Amendment Act 2024 (No. 128, 2024). Canberra: Federal Register of Legislation, 2024. Disponível em: https://www.legislation.gov.au/C2024A00128/latest. Acesso em: 1 jun. 2026.

[41] AUSTRALIA. Office of the Australian Information Commissioner (OAIC). Children's Online Privacy Code. Canberra: OAIC, 2026. Disponível em: https://www.oaic.gov.au/privacy/privacy-registers/privacy-codes/childrens-online-privacy-code. Acesso em: 1 jun. 2026.

sociedade civil e academia (abril a agosto de 2025) e fase 3 de consulta pública sobre o projeto do Código (março a junho de 2026).

Online Safety Codes and Standards Regulatory Guidance[42]

Os Online Safety Codes and Standards são instrumentos regulatórios previstos na Parte 9 do Online Safety Act 2021 para regular o acesso a conteúdos ilegais e restritos por faixa etária. Eles foram desenvolvidos em duas fases. A Fase 1, concluída em 2023 e 2024, produziu os Unlawful Material Codes and Standards, voltados a conteúdo Class 1A e 1B, como CSAM e conteúdo terrorista, aplicáveis a oito setores da indústria online. A Fase 2, concluída em 2025, produziu os Age-Restricted Material Codes, voltados a conteúdo Class 1C e Class 2, incluindo pornografia adulta, com o objetivo específico de impedir que crianças acessem esse tipo de material. Os Códigos são elaborados pelas próprias associações da indústria e registrados pela eSafety Commissioner após avaliação de sua adequação. Quando um código submetido não satisfaz os requisitos legais de proteção, a eSafety tem poder de determinar um padrão de indústria diretamente, sem participação da indústria na elaboração da minuta como ocorreu com os padrões para Relevant Electronic Services e Designated Internet Services na Fase 1. Uma vez registrados, tanto códigos quanto padrões são obrigatórios e sujeitos a enforcement. O documento Online Safety Codes and Standards Regulatory Guidance, emitido pela eSafety Commissioner em dezembro de 2025, orienta a aplicação prática desses instrumentos, descrevendo o perfil de risco dos serviços regulados e as exigências correspondentes.

Guidelines for the Classification of Computer Games[43]

As Guidelines for the Classification of Computer Games integram o Sistema de Classificação Nacional Australiano e passaram por alterações significativas. Elas determinam como jogos eletrônicos devem ser classificados com base em seu conteúdo, incluindo a presença de mecânicas como loot boxes e jogos de azar simulados. As alterações foram motivadas por pesquisa do Australian Institute of Family Studies que identificou associação entre loot boxes e comportamentos de jogo compulsivo, encontrando que jovens que jogam jogos de apostas simuladas eram 40% mais propensos a gastar dinheiro real em apostas na vida adulta. As diretrizes passaram a exigir classificação mínima M (não recomendado para crianças e adolescentes de 15 anos) para jogos que contenham compras vinculadas a elementos de acaso com moeda real ou virtual

[42] AUSTRALIA. eSafety Commissioner. Online Safety Industry Codes. Canberra: eSafety Commissioner, 2026. Disponível em: https://www.esafety.gov.au/industry/codes. Acesso em: 1 jun. 2026.

[43] AUSTRALIA. Guidelines for the Classification of Computer Games 2023. Canberra: Federal Register of Legislation, 2023. Disponível em: https://www.legislation.gov.au/F2023L01424/latest/text. Acesso em: 1 jun. 2026.

adquirida com dinheiro real, e classificação R18+ para jogos com qualquer forma de jogo de azar simulado interativo, como social casino games. A classificação M é meramente indicativa, enquanto a R18+ é juridicamente vinculante e restringe legalmente a venda a adultos. As alterações não se aplicam retroativamente a jogos já classificados antes de 22 de setembro de 2024, salvo se a classificação for revogada ou modificada por outro motivo.

Data Availability and Transparency Act 2022 (DATA Scheme)[44]

O Data Availability and Transparency Act 2022 institui um regime estruturado de compartilhamento de dados do setor público com entidades acreditadas, órgãos governamentais da Commonwealth, dos estados e territórios e universidades australianas públicas, para três finalidades permitidas: entrega de serviços governamentais, formulação de políticas e programas, e pesquisa e desenvolvimento. Os dados compartilhados são exclusivamente dados do setor público federal, detidos por órgãos do Commonwealth que atuam como custodiantes de dados. A acreditação de órgãos governamentais é função do Ministério; a acreditação de universidades e de provedores de serviços de dados credenciados é função da Autoridade de Proteção de Dados que também regula e fiscaliza o sistema. O compartilhamento é formalizado por acordos de compartilhamento de dados registrados. Entidades privadas, pessoas físicas e entidades estrangeiras estão excluídas do esquema. O DAT Act contém uma cláusula de transição que fará a legislação deixar de estar em vigor em 1º de abril de 2027 sem necessidade de nova medida legislativa; a revisão obrigatória da lei concluída em 2026 recomendou sua extensão e a ampliação do escopo para incluir institutos de pesquisa médica e organizações sem fins lucrativos confiáveis.

Consumer Goods (Infant Products) Information Standard 2024[45] *e Consumer Goods (Products Containing Button/Coin Batteries) Information Standard 2020*[46]

Esses dois instrumentos regulatórios foram editados com base no Australian Consumer Law (ACL), que é o Anexo 2 do Competition and Consumer Act 2010, e estabelecem obrigações de rotulagem em embalagens de produtos físicos. O Consumer Goods (Infant Products) Information Standard 2024 cobre produtos destinados a bebês,

---

[44] AUSTRALIA. Office of the National Data Commissioner (ONDC). The DATA Scheme. Canberra: ONDC, 2026. Disponível em: https://www.datacommissioner.gov.au/data-scheme. Acesso em: 1 jun. 2026.

[45] AUSTRALIA. Parliament of Western Australia. Joint Standing Committee on the Commissioner for Children and Young People: Annual Report 2023–2024. Tabled Paper n. 3043. Perth: Parliament of Western Australia, 2024. Disponível em: https://www.parliament.wa.gov.au/publications/tabledpapers.nsf/displaypaper/4113043a726fd07c539991a148258b94001bde8d/$file/tp+3043+(2024).pdf. Acesso em: 1 jun. 2026.

[46] AUSTRALIA. Parliament of Western Australia. Joint Standing Committee on the Commissioner for Children and Young People: Annual Report 2020–2021. Tabled Paper n. 122. Perth: Parliament of Western Australia, 2021. Disponível em: https://www.parliament.wa.gov.au/publications/tabledpapers.nsf/displaypaper/4110122c666eb7378db348f9482586cc0004f5d0/$file/tp-122.pdf. Acesso em: 1 jun. 2026.

com ênfase em produtos de sono infantil e itens de uso nos primeiros meses de vida, e exige avisos obrigatórios no produto, na embalagem e nos pontos de oferta, inclusive em descrições de produtos em ambientes de comércio eletrônico. O Consumer Goods (Products Containing Button/Coin Batteries) Information Standard 2020 regula produtos que contenham baterias de botão ou moeda, impondo avisos com símbolo internacional de segurança e texto específico sobre os riscos que essas baterias representam para crianças pequenas caso ingeridas. Ambos são referenciados no benchmarking no contexto do art. 38 do ECA Digital, que prevê adesivos informativos em embalagens de equipamentos eletrônicos, como exemplo de instrumento de rotulagem física voltado à proteção de crianças em ambiente de consumo.

II. Estados Unidos

Com exceção de alguns temas específicos do benchmarking que remetem a normas federais, a análise concentra-se nas legislações estaduais, que têm avançado de forma mais ambiciosa na regulação do tema. Os quatro estados analisados são Califórnia, Louisiana, Texas e Utah.

Em que pese a existência de diversas legislações estaduais avançando nos EUA com relação a esse tema, importante destacar que, em sua grande maioria, tais legislações não estão em vigor, seja em virtude da data de vigência que ainda não foi atingida, seja em virtude de disputas judiciais que suspenderam a aplicação das leis.

Children's Online Privacy Protection Act (COPPA) — Federal[47]

A COPPA é a principal lei federal de proteção de crianças no ambiente digital, aprovada em 1998 e em vigor desde abril de 2000, administrada pela Federal Trade Commission (FTC). Aplica-se a fornecedores de serviços online direcionados a crianças e adolescentes de até 13 anos ou que tenham conhecimento efetivo de que coletam dados pessoais de crianças e adolescentes dessa faixa etária. Exige notificação aos pais, mães e responsáveis legais, sobre as práticas de coleta, consentimento parental verificável antes da coleta, uso ou divulgação de dados da criança, direito de os pais revisarem e solicitarem a exclusão das informações coletadas, e vedação à exigência de que a criança forneça mais informações do que o razoavelmente necessário para participar de uma atividade. É referenciada no benchmarking como ponto de comparação para a definição de acesso provável e para o regime de consentimento parental.

47 UNITED STATES. Federal Trade Commission (FTC). Children's Online Privacy Protection Rule ("COPPA Rule"). Washington, DC: Federal Trade Commission, 2026. Disponível em: https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa. Acesso em: 1 jun. 2026.

Children's Internet Protection Act (CIPA) — Federal[48]

O CIPA é uma lei federal aprovada em dezembro de 2000 que condiciona o recebimento de dois tipos específicos de financiamento federal por escolas públicas e bibliotecas à adoção de uma política de internet segura e à implementação de medidas tecnológicas de proteção que bloqueiem ou filtrem o acesso a imagens obscenas, pornografia infantil e conteúdo prejudicial a crianças e adolescentes. A filtragem aplica-se apenas a representações visuais, não a textos. Para usuários adultos, o bloqueio deve poder ser desativado mediante solicitação para fins de pesquisa legítima. O CIPA expressamente não exige o rastreamento ou monitoramento do uso da internet por alunos ou adultos. Essa Lei é referenciada no benchmarking em relação a temas de supervisão parental e proteção de crianças e adolescentes no contexto escolar, com a ressalva de que não define padrões técnicos aplicáveis fora desse contexto.

18 U.S.C. §§ 2256[49] *e 2258A*[50] *— Federal*

O § 2256 do Título 18 do Código dos Estados Unidos define pornografia infantil como qualquer representação visual de conduta sexualmente explícita envolvendo uma criança ou adolescente, abrangendo fotografias, vídeos, imagens digitais ou geradas por computador indistinguíveis de uma criança ou adolescente real, e imagens criadas, adaptadas ou modificadas para fazer parecer que uma criança ou adolescente identificável está praticando conduta sexualmente explícita. A conduta sexualmente explícita inclui tanto atos reais quanto simulados. O § 2258A impõe aos provedores de serviços de comunicação eletrônica e de computação remota a obrigação de reportar, o mais rápido possível após obterem conhecimento efetivo, à CyberTipline do National Center for Missing & Exploited Children (NCMEC) qualquer fato ou circunstância indicativo de aparente violação das normas federais sobre pornografia infantil. O NCMEC repassa os relatórios às autoridades policiais competentes. O REPORT Act de 2024 expandiu as obrigações do § 2258A, ampliando o escopo das violações reportáveis para incluir tráfico sexual de crianças e adolescentes e aliciamento, e estendendo o prazo obrigatório de preservação de evidências de 90 dias para 1 ano.

---

[48] UNITED STATES. Federal Communications Commission (FCC). Children's Internet Protection Act (CIPA). Washington, DC: FCC, 2026. Disponível em: https://www.fcc.gov/consumers/guides/childrens-internet-protection-act. Acesso em: 1 jun. 2026.

[49] UNITED STATES. 18 U.S.C. § 2256 – Definitions for chapter. In: UNITED STATES. United States Code. Washington, DC: Office of the Law Revision Counsel, U.S. House of Representatives. Disponível em: https://www.law.cornell.edu/uscode/text/18/2256. Acesso em: 1 jun. 2026.

[50] UNITED STATES. 18 U.S.C. § 2258A – Reporting requirements of providers. In: UNITED STATES. United States Code. Washington, DC: Office of the Law Revision Counsel, U.S. House of Representatives. Disponível em:https://www.law.cornell.edu/uscode/text/18/2258A. Acesso em: 1 jun. 2026.

California Age-Appropriate Design Code Act — AB 2273 (Califórnia, 2022)[51]

A Assembly Bill (AB) 2273 é uma lei estadual californiana sancionada em setembro de 2022, inspirada no Age Appropriate Design Code britânico. Aplica-se a qualquer empresa que ofereça serviços, produtos ou funcionalidades online que crianças, definidas como crianças e adolescentes de 18 anos, "provavelmente acessem". O critério de acesso provável é definido em seis hipóteses alternativas: serviços direcionados a crianças nos termos da COPPA; serviços acessados rotineiramente por número significativo de crianças com base em evidências de audiência; serviços com publicidade direcionada a crianças; serviços substancialmente similares a outros frequentados por crianças; serviços com elementos de design de interesse infantil; e serviços em que pesquisas internas da empresa identificam crianças no público. A lei exige a elaboração de relatórios de impacto a proteção de dados antes de lançar ou atualizar serviços, privacidade por padrão, proibição de uso de dados pessoais de crianças de forma prejudicial ao seu bem-estar, vedação de técnicas de extensão de engajamento prejudiciais a crianças e adolescentes, e disponibilização de ferramentas parentais visíveis, acessíveis e responsivas. Exige ainda que as empresas considerem cinco faixas etárias de desenvolvimento (0–5; 6–9; 10–12; 13–15; 16–17) no design de seus produtos. Esta lei enfrenta contestação judicial desde 2022: em setembro de 2023, o Tribunal Distrital Federal bloqueou sua aplicação por meio de liminar, por considerar que o requisito de relatório de impacto poderia representar uma violação da primeira emenda a Constituição Americana; em agosto de 2024, o poder judiciário americano manteve a liminar apenas quanto ao requisito de elaboração de relatório de impacto e remeteu a nova análise das demais disposições ao Tribunal Distrital, de forma que a aplicação integral da lei permanecia suspensa pendente de decisão final ao tempo do benchmarking.

Digital Age Assurance Act — AB 1043 (Califórnia, vigente a partir de 2027)[52]

A Assembly Bill (AB) 1043, sancionada em outubro de 2025, institui um modelo de aferição de idade baseado em sinais transmitidos por sistemas operacionais e, subsidiariamente, por lojas de aplicativos. Provedores de sistema operacional são obrigados a disponibilizar, no momento da configuração do dispositivo ou da conta, uma interface pela qual o titular da conta informa a data de nascimento ou a idade do usuário, por autodeclaração, sem exigência de documento de identidade ou verificação biométrica.

---

[51] CALIFORNIA (ESTADOS UNIDOS). California Age-Appropriate Design Code Act (Assembly Bill 2273). Sacramento, CA: California Legislative Information, 2022. Disponível em: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB2273. Acesso em: 1 jun. 2026.

[52] CALIFORNIA (ESTADOS UNIDOS). Digital Age Assurance Act (Assembly Bill 1043 – AB 1043). Sacramento, CA: California Legislative Information, 2025. Vigência a partir de 1 jan. 2027. Disponível em: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202520260AB1043. Acesso em: 1 jun. 2026.

Com base nessa informação, o sistema operacional deriva um sinal de faixa de idade indicando em qual das quatro faixas etárias o usuário se enquadra como pessoa com: menos de 13, de 13 a 16 incompletos, de 16 completos a menos de 18 ou 18 ou mais. Esse sinal deve ser transmitido via API em tempo real ao desenvolvedor que o solicitar quando o aplicativo for baixado ou iniciado. As lojas de aplicativos não estão obrigadas a coletar idade, mas são presumidas capazes de fornecer sinais aos desenvolvedores. O desenvolvedor que receber o sinal deve tratá-lo como indicador primário da faixa etária do usuário, a menos que disponha de informação interna clara e convincente indicando faixa etária diferente. O sinal não pode ser compartilhado com terceiros para finalidades alheias ao cumprimento da lei. A lei entra em vigor em 1º de janeiro de 2027, com prazo de adequação até 1º de julho de 2027 para dispositivos configurados antes dessa data. O enforcement é exclusivo do Procurador-Geral da Califórnia, sem direito privado de ação. Dito de outra forma, não é possivel que pessoas questionem esse aspecto da lei de maneira individual.

California Assembly Bill 3080 (Califórnia)[53]

A Assembly Bill (AB) 3080 é um projeto de lei californiano introduzido em 2024 que integra a Parent's Accountability and Child Protection Act e propõe estender às plataformas de pornografia online a obrigação de adotar medidas razoáveis de verificação de idade para impedir o acesso de crianças e adolescentes. O projeto define “site pornográfico na internet” como aquele em que o proprietário, com fins comerciais, publica conscientemente conteúdo sexualmente explícito que exceda um terço do conteúdo total do site anualmente, e define “conteúdo sexualmente explícito” como imagens visuais de atos de masturbação, relação sexual, sexo oral ou outra conduta sexualmente explícita que, consideradas em seu conjunto, carecem de valor literário, artístico, político ou científico sério. O projeto passou unanimemente pela Assembleia, mas foi arquivado pelo Comitê de Apropriações do Senado em agosto de 2024, sem se tornar lei. É referenciado no benchmarking no contexto da definição de conteúdo pornográfico na jurisdição californiana, apesar de seu status de projeto não convertido em lei.

California Assembly Bill 1831 — CHAPTER 926 (Califórnia, 2024)[54]

53 CALIFORNIA (ESTADOS UNIDOS). Assembly Bill No. 3080 (AB 3080) – The Parent’s Accountability and Child Protection Act. Sacramento, CA: California State Legislature, 2024. Disponível em: https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240AB3080. Acesso em: 1 jun. 2026.

54 CALIFORNIA (ESTADOS UNIDOS). Assembly Bill No. 1831 (AB 1831), Chapter 926, Statutes of 2024. Sacramento, CA: California State Legislature, 2024. Disponível em: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240AB1831. Acesso em: 1 jun. 2026.

A Assembly Bill (AB) 1831 é uma lei penal californiana sancionada em setembro de 2024 que amenda o Penal Code do estado para expandir o escopo das proibições existentes sobre pornografia infantil ao conteúdo digitalmente alterado ou gerado por inteligência artificial. A lei parte da proibição preexistente, que cobre a produção, desenvolvimento, duplicação, distribuição e posse de material que retrate pessoa com menos de 18 anos praticando ou simulando conduta sexual, e a estende expressamente ao material equivalente produzido por IA, incluindo representações de pessoas reais ou fictícias geradas por software de inteligência artificial que sejam, ou que uma pessoa razoável consideraria serem, representações de crianças e adolescentes de 18 anos praticando ou simulando conduta sexual. Para preservar proteções da Primeira Emenda, a lei exige que o material gerado por IA se enquadre na definição de obscenidade do estado, que adota o teste Miller: apelo ao interesse lascivo segundo padrões estaduais contemporâneos, descrição ou representação de conduta sexual de forma patentemente ofensiva, e ausência de valor literário, artístico, político ou científico sério. É referenciada no benchmarking no contexto da definição de conteúdo pornográfico infantil, com particular relevância para a quesãot do CSAM sintético ou gerado por IA.

HB 61 (Act 308) — Louisiana (2023)[55], SB 162 (Act 440) — Louisiana (2023)[56] e HB 577 — Louisiana (2024)[57]

A House Bill (HB) 61 de 2023, codificada como R.S. 9:2717.1 (Act 308), exige o consentimento do representante legal da criança ou adolescente, definido como autorização escrita do pai, mãe ou tutor, para que um serviço interativo de computador celebre contrato ou acordo com pessoa com menos de 18 anos, incluindo a criação de conta online. O conceito de "interactive computer service" é amplo, abrangendo qualquer serviço que forneça ou permita acesso a um servidor por múltiplos usuários, incluindo serviços de acesso à internet. A lei entrou em vigor em agosto de 2024 e contratos celebrados sem o consentimento parental exigido são nulos relativamente, podendo ser rescindidos unilateralmente pelo pai ou representante legal. Na mesma sessão legislativa de 2023, foi aprovada a Senate Bill (SB) 162 (Act 440), a Secure Online Child Interaction and Age Limitation Act, que impõe obrigações específicas a plataformas de mídia social com mais de 5 milhões de usuários globais, incluindo verificação de idade e consentimento parental para crianças e adolescentes de 16 anos, restrições de mensagens e vedação de

[55] LOUISIANA (ESTADOS UNIDOS). House Bill 61 (HB 61), Act 308 of 2023. Baton Rouge, LA: Louisiana State Legislature, 2023. Disponível em: https://legis.la.gov/legis/BillInfo.aspx?i=243893. Acesso em: 1 jun. 2026.

[56] LOUISIANA (ESTADOS UNIDOS). Senate Bill 162 (SB 162), Act 440 of 2023. Baton Rouge, LA: Louisiana State Legislature, 2023. Disponível em: https://www.legis.la.gov/Legis/BillInfo.aspx?s=23RS&b=SB162. Acesso em: 1 jun. 2026.

[57] LOUISIANA (ESTADOS UNIDOS). House Bill 577 (HB 577). Baton Rouge, LA: Louisiana State Legislature, 2024. Disponível em:https://www.legis.la.gov/legis/BillInfo.aspx?s=24rs&b=HB577&sbi=y. Acesso em: 1 jun. 2026.

publicidade baseada em dados do usuário. Em dezembro de 2025, a Senate Bill (SB) 162 foi declarada inconstitucional pelo tribunal federal por violação da Primeira Emenda, em ação proposta pela NetChoice. A House Bill (HB) 577, sancionada em junho de 2024, emendou a Senate Bill (SB) 162 para incluir vedação expressa de targeted advertising para crianças e adolescentes de 16 anos e adiou sua data de vigência para julho de 2025. O benchmarking referencia esses instrumentos principalmente no contexto da definição de conteúdo prejudicial a crianças e adolescentes e dos regimes de verificação de idade e consentimento parental.

HB 570 — Louisiana (2025)[58] e Louisiana Revised Statutes, Title 51, Chapter 32-B[59]

A House Bill (HB) 570 de 2025 vigente a partir de 1º de julho de 2026, codificada como R.S. 51:1771–1775, é a Lei de Proteção de Crianças em Aplicativos de Louisiana. Ela regula lojas de aplicativos e os aplicativos distribuídos por elas, exigindo aferição de idade por métodos comercialmente confiáveis no momento em que um usuário cria uma conta com um provedor de loja de aplicativos, baixa um aplicativo ou realiza compras in-app. Se o processo identifica o usuário como pessoa com menos de 18 anos, a conta deve ser afiliada a uma "parent account" (conta de um pai ou responsável) e o provedor deve obter consentimento parental verificável, bem como notificar os pais sobre mudanças significativas nos aplicativos. Os desenvolvedores devem verificar categorias etárias por meio dos dados compartilhados pelas lojas, aplicar padrões de indústria para classificação de conteúdo e adotar medidas de segurança adequadas à faixa etária. A lei proíbe que contratos com crianças e adolescentes sejam impostos sem consentimento parental verificado e autoriza o Procurador Geral (Attorney General) a aplicar multas de até $10.000 por violação, após período de cura de 45 dias. O Capítulo 32-B do Título 51 das Louisiana Revised Statutes, instrumento distinto e preexistente, regula a publicação e distribuição comercial de material prejudicial a crianças e adolescentes, exigindo que sites de conteúdo adulto utilizem métodos comercialmente razoáveis de verificação de idade, sendo a simples autodeclaração expressamente afastada.

[58] LOUISIANA (ESTADOS UNIDOS). House Bill 570 (HB 570), Act No. 481 of 2025 – Protection of Children on Applications Act. Baton Rouge, LA: Louisiana State Legislature, 2025. Disponível em: https://www.legis.la.gov/legis/ViewDocument.aspx?d=1425304. Acesso em: 1 jun. 2026

[59] LOUISIANA (ESTADOS UNIDOS). Louisiana Revised Statutes, Title 51, Chapter 32-B – Commercial Publication and Distribution of Material Harmful to Minors. Baton Rouge, LA: Louisiana State Legislature. Disponível em: https://legis.la.gov/legis/Law.aspx?d=119062. Acesso em: 1 jun. 2026.

Texas Business & Commerce Code, Chapter 509[60] e HB 18 (SCOPE Act), Texas (2023)[61]

O SCOPE Act (Securing Children Online through Parental Empowerment Act) é a lei texana de proteção de crianças e adolescentes em serviços digitais. Aplica-se a qualquer website, aplicativo, programa ou software dotado de conectividade à internet que colete ou processe dados pessoais de seus usuários, com exceções para: pequenas empresas; entidades sujeitas à HIPAA (Health Insurance Portability and Accountability Act) e à GLBA (Gramm-Leach-Bliley Act). Seu modelo central não é de aferição de idade, mas de registro: o provedor deve registrar a idade informada pelo usuário ao criar uma conta. A partir do momento em que o usuário se registra como pessoa com menos de 18 anos, ou em que um pai ou responsável notifica ou contesta com sucesso o registro, o provedor deve tratá-lo como "sabidamente menor de idade" e aplicar um conjunto de obrigações tais como: estratégia documentada de prevenção à exposição a conteúdo nocivo, com filtragem tecnológica, hash-sharing e banco de dados de keywords de evasão de filtros; ferramentas parentais com controle de configurações, restrição de compras e monitoramento do tempo de uso; e restrições de publicidade comportamental. A aplicação de penalidades civis é exclusivo do Procurador-Geral do Texas; pais e responsáveis de known minors podem, contudo, propor ação individual buscando uma decisão declaratória ou liminar, sendo vedada a certificação de class action. A lei enfrenta contestação judicial ativa: em agosto de 2024, tribunal federal bloqueou provisoriamente as disposições de monitoramento e filtragem por violação provável da Primeira Emenda a constituição americana; em fevereiro de 2025, uma segunda liminar bloqueou também as restrições de publicidade e a exigência de verificação de idade, permanecendo as demais disposições em vigor.

Utah Code, Title 13, Chapter 63 — Social Media Regulation Act[62] (SB 152 e HB 311), Utah (2023) — revogado e substituído em 2024

O Social Media Regulation Act de Utah foi aprovado em março de 2023 por meio das leis Senate Bill (SB) 152 e House Bill (HB) 311, tornando Utah o primeiro estado a aprovar legislação regulando o acesso de crianças e adolescentes a plataformas de mídia social. A SB 152 regulava especificamente plataformas de mídia social, definidas como fóruns online que permitem criação de perfil, upload de publicações, visualização de publicações de

[60] TEXAS (ESTADOS UNIDOS). Texas Business & Commerce Code, Chapter 509 – Use of Digital Services by Minors. In: TEXAS. Business and Commerce Code. Austin, TX: Texas Legislature, 2023. Disponível em: https://tcss.legis.texas.gov/resources/BC/pdf/BC.509.pdf. Acesso em: 1 jun. 2026.

[61] TEXAS (ESTADOS UNIDOS). House Bill 18 (HB 18) – Securing Children Online through Parental Empowerment (SCOPE) Act. Austin, TX: Texas Legislature, 2023. Disponível em: https://www.legis.state.tx.us/tlodocs/88R/billtext/html/HB00018F.htm. Acesso em: 1 jun. 2026.

[62] UTAH (ESTADOS UNIDOS). Utah Code, Title 13, Chapter 63 – Social Media Regulation Act. Salt Lake City, UT: Utah State Legislature, 2023. Instituído por SB 152 e HB 311; posteriormente revogado e substituído em 2024. Disponível em: https://le.utah.gov/xcode/Title13/Chapter63/C13-63_2023050320230503.pdf. Acesso em: 1 jun. 2026.

outros usuários e interação entre usuários, exigindo aferição obrigatória de idade, proibindo a simples autodeclaração, e consentimento parental verificado para crianças e adolescentes de 18 anos. O Regulamento administrativo R 152-63, editado pela Utah Division of Consumer Protection, detalhava os métodos aceitáveis de aferição: validação de dados de assinante de celular, autenticação dinâmica baseada em conhecimento aprovada pela FTC, estimativa com base na data de criação da conta, consulta dos últimos quatro dígitos do número de seguridade social em base de dados de terceiros, credencial digital, estimativa por caracterização ou análise facial, e correspondência de documento de identidade governamental com foto ao vivo por webcam ou presença física. Ainda em 2023 e 2024, o regime foi contestado judicialmente pela NetChoice por violação da Primeira Emenda da constituição americana. Em resposta aos questionamento judiciais o legislativo de Utah revogou integralmente a SB 152 e a HB 311 em março de 2024, substituindo-as pelo Utah Minor Protection in Social Media Act, aprovado por meio das leis SB 194 e HB 464. O novo regime, também contestado judicialmente, foi suspenso por liminar em setembro de 2024. O benchmarking referencia a SB 152 e o Regulamento R 152-63 como o quadro normativo de Utah vigente à época de sua elaboração, reconhecendo que os instrumentos foram posteriormente revogados.

III. Índia

A Índia não dispõe de uma lei específica de proteção de crianças no ambiente digital. O arcabouço normativo relevante é fragmentado entre uma lei geral de proteção de dados pessoais, regras de governança de intermediários digitais, legislação setorial de jogos online e uma política nacional para a infância. No entanto, a Índia foi considerada tendo em vista o seu sistema de identificação digital conhecido por Aadhaar. Esse sistema adotado em larga escala fornece um identificador seguro por meio de tecnologia biométrica. Tal sistema é regulado pela Unique Identification Authority of India (UIDAI).

Digital Personal Data Protection Act 2023 (DPDPA)[63]

O DPDPA é a lei geral de proteção de dados pessoais da Índia, aprovada em 2023. Essa lei define criança como qualquer indivíduo com menos de 18 anos e exige que as entidades custodiantes dos dados obtenham consentimento parental verificável antes de processar dados de crianças e adolescentes. Além do consentimento, a lei proíbe expressamente tracking, monitoramento comportamental e publicidade direcionada a crianças e adolescentes de 18 anos, mesmo quando o consentimento parental foi obtido. O governo central pode, por notificação, reduzir o limiar etário de 18 para 16, 13 ou outro

63 INDIA. The Digital Personal Data Protection Act, 2023 (No. 22 of 2023). New Delhi: Ministry of Law and Justice, 11 ago. 2023. Disponível em: https://dpdpact2023.com/. Acesso em: 1 jun. 2026.

número adequado para classes específicas de custodiantes que processem dados de forma "verifiably safe", e pode estabelecer isenções para certas finalidades, como serviços de saúde. As DPDP Rules 2025, publicadas em 2025, operacionalizam a lei e estabelecem os mecanismos de verificação da identidade parental, com as exigências de consentimento entrando em vigor 18 meses após a publicação das Rules, previsto para maio de 2027.

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 (IT Rules), atualizadas em 2023[64]

As IT Rules são normas regulatórias editadas com base no Information Technology Act 2000, em sua versão original de 2021 pelo Ministério da Eletrônica e Tecnologia da Informação (MeitY) e pelo Ministério da Informação e Radiodifusão (MIB), e atualizadas pela emenda de 6 de abril de 2023. Estabelecem obrigações de due diligence para intermediários digitais, plataformas de redes sociais, serviços de streaming, serviços de mensageria e distribuidoras de conteúdo online. Em relação a crianças, proíbem a hospedagem ou transmissão de qualquer conteúdo obsceno, pornográfico ou indecente, e impõem a notificação imediata da autoridade criminal competente quando o conteúdo envolver crimes contra crianças ou adolescentes. A emenda de 2023, administrada pelo MeitY, introduziu um regime específico para jogos online, exigindo a criação de órgãos de auto regulação (SRBs) responsáveis por estabelecer frameworks de verificação de jogos, incluindo salvaguardas com controles parentais, mecanismos de classificação etária e medidas de proteção contra vício, regime esse que foi posteriormente substituído pela Promotion and Regulation of Online Gaming Act 2025, aprovada pelo Parlamento indiano. A Parte III das IT Rules, administrada pelo MIB, estabelece diretrizes de classificação indicativa para conteúdo audiovisual online sob curadoria editorial em cinco faixas: U (universal), U/A 7+, U/A 13+, U/A 16+ e A (apenas adultos), considerando contexto, tema, tom, impacto e audiência-alvo. Plataformas são obrigadas a implementar travas parentais para conteúdo classificado como U/A 13+ ou superior, e mecanismos confiáveis de verificação de idade para conteúdo classificado como A.

Lei de Promoção e Regulamentação dos Jogos Online 2025 (PROG)[65]

64 INDIA. Ministry of Electronics and Information Technology (MeitY). Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. New Delhi: Government of India, 2021. Disponível em: https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf.. Acesso em: 1 jun. 2026.

65 INDIA. The Promotion and Regulation of Online Gaming Act, 2025 (Act No. 32 of 2025). New Delhi: Ministry of Electronics and Information Technology, 2025. Disponível em: https://www.meity.gov.in/static/uploads/2025/10/8a7f103cefc68ed8aaa2ebc9a2ed7c13.pdf. Acesso em: 1 jun. 2026.

A PROG, aprovada pelo Parlamento indiano em agosto de 2025 e operacionalizada pelas PROG Rules 2026, publicadas em 22 de abril de 2026 e em vigor desde 1º de maio de 2026, regula o setor de jogos online na Índia. A lei classifica os jogos online em três categorias: e-sports (jogos competitivos baseados em habilidade), online social games (jogos não monetários voltados a entretenimento ou interação) e online money games, estes últimos completamente proibidos, incluindo sua oferta, publicidade e processamento de transações financeiras relacionadas. A lei substitui o regime de órgãos de auto regulação introduzido pela emenda de 2023 às IT Rules e cria um regulador centralizado, a Online Gaming Authority of India (OGAI), vinculada ao MeitY. Em relação a crianças e adolescentes, a PROG exige verificação de identidade e idade antes do acesso, proíbe publicidade direcionada a crianças e adolescentes e determina que as mensagens publicitárias incluam avisos sobre jogo responsável. As PROG Rules 2026 tornam obrigatórios para os provedores de serviços registrados: verificação etária, classificação etária, controles parentais, restrições de tempo de uso, ferramentas de reporte e suporte de aconselhamento para questões de vício.

National Policy on Children 2013[66]

A National Policy for Children 2013 é um documento de política pública do governo federal indiano aprovado em abril de 2013, que estabelece princípios orientadores para todas as políticas e legislações relacionadas à infância. Afirma o interesse superior da criança como preocupação primordial nas decisões de órgãos legislativos, tribunais, autoridades administrativas e instituições públicas e privadas. Adota o princípio das capacidades em evolução, determinando que as vozes e opiniões das crianças sejam consideradas em todas as matérias que as afetam, em especial em procedimentos judiciais e administrativos, conforme sua idade, maturidade e capacidades em desenvolvimento. Estabelece abordagem de ciclo de vida para garantir direitos em todas as etapas do crescimento. A política não faz referência específica a tecnologias digitais ou ambientes online, mas seus princípios gerais de adequação à faixa etária e ao estágio de desenvolvimento são invocados no benchmarking como fundamento para obrigações de adequação etária em serviços digitais. É referenciada no contexto indiano como o documento que orienta a articulação entre a DPDPA, as IT Rules e as normativas setoriais de proteção de crianças.

66 INDIA. Ministry of Women and Child Development. National Policy for Children, 2013. New Delhi: Government of India, 2013. Disponível em: https://platform.who.int/docs/default-source/mca-documents/policy-documents/policy/IND-CC-46-07-POLICY-2013-eng-The-National-Policy-for-Children-2013.pdf. Acesso em: 1 jun. 2026.

DM/15/2022-DM — Governo da Índia (orientação sobre apostas online e influenciadores)[67]

O DM/15/2022-DM identifica uma série de orientações não vinculantes, emitidas pelo Ministério da Informação e Radiodifusão (MIB) a partir de junho de 2022, com reiterações em outubro de 2022, abril de 2023 e agosto de 2023, e posteriormente pela Central Consumer Protection Authority (CCPA). As orientações tratam da publicidade de plataformas offshore de apostas e jogos de azar online em meios de comunicação, incluindo redes sociais, diante da ilegalidade dessas plataformas na maioria dos estados indianos. Orientam que influenciadores e endossantes em mídias sociais se abstenham de veicular conteúdos promocionais dessas plataformas, inclusive mensagens subliminares ou surrogate advertisements, que intermediários de publicidade online não direcionem esse tipo de conteúdo ao público indiano, e que os próprios intermediários de mídia social realizem esforços de sensibilização entre seus usuários para que não publiquem esse conteúdo. As orientações alertam que o descumprimento pode ensejar procedimentos sob o Consumer Protection Act 2019, inclusive remoção de postagens ou contas, além de responsabilidade penal. A preocupação com o impacto sobre jovens e crianças é explicitamente invocada como motivação das orientações.

IV. Colômbia

A Colômbia é a jurisdição da América Latina mais próxima do ECA Digital em termos de abrangência regulatória, tendo aprovado em 2025 uma lei específica de proteção de crianças e adolescentes em ambiente digitais.

Lei 2489/2025[68]

A Lei 2489/2025, sancionada em 17 de julho de 2025, é a lei colombiana de proteção de crianças e adolescentes (NNA) em ambientedigitais. Estrutura-se em torno de um modelo de corresponsabilidade entre Estado, família, setor privado e sociedade civil. Seus princípios estruturantes incluem o melhor interesse da criança, por remissão ao art. 44 da Constituição Política colombiana e ao art. 8º do Código da Infância e Adolescência (Lei 1098/2006), a proporcionalidade das medidas, a evolução das faculdades dos NNA, o enfoque baseado em direitos humanos e a co-regulação entre Estado e indústria. O Governo Nacional recebe deveres concretos: informar sobre efeitos do uso de dispositivos

[67] INDIA. Ministry of Information and Broadcasting. Advisory No. DM/15/2022-DM: Advisory on Advertisements of Online Betting Platforms. New Delhi: Government of India, 13 jun. 2022. Disponível em: https://www.mib.gov.in/sites/default/files/2024-02/Advisory%20on%20online%20betting%20advertisements%2013.06.2022%282%29_0.pdf. Acesso em: 1 jun. 2026.

[68] COLÔMBIA. Ley 2489 de 2025. Por medio de la cual se establecen disposiciones para el desarrollo de entornos digitales sanos y seguros para los niños, niñas y adolescentes del país. Diario Oficial No. 53.185, Bogotá, 18 jul. 2025. Disponível em: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=260756. Acesso em: 1 jun. 2026.

digitais, especialmente nos primeiros anos de vida; adotar medidas para que NNA não enfrentem exploração e abusos sexuais, ciberagressão e ciberassédio; garantir acesso de pais, cuidadores e educadores a mecanismos de verificação de idade e controle parental; e exigir e fiscalizar a colaboração dos provedores de serviços digitais. A indústria de software é obrigada a proteger os NNA de danos em linha e a promover práticas éticas por meio do design de seus produtos (Art. 9º). A lei também impõe às instituições educativas o dever de realizar capacitações sobre uso seguro de tecnologia para pais e alunos, e determina que o Governo apresente informe anual ao Congresso sobre os avanços na matéria. A definição de mecanismos concretos de implementação, incluindo os de aferição de idade, é remetida à regulamentação posterior pelo Governo Nacional, com prazo de seis meses.

Decreto Regulamentador da Lei 2489/2025 (minuta, 2025)[69]

O Decreto Regulamentador, publicado pelo MinTIC para consulta pública com prazo até 26 de abril de 2026 e portanto ainda em fase de consulta ao tempo do fechamento do benchmarking, operacionaliza as obrigações da Lei 2489/2025. Ele introduz dois conceitos centrais: o Modo NNA (Modo Niña, Niño o Adolescente) e o design seguro por padrão (diseño seguro por defecto). O Modo NNA é a configuração predeterminada aplicada automaticamente a todo usuário identificado como pessoa com menos de 18 anos por mecanismos razoáveis de determinação de idade da plataforma, sem necessidade de intervenção ativa do próprio usuário, de seus pais ou tutores. O design seguro por padrão determina que as plataformas devem incorporar, desde a concepção do serviço, as condições mais elevadas de segurança e proteção de direitos para NNA. O decreto estrutura a classificação de conteúdos por meio da taxonomia de riscos 4C (conteúdo, contato, conduta e consumo) e de uma segmentação etária tripartite com base nas Leis 1098/2006 e 1804/2016: primeira infância (0–6 anos), crianças e pré-adolescentes (7–12 anos) e adolescentes (13–17 anos). Conteúdos absolutamente proibidos, incluindo pornografia infantil e demais conteúdos ilícitos, exigem moderação ou restrição efetiva e imediata. Os aspectos técnicos para os mecanismos de aferição de idade são atribuídos ao MinTIC, com preferência declarada por técnicas de estimação anônima e minimização de dados; a vigilância do processo é atribuída à Superintendência de Indústria e Comércio (SIC). As plataformas devem remeter semestralmente ao MinTIC um informe de seguimento

69 COLÔMBIA. Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). Proyecto de decreto reglamentario de la Ley 2489 de 2025, sometido a participación ciudadana para garantizar entornos digitales sanos y seguros para niños, niñas y adolescentes. Bogotá: MinTIC, 2026. Disponível em: https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/437026:MinTIC-abre-a-participacion-ciudadana-proyecto-de-decreto-para-garantizar-entornos-digitales-sanos-y-seguros-para-ninos-ninas-y-adolescentes. Acesso em: 1 jun. 2026.

avaliado por auditoria externa, e o MinTIC, em coordenação com a CRC, emitirá informe de verificação com possíveis recomendações.

V. Reino Unido

O Reino Unido possui o arcabouço regulatório composto por uma lei federal de amplo escopo, dois códigos de prática emitidos pela OFCOM, um registro de riscos baseado em evidências empíricas, dois guias sobre aferição de idade altamente eficaz, um código de design adequado à idade emitido pelo ICO e uma série de orientações específicas para diferentes categorias de conteúdo e tipos de serviço.

Online Safety Act 2023 (OSA UK)[70]

O Online Safety Act 2023 é a lei britânica de segurança online, administrada pela OFCOM. Para fins de proteção de crianças e adolescentes, a lei divide-se em dois grandes regimes: a Parte 3, aplicável a serviços user-to-user e de busca, e a Part 5, aplicável a serviços que publiquem conteúdo pornográfico do próprio provedor. O OSA impõe aos serviços de provável acesso por crianças deveres de avaliação de risco infantil periódica (Sections 11 e 28), de segurança por design, e de prevenção de acesso a primary priority content, pornografia, conteúdo de suicídio, automutilação e transtornos alimentares (Section 61). O conceito de "likely to be accessed by children[71]" é operacionalizado pela Section 37 em dois estágios cumulativos. A Section 66 impõe aos provedores de serviços user-to-user o dever de reportar à NCA todo conteúdo de abuso sexual infantil detectado e ainda não reportado a órgão equivalente, obrigação que entrou em vigor em 7 de abril de 2026, com extensão posterior a serviços de busca. A Section 162 atribui à Ofcom o poder de facilitar o acesso de pesquisadores verificados a dados das plataformas. O ICO atua de forma complementar quando o descumprimento envolve obrigações de proteção de dados pessoais.

70 UNITED KINGDOM. Online Safety Act 2023 (c. 50). London: The Stationery Office, 2023. Disponível em: https://www.legislation.gov.uk/ukpga/2023/50/contents. Acesso em: 1 jun. 2026.

71 É importante considerar que, de acordo com a legislação do Reino Unido, “children” abrange todos aqueles com menos de 18 anos de idade, isto é, crianças e adolescentes.

Protection of Children Code of Practice for User-to-User Services[72] *e Protection of Children Code of Practice for Search Services — OFCOM (julho de 2025)*[73]

Os dois Códigos de Prática emitidos pela OFCOM, publicados em 24 de abril de 2025 e em vigor desde 25 de julho de 2025, são instrumentos de regulação derivada do Online Safety Act que operacionalizam os deveres de proteção de crianças da Part 3. O Code para serviços user-to-user estabelece medidas recomendadas em blocos temáticos: avaliação de risco infantil (PCU A1–A5), age assurance (PCU B1–B7), moderação de conteúdo (PCU C1–C5), mecanismos de reporte e reclamação (PCU D1–D14), materiais de apoio ao usuário incluindo seção obrigatória para pais e responsáveis (PCU F1–F5), transparência (PCU G1–G3) e ferramentas de autonomia do usuário (PCU J1–J3). O Code para serviços de busca tem estrutura análoga. A adesão às medidas recomendadas gera presunção de conformidade com os deveres legais do OSA. Ambos os Códigos integram o Internet Watch Foundation (IWF) como trusted flagger central em matéria de CSAM e estabelecem o sistema de revisão da aferição etária, mecanismo de apelação para usuários adultos incorretamente classificados como crianças.

Children's Register of Risks — OFCOM[74]

O Children's Register of Risks é um documento de referência elaborado pela OFCOM com base em evidências empíricas sobre os tipos de conteúdo que causam dano a crianças e a intensidade desses danos por faixa etária. Não é instrumento normativo autônomo, mas fundamenta as obrigações dos Codes of Practice. Classifica os conteúdos em três camadas: primary priority content (pornografia, suicídio, automutilação e transtornos alimentares, cujo dano é universal independentemente da faixa etária); priority content (abuso e ódio, bullying, violência, substâncias prejudiciais e stunts perigosos, com impacto variável por faixa etária); e non-designated content (conteúdos que podem causar dano significativo a número considerável de crianças sem se enquadrar nas categorias formais). Para cada

---

72 UNITED KINGDOM. Office of Communications (OFCOM). Protection of Children Code of Practice for User-to-User Services. London: OFCOM, jul. 2025. Disponível em: https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/statement-protecting-children-from-harms-online/main-document/protection-of-children-code-of-practice-for-user-to-user-services.pdf. Acesso em: 1 jun. 2026.

73 UNITED KINGDOM. Office of Communications (OFCOM). Protection of Children Code of Practice for Search Services. London: OFCOM, jul. 2025. Disponível em: https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/statement-protecting-children-from-harms-online/main-document/protection-of-children-code-of-practice-for-search-services.pdf. Acesso em: 1 jun. 2026.

74 UNITED KINGDOM. Office of Communications (OFCOM). Children's Register of Risks. London: OFCOM, 2025. Disponível em:https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/statement-protecting-children-from-harms-online/main-document/childrens-register-of-risks.pdf?v=401302. Acesso em: 1 jun. 2026.

categoria, o Register documenta frequência de exposição, impacto por faixa etária e fatores dos serviços que amplificam esses riscos.

Guidance on Highly Effective Age Assurance for Part 5 Services[75] e Guidance on Highly Effective Age Assurance for Part 3 Services[76] — OFCOM

Esses dois guias da OFCOM definem o que constitui age assurance "altamente eficaz" para fins do Online Safety Act. O guia da Part 5 aplica-se a serviços que publicam conteúdo pornográfico do próprio provedor; o da Part 3 aplica-se a serviços user-to-user e de busca. Ambos adotam definições idênticas, com base no art. 230 do OSA UK, de age assurance (termo guarda-chuva), age verification (verificação da idade exata) e age estimation (estimativa da faixa etária), excluindo expressamente a autodeclaração de ambas as categorias. Os quatro critérios de alta eficácia são: acurácia técnica (com métricas distintas para métodos binários e contínuos), robustez (funcionamento em contextos reais), confiabilidade (reprodutibilidade) e equidade (ausência de viés discriminatório). Os guias listam métodos expressamente admitidos, open banking, photo-ID matching, facial age estimation, MNO age checks, credit card checks, email-based age estimation e Digital Identity Services, e expressamente excluídos, autodeclaração, cartão de débito e restrições contratuais genéricas. Para métodos de estimativa, exige-se o challenge age approach como camada adicional.

Guidance on Content Harmful to Children (Protecting Children from Harms Online)[77] e Illegal Content Judgements Guidance (ICJG)[78] — OFCOM

O Guidance on Content Harmful to Children define, para fins de moderação, o que constitui cada categoria de primary priority content e priority content. Em relação ao conteúdo pornográfico, define-o como todo conteúdo cuja natureza permita

---

75 UNITED KINGDOM. Office of Communications (OFCOM). Guidance on Highly Effective Age Assurance for Part 5 Services. London: OFCOM, 2025. Disponível em: https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/statement-age-assurance-and-childrens-access/guidance-on-highly-effective-age-assurance-and-other-part-5-duties.pdf. Acesso em: 1 jun. 2026.

76 UNITED KINGDOM. Office of Communications (OFCOM). Guidance on Highly Effective Age Assurance for Part 3 Services. London: OFCOM, 2025. Disponível em: https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/statement-age-assurance-and-childrens-access/part-3-guidance-on-highly-effective-age-assurance.pdf. Acesso em: 1 jun. 2026.

77 GREAT BRITAIN. Ofcom (Office of Communications). Protecting Children from Harms Online: Guidance on Content Harmful to Children. London: Ofcom, 2025. Disponível em: https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/statement-protecting-children-from-harms-online/main-document/guidance-on-content-harmful-to-children.pdf. Acesso em: 1 jun. 2026.

78 GREAT BRITAIN. Ofcom (Office of Communications). Illegal Content Judgements Guidance (ICJG). London: Ofcom, 2024. Disponível em: https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/information-for-industry/illegal-harms/illegal-content-judgements-guidance-icjg.pdf. Acesso em: 1 jun. 2026.

razoavelmente presumir que foi produzido única ou principalmente para fins de excitação sexual, com exclusão expressa de conteúdo puramente textual e inclusão de conteúdo gerado por IA e animações. O ICJG delimita quando um conteúdo cruza a fronteira do ilegal, definindo pornografia infantil (imagens indecentes de criança e imagens proibidas de criança, incluindo pseudofotografias e imagens não fotográficas), o critério de intencionalidade criminal e o escopo da pornografia extrema envolvendo adultos.

Children's Access Assessments Guidance[79] — OFCOM

O Children's Access Assessments Guidance operacionaliza o processo de avaliação previsto na Section 36 do OSA UK para determinar se um serviço é "likely to be accessed by children". Estrutura esse processo em dois estágios: o Estágio 1 avalia se é possível que crianças acessem normalmente o serviço, afastável apenas por aferição de idade altamente eficaz; o A Fase 2 avalia se o usuário é menor de idade está preenchida, o que ocorre quando há número significativo de crianças usuárias (em termos absolutos ou proporcionais) ou quando o serviço é do tipo que provavelmente atrai crianças, com base em fatores como benefícios oferecidos a crianças, atratividade do conteúdo e estratégia comercial do provedor.

The Online Safety Act 2023 (Category 1, Category 2A and Category 2B Threshold Conditions) Regulations 2025[80]

Este instrumento de legislação secundária define os limiares de categorização dos serviços para fins do OSA UK. A Categoria 1 abrange serviços user-to-user com mais de 34 milhões de usuários ativos mensais no Reino Unido que utilizem sistema de recomendação de conteúdo, ou com mais de 7 milhões que combinem recomendação com funcionalidade de encaminhamento. A Categoria 2A abrange motores de busca com mais de 7 milhões de usuários ativos mensais. A Categoria 2B abrange serviços user-to-user com mais de 3 milhões de usuários que disponibilizem mensagens diretas restritas. A categorização determina quais obrigações adicionais incidem sobre cada serviço.

Age Appropriate Design Code (AADC/Children's Code) — ICO, versão 2.1.87 (outubro de 2022)[81]

---

79 GREAT BRITAIN. Ofcom (Office of Communications). Children's Access Assessments Guidance. London: Ofcom, 2025. Disponível em: https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/information-for-industry/childrens-safety/childrens-access-assessments-guidance.pdf. Acesso em: 1 jun. 2026.

80 GREAT BRITAIN. The Online Safety Act 2023 (Category 1, Category 2A and Category 2B Threshold Conditions) Regulations 2025. London: Statutory Instruments, 2025. Disponível em: https://www.legislation.gov.uk/ukdsi/2025/9780348267174. Acesso em: 1 jun. 2026.

81 GREAT BRITAIN. Information Commissioner's Office (ICO). Age appropriate design: a code of practice for online services. Wilmslow: ICO, 2022. Versão 2.1.87. Disponível em: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-

O Age Appropriate Design Code é um código estatutário emitido pelo ICO com base no UK GDPR. Aplica-se a todos os serviços da sociedade da informação, aplicativos, jogos online, redes sociais, serviços de streaming, motores de busca, dispositivos conectados e qualquer serviço que ofereça bens ou serviços via internet, que sejam prováveis de ser acessados por crianças no Reino Unido. Estabelece 15 standards de design, com destaque para: melhor interesse da criança como consideração primária (Standard 1); proteção de dados por padrão (Standard 2); aplicação diferenciada das proteções conforme a faixa etária (Standard 3); transparência em linguagem acessível a crianças (Standard 4); proibição de uso detrimental de dados (Standard 5); geolocalização desativada por padrão (Standard 8); controles parentais, condicional à oferta, com exigências mínimas de transparência com a criança e vedação ao monitoramento encoberto (Standard 11); e ferramentas online para exercício de direitos dos titulares (Standard 15). O código estrutura cinco faixas etárias de desenvolvimento (0–5; 6–9; 10–12; 13–15; 16–17) com base em evidências empíricas, e indica o PAS 1296 como padrão técnico de referência para avaliação de serviços terceiros de verificação de idade.

VI. União Europeia

A União Europeia possui o arcabouço regulatório de maior abrangência territorial, estruturado em camadas de instrumentos que se articulam entre si: regulamentos de aplicação direta, diretivas que demandam transposição pelos Estados-Membros, orientações interpretativas da Comissão e declarações de autoridades de supervisão.

General Data Protection Regulation — GDPR (Regulamento UE 2016/679)[82]

O GDPR é o regulamento geral de proteção de dados pessoais da União Europeia, de aplicação direta em todos os Estados-Membros desde 2018. Em relação a crianças, o Artigo 8 estabelece um regime específico para o consentimento no tratamento de dados no contexto da oferta de serviços da sociedade da informação: abaixo de 16 anos, ou do limiar inferior adotado pelo Estado-Membro, nunca inferior a 13, o consentimento deve ser dado ou autorizado pelos titulares do poder parental. O GDPR é o fundamento jurídico do AADC britânico e permeia os instrumentos europeus de proteção de crianças em plataformas digitais. O Artigo 42 prevê a possibilidade de criação de esquemas de certificação e selos de proteção de dados para demonstração de conformidade.

---

resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/. Acesso em: 1 jun. 2026.

82 UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Bruxelas: Parlamento Europeu, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016R0679. Acesso em: 1 jun. 2026.

Digital Services Act — DSA (Regulamento UE 2022/2065)[83]

O Digital Services Act é o regulamento europeu que regula os serviços digitais intermediários, motores de busca, plataformas de hospedagem de conteúdo, redes sociais, marketplaces e plataformas de compartilhamento de vídeo. Plenamente aplicável desde fevereiro de 2024, o DSA estabelece regime escalonado: obrigações gerais para todos os intermediários, obrigações adicionais para plataformas online, e obrigações reforçadas para Very Large Online Platforms (VLOPs) e Very Large Online Search Engines (VLOSEs), definidos pelo critério de 45 milhões de usuários ativos mensais na UE. Para a proteção de crianças, os dispositivos centrais são o Artigo 28[84], que impõe a provedores de plataformas acessíveis a crianças e adolescentes o dever de adotar medidas adequadas e proporcionais para assegurar um nível elevado de privacidade, segurança e proteção dos crianças e adolescentes em seu serviço, e proíbe anúncios baseados em perfilamento para usuários que o provedor saiba com razoável certeza serem crianças e adolescentes, e o Artigo 35, que exige que VLOPs e VLOSEs implementem medidas proporcionais de mitigação dos riscos sistêmicos identificados nos termos do Artigo 34, podendo tais medidas incluir, onde aplicável, verificação de idade e ferramentas de controle parental (Art. 35(1)(j)). O DSA institui o sistema de trusted flaggers (Artigo 22), autoriza ordens de remoção por autoridades (Artigo 9), impõe notificação imediata às autoridades quando houver suspeita de crimes contra a vida ou segurança de pessoas, incluindo crimes de exploração sexual de crianças e adolescentes nos termos da Diretiva 2011/93/UE (Artigo 18), e regula o acesso de pesquisadores vetted a dados de VLOPs e VLOSEs (Artigo 40). O regime de reclamações inclui internal complaint-handling system (Artigo 20) e out-of-court dispute settlement (Artigo 21). O DSA também prevê a suspensão do processamento de notificações de usuários que frequentemente submetam reclamações manifestamente infundadas (Artigo 23).).

83 UNIÃO EUROPEIA. 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). Bruxelas: Parlamento Europeu, 2022. Disponível em: https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng. Acesso em: 1 jun. 2026.

84 Article 28 Online protection of minors 1. Providers of online platforms accessible to minors shall put in place appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors, on their service. 2. Providers of online platform shall not present advertisements on their interface based on profiling as defined in Article 4, point (4), of Regulation (EU) 2016/679 using personal data of the recipient of the service when they are aware with reasonable certainty that the recipient of the service is a minor. 3. Compliance with the obligations set out in this Article shall not oblige providers of online platforms to process additional personal data in order to assess whether the recipient of the service is a minor. 4 The Commission, after consulting the Board, may issue guidelines to assist providers of online platforms in the application of paragraph 1.

Audiovisual Media Services Directive — AVMSD[85]

A AVMSD é uma diretiva europeia que regula os serviços de comunicação social audiovisual, televisão, vídeo on demand e plataformas de compartilhamento de vídeo, demandando transposição pelos Estados-Membros. Determina que conteúdos que possam prejudicar o desenvolvimento físico, mental ou moral de crianças e adolescentes, com ênfase em violência gratuita e pornografia, sejam disponibilizados de modo a impedir que crianças os vejam ou ouçam normalmente. Obriga ainda os Estados-Membros a garantir que provedores de plataformas de compartilhamento de vídeo adotem medidas adequadas contra conteúdos cuja disseminação constitua crime, incluindo crimes de pornografia infantil nos termos da Diretiva 2011/93/UE.

Diretiva 2011/93/UE[86]

A Diretiva 2011/93/UE é uma legislação relativa à luta contra o abuso sexual e a exploração sexual de crianças e a pornografia infantil define, no direito penal europeu, o conceito de pornografia infantil de forma ampla: material que represente visualmente criança em conduta sexualmente explícita real ou simulada; representação dos órgãos sexuais de uma criança com finalidade primordialmente sexual; material que represente visualmente pessoa que aparente ser criança em conduta sexualmente explícita; e imagens realistas de criança em conduta sexualmente explícita. É a referência penal que permeia as obrigações de reporte do DSA (Artigo 18 e Recital 56).

Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online — Comissão Europeia (C/2025/5519)[87]

As Diretrizes da Comissão, publicadas em 14 de julho de 2025 com base no Artigo 28, §4º do DSA, são o instrumento interpretativo central para a aplicação das obrigações de proteção de crianças do regulamento. Tais diretrizes definem os três tipos de mecanismos de aferição de idade, autodeclaração, estimativa e verificação, e concluem que a

---

85 UNIÃO EUROPEIA. Diretiva (UE) 2018/1808 do Parlamento Europeu e do Conselho, de 14 de novembro de 2018, que altera a Diretiva 2010/13/UE relativa à coordenação de certas disposições legislativas, regulamentares e administrativas dos Estados-Membros respeitantes à oferta de serviços de comunicação social audiovisual (Diretiva Serviços de Comunicação Social Audiovisual) tendo em conta a evolução do mercado. Bruxelas: Parlamento Europeu, 2018. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32018L1808. Acesso em: 1 jun. 2026.

86 UNIÃO EUROPEIA. Diretiva 2011/93/UE do Parlamento Europeu e do Conselho, de 13 de dezembro de 2011, relativa à luta contra o abuso sexual e a exploração sexual de crianças e a pornografia infantil, e que substitui a Decisão-Quadro 2004/68/JAI do Conselho. Bruxelas: Parlamento Europeu, 2011. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32011L0093. Acesso em: 1 jun. 2026.

87 UNIÃO EUROPEIA. Comissão Europeia. Commission Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online (C/2025/5519). Bruxelas: Comissão Europeia, 2025. Disponível em: https://digital-strategy.ec.europa.eu/en/library/guidelines-measures-ensure-high-level-privacy-safety-and-security-minors-online. Acesso em: 1 jun. 2026.

autodeclaração é insuficiente para os fins do Artigo 28, §1º. Este documento estabelece, ainda, que métodos admissíveis devem demonstrar precisão, confiabilidade, robustez, não intrusividade e não discriminação, e que a verificação rigorosa é necessária e proporcional para categorias de alto risco, álcool, tabaco, drogas, pornografia e jogos de azar. Para ferramentas de supervisão parental, as Diretrizes determinam que o compliance com o DSA nunca deve depender exclusivamente dessas ferramentas, e definem requisitos funcionais mínimos: facilidade de uso, independência de hardware, transparência radical para a criança, segurança de alteração e interoperabilidade. Organizam os riscos pela tipologia dos cinco "Cs": Content, Contact, Conduct, Consumer e Cross-cutting, e referenciam a EU Digital Identity Wallet, a ser disponibilizada por todos os Estados-Membros até o final de 2026, e a EU age verification solution da Comissão como infraestrutura pública de aferição.

Statement 1/2025 on Age Assurance — European Data Protection Board[88]

O Statement 1/2025 do EDPB é uma declaração de orientação do Conselho Europeu de Proteção de Dados, composto pelas autoridades de proteção de dados de todos os Estados-Membros, sobre aferição de idade. Adota "age assurance" como conceito guarda-chuva que abrange estimativa de idade, verificação de idade e autodeclaração, e estabelece princípios de alto nível para que provedores e terceiros envolvidos na aferição demonstrem conformidade com o GDPR: abordagem proporcional e baseada em risco, respeito aos direitos fundamentais e ao melhor interesse da criança, limitação do tratamento ao estritamente necessário, efetividade, licitude, transparência, segurança, governança e auditabilidade pelas autoridades competentes.

Better Internet for Kids (BIK) — Estratégia da Comissão Europeia[89]

A Better Internet for Kids é uma estratégia da Comissão Europeia que não cria obrigações jurídicas vinculantes, mas orienta ações da União Europeia e dos Estados-Membros voltadas ao empoderamento digital de crianças. Adota, de maneira transversal, a lógica da adequação à idade e do desenvolvimento progressivo de capacidades, prevendo ações de capacitação digital gradual, promoção de experiências online adequadas a diferentes faixas etárias e co-criação, com crianças, de comunicações acessíveis sobre produtos e serviços digitais.

---

88 UNIÃO EUROPEIA. European Data Protection Board (EDPB). Statement 1/2025 on Age Assurance. Bruxelas: EDPB, 2025. Disponível em: https://www.edpb.europa.eu/our-work-tools/our-documents/statements/statement-12025-age-assurance_en. Acesso em: 1 jun. 2026.

89 UNIÃO EUROPEIA. Comissão Europeia. A European strategy for a better internet for kids (BIK+). Bruxelas: Comissão Europeia, 2022. Disponível em: https://digital-strategy.ec.europa.eu/en/policies/strategy-better-internet-kids. Acesso em: 1 jun. 2026.

General Product Safety Regulation — GPSR (Regulamento UE 2023/988)[90]

O GPSR é o regulamento europeu de segurança geral de produtos de consumo, em vigor desde 2024. Para fins do benchmarking, é relevante no contexto do art. 38 do ECA Digital. Exige identificação do produto e do fabricante em produto ou embalagem, instruções e informações de segurança em língua compreensível pelos consumidores, e avaliação de risco que considere grupos vulneráveis incluindo crianças, com referência explícita a riscos à saúde mental decorrentes de produtos digitalmente conectados. Admite QR codes como complemento às informações físicas, mas não como substituto. Não há, no GPSR, exigência de etiquetagem padronizada sobre conteúdo inadequado na internet nas embalagens de dispositivos eletrônicos.

2.2.2. Práticas Regulatórias Identificadas

Esta seção apresenta, para os temas analisados nos eixos (i) e (iii) do benchmarking, uma síntese estruturada das abordagens adotadas pelas jurisdições selecionadas. Para cada tema, a análise está organizada em três partes: a identificação das jurisdições e fontes normativas consultadas; uma primeira clivagem que mapeia quais jurisdições adotam ou rejeitam o conceito ou obrigação em questão; e a descrição das abordagens regulatórias concretas identificadas no direito comparado, incluindo os instrumentos utilizados para operacionalizá-las. Os temas são apresentados na mesma ordem do benchmarking constante do Anexo 2: primeiro os cinco temas do eixo de conceitos gerais e definições, seguidos dos nove temas do eixo de outros dispositivos sujeitos à regulamentação pela ANPD.

I. Conceitos Gerais e Definições

O ECA Digital contém diversos conceitos essenciais à sua interpretação e aplicação prática. Parte deles foi definida pela própria Lei, outra pelo Decreto regulamentador, enquanto outros ainda demandam aprofundamento interpretativo. A proposta inicial de atualização da Agenda Regulatória da ANPD, submetida à tomada de subsídios, previa como tema "Conceitos gerais e definições da Lei nº 15.211/2025 (ECA Digital)". Na versão revisada da Agenda Regulatória para o biênio 2025–2026, contudo, o tema foi incorporado de forma mais restrita, com foco nos conceitos de "produto ou serviço de tecnologia da

[90] UNIÃO EUROPEIA. Regulamento (UE) 2023/988 do Parlamento Europeu e do Conselho, de 10 de maio de 2023, relativo à segurança geral dos produtos, que altera o Regulamento (UE) n.º 1025/2012 do Parlamento Europeu e do Conselho e a Diretiva (UE) 2020/1828 do Parlamento Europeu e do Conselho, e que revoga a Diretiva 2001/95/CE do Parlamento Europeu e do Conselho e a Diretiva 87/357/CEE do Conselho (Regulamento Geral sobre a Segurança dos Produtos). Bruxelas: Parlamento Europeu, 2023. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32023R0988. Acesso em: 1 jun. 2026.

informação", "acesso provável" e nas exceções ao âmbito de incidência do ECA Digital, bem como na interpretação dos deveres de prevenção, proteção, informação e segurança previstos na Lei, com o objetivo de conferir maior clareza e segurança jurídica à sua implementação pelos agentes regulados.

I.1. Acesso Provável (2.1 do Benchmarking)

O ECA Digital utiliza o conceito de acesso provável como critério de ativação das obrigações previstas na lei, estabelecendo os elementos que o caracterizariam (suficiente probabilidade de uso e atratividade do produto ou serviço de tecnologia da informação por crianças e adolescentes; considerável facilidade ao acesso e utilização do produto ou serviço de tecnologia da informação por crianças e adolescentes; e significativo grau de risco à privacidade, à segurança ou ao desenvolvimento biopsicossocial de crianças e de adolescentes, especialmente no caso de produtos ou serviços que tenham por finalidade permitir a interação social e o compartilhamento de informações em larga escala entre usuários em ambiente digital). O benchmarking buscou analisar como diferentes jurisdições definem ou abordam o conceito.

A. Jurisdições e Fontes Normativas Analisadas

Jurisdição	**Fontes Normativas**
Austrália	Basic Online Safety Expectations (BOSE) e BOSE Regulatory Guidance; Privacy and Other Legislation Amendment Act (2024); Children's Online Privacy Code (previsto para dez/2026); Online Safety Act 2021; Social Media Minimum Age Act
Califórnia (EUA)	AB-2273 — California Age-Appropriate Design Code Act (2022)
Louisiana (EUA)	Part II of Chapter 20-A of Title 51 of the Louisiana Revised Statutes
Texas (EUA)	Texas Business & Commerce Code, Chapter 509 — SCOPE Act (HB 18, 2023)
Utah (EUA)	Utah Code, Title 13, Chapter 63 — Social Media Regulation Act (SB 152, 2023)
Índia	Digital Personal Data Protection Act (DPDPA)
Colômbia	Lei 2489/2025; Decreto Regulamentador (minuta, 2025)
Reino Unido	Online Safety Act 2023 (Section 37); OSA Category Threshold Conditions Regulations 2025; Children's Access Assessments Guidance (Ofcom); Age Appropriate Design Code — AADC/Children's Code v. 2.1.87 (ICO, 2022)

União Europeia	Digital Services Act (DSA), Recital 71; Guidelines on measures to ensure a high level of privacy, safety and security for minors (art. 28(4) DSA); Better Internet for Kids

B. Jurisdições que adotam e que não adotam o conceito de acesso provável

O primeiro ponto de divergência entre as jurisdições analisadas é anterior ao conteúdo do conceito: trata-se da própria decisão de adotá-lo ou não como critério de ativação das obrigações de proteção infantojuvenil.

Jurisdições que adotam o conceito — Austrália, Califórnia e Reino Unido constroem positivamente o conceito de acesso provável, estabelecendo que as obrigações de proteção incidem sobre serviços que, independentemente de serem formalmente direcionados a crianças, sejam na prática prováveis de ser por elas acessados. A União Europeia adota lógica equivalente, ainda que de forma menos estruturada, visto que o DSA ancora o conceito principalmente em um Recital e em guidelines não vinculantes, sem definição legal expressa na norma principal.

Jurisdições que rejeitam o conceito e adotam critério substituto — Texas e Utah rejeitam a presunção baseada em probabilidade objetiva. O Texas substitui o conceito pelo critério do conhecimento efetivo do provedor sobre a menoridade do usuário (*known minor*), ao passo que Utah ancora as obrigações na verificação obrigatória de idade como condição de acesso. Em ambos os casos, o acionamento das proteções depende de um fato individualizado, a identificação concreta do usuário como pessoa com menos de 18 anos, e não de uma avaliação probabilística sobre o perfil do serviço. Louisiana tampouco adota o conceito, sem critério substituto claro.

Jurisdições que adotam regime de aplicação universal — Índia e Colômbia optam por uma lógica distinta: as obrigações de proteção incidem sobre todos os serviços digitais acessíveis a crianças e adolescentes, sem qualquer juízo probabilístico intermediário. O conceito de acesso provável é, portanto, desnecessário nesses regimes, pois o escopo de aplicação é definido pela natureza universal da regulação, e não pela probabilidade de acesso por crianças e adolescentes a um serviço específico.

C. Abordagens adotadas pelas jurisdições

Nas jurisdições que adotam o conceito, a caracterização do acesso provável não decorre de um critério único, mas de uma avaliação multifatorial e contextual. A análise

comparada permite identificar os seguintes elementos recorrentes, bem como os instrumentos regulatórios desenvolvidos para operacionalizar o conceito na prática.

Natureza, conteúdo e atratividade do serviço. Austrália, Califórnia e Reino Unido consideram se o conteúdo ou as funcionalidades do serviço são intrinsecamente atrativos para o público infantojuvenil, incluindo jogos, entretenimento, cultura popular, esportes, criação de conexões sociais e conteúdo educacional. A AB-2273 californiana inclui expressamente elementos de design conhecidos por serem do interesse das crianças como indicador autônomo.

Dados de audiência e evidências de uso efetivo. Califórnia e Reino Unido atribuem peso significativo a evidências concretas sobre a composição do público do serviço, como pesquisas internas, dados de comportamento de usuários e análise do perfil de audiência de serviços similares. A OFCOM esclarece que o número significativo de crianças pode referir-se tanto a um número absoluto quanto a uma proporção do total de usuários, e que mesmo um número relativamente pequeno pode ser relevante dependendo da natureza do serviço.

Publicidade direcionada a crianças. A AB-2273 californiana trata como indicador autônomo de acesso provável a presença de anúncios direcionados ao público infantojuvenil no serviço.

Similaridade com serviços já utilizados por crianças. Califórnia e Reino Unido consideram que um serviço substancialmente semelhante a outro já identificado como provável de ser acessado por crianças herda essa caracterização.

Ausência de salvaguardas efetivas de restrição de acesso. Austrália, Reino Unido e União Europeia convergem no entendimento de que a ausência de mecanismos efetivos de restrição, como *age assurance* de alta eficácia, é, por si só, um elemento relevante para a caracterização do acesso provável. Métodos insuficientes para afastar essa caracterização incluem autodeclaração de idade, restrições contratuais genéricas e métodos de pagamento que não exijam comprovação de maioridade.

Estratégia comercial do provedor. O Reino Unido inclui entre os fatores indicativos a circunstância de crianças e adolescentes integrarem a estratégia comercial do provedor, seja como público-alvo de monetização, seja como grupo considerado no desenvolvimento do produto.

Ciência do provedor sobre a presença de crianças e adolescentes. A União Europeia acrescenta um elemento subjetivo: o provedor é considerado ciente da presença de crianças e adolescentes quando já trata dados que revelem a idade, por exemplo

coletados no cadastro, ou quando, de forma razoável, deveria reconhecer que o serviço atrai esse público.

Definição legal expressa combinada com guidance operacional. O Reino Unido adota o modelo mais estruturado: o conceito é definido em lei primária (Section 37 do OSA) e complementado por guidance regulatória detalhada da Ofcom, que operacionaliza os critérios sem engessar o texto legal. Esse modelo combina segurança jurídica com adaptabilidade tecnológica.

Avaliação formal estruturada em estágios. A Ofcom estabelece um procedimento bifásico obrigatório, a *children's access assessment*, com dois estágios sequenciais: primeiro, verificar se o acesso por crianças é tecnicamente possível na ausência de salvaguardas efetivas; depois, avaliar se há número significativo de crianças usuárias ou se o serviço é do tipo que provavelmente as atrai. Esse roteiro reduz a arbitrariedade na aplicação e oferece previsibilidade aos provedores.

Presunção de acesso na ausência de avaliação ou de salvaguardas. O Reino Unido prevê que, se o provedor não realizar a *children's access assessment* no prazo exigido, o serviço será automaticamente tratado como provável de ser acessado por crianças e adolescentes, independentemente de qualquer avaliação de mérito. A Austrália adota lógica equivalente: na ausência de barreiras efetivas, presume-se o acesso. Essa inversão do ônus probatório desincentiva a inércia regulatória.

Listas de fatores indicativos não taxativos. Austrália, Califórnia e Reino Unido utilizam enumerações abertas de critérios, que orientam a avaliação sem criar rol fechado explorável como brecha. Essa técnica legislativa é especialmente adequada para um setor em constante transformação tecnológica.

Cláusula de reavaliação contínua. O AADC britânico prevê expressamente que, se evidências posteriores indicarem acesso significativo por crianças, o provedor deve conformar-se ao código ou rever as restrições de acesso. Essa previsão evita que avaliações iniciais favoráveis ao provedor se tornem imutáveis diante de mudanças no perfil de uso do serviço.

Consolidação futura em código setorial. A Austrália prevê a consolidação e detalhamento do conceito em um código específico, o Children's Online Privacy Code, com publicação prevista para dezembro de 2026, demonstrando que a operacionalização do conceito pode ser feita de forma progressiva e setorializada, sem exigir definição exaustiva desde o primeiro ato normativo.

I.2. Melhor Interesse da Criança e do Adolescente (2.2 do Benchmarking)

O ECA Digital consagra o melhor interesse da criança e do adolescente como princípio orientador da proteção em ambientes digitais, em linha com o Art. 227 da Constituição Federal e o Art. 4º do ECA. Diante da necessidade de operacionalizar essa garantia[91] no contexto regulatório digital, o benchmarking buscou responder à seguinte pergunta: qual abordagem é adotada para o melhor interesse da criança?

A. Jurisdições e Fontes Normativas Analisadas

Jurisdição	Fontes Normativas
Austrália	Children's Online Privacy Code (em elaboração); Basic Online Safety Expectations (BOSE), atualização de mai/2024; BOSE Regulatory Guidance
Califórnia (EUA)	AB-2273 — California Age-Appropriate Design Code Act (2022)
Louisiana (EUA)	Part II of Chapter 20-A of Title 51 of the Louisiana Revised Statutes
Texas (EUA)	Texas Business & Commerce Code, Chapter 509 — SCOPE Act (HB 18, 2023)
Utah (EUA)	Utah Code, Title 13, Chapter 63 — Social Media Regulation Act (SB 152, 2023)
Índia	National Policy on Children (2013)
Colômbia	Lei 2489/2025; Decreto Regulamentador (minuta, 2025)
Reino Unido	Online Safety Act 2023; Age Appropriate Design Code — AADC/Children's Code v. 2.1.87 (ICO, 2022)
União Europeia	Carta dos Direitos Fundamentais da União Europeia (Art. 24); Digital Services Act (DSA); Guidelines on measures to ensure a high level of privacy, safety and security for minors (art. 28(4) DSA)

B. Jurisdições que incorporam e que não incorporam o princípio expressamente

[91] O Comentário Geral nº 14 do Comitê dos Direitos da Criança da ONU elucida que o melhor interesse da criança possui tripla natureza jurídica: é simultaneamente direito substantivo, assegurando à criança e ao adolescente que seu interesse seja considerado primordialmente em qualquer decisão que lhe concerne, princípio jurídico interpretativo fundamental, determinando que, diante de mais de uma interpretação possível de uma norma, deve prevalecer aquela que mais eficazmente atenda ao melhor interesse da criança, e regra de procedimento, impondo que qualquer processo decisório que afete crianças avalie e registre o impacto da decisão sobre elas.

O primeiro eixo de análise diz respeito à própria decisão de incorporar ou não a garantia do melhor interesse da criança como vetor normativo expresso na regulação digital.

Jurisdições que incorporam a garantia expressamente. Austrália, Califórnia, Índia, Colômbia, Reino Unido e União Europeia adotam o melhor interesse da criança como princípio explícito e estruturante de suas regulações digitais. Em todas essas jurisdições, o princípio funciona como vetor interpretativo vinculante que orienta as demais obrigações impostas aos provedores. A ancoragem na Convenção das Nações Unidas sobre os Direitos da Criança (UNCRC) é recorrente, especialmente nos Comentários Gerais nº 14 e nº 25 do Comitê dos Direitos da Criança, e confere ao princípio uma dimensão de direito internacional dos direitos humanos que vai além da obrigação regulatória estrita.

Jurisdições que não incorporam o princípio. Louisiana, Texas e Utah[92] não adotam o melhor interesse da criança como princípio normativo aberto. Nesses regimes, a proteção infantojuvenil é operacionalizada exclusivamente por meio de obrigações objetivas e mandatórias, como limitações de funcionalidades, restrições à publicidade, exigências de verificação de idade e consentimento parental, sem que haja cláusula geral orientadora capaz de preencher lacunas ou guiar a interpretação de situações não previstas expressamente.

C. Abordagens adotadas pelas jurisdições

Entre as jurisdições que adotam o princípio, identificam-se diferenças relevantes quanto à forma de incorporação, ao grau de operacionalização e aos instrumentos regulatórios utilizados.

Princípio como consideração primária no design. Austrália e Reino Unido estabelecem que o melhor interesse da criança deve ser uma consideração primária, e não apenas uma entre várias, no design e na operação de serviços digitais de provável acesso por crianças e adolescentes. As BOSE australianas determinam que essa consideração deve estar presente desde a concepção do serviço até sua revisão contínua. O AADC britânico vai além e o eleva simultaneamente à condição de padrão autônomo (Standard 1) e de princípio transversal que perpassa todos os demais padrões do código.

Primazia sobre interesses comerciais. Califórnia e Reino Unido estabelecem expressamente uma regra de prevalência: em caso de conflito entre o melhor interesse da

92 Cabe salientar que os Estados Unidos da América não ratificaram a Convenção sobre os Direitos da Criança, o que pode explicar a não incorporação expressa da garantia do melhor interesse.

criança e os interesses comerciais do provedor, os primeiros prevalecem. O AADC britânico é explícito ao afirmar que interesses comerciais dos provedores dificilmente prevalecerão sobre o direito à privacidade da criança.

Princípio como vetor interpretativo vinculante para múltiplos atores. A Colômbia adota uma abordagem de corresponsabilidade: o princípio opera como vetor vinculante para todos os atores envolvidos, Estado, família, setor privado e sociedade civil, informando tanto as obrigações impostas ao Governo Nacional quanto as exigidas da indústria de software. A União Europeia adota lógica equivalente, com ancoragem na Carta dos Direitos Fundamentais (Art. 24).

Operacionalização técnica via design seguro por padrão. A Colômbia, por meio de seu Decreto Regulamentador, avança na operacionalização da garantia ao traduzi-la em uma obrigação técnica concreta: o *diseño seguro por defecto*, segundo o qual a proteção mais elevada é a configuração padrão do serviço, e qualquer afastamento exige justificativa legítima, proporcional e documentada. O princípio deixa, assim, de ser apenas um vetor interpretativo e passa a ter expressão funcional direta no produto.

Avaliação integrada de direitos. A União Europeia, por meio das Guidelines do DSA, propõe uma abordagem que considera de forma integrada todos os direitos da criança e do adolescente, proteção, não discriminação, privacidade, participação, liberdade de expressão e acesso à informação, bem como os impactos positivos e negativos das medidas adotadas. Essa perspectiva rejeita a leitura restritiva do melhor interesse como sinônimo exclusivo de proteção, reconhecendo que restrições excessivas podem elas próprias violar direitos da criança. A Colômbia também incorpora expressamente essa cautela, ao prever que as medidas devem ser proporcionais ao risco detectado para evitar restrições que violem direitos fundamentais como o acesso à informação.

Participação de crianças e adolescentes na construção normativa. A Austrália destaca-se pela adoção de um processo faseado de consulta pública que inclui diretamente crianças e adolescentes entre 8 e 18 anos. O pressuposto, em diálogo com o Comentário Geral nº 16 do Comitê dos Direitos da Criança da ONU, é de que a escuta efetiva desse público é condição para que as normas cumpram e dialoguem genuinamente com o seu melhor interesse. Os resultados das consultas com crianças e adolescentes revelaram demandas concretas: pedido de permissão para coleta e uso de dados, maior transparência sobre finalidades, simplificação de políticas, facilidade de acesso a informações e botões relevantes, canais de suporte e garantia de uso justo de dados pessoais.

Ancoragem em instrumentos internacionais de direitos da criança. Austrália, Reino Unido e União Europeia fundamentam expressamente suas definições do princípio nos Comentários Gerais nº 14 e nº 25 do Comitê dos Direitos da Criança da ONU e no Art. 3 da UNCRC. Essa ancoragem confere ao princípio densidade normativa e base interpretativa reconhecida internacionalmente, além de orientar provedores a consultar referenciais já consolidados.

Child rights impact assessment. A União Europeia, por meio das Guidelines do DSA, recomenda a realização de avaliações de impacto sobre os direitos da criança (*child rights impact assessments*) como instrumento para operacionalizar o princípio. As diretrizes indicam ferramentas já disponíveis, como os modelos da UNICEF, do Ministério do Interior holandês e do CEN-CENELEC, e preveem a elaboração de orientações adicionais pela Comissão Europeia. O Reino Unido adota instrumento equivalente por meio do *children's risk assessment*, previsto nas Seções 11 e 28 do OSA.

Padrões tecnologicamente neutros. O AADC britânico adota padrões que não prescrevem soluções técnicas específicas, deixando margem para que cada serviço encontre as implementações adequadas ao seu contexto. Essa neutralidade tecnológica evita que a norma se torne obsoleta diante de mudanças tecnológicas, sendo especialmente relevante para um setor em constante transformação.

Referência a padrões técnicos reconhecidos. A BOSE Regulatory Guidance australiana orienta provedores a consultar, além dos Comentários Gerais da ONU, o padrão IEEE para serviços digitais adequados à idade (*IEEE's Standard for an Age Appropriate Digital Services Empowerment Framework*), baseado nos princípios da organização 5Rights. A remissão a padrões técnicos internacionais facilita a implementação do princípio por provedores sem familiaridade com a literatura de direitos da criança e do adolescente.

I.3. Caixa de Recompensa - Loot Box (2.3 do Benchmarking)

O ECA Digital veda caixas de recompensa oferecidas em jogos eletrônicos direcionados a crianças e a adolescentes ou de acesso provável por ele, definindo-as como funcionalidade disponível em certos jogos eletrônicos que permite a aquisição, mediante pagamento, pelo jogador, de itens virtuais consumíveis ou de vantagens aleatórias, resgatáveis pelo jogador ou usuário, sem conhecimento prévio de seu conteúdo ou garantia de sua efetiva utilidade. O benchmarking buscou analisar definições e abordagens regulatórias para caixas de recompensa (loot boxes) e mecanismos similares em ambientes digitais acessados por crianças e adolescentes.

A. Jurisdições e Fontes Normativas Analisadas

Jurisdição	Fontes Normativas
Austrália	Guidelines for the Classification of Computer Games
Califórnia (EUA)	AB-2273 — California Age-Appropriate Design Code Act (2022)
Louisiana (EUA)	Part II of Chapter 20-A of Title 51 of the Louisiana Revised Statutes
Texas (EUA)	Texas Business & Commerce Code, Chapter 509 — SCOPE Act (HB 18, 2023)
Utah (EUA)	Utah Code, Title 13, Chapter 63 — Social Media Regulation Act (SB 152, 2023)
Índia	Regras de Tecnologia da Informação (Diretrizes Intermediárias e Código de Ética da Mídia Digital de 2021); Lei de Promoção e Regulamentação dos Jogos Online — PROG (2025)
Colômbia	Lei 2489/2025; Decreto Regulamentador (minuta, 2025)
Reino Unido	Online Safety Act 2023; Age Appropriate Design Code — AADC/Children's Code v. 2.1.87 (ICO, 2022)
União Europeia	Audiovisual Media Services Directive (AVMSD); General Data Protection Regulation (GDPR); Digital Services Act (DSA); Artificial Intelligence Act (AI Act); Cyber Resilience Act

B. Jurisdições que definem e que não definem o conceito de loot box

A primeira constatação do benchmarking é que a definição expressa de loot box em norma regulatória é exceção, e não regra, entre as jurisdições analisadas.

Jurisdição que define o conceito. A Austrália é a única jurisdição analisada que estabelece uma definição normativa expressa de loot box. As *Guidelines for the Classification of Computer Games* definem *paid loot boxes* como contêineres virtuais, independentemente da denominação utilizada, que podem ser adquiridos com moeda do mundo real ou com moeda virtual obtida com dinheiro real, e que recompensam o jogador com um ou mais itens digitais cuja natureza exata não é revelada antes da compra. A norma esclarece que o nome dado à funcionalidade é irrelevante: o que importa é a presença de recompensa incerta. Adicionalmente, as diretrizes australianas adotam uma categoria mais ampla, *in-game purchases linked to elements of chance*, que abrange qualquer mecanismo que conceda itens virtuais associados a elemento de sorte ou chance, indo além das loot boxes pagas stricto sensu.

Jurisdições que não definem o conceito, mas o abordam indiretamente. Colômbia e Reino Unido não definem loot boxes como categoria autônoma, mas as abordam por meio de enquadramentos funcionais. O Decreto Regulamentador colombiano tangencia o tema ao incluir "serviços aditivos como apostas e jogos online" entre os conteúdos sujeitos a restrições por faixa etária e ao exigir a limitação de características que possam gerar "exposição a dinâmicas aditivas", formulação que pode abranger os mecanismos de recompensa variável característicos das loot boxes. O AADC britânico, por sua vez, aborda mecanismos funcionalmente equivalentes sob dois ângulos: trata os *reward loops* como estratégias de extensão de engajamento cujo uso para explorar a susceptibilidade de crianças e adolescentes a comportamentos de recompensa e antecipação é expressamente proibido, e veda o uso de dados pessoais para sugerir compras dentro do aplicativo a crianças e adolescentes.

Jurisdições que não definem nem abordam o conceito. Califórnia, Louisiana, Texas, Utah e Índia não definem loot boxes nem estabelecem enquadramento regulatório específico para o mecanismo. A União Europeia tampouco dispõe de definição ou regulação harmonizada: as normas analisadas, AVMSD, GDPR, DSA, AI Act e Cyber Resilience Act, não tratam especificamente do tema.

C. Abordagens adotadas pelas jurisdições

Entre as jurisdições que abordam o tema, identificam-se três abordagens distintas.

Abordagem por classificação indicativa etária. A Austrália optou por integrar as loot boxes ao sistema de classificação de jogos eletrônicos, determinando que qualquer jogo com compras vinculadas a elementos de chance receba, no mínimo, a classificação M (não recomendado para crianças e adolescentes de 15 anos). Jogos com formas de jogo de azar simulado interativo, como caça-níqueis, roletas ou jogos de cartas com mecânicas de apostas, recebem automaticamente a classificação R18+, restrita a adultos. Essa abordagem conecta diretamente a regulação de loot boxes ao sistema de proteção etária já existente, sem exigir a criação de um regime regulatório inteiramente novo.

Abordagem por proteção de dados e design. O Reino Unido, por meio do AADC, enquadra os mecanismos de recompensa variável no âmbito da proteção de dados pessoais: a proibição não incide sobre a funcionalidade em si, mas sobre o uso de dados pessoais para potencializar esses mecanismos ou para sugerir compras a crianças. Essa abordagem é coerente com o foco do AADC em proteção de dados, e não em regulação de jogos de azar, tema que no Reino Unido é tratado separadamente pelo Gambling Act e pelas discussões em curso na Gambling Commission.

Abordagem por enquadramento como jogo de azar. Em âmbito europeu, alguns Estados-membros avançaram individualmente na qualificação de loot boxes como jogos de azar. A Bélgica foi pioneira ao determinar, em 2018, que loot boxes pagas estão sujeitas à legislação de jogos de azar. A Holanda, após um estudo de 2018 da Gaming Authority e um julgamento de 2022 do Conselho de Estado, adotou critérios para aferir quando loot boxes se qualificam como jogos de azar, exigindo que o conteúdo seja decidido pelo acaso e que o prêmio tenha valor econômico, tendo a Netherlands Authority for Consumers and Markets publicado em 2023 diretrizes atualizadas sobre o tema. A Alemanha, por sua vez, adotou uma abordagem mais cautelosa: a USK determinou em 2024 que loot boxes são mecanismos semelhantes a jogos de azar que podem comprometer a autonomia de crianças e jovens, elevando a classificação etária do jogo na ausência de medidas de precaução eficazes.

Pressão por harmonização supranacional. A resolução do Parlamento Europeu de 2023, que instou a Comissão a avaliar loot boxes e considerar medidas como a desativação por padrão de pagamentos in-game ou a proibição de loot boxes pagas, indica uma tendência de busca por abordagem europeia harmonizada. A ausência de regulação supranacional no presente tem resultado em fragmentação entre os Estados-membros, com abordagens distintas na Bélgica, Holanda e Alemanha, o que gera insegurança jurídica para provedores que operam em múltiplos mercados.

I.4. Condição Peculiar de Pessoa em Desenvolvimento (2.4 do Benchmarking)

O ECA Digital prevê a condição peculiar de pessoa em desenvolvimento biopsicossocial como um fundamento de aplicação da Lei. O benchmarking buscou examinar como diferentes jurisdições reconhecem e incorporam a condição peculiar de desenvolvimento de crianças e adolescentes em suas normativas de proteção digital.

A. Jurisdições e Fontes Normativas Analisadas

Jurisdição	Fontes Normativas
Austrália	Abordagem transversal — ver seções Melhor Interesse e Acesso Provável
Califórnia (EUA)	AB-2273 — California Age-Appropriate Design Code Act (2022)
Louisiana (EUA)	Part II of Chapter 20-A of Title 51 of the Louisiana Revised Statutes

Texas (EUA)	Texas Business & Commerce Code, Chapter 509 — SCOPE Act (HB 18, 2023)
Utah (EUA)	Utah Code, Title 13, Chapter 63 — Social Media Regulation Act (SB 152, 2023)
Índia	National Policy on Children (2013)
Colômbia	Lei 2489/2025; Decreto Regulamentador (minuta, 2025)
Reino Unido	Online Safety Act 2023; Children's Register of Risks; UK GDPR (Art. 8); Age Appropriate Design Code — AADC/Children's Code v. 2.1.87 (ICO, 2022)
União Europeia	General Data Protection Regulation — GDPR (Art. 8); Better Internet for Kids; Guidelines on measures to ensure a high level of privacy, safety and security for minors (art. 28(4) DSA)

B. Jurisdições que reconhecem e que não reconhecem a condição peculiar de desenvolvimento

O primeiro eixo de análise diz respeito à própria decisão de reconhecer ou não a condição peculiar de desenvolvimento como premissa normativa da proteção digital infantojuvenil, isto é, de ir além do critério etário binário (pessoa com mais/menos que 18 anos) para incorporar a progressividade e a heterogeneidade do desenvolvimento biopsicossocial infantojuvenil[93].

Jurisdições que reconhecem a condição peculiar de desenvolvimento. Califórnia, Índia, Colômbia, Reino Unido e União Europeia incorporam, em diferentes graus, o reconhecimento de que crianças e adolescentes não formam um grupo homogêneo e que suas capacidades, vulnerabilidades e necessidades de proteção variam conforme a etapa do desenvolvimento. A Austrália adota essa premissa de forma transversal, principalmente por meio da participação de crianças e adolescentes de diferentes faixas etárias na construção normativa. Em todas essas jurisdições, o reconhecimento ancora-se, direta ou indiretamente, no princípio das capacidades em evolução (*evolving capacities*) consagrado pela Convenção sobre os Direitos da Criança da ONU.

93 Vale pontuar que o desenvolvimento biopsicossocial abarca fatores psíquicos, relacionais, culturais e socioeconômicos que variam significativamente entre populações. O desenvolvimento infantojuvenil no Sul Global pode ser atravessado por experiências e condições materiais que não se encaixam nos marcos normativos construídos a partir da infância europeia ou norte-americana. A heterogeneidade não é apenas geográfica: crianças e adolescentes com deficiência, por exemplo, possuem marcos de desenvolvimento que divergem dos parâmetros etários convencionais. Nesse sentido: CASTRO, Lucia Rabello de (org.). Infâncias do sul global: experiências, pesquisa e teoria desde a Argentina e o Brasil. Salvador: EDUFBA, 2021.

Jurisdições que adotam critério exclusivamente etário. Louisiana, Texas e Utah não reconhecem a condição peculiar de desenvolvimento como premissa normativa. Nesses regimes, a proteção infantojuvenil é estruturada a partir de um critério etário binário, pessoa com menos ou mais que 18 anos, sem diferenciação entre faixas etárias, sem reconhecimento de estágios cognitivos ou emocionais e sem gradação das proteções conforme o desenvolvimento progressivo da autonomia.

C. Abordagens adotadas pelas jurisdições

Entre as jurisdições que reconhecem a condição peculiar de desenvolvimento, identificam-se abordagens distintas quanto à forma e ao grau de incorporação.

Segmentação por faixas etárias com perfis de desenvolvimento diferenciados. Califórnia e Reino Unido adotam a abordagem mais detalhada, estruturando cinco faixas etárias com características, capacidades e vulnerabilidades específicas, baseadas em pesquisa empírica sobre desenvolvimento infantil. A AB-2273 californiana define as faixas de 0–5, 6–9, 10–12, 13–15 e 16–17 anos, associando a cada uma delas um estágio de desenvolvimento, da pré-alfabetização à aproximação da vida adulta. O AADC britânico adota segmentação idêntica e a complementa com descrições detalhadas das características de cada faixa: a dependência integral de mediação adulta nos primeiros anos, o aumento da impulsividade e da susceptibilidade a sistemas de recompensa na faixa de 10–12 anos, a identificação da faixa de 13–15 anos como a de maior vulnerabilidade, e o reconhecimento de expectativa legítima de autonomia progressiva na faixa de 16–17 anos. O Children's Register of Risks britânico vai além e documenta dados empíricos específicos por faixa, ancorando as obrigações regulatórias em evidências sobre o impacto real do ambiente digital em cada etapa do desenvolvimento.

Princípio da evolução das faculdades como vetor normativo expresso. A Colômbia consagra expressamente o princípio da *evolución de las facultades* como um dos princípios fundamentais da Lei 2489/2025, reconhecendo que a capacidade de autonomia dos NNA é progressiva e variável conforme a etapa de desenvolvimento. O Decreto Regulamentador operacionaliza esse princípio por meio de dois mecanismos: a proteção gradual baseada em riscos por idade, que exige medidas diferenciadas e proporcionais à faixa etária com transições progressivas entre níveis de proteção; e a classificação etária de conteúdos em três grandes etapas, primeira infância (0–6 anos), crianças e pré-adolescentes (7–12 anos) e adolescentes (13–17 anos), reconhecendo que cada etapa implica capacidades, vulnerabilidades e necessidades de proteção distintas.

Abordagem de ciclo de vida. A Índia adota o conceito de ciclo de vida para estruturar a proteção infantojuvenil, determinando que práticas pedagógicas, uso de tecnologias e atividades de lazer sejam sempre apropriados à idade e ao estágio de desenvolvimento mental, cognitivo e social. A National Policy on Children reconhece expressamente que crianças não são um grupo homogêneo e que suas vozes devem ser consideradas conforme sua idade e maturidade.

Princípio do design adequado à idade. A União Europeia, por meio das Guidelines do DSA, consagra o princípio do *age-appropriate design*, segundo o qual provedores devem conceber seus serviços de forma compatível com as necessidades de desenvolvimento, cognitivas e emocionais das crianças e adolescentes, levando em conta suas capacidades evolutivas. O GDPR reforça esse reconhecimento ao estabelecer regime diferenciado de consentimento para crianças no contexto de serviços da sociedade da informação. O programa Better Internet for Kids adota a lógica da adequação à idade de forma transversal, prevendo ações de capacitação digital gradual e co-criação de comunicações com crianças de diferentes faixas etárias.

I.5. Conteúdo Pornográfico (2.5 do Benchmarking)

O ECA Digital estabelece obrigações específicas em relação ao conteúdo pornográfico: Nesse sentido, o Decreto nº 12.880/2026 conceituo a modalidade de conteúdo em questão e detalhou as obrigações presentes no ECA Digital. O benchmarking buscou analisar definições e critérios adotados por diferentes jurisdições para caracterizar conteúdo pornográfico no contexto da proteção de crianças e adolescentes.

A. Jurisdições e Fontes Normativas Analisadas

Jurisdição	Fontes Normativas
Austrália	Online Safety Act; Online Safety Code and Standards
EUA (federal)	18 U.S.C. § 2256(8); 18 U.S.C. § 1460
Califórnia (EUA)	California Lei Penal (AB 1831, cap. 926/2024); California Assembly Bill 3080
Louisiana (EUA)	Part II of Chapter 20-A of Title 51 of the Louisiana Revised Statutes (HB 570); Louisiana Revised Statutes, Title 51, Chapter 32-B
Texas (EUA)	Texas Business & Commerce Code, Chapter 509 — SCOPE Act (HB 18, 2023)

Utah (EUA)	Utah Code, Title 13, Chapter 63 — Social Media Regulation Act (SB 152, 2023)
Índia	Information Technology Act (2000), Rule 3(1)(b)
Colômbia	Lei 2489/2025; Decreto Regulamentador (minuta, 2025)
Reino Unido	Online Safety Act 2023; Children's Register of Risks; Protecting Children from Harms Online — Guidance on Content Harmful to Children; Protecting People from Illegal Harms Online — Illegal Content Judgements Guidance (ICJG); Age Appropriate Design Code — AADC/Children's Code v. 2.1.87 (ICO, 2022)
União Europeia	Audiovisual Media Services Directive (AVMSD), arts. 6-A e 28-B; Directive 2011/93/EU; Digital Services Act (DSA); Guidelines on measures to ensure a high level of privacy, safety and security for minors (art. 28(4) DSA)

B. Jurisdições que definem e que não definem conteúdo pornográfico

A análise comparada revela que a definição expressa de conteúdo pornográfico em normas digitais é menos comum do que a mera referência ao conceito como categoria sujeita a restrições. A maioria das jurisdições remete à legislação penal ou classificatória preexistente, sem construir definição autônoma no âmbito da regulação digital.

Jurisdições que estabelecem definição expressa. O Reino Unido apresenta o tratamento definitório mais desenvolvido. O *Protecting Children from Harms Online Guidance* define conteúdo pornográfico como todo conteúdo cuja natureza seja tal que seja razoável presumir ter sido produzido única ou principalmente para fins de excitação sexual, critério objetivo, centrado no conteúdo em si e não na intenção do publicador ou na reação do visualizador. Os EUA, em nível federal, trabalham com as categorias de conteúdo obsceno (*Miller test*) e conteúdo nocivo a crianças e adolescentes (*harmful to minors*), esta última definida por três critérios cumulativos: apelo ao interesse lascivo, representação ofensiva e ausência de valor literário, artístico, político ou científico sério para crianças e adolescentes. A Califórnia define conteúdo sexualmente explícito pela ausência de valor literário, artístico, político ou científico sério. A Índia define pornografia infantil como qualquer representação de criança ou adolescente em atividades sexuais explícitas reais ou simuladas ou representação das partes sexuais de criança com fins sexuais.

Jurisdições que mencionam o conceito sem defini-lo. Austrália, Louisiana, Texas, Utah, Colômbia, e União Europeia mencionam conteúdo pornográfico como categoria sujeita a restrições, mas não estabelecem definição autônoma, remetendo implicitamente à legislação penal ou classificatória preexistente. A Austrália define o conceito por remissão ao sistema de classificação indicativa, enquadrando como pornografia o conteúdo classificado ou classificável como R18+ ou X18+. A AVMSD europeia aborda o tema em dois contextos, proteção de crianças e adolescentes e plataformas de compartilhamento de vídeos, sem definir o conceito.

C. Abordagens adotadas pelas jurisdições

Distinção entre pornografia adulta legal e pornografia infantil ilegal. A distinção mais recorrente entre as jurisdições que desenvolvem o conceito é a que separa a pornografia adulta consensual, que não é ilícita em si, mas cujo acesso por crianças e adolescentes deve ser impedido, da pornografia infantil, que constitui crime em todas as jurisdições analisadas. O Reino Unido torna essa distinção especialmente clara: o *Protecting Children from Harms Online Guidance* trata da pornografia como conteúdo prejudicial a crianças, enquanto o ICJG delimita quando o conteúdo pornográfico cruza a fronteira do ilegal, trabalhando com três categorias, imagens indecentes de criança (CSAM), imagens proibidas de criança e pornografia extrema envolvendo adultos. A Austrália faz distinção equivalente entre Class 1 material (ilegal, incluindo CSAM) e Class 2 material (restrito, incluindo pornografia adulta).

Critério funcional centrado na finalidade sexual. O Reino Unido adota critério objetivo centrado na finalidade do conteúdo: é pornográfico o que foi produzido única ou principalmente para fins de excitação sexual, independentemente do meio, imagem fotográfica, vídeo, animação, conteúdo gerado por IA. A exclusão expressa de conteúdo exclusivamente textual é relevante: erótica escrita não se enquadra na definição, ainda que seja de natureza sexual. A Califórnia adota critério convergente ao definir conteúdo sexualmente explícito pela ausência de valor literário, artístico, político ou científico sério.

Subdivisão em categorias com consequências jurídicas distintas. A Austrália subdivide o conteúdo pornográfico em subcategorias, pornografia com sexo explícito real entre adultos consententes (Class 2A), pornografia com atividade sexual realisticamente simulada (Class 2B) e pornografia que envolve fetiches ou práticas específicas (Class 1C), calibrando as obrigações regulatórias conforme o grau de potencial dano. O Reino Unido adota lógica equivalente por meio do ICJG, que distingue CSAM, imagens proibidas de criança e pornografia extrema envolvendo adultos, cada categoria com critérios e consequências jurídicas próprias.

Inclusão de conteúdo sintético e gerado por IA. O Reino Unido é explícito ao afirmar que imagens e vídeos gerados por inteligência artificial, animações, hentai, pinturas e desenhos podem ser conteúdo pornográfico se atenderem ao critério principal. O ICJG enquadra deepfakes e imagens sintéticas realistas como possíveis CSAM ou pornografia extrema. A Directive 2011/93/EU da União Europeia inclui, na definição de pornografia infantil, imagens realistas de criança em conduta sexualmente explícita, abrangendo conteúdo sintético.

Avaliação holística e contextual. O *Protecting Children from Harms Online Guidance* britânico ressalta que a avaliação deve ser holística, nenhum fator isolado é determinante, e lista fatores que tornam a classificação como pornográfico mais ou menos provável. Tornam a classificação mais provável: nudez frontal detalhada, representações de atos sexuais reais, material fetichista e linguagem sexual. Tornam a classificação menos provável: finalidade artística, educacional ou dramática clara, nudez sem contexto sexual e indivíduos vestidos sem simulação de atividade sexual. O documento determina ainda que conteúdo classificado como pornográfico pelo BBFC ou pela própria Ofcom em outros contextos regulatórios deve ser tratado da mesma forma quando compartilhado em serviços digitais, garantindo coerência interinstitucional.

I.6. Conteúdo Impróprio, Inadequado ou Proibido (2.6 do Benchmarking)

O ECA Digital e o Decreto nº 12.880/2026 utilizam as categorias de conteúdo impróprio, inadequado e proibido como critérios de restrição de acesso por crianças e adolescentes, em certa medida importando para o estabelecimento dos contornos do ECA Digital conceitos que vinham já sendo utilizados no arcabouço pátrio no âmbito da classificação indicativa editada pelo Ministério da Justiça.

O benchmarking buscou examinar as categorizações e definições de conteúdos considerados impróprios, inadequados ou proibidos para crianças e adolescentes em diferentes jurisdições.

A. Jurisdições e Fontes Normativas Analisadas

Jurisdição	Fontes Normativas
Austrália	Online Safety Act; Online Safety Codes and Standards Regulatory Guidance

Califórnia (EUA)	AB-2273 — California Age-Appropriate Design Code Act (2022)
Louisiana (EUA)	Part II of Chapter 20-A of Title 51 of the Louisiana Revised Statutes (HB 570); Louisiana Revised Statutes, Title 51, Chapter 32-B
Texas (EUA)	Texas Business & Commerce Code, Chapter 509 — SCOPE Act (HB 18, 2023); Texas Penal Code, Section 43.24
Utah (EUA)	Utah Code, Title 13, Chapter 63 — Social Media Regulation Act (SB 152, 2023)
Índia	Information Technology Act (2000 e atualização de 2023); Lei de Promoção e Regulamentação dos Jogos Online — PROG (2025)
Colômbia	Lei 2489/2025; Decreto Regulamentador (minuta, 2025)
Reino Unido	Online Safety Act 2023; Children's Register of Risks; Protecting Children from Harms Online — Guidance on Content Harmful to Children; Protecting People from Illegal Harms Online — Illegal Content Judgements Guidance (ICJG); Age Appropriate Design Code — AADC/Children's Code v. 2.1.87 (ICO, 2022)
União Europeia	Digital Services Act (DSA), Recital 12 e art. 3(h); Guidelines on measures to ensure a high level of privacy, safety and security for minors (art. 28(4) DSA)

B. Jurisdições que constroem taxonomia própria e jurisdições que remetem a conceitos preexistentes

O primeiro eixo de análise diz respeito à forma como as jurisdições constroem, ou não, uma categorização própria de conteúdo impróprio, inadequado ou proibido.

Jurisdições que constroem taxonomia própria. Austrália, Colômbia e Reino Unido são as jurisdições que mais avançam na construção de uma categorização sistemática e hierarquizada de conteúdo. A Austrália estrutura o sistema em classes normativas (Class 1 e Class 2), distinguindo conteúdo intrinsecamente ilegal de conteúdo lícito mas inadequado para crianças e adolescentes. O Reino Unido adota um sistema de três camadas, conteúdo de prioridade primária (PPC), conteúdo prioritário (PC) e conteúdo não designado (NDC), com obrigações distintas para cada categoria. A Colômbia, por meio do Decreto Regulamentador, opera em três eixos complementares: a taxonomia de riscos 4C, a classificação temática e a categoria de conteúdo absolutamente proibido.

Jurisdições que remetem a conceitos preexistentes. Louisiana, Texas, Utah e Índia não constroem taxonomia própria no âmbito da regulação digital, remetendo à

legislação penal ou a normas classificatórias preexistentes. O SCOPE Act texano remete à definição de *harmful material* do Código Penal estadual. Louisiana utiliza conceitos abertos, *unlawful material*, *obscene material*, *harmful material*, sem conceituação própria, funcionando como cláusula de salvaguarda. Utah não constrói conceito geral de conteúdo impróprio, concentrando as restrições no controle de acesso por idade. A Índia distribui os critérios entre diplomas penais, regras de governança de plataformas e normas de classificação indicativa, com ênfase na *due diligence* das próprias plataformas. A Califórnia adota critério amplo e funcional, conteúdo prejudicial ao bem-estar físico, mental ou ao desenvolvimento de crianças e adolescentes, sem subdivisões formais. A União Europeia trabalha predominantemente com o conceito de conteúdo ilegal definido pelo DSA, sem estabelecer taxonomia própria de conteúdo impróprio ou inadequado para crianças, embora as Guidelines do art. 28(4) mencionem categorias além do ilegal sem defini-las. O AADC britânico, por sua vez, adota critério funcional e referencial, é prejudicial o conteúdo cujo uso de dados pessoais para servi-lo seja obviamente prejudicial à saúde da criança ou contrário a outros regimes regulatórios, sem construir taxonomia própria de categorias de conteúdo.

C. Abordagens adotadas pelas jurisdições

Sistema de classes com distinção entre ilegalidade e inadequação etária. A Austrália estrutura a distinção central de seu sistema entre conteúdo proibido por ser intrinsecamente ilícito (Class 1), independentemente de qualquer medida de controle de acesso, e conteúdo inadequado para crianças e adolescentes por razões etárias, mas lícito para adultos (Class 2). O Class 1 abrange CSAM, conteúdo violento abominável e conteúdo que promova crimes graves. O Class 2 abrange pornografia adulta consensual e outros conteúdos de alto impacto classificados como R18+ ou X18+. A consequência jurídica é distinta: o Class 1 exige remoção; o Class 2 exige restrição de acesso por sistemas eficazes de verificação etária e medidas de *safety by design*. Além das classes formais, o sistema australiano aplica critérios transversais, grau de impacto, probabilidade de acesso por crianças e adolescentes, potencial de dano físico ou psicológico e capacidade do serviço de mitigar riscos, para determinar as exigências regulatórias aplicáveis a cada tipo de serviço.

Sistema hierárquico de três camadas baseado em evidências de dano. O Reino Unido estabelece, por meio do OSA, três categorias legais (PPC, PC e NDC), cada uma com critério de classificação e obrigação regulatória distintos. O *Children's Register of Risks* constrói essas categorias a partir de evidências empíricas sobre frequência de exposição, impacto documentado por faixa etária e fatores amplificadores nos serviços. O PPC abrange pornografia, conteúdo de suicídio, automutilação e transtornos alimentares,

categorias cujo dano é considerado grave e universal, independente da faixa etária ou do tipo de serviço, gerando obrigação de prevenção total. O PC abrange abuso e ódio, bullying, violência, substâncias prejudiciais e desafios perigosos, categorias cujo dano varia conforme faixa etária e contexto, gerando obrigação graduada de proteção dos grupos em risco identificados na avaliação do serviço. O NDC abrange conteúdos que não se encaixam nas categorias formais mas que o Register documenta como capazes de causar dano significativo a um número considerável de crianças, como conteúdo sobre depressão, estigma corporal e misoginia, exigindo que os serviços os considerem em suas avaliações de risco sem a mesma estrutura prescritiva das camadas anteriores. O ICJG acrescenta a distinção entre conteúdo que retrata um crime e conteúdo que constitui um crime, sendo apenas o segundo classificável como conteúdo ilegal para fins regulatórios.

Taxonomia de riscos 4C combinada com categorias de conteúdo proibido. A Colômbia, por meio do Decreto Regulamentador, adota como referencial classificatório a taxonomia de riscos 4C, riscos de conteúdo, de conduta, de contato e de consumo, complementada por uma classificação temática de conteúdos sensíveis sujeitos a restrição etária e por uma categoria de conteúdo absolutamente proibido. A distinção entre conteúdo sujeito a restrição etária graduada e conteúdo vedado de forma absoluta corresponde funcionalmente à distinção australiana entre Class 2 e Class 1, ainda que sem utilizar essa terminologia.

Critério funcional de dano ao desenvolvimento. A Califórnia adota critério amplo e funcional: é impróprio o conteúdo considerado prejudicial ao bem-estar físico, mental ou ao desenvolvimento de crianças e adolescentes de 18 anos, incluindo conteúdo sexualmente explícito, material violento e conteúdo que promova atividades de risco como abuso de substâncias, apostas, distúrbios alimentares e cyberbullying. Esse critério não hierarquiza categorias nem distingue formalmente entre impróprio, inadequado e proibido, operando como standard aberto orientado pelo impacto no desenvolvimento infantojuvenil.

Critério cumulativo de três elementos para conteúdo nocivo a crianças e adolescentes. Os EUA, em nível federal, e o Texas adotam definição de *harmful material* estruturada em três critérios cumulativos: apelo ao interesse lascivo de crianças e adolescentes em relação a sexo, nudez ou excreção; caráter manifestamente ofensivo aos padrões da comunidade adulta quanto ao que é adequado para crianças e adolescentes; e ausência de valor literário, artístico, político ou científico sério para crianças e adolescentes. Essa estrutura tripartite, derivada do *Miller test* constitucional norte-

americano, é mais restrita do que os critérios europeus e australianos, por exigir que os três elementos estejam presentes simultaneamente.

Abordagem referencial e cruzada baseada em regimes preexistentes. O AADC britânico adota um princípio de coerência regulatória: se um tipo de conteúdo é reconhecido como prejudicial em outro contexto normativo, classificações indicativas de filmes, ratings PEGI, diretrizes do CAP ou orientações dos Chief Medical Officers, presume-se que o mesmo conteúdo é prejudicial no ambiente digital. Essa abordagem evita a duplicação de definições e mantém coerência entre diferentes regimes regulatórios, atribuindo ao provedor responsabilidade pelo conteúdo servido algoritmicamente à criança mesmo quando gerado por terceiros.

Confiança na governança das plataformas. A Índia distingue-se das demais jurisdições pela ênfase na *due diligence* das próprias plataformas como mecanismo central de definição e moderação de conteúdo impróprio ou inadequado. Os critérios de classificação são distribuídos entre as normas de governança dos provedores, com orientações de classificação indicativa operando como referência, sem que haja uma taxonomia centralizada e vinculante equivalente às dos sistemas australiano ou britânico.

II. Outros Temas

Os tópicos incluídos na categoria “Outros Temas” não se inserem propriamente na discussão acerca de conceitos e definições gerais do ECA Digital, tampouco na disciplina específica dos mecanismos de aferição de idade. Tratam de aspectos setoriais os quais contam com previsão legal expressa de regulamentação pela ANPD no próprio texto do ECA Digital.

II.1. Medidas de Prevenção e Mitigação de Risco de Acesso (4.1 do Benchmarking)

O art. 6º do ECA Digital elenca categorias específicas de risco cujo acesso, exposição, recomendação ou facilitação de contato devem ser prevenidos e mitigados pelos provedores de serviços digitais. Esta seção busca avaliar se, e em que medida, outras jurisdições regulamentam medidas voltadas à prevenção de riscos relacionados a determinados conteúdos.

A. Jurisdições e Fontes Normativas Analisadas

Jurisdição	Fontes Normativas

Austrália	Basic Online Safety Expectations (BOSE); Online Safety Act 2021; Códigos de Conduta
Califórnia (EUA)	AB-2273 — California Age-Appropriate Design Code Act (2022)
Louisiana (EUA)	HB 577; Louisiana Revised Statutes, R.S. 9:2800.29
Texas (EUA)	Texas Business & Commerce Code, Chapter 509 — SCOPE Act (HB 18, 2023)
Utah (EUA)	Utah Code, Title 13, Chapter 63 — Social Media Regulation Act (SB 152, 2023); R 152-63
Índia	Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (atualizado em abr/2023); Nota DM/15/2022-DM do Ministry of Information & Broadcasting; Lei de Promoção e Regulamentação dos Jogos Online — PROG (2025)
Colômbia	Lei 2489/2025; Decreto Regulamentador (minuta, 2025)
Reino Unido	Online Safety Act 2023, Sections 11, 12, 60, 61, 62 e Schedule 1; Age Appropriate Design Code — AADC/Children's Code v. 2.1.87 (ICO, 2022)
União Europeia	Audiovisual Media Services Directive (AVMSD); Digital Services Act (DSA), arts. 28, 34 e 35; Guidelines on measures to ensure a high level of privacy, safety and security for minors (art. 28(4) DSA)

B. Jurisdições que regulamentam medidas de prevenção e jurisdições com cobertura parcial ou ausente

A análise comparada revela que nenhuma das jurisdições analisadas replica integralmente a estrutura do Art. 6º do ECA Digital, que combina categorias de conteúdo, obrigações de design, mecanismos de apoio a vítimas e programas educativos em um único dispositivo. As jurisdições divergem quanto ao escopo das categorias cobertas, à forma de estruturação das obrigações e às lacunas regulatórias remanescentes.

Jurisdições com cobertura ampla. Reino Unido e União Europeia são as jurisdições com cobertura mais próxima à do Art. 6º, §2º, embora com diferenças relevantes. O OSA britânico apresenta correspondência robusta para conteúdo pornográfico, indução ao suicídio e automutilação, e exploração e abuso sexual, mas não cobre jogos de azar, apostas, tabaco e álcool como categorias de conteúdo prejudicial a crianças, matérias tratadas por legislação setorial distinta, nem impõe obrigações positivas de natureza educativa ou de suporte a vítimas. A União Europeia, por meio do DSA e das Guidelines do art. 28(4), estrutura medidas de prevenção com base na tipologia dos cinco Cs, conteúdo,

contato, conduta, consumo e transversais, cobrindo a maior parte das categorias do Art. 6º, mas com grau variável de especificidade.

Jurisdições com cobertura parcial. Austrália, Califórnia e Colômbia cobrem as principais categorias de risco, mas com lacunas em categorias específicas. A Austrália, por meio das BOSE e do Online Safety Act, cobre exploração e abuso sexual, violência, assédio, práticas enganosas e conteúdo pornográfico, mas não trata de forma específica de jogos de azar, apostas, tabaco e álcool como riscos digitais para crianças no âmbito das normas analisadas. A Califórnia adota cláusula aberta de dano material sem elencar categorias específicas. A Colômbia cobre exploração sexual, violência, assédio, danos à saúde, conteúdo pornográfico e publicidade de produtos aditivos, mas não regulamenta de forma específica práticas publicitárias enganosas nem indução a autodiagnóstico. O Texas cobre suicídio, automutilação, transtornos alimentares, abuso de substâncias, assédio, aliciamento e pornografia infantil, mas limita as obrigações a *known minors* e não abrange jogos de azar ou práticas publicitárias predatórias. A Índia proíbe expressamente conteúdos obscenos, pornográficos e violentos, e trata jogos de azar online por legislação específica, mas a abordagem é fragmentada e dependente da *due diligence* das plataformas.

Jurisdições com cobertura restrita ou ausente. Louisiana, Utah e Índia apresentam cobertura mais restrita. Louisiana foca em publicidade direcionada a crianças e adolescentes e verificação de idade para sites com conteúdo prejudicial, sem estrutura abrangente de prevenção. Utah concentra as medidas no controle de acesso e consentimento parental, sem abordar especificamente as categorias de risco do Art. 6º, §2º. A Índia distribui as obrigações entre diferentes diplomas normativos, sem instrumento unificado equivalente.

C. Abordagens adotadas pelas jurisdições

Abordagem por categorias hierarquizadas de conteúdo prejudicial. O Reino Unido estrutura as medidas de prevenção a partir do sistema de três camadas do OSA (PPC, PC e NDC), com obrigações distintas para cada categoria. Para o PPC (que inclui pornografia, suicídio, automutilação e transtornos alimentares), a obrigação é de prevenção universal para qualquer criança, com verificação de idade obrigatória. Para o PC (que inclui bullying, assédio e violência), a obrigação é graduada conforme os grupos etários identificados como vulneráveis na avaliação de risco do serviço. O AADC complementa esse sistema ao vedar o uso de dados pessoais de crianças para servir, recomendar ou facilitar o acesso a qualquer uma dessas categorias de conteúdo,

atribuindo ao provedor responsabilidade pelo conteúdo servido algoritmicamente mesmo quando gerado por terceiros.

Abordagem pela tipologia dos cinco Cs. A União Europeia, por meio das Guidelines do DSA, organiza as medidas de prevenção a partir de cinco categorias de risco (conteúdo, contato, conduta, consumo e transversais[94]), exigindo medidas proporcionais para cada uma delas. Para riscos de conteúdo, as plataformas devem impedir o acesso de crianças e adolescentes a pornografia, jogos de azar, tabaco e álcool, e mitigar conteúdos que incentivem automutilação e suicídio. Para riscos de contato, devem configurar por padrão as definições de privacidade mais restritivas, limitando quem pode contactar a criança ou adolescente. Para riscos de consumo, devem impedir publicidade baseada em perfilamento quando o usuário for criança ou adolescente. Para riscos transversais, devem garantir que algoritmos de recomendação não amplifiquem ou priorizem conteúdos nocivos. O DSA exige ainda que VLOPs e VLOSEs realizem avaliações periódicas de risco e implementem medidas de mitigação razoáveis, proporcionais e eficazes.

Abordagem por design seguro por padrão combinada com taxonomia de riscos. A Colômbia opera por meio do *diseño seguro por defecto*, que configura automaticamente os parâmetros mais restritivos de proteção em todas as funcionalidades do serviço, combinado com a taxonomia de riscos 4C. Para exploração e abuso sexual, o decreto limita funcionalmente características que facilitem interações danosas com adultos, como mensageria aberta e visibilidade pública de perfis. Para indução a práticas que causem danos à saúde, trata expressamente conteúdos que promovam autolesão e suicídio como categoria de risco sujeita a classificação etária e etiquetado obrigatório. Para promoção de produtos aditivos, elenca expressamente tabaco, vaporizadores, substâncias psicoativas, álcool, apostas e jogos online como temas sujeitos a restrição etária. O Sistema Integral de Monitoreo prevê ferramentas tecnológicas de detecção precoce de exploração sexual online.

Abordagem por *reasonable steps* com cláusula do melhor interesse como transversal. A Austrália estrutura as obrigações de prevenção em torno do conceito de *reasonable steps* — medidas razoáveis proporcionais à natureza do serviço, suas funcionalidades e os riscos previsíveis —, tendo como cláusula transversal a exigência de que o melhor interesse da criança seja a consideração primária no design e na operação de serviços de provável acesso por crianças e adolescentes. O sistema combina deveres gerais das BOSE, schemes regulatórios específicos do Online Safety Act e códigos de conduta de

[94] Relacionados à privacidade e à proteção de dados, como perfilamento, recomendações algorítmicas e ausência de configurações protetoras por padrão.

autorregulação supervisionada, criando um fluxo escalonado de prevenção, denúncia, investigação e remoção.

Abordagem por estratégia obrigatória de prevenção com componente tecnológico. O Texas impõe aos provedores o dever de desenvolver e implementar estratégia específica de prevenção da exposição de *known minors* a conteúdos nocivos, com componentes tecnológicos obrigatórios: lista abrangente de conteúdos a bloquear, tecnologia de filtragem, *hash-sharing*, banco de dados de palavras-chave usadas para evasão de filtros e monitoramento humano periódico. O provedor deve ainda disponibilizar publicamente a descrição das categorias de conteúdo filtradas e, ressalvadas exceções, o código de algoritmo a pesquisadores independentes de segurança.

Abordagem por legislação setorial fragmentada. A Índia distribui as medidas de prevenção entre diferentes diplomas normativos, regras de governança de plataformas, legislação específica de jogos online e orientações setoriais sobre publicidade, sem instrumento unificado. As plataformas devem impedir a hospedagem e disseminação de conteúdo obsceno, pornográfico e violento como parte de suas obrigações de *due diligence*. Jogos de azar são vedados de forma geral para o público, com a legislação de jogos online limitando-se a jogos de habilidade e e-sports oferecidos de forma responsável a jovens, com controle parental e adequação às faixas etárias. A publicidade de apostas e jogos de azar offshore é desaconselhada por orientação ministerial dirigida a influenciadores e intermediários de publicidade online.

Abordagem centrada no uso de dados pessoais. O AADC britânico distingue-se das demais abordagens por não regular conteúdo em si, mas o uso de dados pessoais de crianças e adolescentes para servir, recomendar ou facilitar o acesso a conteúdos ou interações prejudiciais. Para cada categoria de risco do Art. 6º, §2º, a proibição incide sobre o processamento de dados que exponha a criança ou o adolescente ao risco,seja para recomendar conteúdo pornográfico, pró-suicídio ou pró-automutilação, seja para exortar compras, seja para explorar a credulidade ou vulnerabilidade da criança ou adolescente em contexto publicitário.

II.2. Mecanismos de Supervisão Parental (4.2 do Benchmarking)

Os §§ 1º e 3º do Art. 17 do ECA Digital preveem a obrigatoriedade de mecanismos de supervisão parental nos serviços digitais de provável acesso por crianças e adolescentes, atribuindo à autoridade reguladora competência para apreciar esses mecanismos. O benchmarking buscou responder a duas perguntas: se existem padrões mínimos

estabelecidos para mecanismos de supervisão parental em diferentes jurisdições; e o eventual papel da autoridade reguladora na apreciação desses mecanismos.

A. Jurisdições e Fontes Normativas Analisadas

Jurisdição	Fontes Normativas
Austrália	Online Safety Act 2021
Califórnia (EUA)	AB-2273 — California Age-Appropriate Design Code Act (2022)
Louisiana (EUA)	HB 61 (Act 440 / R.S. 9:2717.1); HB 570 (R.S. 51:1772)
Texas (EUA)	Texas Business & Commerce Code, Chapter 509 — SCOPE Act (HB 18, 2023)
Utah (EUA)	Utah Code, Title 13, Chapter 63 — Social Media Regulation Act (SB 152, 2023); R 152-63
Índia	Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (atualizado em abr/2023)
Colômbia	Lei 2489/2025; Decreto Regulamentador (minuta, 2025)
Reino Unido	Online Safety Act 2023, Sections 12, 20, 21 e 75; Protection of Children Code of Practice for Search Services (Ofcom, jul/2025); Protection of Children Code of Practice for User-to-User Services (Ofcom, jul/2025); Age Appropriate Design Code — AADC/Children's Code v. 2.1.87 (ICO, 2022)
União Europeia	Digital Services Act (DSA), arts. 28, 35, 37, 44, 45, 49 e 51; Guidelines on measures to ensure a high level of privacy, safety and security for minors (art. 28(4) DSA)

B. Jurisdições que estabelecem padrões mínimos e jurisdições que não os estabelecem

Jurisdições que estabelecem padrões mínimos expressos. Texas, Utah e Reino Unido são as jurisdições que mais avançam na definição de padrões mínimos concretos para mecanismos de supervisão parental. O SCOPE Act texano enumera funcionalidades obrigatórias (controle de configurações de privacidade da conta do usuários com menos que 18 anos, restrição de compras e transações financeiras, monitoramento e limitação do tempo de uso), exigindo ainda a verificação prévia do pai ou responsável antes do acesso

às ferramentas. Utah prevê consentimento parental verificado, acesso ao conteúdo da conta, controle de acesso por horário, ajuste de configurações e bloqueio de acesso. O AADC britânico estabelece padrões mínimos de forma condicional, ativados apenas quando o provedor opta por oferecer ferramentas parentais, incluindo transparência com a criança sobre o monitoramento ativo, escalonamento por faixa etária, informação aos pais sobre o direito de privacidade da pessoa com menos de 18 anos e vedação ao monitoramento encoberto. Os Codes of Practice da OFCOM fixam padrões mínimos para materiais de apoio a pais e responsáveis, sistemas de reporte e reclamação acessíveis, e sinalização proativa de recursos de apoio em situações de risco.

Jurisdições que reconhecem a supervisão parental sem definir padrões mínimos. Austrália, Califórnia, Índia e Colômbia reconhecem a supervisão parental como elemento do modelo de proteção, mas sem estabelecer requisitos técnicos mínimos detalhados. A Austrália prevê o dever dos provedores de fornecer informações sobre como supervisionar e controlar o acesso de crianças a conteúdos, sem especificar funcionalidades mínimas. A Califórnia exige ferramentas visíveis, acessíveis e responsivas, sem maior detalhamento. A Índia recomenda a implementação de ferramentas de controle e bloqueio parental, sem definir padrões técnicos. A Colômbia garante o acesso a ferramentas de controle parental e impõe ao Governo o dever de capacitar pais sobre os mecanismos disponíveis, sem regulá-los diretamente. A União Europeia menciona ferramentas parentais como medida de mitigação para VLOPs e estabelece diretrizes operacionais relevantes nas Guidelines do art. 28(4), mas sem definir padrões técnicos mínimos vinculantes.

C. Abordagens adotadas pelas jurisdições

Padrões mínimos com funcionalidades obrigatórias enumeradas. O Texas adota a abordagem mais prescritiva, enumerando em lei as funcionalidades que as ferramentas parentais devem necessariamente oferecer: controle de configurações de privacidade e conta, restrição de compras e transações financeiras, e monitoramento e limitação do tempo de uso. O acesso às ferramentas é condicionado à verificação prévia da mãe, do pai ou responsável pelo provedor. Utah adota estrutura equivalente, acrescentando o bloqueio de acesso até conformidade com os requisitos de verificação etária e consentimento parental.

Padrões mínimos condicionais com ênfase na transparência com a criança e o adolescente. O AADC britânico distingue-se das abordagens prescritivas por ativar os padrões mínimos apenas quando o provedor opta por oferecer ferramentas parentais, sem torná-las obrigatórias universalmente. Uma vez oferecidas, devem observar requisitos de

transparência com a criança, incluindo sinal visível de monitoramento ativo, escalonamento por faixa etária e vedação ao monitoramento encoberto. Essa abordagem reflete o reconhecimento de que a supervisão parental não pode operar sem o conhecimento da criança ou do adolescente, sob pena de violar o princípio da lealdade do GDPR e o direito de privacidade consagrado no Art. 16 da UNCRC.

Proteção estruturada pelas plataformas, com papel subsidiário dos pais. O Reino Unido, por meio do OSA, adota uma lógica em que a proteção de crianças e adolescentes é estruturada como dever das plataformas perante todos os usuários, e não como responsabilidade delegada aos pais. Os controles parentais aparecem como instrumento complementar, e não como mecanismo central de proteção. Os Codes of Practice da OFCOM operacionalizam esse modelo ao exigir materiais de apoio específicos para pais e responsáveis, sistemas de reporte e reclamação acessíveis e sinalização de recursos de apoio em situações de risco, sem criar regime autônomo de controles parentais com funcionalidades mínimas definidas.

Ferramentas parentais como medida de mitigação complementar. A União Europeia, por meio das Guidelines do DSA, enquadra as ferramentas parentais como complementares ao *safety by design* e a outras medidas técnicas da plataforma, rejeitando expressamente modelos em que a conformidade dependa exclusivamente delas. As diretrizes estabelecem requisitos operacionais relevantes: facilidade de uso sem necessidade de conta própria do responsável no serviço, independência de hardware e sistema operacional, transparência radical com a criança e adolescente sobre o monitoramento ativo, segurança equivalente à ativação inicial para alterações de configuração e interoperabilidade com ferramentas de balcão único. As funcionalidades possíveis (gestão de configurações padrão, limites de tempo de tela, visualização de contas de contato da criança e adolescente, gestão de limites de gastos) são listadas como exemplos, não como obrigações.

Consentimento parental verificável como substituto de ferramentas de monitoramento. Louisiana adota uma abordagem distinta das demais: em vez de ferramentas de monitoramento contínuo, a proteção é estruturada em torno do consentimento parental verificável como condição de acesso ao serviço e de realização de compras pelos usuários com menos de 18 anos. A vinculação obrigatória da criança e adolescente a uma conta parental cria um mecanismo de supervisão indireta, sem exigir funcionalidades específicas de monitoramento.

Submissão à autoridade reguladora: fiscalização ex post como regra. Nenhuma das jurisdições analisadas prevê submissão prévia ou aprovação formal dos mecanismos de supervisão parental pela autoridade reguladora.

O modelo dominante é de conformidade autorregulatória com fiscalização ex post: os provedores implementam os mecanismos que considerarem adequados e estão sujeitos à verificação posterior pela autoridade competente. O DSA prevê auditorias independentes obrigatórias para VLOPs e VLOSEs, com transmissão dos relatórios ao Coordenador dos Serviços Digitais e à Comissão. A Colômbia prevê relatórios anuais das plataformas ao MinTIC, avaliados por auditoria externa, com possibilidade de recomendações de melhoria. O OSA britânico estrutura a fiscalização por meio de relatórios de transparência anuais das grandes plataformas e dos poderes de investigação da OFCOM, sem aprovação prévia dos mecanismos específicos.

II.3. Procedimento de Apelação para Contas Suspensas (4.3 do Benchmarking)

O Art. 24, §4º do ECA Digital prevê o direito de apelação do titular de conta suspensa quando há indícios de operação por criança ou adolescente. O benchmarking buscou examinar como diferentes jurisdições estabelecem procedimentos de apelação para contas suspensas.

A. Jurisdições e Fontes Normativas Analisadas

Jurisdição	Fontes Normativas
Austrália	Social Media Minimum Age Regulatory Guidance
Califórnia (EUA)	AB-2273; AB 1043
Louisiana (EUA)	—
Texas (EUA)	Texas Business & Commerce Code, Chapter 509 — SCOPE Act (HB 18, 2023)
Utah (EUA)	Utah Code, Title 13, Chapter 63 — Social Media Regulation Act (SB 152, 2023); R 152-63
Índia	—
Colômbia	Lei 2489/2025; Decreto Regulamentador (minuta, 2025)

Reino Unido	Online Safety Act 2023, Section 21(5)(e); Protection of Children Code of Practice for Search Services (Ofcom, jul/2025), medidas PCS D11 e D12; Protection of Children Code of Practice for User-to-User Services (Ofcom, jul/2025), medidas PCU B2.4, B3.4, D11 e D12; Age Appropriate Design Code — AADC/Children's Code v. 2.1.87 (ICO, 2022)
União Europeia	Digital Services Act (DSA), arts. 20 e 21; Guidelines on measures to ensure a high level of privacy, safety and security for minors (art. 28(4) DSA)

B. Jurisdições que estabelecem e que não estabelecem procedimento de apelação

Jurisdições que estabelecem procedimento de apelação. Austrália, Reino Unido e União Europeia são as jurisdições que mais avançam no estabelecimento de procedimentos de apelação, ainda que com estruturas e escopos distintos. A Austrália prevê, na Social Media Minimum Age Regulatory Guidance, que as plataformas devem implementar processos para corrigir erros em suspensões incorretas ou injustas, com informações claras sobre como solicitar revisão. O Reino Unido estrutura o mecanismo mais detalhado, por meio dos Codes of Practice da Ofcom, com procedimentos diferenciados para serviços de busca e serviços user-to-user. A União Europeia obriga as plataformas a manter sistema interno eficaz de tratamento de reclamações para contestar suspensões e encerramento de contas, com acesso adicional a mecanismos de resolução extrajudicial de litígios e recurso judicial.

Jurisdições que não estabelecem procedimento de apelação. Texas, Utah, Colômbia e Índia não preveem procedimento de apelação para contas suspensas em razão de indícios de uso por crianças e adolescentes. A Colômbia reconhece genericamente o direito à livre expressão dos NNA e menciona sistemas de solução de queixas, sem regulamentá-los ou estabelecer garantias procedimentais mínimas. O AADC britânico menciona a possibilidade de os provedores identificarem e encerrarem contas de crianças e adolescentes, mas não regulamenta o procedimento subsequente ao encerramento nem estabelece direito de apelação.

C. Abordagens adotadas pelas jurisdições

Procedimento de apelação por erro de avaliação de idade, lógica inversa ao ECA Digital. A abordagem mais desenvolvida é a britânica, mas opera em lógica distinta à do Art. 24, §4º do ECA Digital. O dispositivo brasileiro pressupõe a suspensão ativa da conta pelo provedor diante de indício de uso por criança/adolescente, sendo o direito de apelação exercido pelo titular da conta suspensa. Os Codes of Practice da OFCOM estruturam o mecanismo no seguinte sentido: a *age assessment appeal* é o instrumento do

usuário adulto incorretamente classificado como criança ou adolescente pelo sistema de *age assurance* para contestar a restrição imposta. Não há obrigação explícita de suspender contas identificadas como de crianças ou adolescentes, o que o Código exige é que o acesso de crianças ou adolescentes a determinados conteúdos seja restringido por controles técnicos, sem que isso implique necessariamente suspensão da conta. O direito de apelação existe, portanto, como proteção contra falsos positivos do sistema de aferição de idade, e não como garantia procedimental ao titular da conta suspensa por ter menos de 18 anos.

Diferenciação por tipo de serviço e porte do provedor. O Reino Unido diferencia os requisitos procedimentais conforme o tipo de serviço, busca ou user-to-user, e o porte do provedor. Para serviços *large* ou *multi-risk (children)*, os Códigos exigem que o provedor considere, na priorização da análise da apelação, a gravidade da restrição imposta, se a decisão foi tomada sem supervisão humana, a taxa histórica de erros em avaliações similares e eventuais representações do usuário sobre impacto em seu sustento. Se a idade tiver sido incorretamente avaliada, o provedor deve restaurar o acesso ao conteúdo ou ao serviço e monitorar tendências nas apelações para aprimorar o processo de *age assurance*. Para os demais serviços, a exigência é de determinação pronta da apelação, com idênticas obrigações de restauração de acesso e monitoramento.

Sistema em camadas com resolução extrajudicial e judicial. A União Europeia estrutura o mecanismo de apelação em três camadas: sistema interno de tratamento de reclamações, resolução extrajudicial de litígios por órgãos certificados e recurso judicial. As Guidelines do art. 28(4) especificam que os sistemas internos de tratamento de queixas devem permitir aos usuários contestar decisões de suspensão ou erros em avaliações de idade de forma gratuita e simplificada. Essa estrutura em camadas oferece vias progressivas de contestação, sem incentivar que se recorra imediatamente à via judicial.

Obrigação de transparência e correção de erros como substituto de procedimento formal. A Austrália adota abordagem menos formalizada: a Regulatory Guidance estabelece a expectativa de que as plataformas garantam informações claras sobre como solicitar revisão de suspensões incorretas e formas fáceis de denunciar contas irregulares, sem estruturar um procedimento formal com etapas, prazos e critérios de priorização definidos em norma.

Ausência de apelação com transparência nas decisões de configuração. A Colômbia, embora não preveja procedimento de apelação, exige que qualquer modificação às configurações de proteção seja compreensível e precedida de informação suficiente, e que transições entre faixas etárias sejam comunicadas de forma clara ao usuário e ao

responsável adulto. Esses dispositivos garantem transparência nas decisões da plataforma sobre o perfil de proteção do usuário, sem constituir procedimento formal de contestação.

II.4. Remoção e Comunicação de Violações Graves (4.4 do Benchmarking)

O Art. 27 e seu §1º do ECA Digital regulamentam a remoção de conteúdos relacionados a exploração, abuso sexual, sequestro e aliciamento de crianças e adolescentes, bem como as obrigações de comunicação às autoridades competentes. O benchmarking buscou responder a três perguntas: (i) quais prazos a jurisdição estabelecia para remoção de conteúdos classificados como violações graves; (ii) quais são as obrigações de comunicação às autoridades competentes; (iii) e se existem requisitos para os relatórios enviados a essas autoridades.

A. Jurisdições e Fontes Normativas Analisadas

Jurisdição	Fontes Normativas
Austrália	Online Safety Act 2021; BOSE Regulatory Guidance
Califórnia (EUA)	—
Louisiana (EUA)	—
Texas (EUA)	Texas Business & Commerce Code, Chapter 509 — SCOPE Act (HB 18, 2023)
Utah (EUA)	Utah Code, Title 13, Chapter 63 — Social Media Regulation Act (SB 152, 2023); R 152-63
Índia	Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (atualizado em abr/2023)
Colômbia	Lei 2489/2025; Decreto Regulamentador (minuta, 2025)
Reino Unido	Online Safety Act 2023, Sections 10, 66 e 67; Protection of Children Code of Practice for Search Services (Ofcom, jul/2025), medidas PCS C1, C2, C4, C5 e A5; Protection of Children Code of Practice for User-to-User Services (Ofcom, jul/2025), medidas PCU C1, C2, C4, C5 e A5; Age Appropriate Design Code — AADC/Children's Code v. 2.1.87 (ICO, 2022)

União Europeia	Digital Services Act (DSA), arts. 9, 16, 18 e 22; Guidelines on measures to ensure a high level of privacy, safety and security for minors (art. 28(4) DSA)

B. Jurisdições que estabelecem obrigações de remoção e comunicação e jurisdições com cobertura parcial ou ausente

Jurisdições com regime estruturado. Austrália, Reino Unido e União Europeia são as jurisdições com regimes mais desenvolvidos de remoção e comunicação de violações graves, combinando prazos ou parâmetros temporais, obrigações de notificação às autoridades e requisitos de relatórios. A Índia estabelece obrigação de remoção imediata e notificação às autoridades criminais competentes em casos envolvendo crianças e adolescentes, mas sem estrutura de relatórios equivalente. A Colômbia reconhece a necessidade de resposta oportuna, mas remete a definição de prazos e obrigações concretas a atos normativos posteriores, configurando lacuna regulatória reconhecida pelo próprio decreto.

Jurisdições sem regime específico. Texas, Utah, Louisiana e Califórnia não estabelecem regime específico de remoção e comunicação de violações graves no âmbito das normas analisadas, sem que o benchmarking identifique instrumento equivalente nessas jurisdições para as categorias de conteúdo do Art. 27 do ECA Digital.

C. Abordagens adotadas pelas jurisdições

Prazo fixo de remoção ativado por notificação regulatória. A Austrália adota o modelo mais preciso em termos de prazo: o eSafety Commissioner pode emitir *removal notice* exigindo remoção ou bloqueio de Class 1 material, que inclui CSAM e conteúdo de exploração infanto juvenil, dentro de 24 horas após a notificação, salvo prazo distinto expressamente autorizado pelo próprio regulador. Esse modelo concentra no regulador a responsabilidade pela ativação do prazo, combinando denúncia do usuário afetado, investigação pela eSafety e emissão de ordem formal ao provedor. O prazo habitual para a eSafety responder ao usuário denunciante é de dois dias úteis após o recebimento da queixa.

Parâmetro de celeridade sem prazo fixo, com metas internas supervisionadas. O Reino Unido adota abordagem distinta: o OSA exige remoção "célere" (*swiftly*) após detecção ou alerta, sem fixar prazo cronológico em horas ou dias. Os Codes of Practice da Ofcom operacionalizam esse parâmetro por meio de um modelo de *performance targets*

internos, os provedores definem suas próprias metas de desempenho para o tempo entre a identificação de suspeita de conteúdo prejudicial e a tomada de ação, equilibrando celeridade e precisão decisória, sujeitas à supervisão da Ofcom. Para *primary priority content*, categoria que abrange CSAM e conteúdo de exploração e abuso sexual de crianças, os Codes exigem remoção célere ou, onde não for tecnicamente viável a remoção imediata, aplicação célere de controles técnicos que impeçam o acesso por usuários não verificados como adultos. O sistema de *trusted flaggers*, operacionalmente a Internet Watch Foundation (IWF) em matéria de CSA, funciona como vetor de priorização: conteúdo reportado por *trusted flaggers* recebe tratamento prioritário na fila de revisão.

Remoção imediata por obrigação legal direta. A Índia estabelece obrigação de remoção imediata de conteúdo ilegal, incluindo conteúdo envolvendo exploração e abuso sexual de crianças, como parte das obrigações gerais de *due diligence* dos intermediários. Não há prazo expresso em horas, mas a imediatidade é o parâmetro normativo adotado.

Parâmetro de "efetividade e imediatidade" sem prazo concreto. A Colômbia, por meio do Decreto Regulamentador, exige moderação ou restrição "efetiva e imediata" para conteúdos ilegais e ilícitos, sem traduzir esse parâmetro em prazo concreto. Para os demais conteúdos classificados como prejudiciais, o decreto reconhece expressamente a lacuna regulatória, prevendo que o MinTIC revisará e implementará lineamentos e protocolos para resposta oportuna das plataformas em prazo ainda não definido na minuta.

Obrigação de notificação imediata às autoridades com conteúdo da comunicação definido. A União Europeia, por meio do Art. 18 do DSA, impõe aos provedores de serviços intermediários o dever de notificar imediatamente as autoridades policiais ou judiciais sempre que tiverem conhecimento de informações que suscitem suspeita de crime grave envolvendo ameaça à vida ou à segurança de pessoas, categoria que abrange, por remissão expressa do Recital 56, os crimes de abuso sexual e exploração sexual de crianças nos termos da Diretiva 2011/93/EU. O conteúdo da comunicação deve incluir toda a informação relevante disponível. Na ausência de identificação do Estado-Membro competente, a notificação deve ser feita à autoridade do país de estabelecimento do provedor ou à Europol. As Guidelines do art. 28(4) reafirmam essa obrigação e determinam que as denúncias enviadas por *trusted flaggers* devem ser processadas com prioridade absoluta e sem atraso indevido, em regime de disponibilidade 24/7.

Obrigação absoluta e imperativa de reporte à autoridade nacional. O Reino Unido, por meio da Section 66 do OSA, impõe dever absoluto de reporte à National Crime Agency (NCA) de todos os conteúdos de exploração e abuso sexual de crianças detectados

e não reportados, independentemente de considerações de privacidade. A Section 67 regulamenta a forma e o conteúdo desses reportes. Essa obrigação é estruturalmente distinta do regime de moderação de conteúdo dos Codes of Practice: enquanto os Codes regulam o processo interno de identificação e remoção de conteúdo, as Sections 66 e 67 do OSA impõem obrigação de reporte às autoridades que opera em paralelo e de forma autônoma.

Obrigação de notificação com encaminhamento centralizado. A Califórnia, e os EUA de forma mais ampla, estruturam a notificação por meio da NCMEC (National Center for Missing & Exploited Children), que funciona como intermediário centralizado entre os provedores e as autoridades policiais. Os relatórios encaminhados à NCMEC podem incluir informações sobre o indivíduo envolvido, referência histórica, informações de localização geográfica, representações visuais de aparente pornografia infantil e comunicação completa. A NCMEC encaminha o relatório às autoridades policiais e notifica os provedores.

Regime de relatórios periódicos e não periódicos supervisionados pelo regulador. A Austrália estrutura o regime de relatórios em dois tipos: relatórios periódicos, exigidos em intervalos regulares entre seis e vinte e quatro meses, e relatórios não periódicos, obrigatórios quando há pedido específico do eSafety Commissioner. O conteúdo dos relatórios pode abranger número de queixas recebidas, tempo de resposta para remoção após *removal notice*, medidas adotadas para garantir uso seguro do serviço e número de usuários ativos na Austrália. O prazo máximo de resposta é de 30 dias, e a falha em responder autoriza o eSafety a publicar declaração de não conformidade com as BOSE. A Colômbia prevê relatório anual das plataformas ao MinTIC com auditoria externa, mas sem requisitos específicos sobre remoção de conteúdos ou comunicação de violações graves.

II.5. Notificação de Violações aos Direitos de Crianças (4.5 do Benchmarking)

O parágrafo único do Art. 28 do ECA Digital prevê a obrigação de notificação de violações aos direitos de crianças e adolescentes às autoridades competentes. O benchmarking buscou avaliar três aspectos em outras jurisdições: (i) quais violações devem ser notificadas; (ii) a quem as notificações devem ser enviadas; e (iii) quais são os requisitos para os relatórios enviados.

A. Jurisdições e Fontes Normativas Analisadas

Jurisdição	Fontes Normativas

Austrália	Online Safety Act 2021; BOSE Regulatory Guidance
EUA (federal)	18 U.S.C. § 2258A
Califórnia (EUA)	—
Louisiana (EUA)	—
Texas (EUA)	Texas Business & Commerce Code, Chapter 509 — SCOPE Act (HB 18, 2023)
Utah (EUA)	Utah Code, Title 13, Chapter 63 — Social Media Regulation Act (SB 152, 2023); R 152-63
Índia	Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (atualizado em abr/2023); Protection of Children from Sexual Offences Act (POCSO), 2012 (atualizado em fev/2023)
Colômbia	Lei 2489/2025; Decreto Regulamentador (minuta, 2025)
Reino Unido	Online Safety Act 2023, Sections 20, 21, 66 e 67; Protection of Children Code of Practice for Search Services (Ofcom, jul/2025), medidas PCS D1, D2, D7 e A5; Protection of Children Code of Practice for User-to-User Services (Ofcom, jul/2025), medidas PCU C1, C2, D1, D2, D7 e A5; Age Appropriate Design Code — AADC/Children's Code v. 2.1.87 (ICO, 2022)
União Europeia	Digital Services Act (DSA), arts. 18 e 22; Guidelines on measures to ensure a high level of privacy, safety and security for minors (art. 28(4) DSA) — ver Seção X

B. Jurisdições que estabelecem regime de notificação e jurisdições com cobertura parcial ou ausente

Jurisdições com regime estruturado. EUA, Austrália, Índia e Reino Unido são as jurisdições com regimes mais desenvolvidos de notificação de violações aos direitos de crianças e adolescentes, com categorias de violações notificáveis definidas, autoridades destinatárias identificadas e fluxos de comunicação formalizados. A União Europeia estrutura o regime de notificação por meio do DSA, tratado na Seção X deste relatório, para onde se remete.

Jurisdições sem regime específico. Colômbia, Texas, Utah, Louisiana e Califórnia não estabelecem regime específico de notificação de violações aos direitos de crianças no âmbito das normas analisadas. A Colômbia reconhece implicitamente a necessidade de um

regime de notificação, mas difere sua definição para atos normativos posteriores. O AADC britânico limita as obrigações de notificação ao regime de violações de dados pessoais do GDPR, sem regime autônomo de notificação de violações aos direitos das crianças e adolescentes em sentido amplo.

C. Abordagens adotadas pelas jurisdições

Intermediário regulatório especializado como filtro entre provedores e autoridades. A Austrália estrutura o fluxo de notificação por meio da eSafety Commissioner como autoridade intermediária especializada. Reclamações e informações sobre conteúdos nocivos ou ilegais são encaminhadas à eSafety, que realiza triagem entre regulação administrativa e enforcement penal, avaliando a gravidade do conteúdo, o risco envolvido e a necessidade de medidas coercitivas ou encaminhamento penal. Quando o conteúdo ou a conduta é considerada suficientemente grave, a eSafety encaminha o caso às autoridades policiais competentes. Esse modelo concentra no regulador a responsabilidade pelo fluxo de notificação, evitando que provedores se relacionem diretamente com múltiplas autoridades para diferentes categorias de violação.

Notificação direta a autoridade centralizada para abuso sexual infantil. Os EUA, por meio do 18 U.S.C. § 2258A, impõem aos provedores obrigação de notificação direta à NCMEC (National Center for Missing & Exploited Children) em casos de abuso sexual e pornografia infantil. A NCMEC funciona como intermediário centralizado, encaminhando os reportes às autoridades policiais competentes e notificando os provedores. Em paralelo, violações à COPPA são reportadas à FTC. Esse modelo de notificação centralizada por tipo de violação reduz a fragmentação institucional e cria um ponto único de contato para a categoria de maior gravidade.

Dever absoluto de reporte a autoridade especializada com regime regulamentado. O Reino Unido adota o modelo mais formalizado para a categoria de maior gravidade. A Section 66 do OSA impõe dever absoluto de reporte à National Crime Agency (NCA), operacionalmente por meio do CEOP Command, de todos os conteúdos de exploração e abuso sexual de crianças e adolescentes (CSEA) detectados, dever que se sobrepõe a considerações de privacidade. A Section 67 regulamenta a forma e o conteúdo desses reportes por meio de regulamento secundário. Para violações aos demais deveres regulatórios do OSA, a autoridade destinatária é a Ofcom. O Internet Watch Foundation (IWF) opera como *trusted flagger* credenciado, estabelecendo ponte funcional entre o sistema de moderação dos provedores e o sistema de reporte à NCA.

Sistema em duas camadas: notificação pelos usuários e notificação às autoridades. O Reino Unido, por meio dos Codes of Practice da Ofcom, estrutura o regime de notificação em duas camadas complementares. Na primeira camada, os provedores devem disponibilizar sistemas de reporte acessíveis a usuários, *affected persons* e *interested persons* para todas as categorias de conteúdo prejudicial a crianças e adolescentes (primary priority content, priority content e non-designated content), com os reportes recebidos ativando diretamente o sistema de moderação do provedor. Na segunda camada, o conteúdo identificado como CSEA aciona a obrigação de reporte à NCA nos termos da Section 66 do OSA. A medida PCU A5 exige que grandes provedores e serviços *multi-risk (children)* rastreiem evidências de novos tipos de conteúdo prejudicial e de aumentos incomuns em categorias existentes, incluindo informações de *trusted flaggers* e grupos especializados.

Categorias amplas de violações notificáveis com fragmentação institucional. A Índia define categorias amplas de conteúdo sujeito a notificação, abuso sexual, pornografia, uso de drogas, entorpecentes, álcool e tabaco, automutilação, induzimento ao suicídio, terrorismo e uso de armas, com obrigação específica de notificação às autoridades criminais competentes em casos envolvendo crianças e adolescentes. A fragmentação entre diferentes diplomas normativos (IT Rules, POCSO e legislação criminal geral) resulta em fluxos de notificação distribuídos entre diferentes autoridades conforme a natureza da violação, sem autoridade destinatária única para todas as categorias.

Regime de notificação remetido a atos normativos posteriores. A Colômbia reconhece implicitamente a necessidade de um regime de notificação ao prever que o MinTIC desenvolverá protocolos para resposta frente a conteúdos que gerem riscos para NNA, com coordenação com as autoridades respectivas. A arquitetura institucional desenhada pelo decreto, distribuindo competências entre MinTIC, SIC, ICBF, Ministério da Justiça e Fiscalía, sugere que diferentes tipos de violações seriam direcionados a diferentes autoridades, mas sem formalização dos fluxos de notificação nem definição da autoridade destinatária principal para cada categoria.

Notificação de violações de dados pessoais como único regime autônomo. O AADC britânico limita as obrigações de notificação ao regime de violações de dados pessoais do GDPR: violações que representem risco aos direitos e liberdades dos titulares devem ser notificadas ao ICO no prazo de 72 horas, com notificação adicional aos próprios titulares — e, no caso de crianças crianças e adolescentes, a seus pais ou responsáveis, quando o risco for alto. Não há no AADC regime autônomo de notificação de violações aos

direitos das crianças em sentido amplo, matéria tratada pelo OSA e pela legislação penal específica.

II.6. Acesso a Dados para Pesquisa (4.6 do Benchmarking)

O parágrafo único do Art. 31 do ECA Digital prevê o acesso a dados por instituições acadêmicas, científicas, tecnológicas, inovadoras ou jornalísticas para realização de pesquisas. O benchmarking buscou responder a duas perguntas: (i) quais critérios definem a elegibilidade para acesso a dados; e (ii) como ocorre o processo de aprovação para o acesso.

A. Jurisdições e Fontes Normativas Analisadas

Jurisdição	Fontes Normativas
Austrália	Data Availability and Transparency Act (2022); Recomendações do Joint Select Committee on Social Media and Australian Society
EUA (federal)	Family Educational Rights and Privacy Act (FERPA)
Califórnia (EUA)	AB-2273 — California Age-Appropriate Design Code Act (2022)
Louisiana (EUA)	—
Texas (EUA)	Texas Business & Commerce Code, Chapter 509 — SCOPE Act (HB 18, 2023)
Utah (EUA)	Utah Code, Title 13, Chapter 63 — Social Media Regulation Act (SB 152, 2023); R 152-63
Índia	—
Colômbia	Lei 2489/2025; Decreto Regulamentador (minuta, 2025)
Reino Unido	Online Safety Act 2023, Section 162; Age Appropriate Design Code — AADC/Children's Code v. 2.1.87 (ICO, 2022)
União Europeia	Digital Services Act (DSA), art. 40

B. Jurisdições que estabelecem regime de acesso a dados para pesquisa e jurisdições sem regime específico

Jurisdições com regime estruturado. União Europeia, Austrália e Reino Unido são as jurisdições que mais avançam na criação de regimes estruturados de acesso a dados para pesquisa, com critérios de elegibilidade definidos, processos de aprovação formalizados e salvaguardas explícitas. Os EUA dispõem de regime específico para dados educacionais por meio do FERPA, com escopo mais restrito. As demais jurisdições analisadas não estabelecem regime equivalente no âmbito das normas digitais relevantes.

Jurisdições sem regime específico. Califórnia, Louisiana, Texas, Utah, Índia e Colômbia não estabelecem regime de acesso a dados para pesquisa no âmbito das normas analisadas. A Colômbia reconhece a relevância da pesquisa para o aprimoramento do marco regulatório, mas sem criar obrigações de acesso a dados por parte das plataformas ou do Estado, remetendo o tema ao marco geral de proteção de dados da Lei 1581/2012.

C. Abordagens adotadas pelas jurisdições

Critérios cumulativos de elegibilidade com mediação por autoridade independente. A União Europeia adota o modelo mais estruturado e detalhado. O Art. 40 do DSA define seis critérios cumulativos de elegibilidade para *vetted researchers*: vínculo institucional com organização de pesquisa nos termos da Diretiva 2019/790; independência de interesses comerciais; transparência sobre fontes de financiamento; capacidade técnica de proteção e confidencialidade dos dados; demonstração de que o acesso e os prazos solicitados são necessários e proporcionais à finalidade da pesquisa, centrada na compreensão de riscos sistêmicos na UE; e compromisso formal de confidencialidade e segurança. O acesso é mediado pelo *Digital Services Coordinator*, que emite pedido fundamentado após conferir o status de pesquisador habilitado. O provedor deve entregar os dados em formato legível por máquina, dispondo de quinze dias para solicitar alteração do pedido caso comprove riscos a segredos comerciais ou vulnerabilidades de segurança.

Regime de acreditação institucional com supervisão por autoridade nacional. A Austrália estrutura o acesso a dados por meio do Data Availability and Transparency Act 2022, que institui um regime de acreditação para entidades elegíveis (órgãos governamentais da Commonwealth, estados e territórios, e universidades australianas), condicionado à demonstração de finalidade permitida, uso por pessoas apropriadas, ambiente controlado e seguro, e proteções adequadas sobre os dados e seus resultados. O processo envolve acreditação formal pelo Ministro ou pelo National Data Commissioner,

submissão de pedido formal ao *Data Custodian*, análise em prazo de quatorze a vinte e oito dias, celebração de acordo formal de compartilhamento de dados e registro pelo Comissário antes do início do compartilhamento. O benchmarking identifica, contudo, limitação de escopo relevante para o contexto do ECA Digital: o regime australiano aplica-se a dados do setor público, e não a dados detidos por plataformas digitais privadas, diferença que exige adaptação do modelo para o contexto brasileiro, que demanda acesso a dados de atores privados.

Mediação regulatória com avaliação de legitimidade e riscos à privacidade. O Reino Unido, por meio da Section 162 do OSA, atribui à OFCOM a responsabilidade de facilitar o acesso de pesquisadores a informações das plataformas para estudar riscos online, com publicação de relatórios sobre essa governança de dados. O processo é mediado pela OFCOM, que avalia a legitimidade da pesquisa e os riscos à privacidade. O regime britânico é menos detalhado que o europeu em termos de critérios formais de elegibilidade, conferindo à OFCOM maior discricionariedade na avaliação de cada pedido.

Regime setorial restrito a dados educacionais. Os EUA, por meio do FERPA, estabelecem regime de acesso a registros educacionais sem consentimento de pais ou alunos para organizações que conduzam estudos em nome de instituições educacionais, com finalidade de desenvolver ou validar testes, melhorar a instrução ou aprimorar a gestão educacional. As condições obrigatórias incluem finalidade exclusivamente educacional, uso limitado ao estudo autorizado, proibição de redistribuição e destruição dos dados após o término do estudo. Esse regime é mais restrito do que os modelos europeu e australiano, tanto no escopo dos dados acessíveis quanto no perfil dos destinatários elegíveis.

Recomendação parlamentar sem regime legal vigente. A Austrália, por meio do Joint Select Committee on Social Media and Australian Society, formulou recomendação explícita para que o governo introduza disposições legislativas que permitam acesso obrigatório a dados para pesquisadores independentes e organizações de interesse público como parte do arcabouço regulatório para plataformas digitais, com apoio a pesquisas sobre o impacto de redes sociais no bem-estar e na saúde. Essa recomendação evidencia o reconhecimento da lacuna regulatória existente no modelo australiano quanto ao acesso a dados de plataformas privadas, e sinaliza uma tendência de expansão do regime além do setor público.

Ausência de regime com remissão ao marco geral de proteção de dados. Colômbia, Louisiana, Texas, Utah e Índia não constroem regime específico de acesso a

dados para pesquisa no âmbito da regulação digital de proteção de crianças e adolescentes.

II.7. Registros de Uso Abusivo de Denúncias (4.7 do Benchmarking)

O §3º do Art. 33 do ECA Digital prevê a manutenção de registros de uso abusivo de ferramentas de denúncia. O benchmarking buscou avaliar normas que tratam de registros de uso abusivo de ferramentas de denúncia, analisando como diferentes jurisdições definem o conceito de uso abusivo, requisitos para manutenção de registros e medidas de mitigação.

A. Jurisdições e Fontes Normativas Analisadas

Jurisdição	Fontes Normativas
Austrália	Online Safety Act 2021; BOSE Regulatory Guidance
Califórnia (EUA)	—
Louisiana (EUA)	—
Texas (EUA)	Texas Business & Commerce Code, Chapter 509 — SCOPE Act (HB 18, 2023)
Utah (EUA)	Utah Code, Title 13, Chapter 63 — Social Media Regulation Act (SB 152, 2023); R 152-63
Índia	—
Colômbia	Lei 2489/2025; Decreto Regulamentador (minuta, 2025)
Reino Unido	Online Safety Act 2023, Sections 21, 23, 32 e 34; Protection of Children Code of Practice for Search Services (Ofcom, jul/2025), medida PCS D14; Protection of Children Code of Practice for User-to-User Services (Ofcom, jul/2025), medida PCU D14; Age Appropriate Design Code — AADC/Children's Code v. 2.1.87 (ICO, 2022)
União Europeia	Digital Services Act (DSA), arts. 23, §§2º e 3º; Guidelines on measures to ensure a high level of privacy, safety and security for minors (art. 28(4) DSA)

B. Jurisdições que definem uso abusivo de denúncias e jurisdições sem regime específico

Jurisdições com regime estruturado. Reino Unido e União Europeia são as jurisdições que mais avançam na definição e no tratamento do uso abusivo de instrumentos de denúncia, com critérios de caracterização, requisitos de registro e medidas de resposta formalizados. A Austrália compreende o uso abusivo de forma implícita e funcional, sem tipificação expressa nem requisitos formais de registro.

Jurisdições sem regime específico. Califórnia, Louisiana, Texas, Utah, Índia e Colômbia não estabelecem regime específico sobre uso abusivo de instrumentos de denúncia no âmbito das normas analisadas. A Colômbia menciona sistemas de solução de queixas sem regulá-los, e o decreto reconhece implicitamente a existência de mecanismos de denúncia sem abordar seu uso abusivo. O AADC britânico tampouco define nem regula o tema. A Índia, embora não preveja regime sobre uso abusivo, impõe aos provedores a obrigação de manter canais de denúncia e remover imediatamente conteúdos proibidos prejudiciais a crianças e adolescentes.

C. Abordagens adotadas pelas jurisdições

Definição funcional implícita por desvio de finalidade. A Austrália compreende o uso abusivo de forma implícita e funcional: há uso abusivo quando os mecanismos de reporte são utilizados fora de sua finalidade regulatória, isto é, para fins que não a identificação de conteúdo nocivo, ilegal ou que represente risco sério à segurança. Denúncias repetitivas, manifestamente infundadas, desalinhadas das categorias de material nocivo previstas ou que sobrecarreguem o sistema e prejudiquem a resposta a casos legítimos configuram uso incompatível com as expectativas regulatórias. Não há tipificação expressa nem requisitos formais de registro associados a esse entendimento.

Definição por critérios cumulativos com avaliação caso a caso. A União Europeia, por meio do Art. 23 do DSA, estabelece o regime mais detalhado de caracterização de uso abusivo. O §2º autoriza a suspensão do processamento de denúncias de usuários ou entidades que frequentemente submetam notificações ou reclamações manifestamente ilegais ou manifestamente infundadas. O §3º exige que a decisão de suspensão seja tomada caso a caso, de forma tempestiva, diligente e objetiva, considerando ao menos: o número absoluto de itens manifestamente ilegais ou infundados submetidos em determinado período; a proporção relativa desses itens em relação ao total de notificações do mesmo período; a gravidade dos abusos, incluindo a natureza do conteúdo ilegal e suas consequências; e, quando identificável, a intenção do usuário ou entidade. Esse modelo combina critérios quantitativos e qualitativos, evitando que a suspensão decorra automaticamente de volume, sem consideração do contexto e da intenção.

Definição por política interna supervisionada com assimetria protetiva. O Reino Unido, por meio dos Codes of Practice da OFCOM, adota modelo de autorregulação supervisionada: cada provedor deve elaborar política interna que estabeleça os atributos indicativos de que uma reclamação é manifestly unfounded, o equivalente funcional ao uso abusivo. O Code não impõe definição substantiva uniforme, mas exige que, ao desenhar a política, o provedor considere dois fatores expressamente previstos: a necessidade de identificar com precisão as reclamações manifestamente infundadas, e os riscos impostos a grupos vulneráveis e a crianças caso reclamações legítimas sejam incorretamente classificadas como tal, introduzindo assimetria protetiva que privilegia o não-descarte de denúncias em caso de dúvida. O mecanismo de descarte não se aplica a content appeals nem a age assessment appeals, categorias com regime próprio que não podem ser afastadas por essa via. Quanto ao registro, os Codes impõem três obrigações concretas de documentação: o provedor deve formalizar a política antes de poder descartar qualquer reclamação como manifestamente infundada; deve manter processo ativo de monitoramento do grau em que a política identifica incorretamente reclamações legítimas; e deve manter registro escrito do processo de revisão e de quaisquer alterações realizadas na política, datado no momento de elaboração e em cada atualização subsequente. A revisão deve ser realizada ao menos anualmente, e eventuais incorreções identificadas devem gerar alterações na política com registro correspondente. O OSA complementa esse regime ao exigir que os provedores mantenham registros detalhados de suas avaliações e da gestão de seus sistemas de denúncia para fins de auditoria.

Requisitos de registro com monitoramento contínuo e revisão periódica. O Reino Unido estabelece o regime de registro mais detalhado. Os Codes da Ofcom impõem três obrigações concretas de documentação: o provedor deve formalizar a política antes de poder descartar qualquer reclamação como manifestamente infundada; deve manter processo ativo de monitoramento do grau em que a política identifica incorretamente reclamações legítimas; e deve manter registro escrito do processo de revisão e de quaisquer alterações realizadas na política, datado no momento de elaboração e em cada atualização subsequente. A revisão deve ser realizada ao menos anualmente, e eventuais incorreções identificadas devem gerar alterações na política com registro correspondente. O OSA complementa esse regime ao exigir que os provedores mantenham registros detalhados de suas avaliações e da gestão de seus sistemas de denúncia para fins de auditoria.

Suspensão como medida de resposta com requisito de aviso prévio. A União Europeia prevê como medida de resposta ao uso abusivo a suspensão, por prazo razoável, do processamento de denúncias do usuário ou entidade abusiva, condicionada à emissão

de aviso prévio. Esse modelo gradualista (aviso antes da suspensão) evita que a primeira ocorrência resulte em exclusão imediata do acesso ao mecanismo de denúncia, preservando o direito de participação do usuário enquanto desincentiva o comportamento abusivo.

II.8. Adesivos Informativos em Embalagens (4.8 do Benchmarking)

O Art. 38 do ECA Digital prevê a obrigatoriedade de adesivos informativos em embalagens de equipamentos eletrônicos sobre proteção de crianças e adolescentes. O benchmarking buscou responder se existem jurisdições com requisitos de rotulagem estabelecidos e, caso positivos, quais seriam eles.

A. Jurisdições e Fontes Normativas Analisadas

Jurisdição	Fontes Normativas
Austrália	Consumer Goods (Infant Products) Information Standard 2024; Consumer Goods (Products Containing Button/Coin Batteries) Information Standard 2020
Califórnia (EUA)	—
Louisiana (EUA)	—
Texas (EUA)	Texas Business & Commerce Code, Chapter 509 — SCOPE Act (HB 18, 2023)
Utah (EUA)	Utah Code, Title 13, Chapter 63 — Social Media Regulation Act (SB 152, 2023); R 152-63
Índia	—
Colômbia	Lei 2489/2025; Decreto Regulamentador (minuta, 2025)
Reino Unido	Online Safety Act 2023; Age Appropriate Design Code — AADC/Children's Code v. 2.1.87 (ICO, 2022)
União Europeia	General Product Safety Regulation — GPSR, Regulamento (UE) 2023/988

B. Jurisdições que estabelecem e que não estabelecem requisitos de rotulagem em embalagens de equipamentos eletrônicos

A análise comparada revela que nenhuma das jurisdições analisadas estabelece requisito específico de adesivo ou aviso físico padronizado em embalagens de dispositivos eletrônicos orientando pais e responsáveis sobre conteúdo inadequado na internet, nos termos do que prevê o Art. 38 do ECA Digital. As normas identificadas tratam de rotulagem de segurança física de produtos ou de rotulagem digital de conteúdos online, sem equivalente funcional à obrigação brasileira.

Jurisdições com requisitos de rotulagem em embalagens físicas, mas sem foco em proteção digital. Austrália e União Europeia estabelecem requisitos de rotulagem em embalagens físicas de produtos, com menção a riscos para crianças e adolescentes, mas voltados à segurança física dos produtos e não à proteção contra conteúdo inadequado na internet. A Austrália prevê rotulagem obrigatória em produtos destinados a bebês e crianças, com avisos de segurança visíveis na embalagem externa independentemente da abertura do produto, e estende essas obrigações ao comércio eletrônico. O GPSR europeu exige identificação do produto e do fabricante, instruções de segurança em língua compreensível pelo consumidor e avaliação de risco para grupos vulneráveis incluindo crianças e adolescentes, com previsão expressa de que riscos à saúde mental decorrentes de produtos digitalmente conectados integrem a avaliação de segurança, sem, contudo, exigir aviso padronizado sobre conteúdo inadequado na internet.

Jurisdições sem qualquer requisito equivalente. EUA, Califórnia, Louisiana, Texas, Utah, Índia, Colômbia e Reino Unido não estabelecem requisitos de rotulagem em embalagens de equipamentos eletrônicos relacionados à proteção de crianças e adolescentes em ambientes digitais. A Colômbia prevê dever do Governo Nacional de informar sobre os efeitos do uso de dispositivos digitais nos NNA e de orientar pais, cuidadores e educadores, mas sem qualquer exigência de rotulagem física. O decreto colombiano regula o etiquetamento de conteúdos digitais nas plataformas, avisos informativos sobre riscos e características do conteúdo para usuários em Modo NNA, mas não estende essas obrigações ao ambiente físico de comercialização de equipamentos. O AADC britânico menciona embalagens físicas apenas de forma facultativa e pontual, ao sugerir que provedores de serviços que incluam produtos físicos podem utilizar a embalagem para destacar ferramentas de denúncia disponíveis online.

C. Abordagens adotadas pelas jurisdições

Rotulagem de segurança física com extensão ao comércio eletrônico. A Austrália estabelece requisitos de rotulagem obrigatória para produtos destinados a bebês e crianças, com avisos de segurança visíveis na embalagem externa, em pontos de venda física e, de forma visível e proeminente, nas descrições de produtos no comércio eletrônico.

Para produtos com baterias pequenas, categoria que abrange diversos equipamentos eletrônicos , a norma exige aviso claro com palavras como *warning*, *danger* ou *caution*, símbolo internacional de alerta de segurança e mensagem específica sobre riscos para crianças. Essa abordagem demonstra que a extensão das obrigações de rotulagem física ao ambiente digital de comercialização é tecnicamente viável e já adotada em outros contextos regulatórios.

Avaliação de risco para crianças e adolescentes como componente da segurança do produto digitalmente conectado. A União Europeia, por meio do GPSR, incorpora a avaliação de riscos específicos para crianças e adolescentes, incluindo riscos à saúde mental decorrentes de produtos digitalmente conectados, como componente obrigatório da avaliação de segurança do produto. Quando informações específicas forem necessárias para tornar o produto seguro para determinada categoria de pessoas, sua presença e acessibilidade devem integrar essa avaliação. Embora o GPSR não exija aviso padronizado sobre conteúdo inadequado na internet, essa disposição abre espaço para que autoridades nacionais ou a Comissão Europeia determinem avisos específicos para dispositivos com acesso à internet destinados ou prováveis de serem utilizados por crianças e adolescentes. O GPSR admite ainda o uso de QR codes e soluções eletrônicas como complemento às informações físicas, mas não como substituto.

II.9. Critérios de Adequação Etária e Modulação (4.9 do Benchmarking)

O Art. 39, §1º, I e §3º do ECA Digital tratam dos critérios de adequação etária para serviços com controle editorial e da modulação de obrigações conforme o grau de intervenção dos provedores. O benchmarking buscou analisar critérios internacionais sobre adequação etária para serviços com controle editorial e modulação de obrigações conforme o grau de intervenção dos provedores.

A. Jurisdições e Fontes Normativas Analisadas

Jurisdição	Fontes Normativas
Austrália	Basic Online Safety Expectations (BOSE); BOSE Regulatory Guidance
EUA (federal)	COPPA; CIPA
Califórnia (EUA)	AB-2273 — California Age-Appropriate Design Code Act (2022); AB 1043

Louisiana (EUA)	HB 570
Texas (EUA)	Texas Business & Commerce Code, Chapter 509 — SCOPE Act (HB 18, 2023)
Utah (EUA)	Utah Code, Title 13, Chapter 63 — Social Media Regulation Act (SB 152, 2023); R 152-63
Índia	Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (atualizado em abr/2023)
Colômbia	Lei 2489/2025; Decreto Regulamentador (minuta, 2025)
Reino Unido	Online Safety Act 2023; Age Appropriate Design Code — AADC/Children's Code v. 2.1.87 (ICO, 2022)
União Europeia	Digital Services Act (DSA), arts. 14, 19 e 33

B. Jurisdições que adotam critérios de adequação etária e jurisdições que adotam controle editorial como modulador

Critérios de adequação etária. Todas as jurisdições analisadas que abordam o tema adotam alguma forma de critério de adequação etária, ainda que com graus variáveis de sistematização. As abordagens oscilam entre critérios puramente etários e binários, menor ou maior de determinada idade, critérios desenvolvimentais baseados em faixas etárias com perfis de risco diferenciados, e critérios funcionais baseados na natureza do conteúdo e nos riscos previsíveis para cada grupo etário.

Controle editorial como modulador de obrigações. A adoção do controle editorial como critério modulador de obrigações é exceção, e não regra, entre as jurisdições analisadas. O AADC britânico é o único instrumento que formaliza o controle editorial como modulador em sentido estrito, e ainda assim de forma circunscrita a contexto específico. As demais jurisdições adotam outros critérios de modulação (porte do serviço, natureza das funcionalidades, probabilidade de acesso por crianças, tipo de conteúdo) sem atribuir ao grau de intervenção editorial papel determinante na graduação das obrigações.

C. Abordagens adotadas pelas jurisdições

Adequação etária por critério funcional baseado em risco. A Austrália adota modelo funcional no qual a adequação etária é avaliada a partir da natureza do conteúdo, do serviço e dos riscos previsíveis para crianças e adolescentes, considerando a

classificação legal dos conteúdos na plataforma, o risco de dano previsível, as funcionalidades do serviço incluindo mecanismos de interação, recomendação e amplificação, e a facilidade de contato entre crianças e adolescentes e adultos. A expectativa regulatória é de que os provedores demonstrem que crianças e adolescentes podem usar o serviço com segurança, ou que o acesso seja limitado, condicionado ou impedido quando isso não for possível. As obrigações são expressamente condicionadas ao que é *reasonable in the circumstances*, considerando tamanho e alcance do serviço, grau de influência editorial sobre o conteúdo, capacidade técnica e operacional do provedor e nível de risco para crianças. No que diz respeito à modulação, o regime australiano infere diferenciação de tratamento entre serviços com controle editorial, como streamings com curadoria de catálogo, que têm obrigações deslocadas para prevenção ex ante de classificação e restrição de acesso, e serviços com funcionalidades interativas ou conteúdo ao vivo, que ficam sujeitos a obrigações adicionais de denúncia, resposta a riscos graves e capacidade de intervenção em transmissões ao vivo. Essa diferenciação, contudo, decorre da análise baseada em riscos e não de menção expressa ao controle editorial como critério normativo.

Adequação etária por faixas etárias com perfis desenvolvimentais e critérios materiais de conteúdo. O AADC britânico estrutura a adequação etária a partir de dois eixos complementares: o eixo desenvolvimental, com cinco faixas etárias (0–5, 6–9, 10–12, 13–15 e 16–17 anos), cada uma com perfil cognitivo, emocional e comportamental distinto que orienta o design do serviço e a calibração das proteções, e o eixo de risco do processamento de dados, que avalia o tipo de dados coletados, o volume, a intrusividade do perfilamento, a existência de decisões automatizadas e o compartilhamento com terceiros. A combinação dos dois eixos determina tanto o nível de certeza exigido na aferição de idade quanto a intensidade das proteções aplicáveis. O AADC é o único instrumento analisado que formaliza o controle editorial como modulador de obrigações em sentido estrito, e ainda assim de forma circunscrita: admite que o perfilamento para curadoria de feeds de notícias para crianças seja ativado por padrão — exceção à regra geral de *off by default* para perfilamento — quando o provedor demonstrar adesão a códigos regulatórios de conduta para mídia e exercício de controle editorial sobre o conteúdo apresentado. Adicionalmente, a adesão a códigos editoriais ou de broadcasting isenta os provedores de notícias online de obrigações adicionais de proteção de dados em relação ao conteúdo noticioso. O controle editorial funciona, portanto, como modulador em dois sentidos: ampliativo, permitindo perfilamento por padrão que seria proibido sem ele; e substitutivo, dispensando obrigações adicionais de proteção de dados exigíveis de outros provedores.

Adequação etária por critérios materiais de conteúdo com classificação indicativa estruturada. A Índia adota critérios de adequação etária baseados em contexto, tema, tom, impacto e público-alvo do conteúdo, combinados com rol de diretrizes temáticas (nudez, sexo, substâncias psicotrópicas, álcool, fumo, discriminação, linguagem e comportamentos imitáveis que incitem violência, suicídio ou automutilação). O conteúdo online selecionado com curadoria deve ser classificado pelo próprio editor nas categorias previstas na lei, considerando esses parâmetros. O sistema de classificação etária estrutura-se em cinco faixas: U (universal), U/A 7+, U/A 13+, U/A 16+ e A (apenas adultos). O controle editorial é incorporado como critério de responsabilidade pela classificação, o editor do conteúdo curado é o responsável pela atribuição da faixa etária adequada, sem que isso implique modulação de obrigações regulatórias em função do grau de intervenção editorial.

Adequação etária por porte do serviço combinado com funcionalidades. O OSA britânico estrutura a modulação de obrigações não pelo controle editorial, mas pela combinação de porte do serviço com funcionalidades específicas — presença de sistema de recomendação de conteúdo e capacidade de encaminhamento ou recompartilhamento por usuários. Os critérios efetivos de modulação são a tipologia do serviço (user-to-user, serviço de busca ou serviço com conteúdo do próprio provedor), a probabilidade de acesso por crianças como gatilho binário para obrigações adicionais, a categoria regulatória definida por porte e funcionalidades, e o tipo de conteúdo que gradua a intensidade das obrigações dentro de um mesmo serviço. A distinção entre provedor que publica e provedor que hospeda opera como fronteira de regime, e não como escala de graduação de obrigações, configurando exemplo de modulação sem uso do controle editorial como critério.

Adequação etária por segmentação tripartite com taxonomia de riscos. A Colômbia, por meio do Decreto Regulamentador, operacionaliza a adequação etária em três eixos: segmentação etária tripartite, primeira infância (0–6 anos), crianças e pré-adolescentes (7–12 anos) e adolescentes (13–17 anos) , taxonomia de riscos 4C como critério material de adequação, e proteção gradual baseada em riscos por idade com transições progressivas entre faixas. A modulação de obrigações ocorre em função do grupo etário dos usuários e da proporcionalidade à natureza do serviço e aos riscos identificados, sem formalização do controle editorial como critério modulador.

Adequação etária por porte do provedor como modulador de obrigações. A União Europeia, por meio do DSA, modula obrigações em função do porte do provedor: micro e pequenas empresas são isentas das exigências operacionais mais complexas,

enquanto VLOPs e VLOSEs estão sujeitos a obrigações adicionais de avaliação de risco e mitigação. O DSA exige que provedores de serviços primariamente dirigidos a crianças e adolescentes ou predominantemente utilizados por eles expliquem as condições de uso em linguagem compreensível por crianças, sem estabelecer critérios substantivos de adequação etária para o conteúdo.

Adequação etária por probabilidade de acesso combinada com padrões setoriais. Louisiana adota abordagem que combina o conceito de *age rating*, classificação de adequação do conteúdo para faixas etárias, com remissão a padrões setoriais amplamente adotados pela indústria (*widely adopted industry standards*) para determinar categorias de idade e descrições de conteúdo, exigindo aplicação consistente e de boa-fé. Esse modelo delega à indústria a definição dos critérios substantivos de adequação, supervisionada pela exigência de consistência e boa-fé na aplicação.

PARTE III – O Desafio Técnico: Aferição de Idade

A aferição de idade figura entre os temas de maior centralidade no ECA Digital, no Decreto nº 12.880/2026 e na agenda regulatória da ANPD. A Lei nº 15.211/2025 dedica os arts. 9º a 15 ao tema, impondo obrigações específicas a fornecedores de produtos e serviços de tecnologia da informação, lojas de aplicativos e sistemas operacionais. O Decreto regulamentou conceitos estruturantes e atribuiu à ANPD a definição dos requisitos mínimos de transparência, segurança e interoperabilidade dos mecanismos a serem adotados. A Agência, por sua vez, incluiu a regulamentação dos mecanismos de aferição de idade entre as iniciativas prioritárias da Agenda Regulatória 2025–2026, e publicou orientações preliminares em março de 2026. É nesse cenário de intensa e ainda inconclusa produção normativa que a Parte III se insere.

A Parte III mapeia o campo técnico da aferição de idade em quatro dimensões complementares. A seção 3.1 apresenta os principais padrões técnicos internacionais — ISO/IEC 27566-1:2025, NIST SP 800-63-4 e IEEE 2089.1-2024 — que constituem o estado da arte normativo para o desenvolvimento e avaliação de sistemas de aferição de idade, oferecendo à ANPD referências consolidadas. A seção 3.2 examina as práticas internacionais identificadas no benchmarking, organizadas em três eixos: a distinção conceitual entre verificação e aferição de idade adotada pelas diferentes jurisdições; os fundamentos regulatórios que moldam o escopo, os objetivos e os atores responsáveis pela aferição; e os mecanismos concretos admitidos, os critérios de seleção e os momentos em que a aferição deve ocorrer. A seção 3.3 analisa as iniciativas do setor público, com base em entrevistas conduzidas, bem como experiências de outras jurisdições; enquanto a seção 3.4 examina as práticas do setor privado, com base no levantamento da OCDE sobre 50 serviços globais, no estudo do Cetic.br sobre 25 serviços no Brasil, nos relatos das entrevistas conduzidas pelo GT-6 e nos achados do Age Assurance Technology Trial australiano.

As seções 3.5 a 3.7 aprofundam três temas de particular relevância para a regulamentação brasileira: a implementação dos sinais de idade previstos no ECA Digital e no Decreto nº 12.880/2026, com análise comparada das cinco jurisdições que já adotam obrigações equivalentes para lojas de aplicativos e sistemas operacionais; as especificidades da estimativa facial de idade, tecnologia em rápida expansão que levanta questões próprias sobre uso de dados biométricos, acurácia e equidade algorítmica; e as reações à implementação de mecanismos de aferição de idade em diferentes jurisdições, com atenção aos riscos de backlash regulatório e às lições extraídas de outras jurisdições que já avançaram na matéria.

3.1. Padrões Técnicos Internacionais

A implementação técnica dos mecanismos de aferição de idade, conforme exigido pelo ECA Digital, depende de arquiteturas que garantam um equilíbrio estrito entre segurança da informação, precisão técnica e proteção de dados. Nesse cenário, os padrões técnicos internacionais elaborados pela International Organization for Standardization (ISO), pelo National Institute of Standards and Technology (NIST) e pelo Institute of Electrical and Electronics Engineers (IEEE).

I. A Norma ISO/IEC 27566-1:2025 (Sistemas de Aferição de Idade)[95]

A recém-publicada Norma ISO/IEC 27566-1:2025 (Segurança da informação, cibersegurança e proteção da privacidade — Sistemas de Aferição de Idade — Parte 1: Estrutura) estabelece um framework e as características centrais para o desenvolvimento e operação de sistemas de aferição de idade em nível global.

A Norma ISO diferencia os métodos de aferição (*age assurance methods*) organizando os métodos tecnológicos em três grandes categorias funcionais, dependendo da forma como a informação etária é obtida ou deduzida:

- **Métodos de Verificação de idade (*Age verification*):** É o método baseado no cálculo da diferença entre o ano ou a data de nascimento de um indivíduo e uma data atual ou subsequente. Geralmente esse processo utiliza informações extraídas de um documento de identidade oficial. A norma exige que os sistemas de verificação atestem obrigatoriamente que o documento apresentado é genuíno, pertence ao indivíduo correto, não está expirado e não foi revogado ou suspenso;

- **Métodos de Estimativa de idade (*Age estimation*):** É o método fundamentado na análise de características biológicas ou comportamentais humanas que variam com o amadurecimento e a idade. Tais métodos podem incluir a correlação de traços físicos de um indivíduo (por exemplo, rosto, voz, geometria da mão) ou a análise de dados derivados do comportamento do usuário (por exemplo, utilizando dados de redes sociais, uso de e-mail) Segundo a Norma, a análise de dados comportamentais pode envolver o uso de sistemas de inteligência artificial, mas também pode envolver o simples uso de técnicas como a detecção de palavras;

[95] ISO/IEC 27566-1:2025. Information security, cybersecurity and privacy protection — Age assurance systems — Part 1: Framework. Geneva: International Organization for Standardization (ISO), 2025. Disponível em: https://www.iso.org/standard/88143.html. Acesso em: 01 jun. 2026.

- **Métodos de Inferência de idade (*Age inference*):** Consiste na dedução indireta da idade, baseada em informações ou evidências verificadas que implicam que o indivíduo está acima, abaixo ou dentro de uma determinada faixa etária. Exemplos práticos trazidos pela norma incluem a apresentação de uma certidão de casamento ou a posse de um cartão de crédito validado, fatores que pressupõem que o titular atingiu a idade mínima exigida na jurisdição para obter esses itens.

Além dessas três formas primárias, a ISO descreve também a **Validação Sucessiva (*Successive validation*)**, que consiste em aplicar múltiplos métodos de forma sequencial (por exemplo, iniciar com a estimativa de idade e, caso necessário, prosseguir para a verificação documental) com o objetivo de reduzir o risco de erros e aumentar a confiabilidade do resultado.

Do ponto de vista da segurança da informação, a norma ISO/IEC 27566-1 estabelece que os provedores de aferição de idade implementem proteções robustas contra vetores de ataque específicos. A norma divide essas características de segurança em cinco pilares fundamentais (itens 8.1 a 8.5) para garantir que a arquitetura tecnológica seja resistente, confiável e preserve os dados do usuário.

A norma ISO estrutura essas exigências técnicas em cinco pilares:

01. **Segurança desde a concepção e por padrão (*Security by design and default*):** A ISO estabelece que a segurança não pode ser reativa; ela deve ser incorporada de forma proativa desde o início do desenvolvimento e durante todo o ciclo de vida do sistema. Para isso, a norma exige a implementação de: (i) Modelagem de ameaças e avaliações de risco contínuas para identificar e corrigir vulnerabilidades rapidamente; (ii) Criptografia forte para proteger as informações tanto em repouso quanto em trânsito; (iii) Segurança em múltiplas camadas (estratégia de defesa em profundidade), utilizando firewalls, controles de acesso rigorosos e sistemas de detecção de intrusão; (iv) Monitoramento contínuo para ameaças e rastreabilidade total de quaisquer mudanças no sistema, além da manutenção de um plano eficaz de resposta a incidentes.

02. **Proteção contra repetição, repasse ou reutilização (*Replay, forwarding or reuse*)** Os resultados da aferição de idade gerados para conceder um acesso não podem ser explorados por agentes mal-intencionados:
    - **Proteção contra repetição (*Replay*):** O resultado deve ser blindado contra reúso não planejado. Quando se usa uma prova criptográfica digital, o sistema deve incluir um parâmetro variável no tempo ou um

"desafio" emitido pela plataforma final para garantir que a prova de idade seja atual e precisa;

- **Proteção contra repasse (*Forwarding*):** O sistema deve impedir que o resultado de uma aferição aprovada seja repassado de uma plataforma para outra burlando controles;
- **Memorização planejada ou reutilização de um resultado de aferição de idade :** Caso a parte consiga memorizar o resultado da aferição de forma confiável um indivíduo específico, o resultado pode ser memorizado ou reutilizado em acessos futuros (evitando que o usuário repita todo o processo), desde que a duração dessa memorização seja adequadamente determinada.

03. **Resistência a ataques (*Resistance to attack*)**: Os sistemas de aferição de idade devem ser projetados e gerenciados de forma a serem resistentes a ataques. A norma recomenda que os provedores de aferição de idade tomem algumas ações para antecipar as vulnerabilidades e os vetores de ataque. Neste contexto, a norma destaca que os prestadores de serviços de verificação de idade não devem ser obrigados a divulgar seus vetores de mecanismos de prevenção de ataque em sua declaração de práticas
    - **Detecção de Ataques de Apresentação Biométrica:** A norma sugere que o sistema de aferição de idade incorpore tecnologias de detecção de vivacidade (*liveness detection*). O objetivo prático dessa verificação é garantir que a amostra biométrica esteja sendo capturada de um sujeito vivo presente no momento da interação, rejeitando tentativas de burlar o sistema com o uso de fotos estáticas, vídeos gravados ou máscaras 3D. A norma define que a vivacidade é comprovada por meio da análise de características anatômicas, reações involuntárias (como a reação da íris à luz ou pulsação), ou reações voluntárias (comportamentos do sujeito). Na prática, a ISO estabelece que essa detecção pode ser implementada de duas formas para combater os ataques:
        - **Detecção de vivacidade passiva (Passive liveness detection):** Não exige que o usuário realize nenhuma ação específica. O sistema analisa o rosto do indivíduo em tempo real, utilizando sinais reflexos e involuntários (como piscar de olhos ou movimentos da cabeça) e avaliando pistas de textura e do contexto da imagem para determinar se há uma pessoa real ou apenas uma foto diante da câmera;

    - **Detecção de vivacidade ativa (Active liveness detection):** Exige que o usuário execute ações específicas solicitadas pelo sistema, como piscar os olhos, inclinar a cabeça, virar o rosto ou sorrir em um momento exato. Para garantir a segurança, a ordem das ações solicitadas muda a cada nova verificação. A norma ressalta, no entanto, que este método é mais intrusivo e consome mais tempo do que a verificação passiva
- **Defesa contra *Spoofing*:** O sistema de aferição de idade deve ser resistente às tentativas em que o indivíduo tenta parecer mais velho para enganar a IA, como o uso de chapéus, óculos, maquiagem ou barba falsa;
- **Combate à Falsificação (*Counterfeiting*):** É obrigatório proteger a arquitetura contra a apresentação de documentos de identidade forjados ou cujas origens não possam ser validadas de modo seguro, utilizando sistemas e equipes bem treinadas para cada tipo de documento;
- **Tratamento de Contraindicadores (*Contra indicators*):** Sistemas de aferição frequentemente utilizam mais de uma fonte de dados para compor um resultado. Se as informações se contradizem (por exemplo, um documento sugere uma idade e a estimativa facial sugere outra radicalmente diferente ou há suspeita de fraude no sistema), isso é chamado de "contraindicador". Diante disso, o provedor deve tomar atitudes como coletar mais evidências para tentar resolver a divergência e atestar a veracidade, ou comunicar a existência do contraindicador à plataforma final
- **Proteção contra falhas (*Fail False):*** A norma afirma que um sistema de aferição de idade deve ser a prova de falhas, ou seja, um resultado de aferição de idade não deve levar uma parte confiável a tomar uma decisão incorreta sobre a elegibilidade relacionada à idade devido a uma falha do sistema.

Neste contexto, a Norma ISO estabelece uma distinção técnica e conceitual entre o que constitui um erro na avaliação da idade e o que constitui uma falha operacional do sistema. A norma destaca expressamente que uma decisão incorreta devido a uma falha do sistema (fail safe) é uma questão totalmente diferente de um resultado incorreto gerado pela aferição da idade (falso positivo ou falso negativo). A norma afirma que essa proteção contra falhas é diferente da ocorrência de um falso positivo ou falso negativo no resultado da aferição etária.

Isso ocorre porque o mecanismo de falha segura atua como um protocolo emergencial estrutural: caso haja um defeito, comprometimento de rede ou falha de coleta de dados, a decisão padrão exigida é a de interromper o processamento, reter qualquer exposição de dados e negar o acesso. Em contrapartida, os falsos positivos (conceder acesso a quem não deveria) e os falsos negativos (bloquear acesso a quem possui o direito) ocorrem durante o pleno funcionamento do sistema e são inerentes à natureza probabilística das tecnologias de estimativa de idade baseadas em Inteligência Artificial.

A ISO/IEC 27566-1 classifica a Taxa de Falsos Positivos (FPR) como uma métrica primária de desempenho (*Primary metrics*) e não exige sua total erradicação - o que violaria o princípio de minimização de dados e forçaria o uso desproporcional de verificação documental massiva em casos de baixo risco. O pilar essencial exigido pela norma é a Paridade de Erro de Resultado (*Outcome Error Parity*), que determina que a taxa de falsos positivos e negativos do algoritmo seja justa, consistente e não discrimine usuários baseando-se em suas etnias, gêneros ou outros fatores demográficos, tratando a margem de erro como uma variável gerenciável e auditável.

II. Diretrizes de Identidade Digital e Autenticação (Série NIST SP 800-63)[96]

O National Institute of Standards and Technology (NIST), por meio da série de publicações especiais SP 800-63, estabelece os requisitos técnicos para a arquitetura e implementação de serviços de identidade digital. Diferentemente das normativas focadas exclusivamente na estimativa etária isolada, o padrão do NIST integra a aferição de idade ao processo mais amplo de comprovação de identidade (identity proofing), tratando a idade como um atributo verificado.

A mais recente versão do framework, publicada em julho de 2025 como SP 800-63, Revisão 4, representa a atualização mais abrangente desde 2017 e é estruturada em quatro volumes complementares, cada um tratando de uma dimensão distinta do ciclo de vida de identidades digitais:

- **SP 800-63-4** (*Digital Identity Guidelines*): documento-base que estabelece o modelo geral de identidade digital, a metodologia de gestão de risco e o processo de seleção dos níveis de garantia aplicáveis a cada serviço;
- **SP 800-63A-4** (*Identity Proofing and Enrollment*): define os requisitos técnicos e procedimentais para os processos de comprovação de identidade e cadastramento de usuários;

[96] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). SP 800-63-4: Digital Identity Guidelines. Gaithersburg, MD: NIST, 2025. Disponível em: https://pages.nist.gov/800-63-4/. Acesso em: 01 jun. 2026.

- **SP 800-63B-4** (*Authentication and Authenticator Management*): especifica os requisitos para processos de autenticação e para o ciclo de vida dos autenticadores;
- **SP 800-63C-4** (*Federation and Assertions*): regulamenta o uso de arquiteturas federadas de identidade e os requisitos para asserções transmitidas entre provedores de identidade e partes confiantes.

Embora originalmente desenvolvido para atender demandas da agências federais norte-americanas, o SP 800-63 tornou-se referência técnica de adoção global — sendo citado diretamente por reguladores europeus, australianos, canadenses e pela própria indústria de tecnologia como base para arquiteturas de verificação de identidade. Sua relevância para o presente relatório deriva precisamente do fato de ser o único framework que trata de forma sistemática e mensurável os três problemas técnicos centrais da aferição de idade digital: a **comprovação de que o atributo de idade existe e é verdadeiro**, a **autenticação de que o portador da credencial é o seu titular legítimo**, e a **transmissão confiável dessas informações** entre diferentes sistemas e organizações.

a) O Modelo de Garantia por Níveis: IAL, AAL e FAL

O núcleo conceitual do SP 800-63-4 é a decomposição do problema de identidade digital em três dimensões ortogonais, cada uma com três níveis crescentes de garantia, denominados genericamente de xAL (*assurance levels*):

I. Nível de Garantia de Identidade (IAL - *Identity Assurance Level*): O IAL (detalhado no volume NIST SP 800-63A) mensura o grau de confiança de que a identidade apresentada pelo solicitante corresponde a uma pessoa real e que os atributos declarados (incluindo a data de nascimento) são precisos e verificáveis em fontes autorizadas;

II. Nível de Garantia de Autenticador (AAL - *Authenticator Assurance Level*): O AAL (detalhado no volume NIST SP 800-63B) mensura o grau de confiança de que o indivíduo que utiliza uma credencial no momento de acesso é, de fato, o titular registrado.

III. Nível de Garantia de Federação (FAL - Federation Assurance Level) mensura o grau de segurança na transmissão de informações de identidade entre diferentes entidades técnicas, sendo relevante nos cenários em que a verificação de idade é realizada por um provedor especializado (IdP) e o resultado é comunicado à plataforma que presta o serviço (*Relying Party*).

A seleção dos níveis adequados em cada dimensão não é arbitrária: o SP 800-63 prescreve um processo estruturado de gestão de risco (Digital Identity Risk Management - DIRM) pelo qual as organizações devem avaliar os impactos potenciais de falhas nos

processos de identidade (tanto para a organização quanto para os indivíduos afetados) e selecionar os controles mínimos correspondentes. Para fins de proteção de pessoas com menos de dezoito anos, esse processo de avaliação de risco deve necessariamente considerar o impacto sobre o usuário criança ou adolescente como variável central, e não como externalidade.

b) Os Níveis de Garantia de Identidade (IAL) e sua Aplicação à Aferição de Idade

O SP 800-63A-4 define três níveis de garantia de identidade com requisitos técnicos e procedimentais específicos que determinam quais tipos de evidência são aceitas, como são validadas e como se confirma o vínculo entre o portador e a identidade declarada.

No IAL1, o processo de comprovação de identidade deve suportar a existência real da identidade reivindicada, com validação de atributos essenciais (core attributes) junto a fontes autorizadas ou confiáveis. Os atributos centrais incluem obrigatoriamente um identificador governamental (como CPF, no contexto brasileiro) e, de forma recomendada, nome completo, data de nascimento e endereço físico ou digital para comunicações. O processo pode ser conduzido de forma completamente remota e automatizada, sem intervenção humana. A principal inovação desta revisão no nível IAL1 é o requisito de implementação de controles especificamente desenhados para limitar ataques de cadastramento automatizado em escala, como bots que criam contas fraudulentas massivamente, e para proteger contra o uso de identidades sintéticas e de dados de identidade comprometidos obtidos em vazamentos.

O **IAL2** exige a coleta de evidências de identidade de força *Strong* ou superior, com validação documental e verificação do vínculo entre o portador e a evidência. O processo pode ser realizado remotamente. A revisão 4 introduz, neste nível, requisitos para controles contra ataques de injeção de imagem e mídia sintética (*deepfakes*), respondendo ao avanço das ferramentas de inteligência artificial generativa. É importante notar, contudo, que o IAL2 representa uma exigência de implementação significativamente mais onerosa do que o IAL1, envolvendo processos de validação documental, captura e comparação biométrica, e integração com bases de dados de identidade, e que sua imposição generalizada a todas as plataformas, independentemente do perfil de risco do serviço, não encontra respaldo na própria metodologia do NIST. O framework reserva o IAL2 para serviços nos quais a avaliação de risco indique que os controles do IAL1 são insuficientes, e não como padrão universal.

O **IAL3**, que adiciona a obrigatoriedade de presença física perante agente treinado e coleta biométrica em sessão controlada, apresenta desafios de implementação que o

tornam inviável como modelo de verificação de idade para plataformas digitais de consumo em larga escala. Sua aplicação deve ser restrita a contextos nos quais o nível de risco e a natureza do serviço o justifiquem de forma inequívoca, sob pena de inviabilizar operacionalmente serviços de amplo acesso público.

O framework define ainda que a autodeclaração de maioridade não satisfaz nenhum dos níveis IAL. Isso não significa, porém, que a regulamentação deva impor processos de verificação documental plena a todos os serviços: o próprio SP 800-63A-4 reconhece que o nível de evidência exigível é função do risco, e que controles proporcionais — como a validação de atributos contra bases de dados confiáveis, sem necessidade de captura e análise documental presencial — são tecnicamente suficientes para os cenários de risco moderado que compõem a maior parte do universo regulatório em questão.

c) Autenticação e o Problema do Uso de Credenciais de Terceiros

Independentemente do rigor do processo de comprovação de identidade, persiste um risco técnico estrutural: após a emissão de uma credencial que atesta a maioridade do titular, em princípio nada impede tecnicamente que um terceiro, incluindo alguém com menos de 18 anos, utilize essa credencial para acessar serviços restritos. Este é o problema endereçado pela dimensão de autenticação (AAL) do framework.

d) Federação de Identidade e a Arquitetura de Verificação de Idade por Terceiros

O modelo que mais diretamente se aplica à verificação de idade em plataformas digitais de grande escala é o de **identidade federada**: o modelo de identidade federada, no qual um provedor especializado realiza a comprovação de identidade (com o nível de rigor adequado) e comunica o resultado, na forma de uma asserção criptograficamente assinada, às plataformas que dele dependem. Estas recebem apenas a informação necessária, sem acesso aos dados brutos do usuário.

O SP 800-63C-4 define os **Federation Assurance Levels (FAL)**, regulam a segurança dessa transmissão em três níveis progressivos. No **FAL1**, a asserção deve ser assinada criptograficamente e ter a audiência restrita à plataforma destinatária, com proteção contra reutilização — requisito tecnicamente acessível e compatível com os padrões de mercado já em uso em protocolos como OpenID Connect e SAML. O **FAL2** adiciona proteção contra ataques de injeção de asserção e exige acordo de confiança pré-estabelecido entre o provedor e a plataforma. O **FAL3** impõe verificação adicional de controle de autenticador

pelo usuário no momento do acesso, adequado apenas para cenários de risco muito elevado.

A revisão 4 introduz uma inovação arquitetural relevante ao reconhecer formalmente as **carteiras digitais controladas pelo usuário** (*subscriber-controlled wallets*) como modalidade de federação. Neste modelo, o IdP não opera como servidor centralizado: o CSP emite pacotes de atributos digitalmente assinados (incluindo, por exemplo, uma credencial que atesta que o titular tem mais de 18 anos, sem revelar a data de nascimento exata) e o usuário armazena esses pacotes em uma carteira digital em seu dispositivo. Quando necessário, o usuário apresenta seletivamente os atributos relevantes ao RP, sem interação com o IdP. Esta arquitetura representa uma implementação técnica nativa do princípio de **minimização de dados**: a plataforma recebe apenas a confirmação binária de maioridade, e não os dados biográficos completos do usuário.

Esta abordagem converge com desenvolvimentos recentes no campo das **credenciais verificáveis** (*Verifiable Credentials*) e da **identidade descentralizada** (*Decentralized Identity*), cujos padrões técnicos são desenvolvidos pelo World Wide Web Consortium (W3C) e estão em processo de adoção regulatória crescente, notadamente no contexto da Identidade Digital Europeia (EUDI Wallet) estabelecida pelo Regulamento (UE) 2024/1183.

III. A Norma IEEE 2089.1-2024 (Verificação Etária Online)[97]

A IEEE 2089.1-2024 foi desenvolvida pelo *Emerging Technology Standards Committee* da IEEE Consumer Technology Society, aprovada em 21 de março de 2024 e publicada em 24 de maio de 2024. Não se trata de uma norma isolada, mas da segunda peça de uma família crescente de padrões técnicos internacionais concebidos com o objetivo comum de tornar o ambiente digital seguro e adequado para crianças. Essa família, conhecida como IEEE 2089, tem como espinha dorsal os *5Rights Principles*, uma estrutura de direitos digitais da infância desenvolvida pela 5Rights Foundation com base na Convenção das Nações Unidas sobre os Direitos da Criança (UNCRC) e no Comentário Geral nº 25 (GC25) de 2021.[2]

A arquitetura da família IEEE 2089 é a seguinte: a norma fundacional **IEEE 2089-2021** estabeleceu o framework geral de serviços digitais adequados à idade (*age-appropriate digital services*), fixando os princípios orientadores que vinculam toda a

[97] IEEE STANDARDS ASSOCIATION. IEEE Std 2089.1-2024: IEEE Standard for Online Age Verification. New York: IEEE, 2024. Disponível em: <https://standards.ieee.org/ieee/2089.1/10700/>. Acesso em 27 de mai. de 2026.

família[98]. A **IEEE 2089.1-2024** desce ao plano técnico-operacional, disciplinando especificamente o *como* verificar ou estimar a idade de usuários em serviços digitais. Encontram-se ainda em desenvolvimento duas normas complementares: a **IEEE P2089.2**, voltada à padronização dos termos e condições apresentados a crianças em ambientes digitais, e a **IEEE P2089.3**, dedicada aos mecanismos de gestão e verificação do consentimento parental online[99]. Juntas, essas normas buscam cobrir os principais vetores de proteção da criança e do adolescente no ambiente digital, da adequação de conteúdo à aferição de idade, passando pela transparência contratual e pelo controle parental.

Um desenvolvimento institucional relevante e recente reforça o peso normativo da IEEE 2089.1 no cenário internacional: em janeiro de 2026, o IEEE anunciou um novo esquema de certificação baseado na norma, desenvolvido em parceria com a própria 5Rights Foundation e com o *Age Check Certification Scheme* (ACCS) do Reino Unido[100]. O esquema oferece aos reguladores um benchmark internacionalmente reconhecido para aferir se sistemas de verificação de idade são proporcionais, *privacy-preserving* e respeitadores dos direitos das crianças e dos adolescentes.

Objeto e escopo

A norma estabelece um framework de processos para que organizações determinem a necessidade, selecionem os métodos, executem a aferição e categorizem o nível de confiança dos seus sistemas de verificação de idade online. O termo central adotado é *age assurance*, tratado como guarda-chuva que abrange dois métodos distintos: *age verification* (verificação baseada em identificadores físicos ou bases autorizadas, com alta certeza sobre a data de nascimento específica) e *age estimation* (estimativa probabilística a partir de características biométricas ou comportamentais, sem necessidade de identificação exata). A norma não especifica algoritmos, sensores ou contramedidas técnicas detalhadas, seu foco é de processo e governança, não de implementação técnica prescritiva.

Estrutura de processos

---

98 IEEE STANDARDS ASSOCIATION. *IEEE Std 2089-2021: IEEE Standard for an Age-Appropriate Digital Services Framework Based on the 5Rights Principles for Children*. New York: IEEE, 2021.

99 PERSONA. *IEEE 2089: A Guide to the Global Age Assurance Standard*. Disponível em: https://withpersona.com/blog/ieee-2089. Acesso em: 27 maio 2026.

100 5RIGHTS FOUNDATION. *Age checking systems can now be certified against 5Rights-led technical standard*. Disponível em: https://5rightsfoundation.com/age-checking-systems-can-now-be-certified-against-5rights-led-technical-standard/. Acesso em: 27 maio 2026.

A norma organiza a implementação em sete processos, dos quais quatro são sequenciais e três transversais.

Os sequenciais são: (i) *Determination* — mapeamento das exigências legais, regulatórias e éticas de cada jurisdição em que o serviço opera; (ii) *Selection* — escolha dos métodos de aferição proporcionais ao perfil de risco identificado; (iii) *Assurance* — execução da aferição propriamente dita; e (iv) *Categorization* — classificação do nível de confiança atingido.

Os transversais, que permeiam todo o ciclo, são: *Privacy* (privacidade desde a concepção), *Data Security* (segurança dos dados pessoais processados) e *Interoperability* (possibilidade de reaproveitamento de verificações entre provedores distintos, de forma *privacy-preserving*).

Níveis de confiança (Annex A — normativo)

O elemento mais operacionalmente relevante da norma é o sistema de cinco níveis de confiança definido no Anexo A normativo, derivado de seis indicadores: precisão do resultado, frequência da aferição, extensão das medidas antifraude, autenticidade do usuário, frequência de autenticação e necessidade de uso da data de nascimento específica. Os cinco níveis são:

- **Asserted**: autodeclaração sem qualquer validação. Confiança zero. Aplicável apenas a fluxos de baixíssimo risco (ex.: cadastro em newsletter infantil com conteúdo adequado a todas as idades).
- **Basic**: controles mínimos, validade indefinida, falsa positiva tolerável até 5%. Indicado para restrições de conteúdo sem risco significativo.
- **Standard**: verificação anual, falsa positiva máxima de 3%, *liveness detection* obrigatória, paridade de erro por grupos protegidos máxima de 1%. Indicado para acesso a conteúdo pornográfico.
- **Enhanced**: verificação mensal, falsa positiva máxima de 1%, autenticação de dois fatores, contraindicadores resolvidos. Indicado para jogos de azar online.
- **Strict**: verificação semanal, falsa positiva máxima de 1%, autenticação biométrica com *liveness detection*, maior exigência de antifraude. Indicado para aquisição de produtos de alto risco.

Um ponto técnico relevante é o conceito de *buffer*: quando se utiliza estimativa de idade, a "idade desafio" (*challenge age*) testada deve ser suficientemente superior à idade mínima exigida para absorver a margem de erro probabilística, assegurando que o nível de

confiança requerido seja atingido mesmo diante da natureza estatística do método. Quando a idade do usuário estiver próxima demais da fronteira etária regulatória, a norma determina que se migre para verificação documental.

Atores e responsabilidades

A norma estrutura três papéis centrais: (i) *relying party* — a organização que exige a aferição (a plataforma); (ii) *age assurance provider* — o fornecedor do sistema de verificação ou estimativa, interno ou terceirizado; e (iii) *user* — o usuário cujo acesso está sendo avaliado. Um quarto ator, o *process assessor*, pode intervir para fins de certificação e auditoria independente, conforme os requisitos regulatórios aplicáveis, não sendo, portanto, um papel de presença obrigatória em todos os arranjos. A norma é explícita ao exigir que, quando a aferição for realizada internamente pela própria plataforma, ela deve ser mantida em separação operacional suficiente para garantir independência e ausência de conflito de interesse.

Privacidade e minimização de dados

O regime de privacidade da norma é centrado em dois princípios operacionais. Primeiro, a resposta da aferição deve ser transmitida como resultado binário ("pass"/"fail") ou, quando regulatoriamente exigido, como faixa etária, e não como data de nascimento completa. Segundo, todos os dados coletados para fins de aferição não podem ser reaproveitados para qualquer outra finalidade, inclusive perfilamento. O processo de interoperabilidade entre provedores deve igualmente compartilhar apenas o atributo de idade, sem criar rastro digital da criança ou do adolescente (*digital footprint*).

Tais premissas são integralmente condizentes com os mandamentos da LGPD e do ECA Digital, sinalizando que as soluções tecnológicas hoje existentes são importantes ferramentais para a operacionalização da lei e seus mandamentos, de maneira protetiva dos direitos das crianças e adolescentes.

Avaliação de risco — os 4 Cs (Annex B — normativo)

O Anexo B normativo introduz o framework dos *4 Cs of Online Risk*, que classifica os riscos a crianças e adolescentes em quatro categorias: *Content* (exposição a material nocivo), *Contact* (interação com agentes maliciosos), *Conduct* (participação em trocas prejudiciais entre pares) e *Contract/Commercial* (exposição a relações comerciais inadequadas). O framework serve de instrumento para que as organizações realizem a fase de *Determination* de forma estruturada, mapeando quais funcionalidades do serviço geram

quais categorias de risco e, portanto, qual nível de confiança de aferição se justifica proporcionalmente.

3.2. Práticas Internacionais

Esta seção traz as lições extraídas do benchmarking sobre mecanismos de aferição de idade, organizado em dois blocos. O primeiro examina as distinções conceituais e práticas entre verificação e aferição de idade adotadas pelas jurisdições analisadas. O segundo é dedicado especificamente aos mecanismos de aferição de idade enquanto objeto regulatório autônomo e aborda três dimensões: os fundamentos regulatórios da aferição de idade em diferentes jurisdições, incluindo definições, objetivos e delimitação de escopo de aplicação; os atores relevantes e suas responsabilidades, incluindo o papel do Estado e a eventual previsão de entidades certificadoras; e a implementação prática, examinando os tipos de mecanismos admitidos, os critérios utilizados para selecionar o mecanismo mais adequado a cada contexto e o momento em que a aferição deve ocorrer.

I. Verificação de Idade vs. Aferição de Idade (2.7 do Benchmarking)

O ECA Digital utiliza os termos “aferição de idade” e “verificação de idade” sem defini-los expressamente. Nesse contexto, o benchmarking analisou as distinções conceituais e práticas entre aferição e verificação de idade adotadas em diferentes jurisdições. Posteriormente, o Decreto nº 12.880/2026 conceituou ambos os termos.

A. Jurisdições e Fontes Normativas Analisadas

Jurisdição	Fontes Normativas
Austrália	Online Safety Amendment (Social Media Minimum Age) Act 2024; Social Media Minimum Age Regulatory Guidance
Califórnia (EUA)	AB 1043 — Digital Age Assurance Act; AB-2273 — California Age-Appropriate Design Code Act (2022)
Louisiana (EUA)	—
Texas (EUA)	Texas Business & Commerce Code, Chapter 509 — SCOPE Act (HB 18, 2023)
Utah (EUA)	Utah Code, Title 13, Chapter 63 — Social Media Regulation Act (SB 152, 2023); R 152-63
Índia	Information Technology Act (2021)
Colômbia	Lei 2489/2025; Decreto Regulamentador (minuta, 2025)

Reino Unido	Online Safety Act 2023 (Section 230); Guidance on Highly Effective Age Assurance and Other Part 5 Duties (Ofcom); Guidance on Highly Effective Age Assurance for Part 3 Services (Ofcom); Age Appropriate Design Code — AADC/Children's Code v. 2.1.87 (ICO, 2022)
União Europeia	Digital Services Act (DSA); Guidelines on measures to ensure a high level of privacy, safety and security for minors (art. 28(4) DSA); European Data Protection Board's Statement 1/2025 on Age Assurance

B. Jurisdições que diferenciam e que não diferenciam os conceitos

Jurisdições que estabelecem distinção conceitual expressa. Reino Unido e Austrália são as jurisdições que mais avançam na distinção conceitual entre os diferentes métodos de garantia etária. O OSA britânico estabelece em lei primária a distinção entre *age verification* e *age estimation*, e as guidances da OFCOM adotam o termo guarda-chuva *age assurance* para abranger ambos, esclarecendo expressamente que autodeclaração não se enquadra em nenhuma das duas categorias. A Social Media Minimum Age Regulatory Guidance australiana distingue três categorias: estimativa de idade, baseada em características biológicas ou comportamentais; inferência de idade, baseada em informações indiretas; e verificação de idade, baseada no cálculo da diferença entre uma data de nascimento verificada e uma data subsequente. A União Europeia, por meio das Guidelines do DSA e do Statement 1/2025 do EDPB, adota *age assurance* como conceito guarda-chuva que abrange estimativa de idade, verificação de idade e autodeclaração, diferenciando os métodos por grau de certeza.

Jurisdições que adotam abordagem funcional sem distinção conceitual expressa. Califórnia, Utah e Colômbia não estabelecem distinção conceitual formal, mas adotam implicitamente abordagens mais próximas da aferição por estimativa. A AB 1043 californiana introduz o conceito de *age bracket data*, um sinal de faixa etária gerado a partir da data de nascimento coletada pelo dispositivo ou sistema operacional, sem nomear formalmente o método como verificação ou estimativa. Utah exige verificação obrigatória de idade com proibição de autodeclaração e enumera métodos aceitáveis que incluem tanto estimativa por análise facial quanto correspondência com documento de identidade emitido pelo governo, sem diferenciar conceitualmente as duas abordagens. O Decreto colombiano consagra a minimização de dados como critério orientador ao referir-se a técnicas de estimação anônima como método prioritário, remetendo a definição dos critérios concretos a delineamentos técnicos futuros do MinTIC.

Jurisdições que não diferenciam os conceitos. Texas, Louisiana, Índia, a norma primária australiana. O SCOPE Act texano admite autodeclaração. A Índia define mecanismo de controle de acesso de forma ampla, como qualquer medida confiável que permita restringir acesso com base na verificação da identidade ou da idade, sem diferenciar métodos. O OSA australiano adota abordagem funcional, exigindo apenas que o provedor tome medidas razoáveis para impedir o acesso de crianças e adolescentes.

C. Abordagens adotadas pelas jurisdições

***Age assurance* como conceito guarda-chuva.** Reino Unido, Austrália e União Europeia convergem na adoção de *age assurance* como termo guarda-chuva que abrange o conjunto de métodos disponíveis para determinar ou estimar a idade dos usuários. Essa escolha terminológica é deliberada: evita a equiparação entre métodos com graus distintos de confiabilidade e acomoda a diversidade tecnológica sem fixar um único método obrigatório.

Distinção por grau de certeza com consequências operacionais distintas. O Reino Unido é a jurisdição que mais desenvolve as consequências práticas da distinção entre verificação e estimativa. As guidances da OFCOM estabelecem métricas de acurácia técnica distintas para cada tipo de método: métricas de resultado binário (TPR, FPR, FNR) para verificação, e métricas de resultado contínuo (Standard Deviation, MAPE, Cumulative Score) para estimativa. Adicionalmente, métodos de estimativa estão sujeitos a uma exigência que não se aplica à verificação: o *challenge age approach*, pelo qual usuários estimados abaixo de determinada idade-gatilho são submetidos a uma segunda camada de verificação para compensar a imprecisão inerente à estimativa.

Proporcionalidade ao risco como critério de seleção do método. O AADC britânico e as Guidelines do DSA convergem no entendimento de que o método de aferição deve ser proporcional ao risco: quanto maiores os riscos do processamento de dados ou do conteúdo acessível, maior o nível de certeza exigido sobre a idade dos usuários. Essa lógica evita a imposição universal de métodos mais intrusivos para serviços de baixo risco, calibrando a intensidade da obrigação ao contexto específico do serviço.

Minimização de dados como critério orientador. AADC britânico e Decreto colombiano convergem na adoção da minimização de dados como princípio orientador dos mecanismos de aferição. O AADC reconhece expressamente a tensão entre robustez da aferição e proteção de dados, resolvendo-a pela restrição ao estritamente necessário para estabelecer a idade, sem reutilização para outras finalidades. O decreto colombiano prioriza técnicas de estimação anônima precisamente como expressão desse princípio.

Exclusão expressa da autodeclaração. Reino Unido e Austrália excluem expressamente a autodeclaração do âmbito dos métodos aceitáveis de *age assurance*. As guidances da Ofcom esclarecem que autodeclaração não se enquadra nem em verificação nem em estimativa de idade. Essa exclusão é diretamente convergente com o ECA Digital, que também veda a autodeclaração como mecanismo suficiente.

II. Fundamentos Regulatórios da Aferição de Idade (3.A do Benchmarking)

O ECA Digital, em seus arts. 9º a 15, estabelece obrigações relacionadas à aferição de idade, incluindo a exigência de mecanismos confiáveis, a observância dos princípios da proporcionalidade e da segurança, deveres atribuídos a lojas de aplicativos e sistemas operacionais, o fornecimento de sinais etários por meio de APIs com salvaguardas específicas, limitações ao uso de dados e responsabilidades compartilhadas entre os agentes da cadeia digital. Nesse contexto, a presente seção do benchmarking buscou responder às seguintes questões: (i) quais são as definições relevantes; (ii) se a jurisdição define os objetivos da aferição de idade; e (iii) quais produtos e serviços estão sujeitos à aferição obrigatória.

A. Jurisdições e Fontes Normativas Analisadas

Jurisdição	Fontes Normativas
Austrália	Online Safety Amendment (Social Media Minimum Age) Act 2024
Califórnia (EUA)	AB 1043 — Digital Age Assurance Act
Louisiana (EUA)	HB 61 (2023); HB 570 (2025)
Texas (EUA)	Texas Business & Commerce Code, Chapter 509 — SCOPE Act (HB 18, 2023)
Utah (EUA)	Utah Code, Title 13, Chapter 63 — Social Media Regulation Act (SB 152, 2023); R 152-63

Índia	Digital Personal Data Protection Act (2023); Information Technology Act (2021 e 2000); Lei de Promoção e Regulamentação dos Jogos Online — PROG (2025)
Colômbia	Lei 2489/2025; Decreto Regulamentador (minuta, 2025)
Reino Unido	Online Safety Act 2023; Guidance on Highly Effective Age Assurance and Other Part 5 Duties (Ofcom); Guidance on Highly Effective Age Assurance for Part 3 Services (Ofcom); Age Appropriate Design Code — AADC/Children's Code v. 2.1.87 (ICO, 2022)
União Europeia	Digital Services Act (DSA), arts. 3(i), 28, 33 e 35; Guidelines on measures to ensure a high level of privacy, safety and security for minors (art. 28(4) DSA); European Data Protection Board's Statement 1/2025 on Age Assurance

B. Definições relevantes adotadas pelas jurisdições

As jurisdições analisadas divergem significativamente quanto ao grau de desenvolvimento conceitual aplicado à aferição de idade. O espectro vai desde arcabouços definitórios detalhados e tecnicamente precisos até normas que operam sem qualquer definição expressa.

Jurisdições com arcabouço definitório estruturado. O Reino Unido apresenta o conjunto de definições mais desenvolvido. O OSA estabelece em lei primária as definições de *age verification* como medida destinada a verificar a idade exata dos usuários, e de *age estimation* como medida destinada a estimar a idade ou faixa etária dos usuários, excluindo expressamente a autodeclaração de ambas as categorias. As guidances da Ofcom ampliam esse arcabouço com definições operacionais adicionais: *age assurance* como termo guarda-chuva que abrange ambos os métodos; *age assurance method* como o sistema ou tecnologia que sustenta o processo; *age assurance process* como o processo de ponta a ponta pelo qual o método é implementado; *access controls* como mecanismo técnico que impede o acesso de usuários identificados como crianças e adolescentes; *relying party* como o serviço que busca estabelecer a idade do usuário; e *age tokens* como tokens digitais reutilizáveis que representam a conclusão de uma verificação de idade e podem ser compartilhados entre serviços. A União Europeia, por meio das Guidelines do DSA e do Statement 1/2025 do EDPB, adota *age assurance* como conceito guarda-chuva que abrange estimativa de idade, verificação de idade e autodeclaração, diferenciando os métodos por grau de certeza. A Austrália, por meio da Social Media Minimum Age Regulatory Guidance,

distingue estimativa de idade, inferência de idade e verificação de idade, e define os conceitos de plataforma de rede social restrita por idade e usuário de idade restrita.

Jurisdições com definições parciais ou instrumentais. Califórnia e Colômbia introduzem conceitos específicos sem construir um arcabouço definitório completo. A AB 1043 californiana define *age bracket data* como dados de faixa etária e *signal* como o sinal transmitido via API pelo sistema operacional às aplicações, sem definir os métodos subjacentes. O Decreto colombiano introduz o Modo NNA como configuração predeterminada aplicada aos usuários identificados como crianças e adolescentes por mecanismos razoáveis de determinação de idade, e referencia técnicas de estimação anônima como método prioritário, sem defini-las. O AADC britânico opera com o conceito funcional de *establish age with an appropriate level of certainty*, sem glossário formal, utilizando *age assurance* como guarda-chuva e *age verification* em sentido mais restrito para serviços terceiros de confirmação de idade. Louisiana define *age category* e *age rating* no contexto de lojas de aplicativos, sem definir os métodos de aferição. Utah enumera formas e métodos aceitáveis de identificação na regulamentação administrativa, sem definição conceitual dos métodos.

Jurisdições sem definições relevantes. Texas, Índia e o texto primário do DSA europeu não apresentam definições técnicas relacionadas à aferição de idade. O SCOPE Act texano opera com o conceito de *known minor*, pessoa que o provedor sabe ter menos de 18 anos, sem definir métodos de identificação. A Índia define mecanismo de controle de acesso de forma ampla, como qualquer medida confiável que permita restringir acesso com base na verificação de identidade ou de idade, sem diferenciar métodos.

C. Objetivos da regulação adotados pelas jurisdições

As jurisdições analisadas também divergem quanto à definição explícita dos objetivos da aferição de idade, oscilando entre objetivos claramente articulados em lei e objetivos apenas inferíveis do conjunto normativo.

Jurisdições com objetivo expressamente definido. O Reino Unido é a jurisdição que mais articula os objetivos da aferição de idade de forma precisa e diferenciada por regime. No âmbito da Part 5 do OSA, o objetivo é garantir que crianças e adolescentes não sejam normalmente capazes de encontrar conteúdo pornográfico regulado. No âmbito da Part 3, o objetivo opera em dois contextos: na *children's access assessment*, permitir que o provedor conclua que crianças e adolescentes não conseguem normalmente acessar o serviço; e no Protection of Children Code, implementar *age assurance* altamente eficaz para proteger crianças de conteúdo primário prioritário prejudicial. A Austrália define o

objetivo como impedir que usuários com idade inferior à permitida mantenham contas em plataformas de redes sociais consideradas inapropriadas para a faixa etária, com o objetivo de reduzir danos. Utah define o objetivo como identificar se o usuário tem menos de 18 anos para exigir consentimento parental, aplicar restrições de funcionalidades e impedir acesso não autorizado.

Jurisdições com objetivo inferível mas não articulado. Califórnia, Colômbia, União Europeia e AADC britânico tratam a aferição de idade como mecanismo instrumental, cujo objetivo deve ser inferido do conjunto normativo. A AB 1043 californiana limita-se a descrever funcionalmente o objetivo do sinal de faixa etária: fornecer às aplicações informação sobre a faixa etária do usuário via API. O Decreto colombiano conecta a determinação de idade à ativação do Modo NNA e do design seguro por padrão, sem articular um objetivo autônomo. As Guidelines do DSA e o AADC britânico identificam como objetivo assegurar elevado nível de privacidade, segurança e proteção de crianças e adolescentes, com a aferição operando como pressuposto instrumental. O EDPB aponta que, na maioria dos casos, o objetivo é tomar decisões de controle de acesso relacionadas à idade, prevenir danos online para crianças ou adolescentes, e oferecer design ou experiência adequados à idade.

Jurisdições sem objetivo definido. Texas e Índia não definem objetivos específicos para a aferição de idade. O SCOPE Act texano opera com um sistema de registro de idade autodeclarada vinculado ao conceito de *known minor*, sem articular um objetivo regulatório autônomo para a identificação etária.

D. Escopo de aplicação adotado pelas jurisdições

O escopo de aplicação das obrigações de aferição de idade varia amplamente entre as jurisdições analisadas, tanto em termos dos serviços sujeitos à obrigação quanto dos critérios utilizados para delimitar esse universo.

Escopo restrito a categorias específicas de serviços. Austrália e Texas adotam os escopos mais restritos. A Austrália limita a obrigação de aferição às plataformas de redes sociais restritas por idade, aquelas cuja finalidade principal é garantir conexão entre usuários, que permitem interações e publicação de conteúdo, com exclusões expressas para serviços de mensageria, jogos, networking profissional, educação, saúde e comunicação entre instituições educacionais e famílias. O SCOPE Act texano circunscreve as obrigações a serviços digitais que coletam ou processam dados pessoais com conectividade à internet, com o regime de aferição mais robusto reservado apenas a

provedores que publiquem ou distribuam conteúdo prejudicial ou obsceno acima de um terço do total de conteúdo.

Escopo definido por critério funcional de probabilidade de acesso por crianças. Reino Unido e União Européia adotam critérios funcionais que evitam a enumeração fechada de tipos de serviço. O OSA britânico delimita o escopo da Part 5 por três condições cumulativas: publicação de conteúdo pornográfico regulado pelo próprio provedor, ausência de isenção e vínculo com o Reino Unido. O escopo da Part 3 não é definido por lista fechada, mas pelo critério funcional de probabilidade de acesso por crianças e presença de conteúdo primário prioritário prejudicial. O AADC britânico adota o escopo mais amplo: todos os serviços da sociedade da informação com probabilidade de acesso por crianças, abrangendo aplicativos, brinquedos e dispositivos conectados, motores de busca, redes sociais, streaming, jogos online, sites de notícias ou educacionais e marketplaces. O DSA aplica o art. 28 a plataformas online acessíveis a crianças e adolescentes, com o art. 35 reservado a VLOPs e VLOSEs com 45 milhões ou mais de usuários ativos mensais na UE.

Escopo amplo sem delimitação específica. Índia e Colômbia adotam os escopos mais abrangentes, sem delimitar categorias específicas de serviços. A Índia trata a aferição de idade como condição para acesso a mídias sociais, produtos e serviços online em geral, incluindo jogos, filmes e séries, com controvérsias sobre a extensão da obrigação de consentimento parental a todos os serviços digitais. O Decreto colombiano aplica as obrigações de determinação de idade a todas as plataformas digitais e serviços de internet por meio dos quais os NNA exercem direitos digitais, exploram, aprendem, socializam, publicam conteúdo, acessam conteúdo audiovisual ou interagem com terceiros, sem lista fechada de tipos de serviço.

Escopo na camada de sistema operacional e lojas de aplicativos. Califórnia adota abordagem distinta das demais, deslocando a obrigação de aferição da camada de aplicação para a camada de sistema operacional e lojas de aplicativos. A AB 1043 impõe a obrigação aos sistemas operacionais de computadores e dispositivos móveis, às lojas de aplicativos e às aplicações de software, com o sinal de faixa etária gerado pelo sistema operacional e transmitido às aplicações via API.

III. Atores Relevantes na Aferição de Idade (3.B do Benchmarking)

O ECA Digital distribui responsabilidades relacionadas à aferição de idade entre diferentes atores da cadeia digital, incluindo o Estado, os fornecedores de produtos e serviços de tecnologia da informação, as lojas de aplicativos e os sistemas operacionais.

Nesse contexto, o benchmarking buscou responder às seguintes questões: (i) quais atores são responsáveis pela implementação dos mecanismos de aferição de idade; (ii) qual é o papel atribuído ao Estado; e (iii) se há previsão ou exigência de entidades certificadoras.

A. Jurisdições e Fontes Normativas Analisadas

Jurisdição	Fontes Normativas
Austrália	Social Media Minimum Age Regulatory Guidance
Califórnia (EUA)	AB 1043 — Digital Age Assurance Act; AB-2273 — California Age-Appropriate Design Code Act (2022)
Louisiana (EUA)	HB 61 (2023); HB 577 (2024); HB 570 (2025)
Texas (EUA)	Texas Business & Commerce Code, Chapter 509 — SCOPE Act (HB 18, 2023)
Utah (EUA)	Utah Code, Title 13, Chapter 63 — Social Media Regulation Act (SB 152, 2023); R 152-63
Índia	Digital Personal Data Protection Act (2023); Information Technology Act (2021)
Colômbia	Lei 2489/2025; Decreto Regulamentador (minuta, 2025)
Reino Unido	Online Safety Act 2023; Guidance on Highly Effective Age Assurance and Other Part 5 Duties (Ofcom); Guidance on Highly Effective Age Assurance for Part 3 Services (Ofcom); Age Appropriate Design Code — AADC/Children's Code v. 2.1.87 (ICO, 2022)
União Europeia	Digital Services Act (DSA), arts. 3(i), 28, 33 e 35; Guidelines on measures to ensure a high level of privacy, safety and security for minors (art. 28(4) DSA); European Data Protection Board's Statement 1/2025 on Age Assurance

B. Atores responsáveis pela implementação dos mecanismos de aferição de idade

Responsabilidade centrada nos provedores de serviços. A maioria das jurisdições analisadas concentra a responsabilidade primária pela implementação dos mecanismos de aferição de idade nos próprios provedores de serviços digitais. Austrália, Louisiana, Utah, Índia, Colômbia, Reino Unido e União Européia adotam esse modelo, variando apenas quanto ao grau de detalhamento das obrigações e à possibilidade de delegação a terceiros. Em todas essas jurisdições, o provedor permanece responsável pelo resultado ainda que contrate soluções externas de aferição: a Austrália exige due diligence em relação a terceiros e esclarece que falhas na prestação não isentam o provedor; o AADC britânico atribui ao controlador de dados a responsabilidade de avaliar os riscos e decidir o método adequado ao seu contexto, podendo contratar serviços terceiros de verificação de idade como instrumentos de apoio.

Responsabilidade distribuída pela cadeia digital. A Califórnia adota abordagem distinta ao distribuir a responsabilidade entre diferentes camadas da cadeia digital. A AB 1043 atribui ao provedor do sistema operacional a obrigação de fornecer interface para coleta da data de nascimento e geração do sinal de faixa etária; à loja de aplicativos, responsabilidade complementar de transmissão do sinal; e ao desenvolvedor de aplicações, a obrigação de consultar e tratar o sinal recebido como conhecimento efetivo da idade do usuário. Esse modelo desloca parte significativa da responsabilidade da camada de aplicação para as camadas de sistema operacional e distribuição.

Responsabilidade compartilhada com usuários e responsáveis. O Texas adota modelo centrado no próprio usuário: é o usuário quem registra sua idade, e pais ou responsáveis podem notificar ou contestar o registro. O provedor assume obrigações apenas a partir do momento em que passa a ter conhecimento efetivo de que o usuário tem menos de 18 anos, seja pelo autorregistro, seja pela notificação parental. Utah prevê estrutura equivalente para o consentimento parental, com as plataformas de mídia social responsáveis pela verificação, mas com participação ativa dos pais no processo.

C. Papel do Estado quanto às obrigações de aferição de idade

Estado como regulador e fiscalizador. A totalidade das jurisdições analisadas reserva ao Estado papel predominantemente regulatório e fiscalizatório, sem atribuir-lhe responsabilidade pela implementação direta dos mecanismos. As variações dizem respeito ao grau de intervenção normativa, à distribuição de competências entre órgãos e à intensidade dos poderes de enforcement.

Modelo de regulador especializado com poderes amplos de enforcement. Austrália e Reino Unido adotam o modelo mais robusto de intervenção estatal. Na

Austrália, a eSafety Commissioner atua como regulador especializado com competência para emitir diretrizes, requisitar informações, publicar declarações de avaliação de conformidade, advertir formalmente, aplicar notificações de infração, solicitar sanções civis ao Tribunal Federal e aceitar compromissos executáveis. O Ministro das Comunicações expede atos normativos de exceção de escopo e conduz a revisão periódica do ato, enquanto o OAIC monitora as técnicas de aferição em relação ao Privacy Act. No Reino Unido, a Ofcom é o regulador executivo com competência para emitir guidances, fiscalizar e aplicar penalidades financeiras de até £18 milhões ou 10% das receitas mundiais qualificadas. O ICO atua de forma coordenada com a Ofcom no âmbito da proteção de dados, podendo aplicar multas de até €20 milhões ou 4% do faturamento global anual. O Secretário de Estado mantém prerrogativas estratégicas de direcionamento.

Modelo de regulação por autoridade de dados. O AADC britânico exemplifica o modelo em que a autoridade de proteção de dados exerce papel normativo central: é o ICO que elabora, publica e atualiza o código, oferece orientações, realiza auditorias proativas e pode adotar medidas que vão de advertências a multas administrativas. O ICO também se comprometeu a apoiar o desenvolvimento de padrões setoriais e esquemas de certificação para instrumentos de age assurance.

Modelo de regulação por autoridade setorial com supervisão especializada. A Colômbia prevê distribuição de competências entre o MinTIC, responsável por estabelecer lineamentos técnicos e fiscalizar o cumprimento das medidas pelas plataformas, e a Superintendência de Indústria e Comércio, com atribuição específica de vigilância sobre os processos de determinação de idade em razão de sua competência sobre tratamento de dados pessoais. A Comissão de Regulação de Comunicações atua em coordenação com o MinTIC na definição dos mecanismos de reporte.

Estado como provedor de infraestrutura técnica. A União Europeia introduz uma dimensão adicional ao papel estatal: além de regular e fiscalizar, os Estados-Membros devem fornecer infraestrutura técnica padronizada de identificação. As Guidelines do DSA preveem que cada Estado-Membro deverá disponibilizar a EU Digital Identity Wallet até o final de 2026, permitindo o recebimento de um token de idade por usuários. Como medida de transição, a Comissão desenvolveu o mini-wallet, a primeira versão do *blueprint* técnico foi publicada em 14 de julho de 2025; a segunda versão, com suporte a passaporte e cartão de identidade para emissão da credencial, foi publicada em 10 de outubro de 2025.

Modelo de enforcement por Ministério Público. O Texas concentra o poder de enforcement na Divisão de Proteção ao Consumidor do Gabinete do Procurador-Geral, que pode buscar medidas cautelares e penalidades civis de até US$10.000 por violação. A lei

não confere direito privado de ação, mas permite que pais e responsáveis de crianças e adolescentes ingressem com ação para obter sentença declaratória.

D. Entidades certificadoras para avaliação ou validação dos mecanismos de aferição de idade

Certificação como possibilidade, não como requisito. Nenhuma das jurisdições analisadas estabelece entidades certificadoras obrigatórias para avaliação ou validação dos mecanismos de aferição de idade. O modelo dominante é de conformidade autorregulatória com fiscalização ex post pela autoridade competente. Onde a certificação é mencionada, aparece como elemento auxiliar de demonstração de conformidade, não como requisito de validade do mecanismo adotado.

Esquemas voluntários de certificação como referência. O Reino Unido é a jurisdição que mais desenvolve o papel da certificação voluntária. As guidances da OFCOM mencionam o UK Digital Identity and Attributes Trust Framework, administrado pelo Office for Digital Identities and Attributes, como esquema de certificação relevante para demonstrar confiabilidade de evidências utilizadas por fornecedores terceiros de identidade digital. O uso de serviço certificado contra esse framework não implica compliance automático, mas pode ajudar a evidenciar que o provedor considerou os critérios de eficácia estabelecidos. O AADC britânico indica o PAS 1296 como padrão técnico de referência para due diligence na contratação de serviços terceiros de verificação de idade, e prevê a possibilidade futura de criação de esquemas de certificação com fundamento no Art. 42 do GDPR, comprometendo o ICO a apoiar esse desenvolvimento.

Avaliação técnica independente como referência regulatória. A Austrália incentiva os provedores a considerarem métodos de aferição que tenham sido certificados ou acreditados de forma independente com base em padrões internacionais e nacionais, especialmente quanto à precisão, segurança e resiliência a fraudes. A eSafety utilizou os achados do Age Check Certification Trial, conduzido pelo Age Check Certification Scheme (ACCS) com financiamento governamental, como referência para suas diretrizes, sem endossar tecnologias específicas.

Auditoria externa como substituto funcional da certificação. A Colômbia prevê modelo de verificação por auditoria externa anual, por meio do qual as plataformas devem comprovar ao MinTIC o cumprimento das disposições do decreto, incluindo os mecanismos de determinação de idade. Os informes resultantes podem ser revisados pelo Comitê Nacional de Tecnologia, Niñez y Adolescencia. Trata-se de verificação por auditoria privada com supervisão pública, e não de certificação prévia por entidade habilitada.

Padronização por organismos de normalização. A União Europeia orienta o papel da certificação para a esfera dos organismos de normalização, sem designar entidades certificadoras específicas. O DSA prevê que a Comissão apoie o desenvolvimento de normas técnicas voluntárias por organismos europeus e internacionais de normalização. O EDPB menciona que padrões, boas práticas e códigos de conduta podem ser úteis, com a validação tratada sob a ótica de auditabilidade e conformidade com padrões técnicos.

IV. Implementação Prática dos Mecanismos de Aferição de Idade (3.C do Benchmarking)

O ECA Digital exige a adoção de mecanismos confiáveis de aferição de idade, sem, contudo, especificar quais mecanismos podem ser utilizados nem em que momento devem ser implementados. Nesse contexto, o benchmarking buscou responder às seguintes questões: (i) quais mecanismos de aferição de idade são admitidos; (ii) quais critérios são utilizados para definir o mecanismo mais adequado a cada contexto; e (iii) em que momento a aferição deve ocorrer. Vale pontuar, que posteriormente o Decreto nº 12.880/2026 respondeu parte dessas questões.

A. Jurisdições e Fontes Normativas Analisadas

Jurisdição	Fontes Normativas
Austrália	Social Media Minimum Age Regulatory Guidance
Califórnia (EUA)	AB 1043 — Digital Age Assurance Act; AB-2273 — California Age-Appropriate Design Code Act (2022)
Louisiana (EUA)	HB 570 (2025); Louisiana Revised Statutes, Title 51, §2123(A)
Texas (EUA)	Texas Business & Commerce Code, Chapter 509 — SCOPE Act (HB 18, 2023)
Utah (EUA)	Utah Code, Title 13, Chapter 63 — Social Media Regulation Act (SB 152, 2023); R 152-63
Índia	Digital Personal Data Protection Act (2023); Information Technology Act (2021)
Colômbia	Lei 2489/2025; Decreto Regulamentador (minuta, 2025)

Reino Unido	Online Safety Act 2023; Guidance on Highly Effective Age Assurance and Other Part 5 Duties (Ofcom); Guidance on Highly Effective Age Assurance for Part 3 Services (Ofcom); Age Appropriate Design Code — AADC/Children's Code v. 2.1.87 (ICO, 2022)
União Europeia	Digital Services Act (DSA), arts. 28 e 35; Guidelines on measures to ensure a high level of privacy, safety and security for minors (art. 28(4) DSA); European Data Protection Board's Statement 1/2025 on Age Assurance

B. Mecanismos de aferição admitidos pelas jurisdições

Jurisdições com catálogo estruturado de mecanismos admitidos e excluídos. O Reino Unido apresenta o tratamento mais detalhado. As guidances da OFCOM estabelecem lista não exaustiva de métodos considerados capazes de ser altamente eficazes: *open banking* (confirmação de maioridade via dados bancários com consentimento, sem repasse da data de nascimento ao serviço); *photo-ID matching* (captura de documento de identidade com foto e comparação com imagem do usuário); *facial age estimation* (estimativa de idade por análise de características faciais); verificação por operadora de rede móvel (confirmação de que o filtro de restrição de conteúdo foi removido pelo titular adulto do dispositivo); verificação por cartão de crédito (validação da validade do cartão junto ao banco emissor como evidência de maioridade); *email-based age estimation* (estimativa de idade por análise dos serviços associados ao endereço de e-mail); e *digital identity services* (identidades digitais reutilizáveis, incluindo carteiras digitais que permitem compartilhar atributos de idade entre serviços). São expressamente considerados incapazes de ser altamente eficazes: autodeclaração de idade, verificação por métodos de pagamento que não exigem maioridade e restrições contratuais genéricas. O AADC britânico adota lista igualmente não exaustiva, incluindo autodeclaração para baixo risco, estimativa por inteligência artificial, serviços terceiros de verificação de idade por sistema de atributo, confirmação por titular de conta adulta, medidas técnicas de apoio e identificadores formais, desaconselhando estes últimos como mecanismo exclusivo salvo quando os riscos efetivamente o justificam.

Jurisdições com modelo normativo único. A Califórnia, por meio da AB 1043, define um único modelo: coleta da data de nascimento no momento da configuração do dispositivo, derivação de dados de faixa etária e fornecimento de sinal de faixa etária às aplicações via API. Não há escolha de método pelo provedor, o legislador fixou o mecanismo. A AB 2273, por outro lado, admite qualquer mecanismo que permita

estabelecer ou estimar a idade com nível razoável de certeza, sem prescrever nem vedar métodos específicos.

Jurisdições com enumeração administrativa de métodos aceitáveis. Utah define por regulamentação administrativa os métodos aceitáveis de identificação, incluindo: validação de informações de assinante de telefonia móvel; autenticação dinâmica baseada em conhecimento; estimativa de idade com base na data de criação da conta; verificação dos quatro últimos dígitos do número de seguridade social em base de dados de terceiros; credencial digital; estimativa de idade por análise facial; e correspondência de documento de identidade governamental com foto ao vivo ou presença física.

Jurisdições com abordagem de razoabilidade sem enumeração. Austrália, Louisiana e Texas adotam critério de razoabilidade sem listar métodos específicos, com variações relevantes. A Austrália afasta expressamente mecanismos insuficientes (autodeclaração, validação por responsáveis sem medida robusta adicional, métodos que dependem do uso prolongado da plataforma, e métodos que não mitiguem a reativação de contas suspensas), sem prescrever métodos obrigatórios. Louisiana exige métodos comercialmente razoáveis, admitindo documento de identidade governamental ou sistemas comerciais de verificação que utilizem dados públicos ou privados confiáveis, e afasta expressamente a autodeclaração simples. O Texas admite autodeclaração como forma de registro, reservando a exigência de método comercialmente razoável apenas para provedores que publiquem ou distribuam materiais prejudiciais ou obscenos acima de determinado limiar.

Jurisdições sem mecanismos definidos. Colômbia e Índia não especificam mecanismos admitidos. A Colômbia remete integralmente a definição dos métodos concretos aos lineamentos técnicos futuros do MinTIC, indicando apenas preferência por técnicas de estimação anônima. A Índia exige verificação de identidade do responsável adulto por documento, como condição para consentimento parental, sem detalhar métodos para identificação de que o usuário tem menos de 18 anos. A União Europeia, por meio do DSA, não prescreve mecanismos específicos, mas as Guidelines do DSA estabelecem que a autodeclaração não atende os requisitos de adequação do Art. 28(1), e listam as três categorias principais (autodeclaração, estimativa e verificação) identificando a verificação rigorosa como proporcional para conteúdos de maior risco como álcool, tabaco, drogas, pornografia e jogos de azar.

C. Critérios utilizados para selecionar o mecanismo de aferição

Critério de alta eficácia com parâmetros técnicos definidos. O Reino Unido adota o critério mais estruturado e tecnicamente detalhado. O OSA estabelece como critério central a alta eficácia na determinação correta da idade, e as guidances da Ofcom desdobram esse critério em quatro dimensões: acurácia técnica, avaliada por métricas específicas conforme o método seja de resultado binário ou contínuo; robustez, aferida pela capacidade de funcionar em contextos reais e resistir a técnicas de contorno acessíveis a crianças; confiabilidade, referida à reprodutibilidade dos resultados e à qualidade das evidências, com exigências adicionais para métodos baseados em IA ou *machine learning*; e equidade, entendida como a ausência de vieses e resultados discriminatórios entre grupos populacionais. A esses quatro critérios somam-se dois princípios adicionais: acessibilidade, garantindo que o processo funcione para todos os usuários independentemente de suas características, e interoperabilidade, incentivando a adoção de soluções compatíveis entre serviços para reduzir o ônus sobre o usuário.

Critério de proporcionalidade ao risco. AADC britânico, Guidelines do DSA, decreto colombiano e Austrália convergem na adoção da proporcionalidade ao risco como critério central de seleção. O AADC é o que mais desenvolve os fatores de risco a considerar: tipo e volume de dados coletados, intrusividade do perfilamento, existência de decisões automatizadas e compartilhamento com terceiros. As Guidelines do DSA estabelecem que métodos devem demonstrar precisão, confiabilidade, robustez, não intrusividade e não discriminação, e indicam a verificação rigorosa como proporcional para as categorias de maior risco. A Austrália desenvolve os princípios de avaliação da solução: confiabilidade, precisão, robustez e eficácia; preservação da privacidade e minimização de dados; acessibilidade, inclusividade e justiça; transparência; proporcionalidade; e fundamentação em evidências com responsividade às tecnologias emergentes.

Critério de minimização de dados. Colômbia, AADC britânico e Guidelines do DSA convergem na adoção da minimização de dados como critério orientador da seleção, com preferência por métodos que não exijam tratamento extensivo de informações pessoais. O decreto colombiano eleva a minimização ao status de critério autônomo de seleção, ao lado da proporcionalidade e da neutralidade tecnológica. As Guidelines do DSA expressam essa preferência pela indicação de tokens e *zero-knowledge proofs* como tecnologias que preservam a privacidade.

Critério de razoabilidade comercial. Texas e Louisiana adotam o critério mais flexível: exigem apenas que o método seja comercialmente razoável, sem detalhar parâmetros técnicos ou definir o que torna um método razoável. Esse critério oferece

máxima flexibilidade aos provedores, mas também menor previsibilidade sobre o que constitui cumprimento adequado da obrigação.

D. Momento em que a aferição deve ocorrer

Momento único no cadastro ou acesso inicial. Louisiana, Utah e Texas concentram a aferição em um momento específico. Louisiana exige a verificação antes de permitir o acesso ao conteúdo ou de autorizar o download e compras pelo usuário. Utah exige a verificação antes da criação ou manutenção da conta, incluindo contas preexistentes à lei. O Texas concentra a identificação da idade no momento do registro inicial ou da notificação parental, sem prever aferição contínua.

Aferição em múltiplos momentos ao longo da jornada do usuário. Austrália, Reino Unido e União Europeia estruturam a aferição como processo dinâmico e não como verificação pontual. A Austrália prevê três momentos: criação da conta, identificação de contas preexistentes quando da entrada em vigor da lei, e monitoramento contínuo para prevenir novos registros e responder a riscos emergentes. A guidance da Ofcom para a Part 5 é explícita: a age assurance deve ocorrer no ponto de entrada ao serviço, antes que qualquer conteúdo pornográfico seja acessível, sendo exemplo de não conformidade a visibilidade de qualquer conteúdo pornográfico durante ou antes da conclusão do processo. As Guidelines do DSA estruturam três momentos distintos: criação de conta ou primeiro uso, como garantia de experiência adequada desde a origem; acesso a conteúdos ou seções específicas de risco, como verificação pontual em áreas restritas; e acesso recorrente a cada sessão, como exigência mandatória para plataformas de conteúdo adulto, para impedir o compartilhamento de credenciais entre adultos e crianças e adolescentes.

Aferição integrada ao ciclo de vida do serviço. O AADC britânico e o decreto colombiano adotam a abordagem mais ampla: a aferição não se limita a um momento processual, mas deve estar integrada ao design e ao ciclo de vida do serviço. O AADC prevê que a avaliação do mecanismo adequado deve integrar a DPIA antes do início do processamento, com mecanismos como inteligência artificial operando de forma contínua ao longo do uso e com revisão obrigatória se evidências posteriores indicarem acesso significativo de crianças. O decreto colombiano, por sua lógica de design seguro por padrão, pressupõe que a determinação da condição de que o usuário tem menos de 18 anos deve anteceder a exposição do usuário às funcionalidades e conteúdos da plataforma, com monitoramento contínuo e ajustes progressivos nas transições entre faixas etárias.

3.3. Práticas do Setor Público

Diversas jurisdições têm estruturado ou acelerado iniciativas governamentais destinadas a fornecer infraestrutura pública de identidade digital reutilizável como instrumento de aferição de idade. Esta seção mapeia as principais práticas identificadas em três frentes: (i) o Brasil, com as iniciativas da Secretaria de Governo Digital do MGI (Gov.br) e da Dataprev; (ii) a União Europeia, com o quadro eIDAS 2.0 e o aplicativo de verificação etária da Comissão Europeia; e (iii) a Índia, com o sistema Aadhaar e sua recente integração com carteiras digitais privadas.

I. Brasil: infraestrutura pública de verificação etária e o papel do Gov.br

a) A solução em desenvolvimento pela SGD/MGI

O Ministério da Gestão e da Inovação em Serviços Públicos (MGI), por meio da Secretaria de Governo Digital (SGD), apresentou ao GT-6 a solução pública de aferição de idade em desenvolvimento pelo governo federal, integrada ao aplicativo Gov.br. A arquitetura parte de três pilares da infraestrutura nacional preexistente: Carteiras de Identidade Nacional (CIN) emitidas; o CPF como identificador praticamente universal, com acurácia robusta em relação a datas de nascimento; e um número bastante relevante de contas cadastradas no Gov.br, sendo muitas classificadas nos níveis Ouro ou Prata. A partir dessa base, o representante do MGI pontuou que o Brasil dispõe de vantagem comparativa expressiva em relação a outras jurisdições.

A solução em desenvolvimento baseia-se no modelo de credenciais verificáveis (padrão W3C). A opção que vem sendo explorada pelo governo brasileiro é de se aproveitar a infraestrutura existente, ao invés de se criar um aplicativo dedicado exclusivamente à verificação de idade, por opção estratégica de aproveitar a robusta base instalada e o alcance do Gov.br. A opção pela plataforma já existente foi deliberada: o usuário acessa o Gov.br, que atua como emissor (Issuer), gerando a credencial com base nas bases de dados estatais confiáveis. A credencial é emitida pelo Gov.br e armazenada localmente no dispositivo do usuário, dentro do enclave seguro do aplicativo, sem que fique disponível em servidores do governo ou na nuvem.

Do ponto de vista da arquitetura de privacidade, a solução segue uma lógica de atributo, e não de dado pessoal, o objetivo é certificar uma propriedade do usuário (ser maior de 18 anos ou outra faixa etária estabelecida), sem revelar sua identidade. No momento da aferição, o aplicativo verificador (Relying Party) faz a chamada ao dispositivo do usuário, que responde com a credencial mediante autenticação local. A credencial transmitida contém apenas o atributo binário "18+ sim/não", sem CPF, nome, data de

nascimento ou qualquer dado pessoal identificável. A solução é concebida como agnóstica em relação ao domínio de aplicação, qualquer empresa poderá integrá-la.

A previsão inicial de casos de uso prioritários abrange acesso a conteúdo adulto e bebidas alcoólicas. Para cenários classificados como de alto risco, a credencial pública poderá ser complementada por camadas adicionais de aferição, conforme classificação a ser definida em conjunto com a ANPD.

O projeto Govinho, iniciativa em desenvolvimento por diretoria irmã da SGD, que tem por objetivo adaptar a experiência do Gov.br para crianças e adolescentes e estruturar a vinculação entre contas de mães, pais ou responsáveis legais e de seus filhos, também está integrado ao planejamento de longo prazo da agenda de interoperabilidade. A API de relacionamento parental já existente no ecossistema Gov.br está sendo avaliada como motor técnico para a criação de uma credencial verificável de vínculo parental reutilizável, com aplicações tanto no Govinho quanto em outros serviços que demandem o consentimento do responsável legal.

b) A proposta tecnológica da Dataprev: plataforma MOSIP e credenciais verificáveis anônimas

A Dataprev (Empresa de Tecnologia e Informações da Previdência) apresentou ao GT-6 proposta estruturada em software livre, baseada na plataforma MOSIP (*Modular Open Source Identity Platform*), já adotada como infraestrutura de identidade nacional em múltiplos países de alta densidade demográfica.[101] O modelo proposto parte de uma crítica estrutural ao *Know Your Customer* (KYC) tradicional, identificado como gerador de uma escalada de intrusividade: da exigência de documentos simples para selfies, de selfies para vídeos com prova de vida (*liveness*), e desta para o monitoramento comportamental, sem contrapartida proporcional de segurança ou proteção.

A solução da Dataprev utiliza o conceito de credenciais verificáveis (padrão W3C) combinado com provas de conhecimento zero (*Zero-Knowledge Proof* — ZKP). Nesse fluxo, a informação de idade é "tokenizada" e armazenada em enclave seguro no dispositivo do usuário. Em vez de enviar CPF ou data de nascimento, o sistema processa um predicado criptográfico que informa à plataforma apenas a afirmação necessária, por exemplo, "este usuário tem mais de 18 anos", sem que o emissor da credencial (o governo) saiba em quais serviços o usuário está se autenticando, e sem que a plataforma saiba a identidade civil do

[101] Sobre o modelo MOSIP, ver: MOSIP — MODULAR OPEN SOURCE IDENTITY PLATFORM. Resource Centre. Disponível em: https://www.mosip.io/resource_centre. Acesso em: 29 maio 2026. O MOSIP é adotado como infraestrutura de identidade nacional em países como Etiópia, Filipinas, Marrocos, Serra Leoa e Sri Lanka, cobrindo populações superiores a 700 milhões de pessoas.

titular. A credencial é interoperável e pode ser alocada na *wallet* de preferência do usuário, seja no próprio app Gov.br, seja em ecossistemas de terceiros.

A Dataprev preconiza mecanismos de atualização dinâmica de status: uma credencial emitida para um usuário de 16 anos pode ser automaticamente revogada e renovada quando o usuário atingir a maioridade, e os usuários terão autonomia plena para revogar o acesso concedido a qualquer momento. Sobre o cenário de compartilhamento de aparelhos, realidade que poderia comprometer a eficácia da solução, a representante apontou que, com base em dados do Cetic.br, a incidência desse fenômeno no Brasil é inferior ao senso comum (abaixo de 20%, concentrada em comunidades rurais e de baixa renda) e que a solução tecnológica deverá ser acompanhada de campanha educacional e de mecanismos de isolamento de ambientes no nível do dispositivo.

II. União Europeia: eIDAS 2.0, a EUDI Wallet e o aplicativo de verificação etária da Comissão Europeia

O ponto de partida da iniciativa europeia é um diagnóstico de fragmentação. A União Europeia contava, desde 2014, com o Regulamento eIDAS (Regulation on Electronic Identification, Authentication and Trust Services), que estabeleceu um quadro comum para assinaturas eletrônicas e identificação digital. O problema é que o eIDAS original deixava a cargo de cada Estado-membro a decisão de desenvolver ou não um sistema nacional de identidade eletrônica, o que resultou, na prática, em uma paisagem heterogênea: alguns países dispunham de soluções nacionais maduras; outros,não tinham nada equivalente. A consequência prática era que apenas 59% dos residentes da UE podiam usar um documento de identidade eletrônico reconhecido fora de seu país de origem, e a adoção por serviços privados era marginal. O sistema funcionava para serviços públicos transfronteiriços, mas não chegava ao cotidiano digital dos cidadãos.[102]

A resposta da UE a esse diagnóstico foi o eIDAS 2.0 (Regulamento (UE) 2024/1183), aprovado em abril de 2024. A revisão introduziu uma mudança estrutural: em vez de apenas habilitar os Estados-membros a desenvolverem sistemas de identidade eletrônica, o novo regulamento os obriga a tanto. Cada país deve disponibilizar ao menos uma carteira de identidade digital nacional, a chamada EUDI Wallet (EU Digital Identity Wallet) com foco inicial em identidade e aferição de idade como funcionalidades obrigatórias de

[102] ENTRUST. eIDAS Regulation: From Fragmented to Trusted Identities. 12 fev. 2026. Disponível em: https://www.entrust.com/blog/2026/02/history-and-significance-of-eidas-regulation. Acesso em: 29 maio 2026. Para o dado de 59% de cobertura transfronteiriça: ENTRUST. What is eIDAS 2? Explore Today's Compliance Landscape. Disponível em: https://www.entrust.com/resources/learn/eidas-2. Acesso em: 29 maio 2026. Ver também: CEUR-WS. eIDAS Regulation: History, Key Success Factors, and Future Developments. CEUR Workshop Proceedings, Vol. 3863. Disponível em: https://ceur-ws.org/Vol-3863/invited1.pdf. Acesso em: 29 maio 2026.

lançamento, a todos os seus cidadãos, residentes e empresas até dezembro de 2026. Todas as carteiras nacionais devem seguir especificações técnicas comuns, serem mutuamente interoperáveis e incluírem um painel de controle que permite ao usuário ver com quem compartilhou dados e revogar esse compartilhamento a qualquer momento. A lógica é de autonomia do titular: o usuário não entrega documentos a um serviço, mas seleciona, para cada interação, exatamente quais atributos deseja apresentar.[103]

Avaliando que o prazo de 2026 para a EUDI Wallet plena era muito distante para endereçar as urgências imediatas de proteção infantil impostas pelo DSA, a Comissão Europeia desenvolveu, em paralelo, um aplicativo de aferição etária focado exclusivamente nessa função, denominado internamente como "mini-wallet". A primeira versão do *blueprint* técnico foi publicada em 14 de julho de 2025; a segunda versão, com suporte a passaporte e cartão de identidade para emissão da credencial, foi publicada em 10 de outubro de 2025.[104] A solução é desenvolvida pelo consórcio T-Scy (Scytáles/Suécia e T-Systems/Alemanha), sob contrato de dois anos firmado com a Comissão em fevereiro de 2025, e suas especificações técnicas e código-fonte estão disponíveis publicamente.[105]

Em 15 de abril de 2026, a presidente da Comissão Europeia, Ursula von der Leyen, anunciou a "prontidão técnica" do aplicativo.[106] No mesmo dia, o pesquisador de segurança Paul Moore reportou publicamente vulnerabilidades que, segundo sua análise, permitiam contornar mecanismos de proteção do aplicativo mediante alterações locais de

[103] UNIãO EUROPEIA. Regulamento (UE) 2024/1183 do Parlamento Europeu e do Conselho, de 11 de abril de 2024 (eIDAS 2.0), considerandos 4, 5 e 6 e arts. 5-A e 5-B. Jornal Oficial da União Europeia, L nº 1183, 30 abr. 2024. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=OJ:L_202401183. Acesso em: 29 maio 2026. Para análise: KENNEDYS LAW. The European Digital Identity Framework: introducing the new EU Digital Identity Wallet. 25 mar. 2026. Disponível em: https://www.kennedyslaw.com/en/thought-leadership/article/2026/the-european-digital-identity-framework-introducing-the-new-eu-digital-identity-wallet/. Acesso em: 29 maio 2026.

[104] COMISSÃO EUROPEIA. EU Age Verification Blueprint. Primeira versão publicada em 14 jul. 2025; segunda versão publicada em 10 out. 2025. Portal técnico dedicado: https://ageverification.dev. Acesso em: 29 maio 2026. Ver também: EUROPEAN COMMISSION DIGITAL BUILDING BLOCKS. The Age Verification Manual. Disponível em: https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/930450954/The+Age+Verification+Manual. Acesso em: 29 maio 2026.

[105] A solução é desenvolvida pelo consórcio T-Scy (Scytáles/Suécia e T-Systems/Alemanha, subsidiária da Deutsche Telekom), sob contrato de dois anos firmado com a Comissão Europeia em fevereiro de 2025. Ver: BIOMETRIC UPDATE. EC's use case manual explains age verification with EUDI Wallet. 12 mar. 2026. Disponível em: https://www.biometricupdate.com/202603/ecs-use-case-manual-explains-age-verification-with-eudi-wallet. Acesso em: 29 maio 2026.

[106] EUROPEAN COMMISSION. European age verification app to keep children safe online. Brussels: European Commission, 15 abr. 2026. Disponível em: https://commission.europa.eu/news-and-media/news/european-age-verification-app-keep-children-safe-online-2026-04-15_en. Acesso em: 29 maio 2026.

configuração, gerando críticas expressivas da comunidade técnica europeia.[107] Sete Estados-membros, França, Dinamarca, Grécia, Itália, Espanha, Chipre e Irlanda, estão conduzindo projetos piloto, com distribuição nas lojas de aplicativos prevista para o verão de 2026 e integração nativa às carteiras nacionais no final de 2026.[108]

Do ponto de vista técnico, o aplicativo opera sob a mesma arquitetura das futuras EUDI Wallets: credenciais verificáveis e chaves armazenadas na carteira do usuário. A solução é concebida para permitir comprovação seletiva de atributos e divulgação mínima de dados, inspirando-se em técnicas associadas à identidade digital preservadora de privacidade, incluindo, em alguns contextos, abordagens próximas a provas de conhecimento zero. O grande diferencial de proteção de dados é o compartilhamento seletivo de atributos: em vez de compartilhar um documento completo, o usuário pode selecionar quais dados repassar, permitindo que o sistema envie apenas uma resposta binária ("sim" ou "não") para confirmar se a pessoa possui a idade exigida pela plataforma.[109] O modelo é projetado sob lógica de *separação entre emissor e verificador*: o modelo busca alcançar uma lógica em que o emissor da credencial (o governo) não saiba em qual serviço o usuário está autenticando a idade, e o serviço verificador não saiba a identidade civil do titular.[110]

A pesquisadora Elora Fernandes, ouvida pelo GT-6, contextualizou que, embora o conceito da carteira europeia seja sólido e represente referência relevante para inspirar o ecossistema brasileiro, a execução técnica dos protocolos de duplo-cego ainda é objeto de críticas severas por parte de criptógrafos europeus, que contestam que as garantias de privacidade afirmadas pela Comissão sejam plenamente realizadas na arquitetura técnica concreta

Um mecanismo de coordenação supranacional foi anunciado pela Comissão em 15 de abril de 2026, para apoiar a acreditação de soluções nacionais e a emissão e aceitação transfronteiriça de atestados de prova de idade, com o objetivo de que a União convirja em

---

[107] GATACA. EU Age App Hacked in 2 Minutes and EUDI Wallet Impact. Abr. 2026. Disponível em: https://www.gataca.io/resources/blog/eu-age-verification-app-hacked-eudi-wallet/. Acesso em: 29 maio 2026.

[108] EUROPEAN COMMISSION. EU Age Verification Blueprint: the dedicated technical portal. [S. l.], [2025?]. Disponível em: https://ageverification.dev. Acesso em: 29 maio 2026.

[109] UNIÃO EUROPEIA. Regulamento (UE) 2024/1183 (eIDAS 2.0), Art. 5-A. O mecanismo de compartilhamento seletivo de atributos permite que o usuário apresente apenas a resposta binária ("sim" ou "não") à pergunta sobre maioridade, sem revelar nome, data de nascimento, endereço ou número de documento.

[110] BIOMETRIC UPDATE. EU recommends white label age verification app, but member states are wary. Abr. 2026. Disponível em: https://www.biometricupdate.com/202604/eu-recommends-white-label-age-verification-app-but-member-states-are-wary. Acesso em: 29 maio 2026. Sobre os mecanismos de prova de conhecimento zero e o modelo duplo-cego, ver também: EFF. Age Verification in the European Union: Mini ID Wallet. Abr. 2025. Disponível em: https://www.eff.org/deeplinks/2025/04/age-verification-european-union-mini-id-wallet. Acesso em: 29 maio 2026.

uma solução interoperável em vez de vinte e sete soluções divergentes. Os emissores de atestados de prova de idade devem ser incluídos em lista de confiança mantida e publicada pela Comissão, com notificação pelos Estados-membros dos emissores acreditados.[111]

III. Índia: Aadhaar, atributos verificáveis seletivos e integração com wallets privadas[112]

O Aadhaar é o sistema nacional de identificação da Índia e o maior banco de dados biométrico do mundo. Criado em 2009 pela Unique Identification Authority of India (UIDAI), órgão vinculado ao Ministério da Eletrônica e Tecnologia da Informação (MeitY), o sistema foi concebido a partir de um problema concreto e urgente: a Índia tinha, à época, centenas de milhões de pessoas sem qualquer documento formal de identidade s. A solução desenhada cria um número único de 12 dígitos para cada residente da Índia, vinculado a dados biométricos (dez impressões digitais, escaneamento de íris e fotografia facial) que garantiriam a unicidade de cada cadastro. No auge da operação, 35.000 estações de cadastramento funcionavam simultaneamente em todo o país, chegando a registrar 1,5 milhão de pessoas por dia. Em 2017, o Aadhaar tinha chegado a 1,14 bilhão de pessoas cobrindo mais de 85% da população indiana. Hoje, com 1,38 bilhão de cadastros, é o maior sistema de identificação biométrica já construído por qualquer governo.[113]

A trajetória do Aadhaar não foi linear. Em 2018, o Supremo Tribunal da Índia julgou a constitucionalidade do sistema no paradigmático caso Justice K.S. Puttaswamy v. Union of India. O acórdão, por maioria de 4 a 1, validou o Aadhaar para fins de entrega de benefícios e serviços públicos, mas derrubou a Seção 57 do Aadhaar Act 2016 que permitia a entidades privadas requerer autenticação por Aadhaar, declarando-a inconstitucional por violar o direito fundamental à privacidade consagrado no Artigo 21 da Constituição indiana. A decisão estabeleceu que o Aadhaar poderia ser exigido para acesso a programas

---

[112] UIDAI — UNIQUE IDENTIFICATION AUTHORITY OF INDIA. Lançamento do novo aplicativo Aadhaar com funcionalidades de biometric liveness, verificação etária, minimização de dados e compartilhamento de credenciais. Jan. 2026. Ver: BIOMETRIC UPDATE. New Aadhaar app launches, India's digital ID coming to Google Wallet. 29 jan. 2026. Disponível em: https://www.biometricupdate.com/202601/new-aadhaar-app-launches-indias-digital-id-coming-to-google-wallet. Acesso em: 29 maio 2026.

[113] BIOMETRIC UPDATE. What is Aadhaar? Disponível em: https://www.biometricupdate.com/202505/what-is-aadhaar. Acesso em: 29 maio 2026. Para histórico da criação: ROLAND BERGER. The making of India's biometric Aadhaar ID program. Ago. 2018. Disponível em: https://www.rolandberger.com/en/Insights/Publications/The-making-of-India-s-biometric-Aadhaar-ID-program.html. Acesso em: 29 maio 2026. Para dados de cobertura: WIKIPEDIA. Aadhaar. Disponível em: https://en.wikipedia.org/wiki/Aadhaar. Acesso em: 29 maio 2026 (1,38 bilhão de cadastros a outubro de 2024). Ver também: CHANDLER GOVERNANCE. India's Aadhaar System: Bringing E-Government to Life. Disponível em: https://chandlergovernance.com/governancematters/indias-aadhaar-system-bringing-e-government-to-life. Acesso em: 29 maio 2026.

financiados com recursos públicos, mas não poderia ser tornado obrigatório para abertura de conta bancária, obtenção de chip telefônico ou matrícula escolar, casos que o governo havia tentado vincular ao sistema. Esse julgamento moldou os limites do sistema por quase uma década e permanece central no debate atual sobre a reintegração do Aadhaar em ecossistemas privados.[114]

Em janeiro de 2026, a UIDAI (Autoridade de Identificação Única da Índia) lançou novo aplicativo Aadhaar com funcionalidades ampliadas de *biometric liveness*, aferição etária, minimização de dados e compartilhamento de credenciais. O aplicativo suporta verificação facial como prova de presença, bloqueio e desbloqueio biométrico, histórico de autenticação e compartilhamento de credenciais via QR Code. A funcionalidade "Uma Família — Um App" permite que até cinco perfis Aadhaar sejam gerenciados em um único dispositivo. O MeitY destacou que o aplicativo foi projetado para promover o compartilhamento seletivo de dados, em linha com o *Digital Personal Data Protection Act*: os verificadores recebem credenciais digitalmente assinadas adaptadas a casos de uso específicos, como aferição de idade para compra de ingressos, sem acesso ao número completo do Aadhaar.

Em 28 de abril de 2026, o Google anunciou o lançamento do suporte a credenciais verificáveis Aadhaar no Google Wallet, em parceria com a UIDAI,[115] baseado nos padrões ISO/IEC 18013-5 e W3C Digital Credentials API. A integração concretiza o modelo de compartilhamento seletivo de atributos em larga escala populacional, o usuário decide quais dados compartilhar em cada interação, preservando dados desnecessários à finalidade da verificação. Os primeiros serviços a aceitar a verificação foram PVR INOX (verificação de idade para filmes), BharatMatrimony (perfis verificados) e Atlys (vistos internacionais).[116] O caso indiano é referência de escalabilidade em identidade digital com atributos seletivos para países de alta densidade demográfica, e sua adoção pelo Google

[114] PRIVACY INTERNATIONAL. Initial analysis of Indian Supreme Court decision on Aadhaar. Disponível em: https://privacyinternational.org/long-read/2299/initial-analysis-indian-supreme-court-decision-aadhaar. Acesso em: 29 maio 2026. GLOBAL FREEDOM OF EXPRESSION (Columbia University). Puttaswamy v. Union of India (II). Disponível em: https://globalfreedomofexpression.columbia.edu/cases/puttaswamy-v-union-of-india-ii. Acesso em: 29 maio 2026.

[115] GOOGLE. Google Wallet now supports Aadhaar Verifiable Credentials in India. Blog oficial, 28 abr. 2026. Disponível em: https://blog.google/products-and-platforms/platforms/google-pay/aadhaar-digital-id/. Acesso em: 29 maio 2026. A integração é baseada nos padrões ISO/IEC 18013-5 e W3C Digital Credentials API.

[116] MEDIANAMA. Google Wallet integrates Aadhaar as digital ID, expands India's mobile identity ecosystem. Abr. 2026. Disponível em: https://www.medianama.com/2026/04/223-google-wallet-aadhaar-digital-id-india-mobile-identity/. Acesso em: 29 maio 2026. Primeiros serviços a aceitar verificação via Aadhaar no Google Wallet: PVR INOX (verificação de idade para filmes), BharatMatrimony (perfis verificados) e Atlys (vistos internacionais).

Wallet sinaliza que a fronteira entre infraestruturas públicas e privadas de identidade tende a se tornar crescentemente porosa.[117]

3.4. Práticas do Setor Privado

A análise das práticas de aferição de idade adotadas pelo setor privado apoia-se em quatro fontes complementares: o levantamento empírico da OCDE sobre 50 serviços globais[118]; o estudo nacional conduzido pelo Cetic.br sobre 25 serviços utilizados por crianças no Brasil[119]; as entrevistas realizadas pelo GT-6 com stakeholders nacionais; e o *Age Assurance Technology Trial* australiano[120].

I. O mapeamento global da OCDE: práticas identificadas em 50 serviços digitais

O *technical paper* "Age Assurance Practices of 50 Online Services Used by Children", publicado pela OCDE em junho de 2025[121], examinou as políticas e práticas de aferição de idade de 50 serviços digitais utilizados por crianças e adolescentes, abrangendo dez categorias: lojas de aplicativos, redes sociais, mensageria, jogos, aplicativos de relacionamento, vídeo ao vivo aleatório, IA generativa, pornografia, ambientes imersivos e serviços voltados especificamente a crianças. A análise baseou-se em documentos de governança publicamente disponíveis (termos de uso, políticas de privacidade e códigos de conduta complementados por manifestações dos próprios serviços consultados.

Definição de idades mínimas. De acordo com o estudo, dois terços dos serviços (34 de 50) estabelecem uma idade mínima numérica que não pode ser sobreposta por consentimento parental. Os demais ou admitem acesso de crianças abaixo da idade mínima mediante consentimento parental, ou não fixam qualquer idade mínima. A clareza e precisão na comunicação da idade mínima variam significativamente: enquanto cerca de um terço dos serviços utiliza um número preciso, os demais recorrem a expressões como "a maioridade na jurisdição do usuário", transferindo ao próprio usuário a tarefa de apurar

[117] GOOGLE. Google Wallet adds Aadhaar support in India, expands digital IDs to more countries. Blog oficial, 28 abr. 2026. Disponível em: https://blog.google/products-and-platforms/platforms/google-pay/aadhaar-digital-id/. Acesso em: 29 maio 2026. O Brasil está entre os países que receberam suporte a ID passes baseados em passaporte no Google Wallet no mesmo comunicado.

[118] OECD. Age Assurance Practices of 50 Online Services Used by Children. OECD Publishing, Paris, junho de 2025. Disponível em: https://doi.org/10.1787/a19853ab-en.

[119] CGI.br; NIC.br; CETIC.BR. Práticas de Aferição de Idade em 25 Serviços Digitais Usados por Crianças no Brasil. São Paulo: Cetic.br, março de 2026. Disponível em: https://cetic.br/media/analises/Ceticbr_Estudo_Afericao_Idade_Servicos_Digitais_Criancas.pdf.

[120] AGE CHECK CERTIFICATION SCHEME. Age Assurance Technology Trial — Report (Parts A to K). Australian Government, agosto de 2025. Disponível em: https://ageassurance.com.au/report.

[121] OECD. Age Assurance Practices of 50 Online Services Used by Children. OECD Publishing, Paris, junho de 2025. Disponível em: https://doi.org/10.1787/a19853ab-en.

esse limiar. A terminologia para designar o público infantojuvenil também é heterogênea, os termos "crianças", "adolescentes", "crianças e adolescentes" e "jovens" são utilizados de forma intercambiável e sem definição clara em vários serviços.

Mecanismos de aferição *ex ante* **(no momento do cadastro).** Nos termos do estudo, apenas dois dos 50 serviços realizam a aferição de idade de forma sistemática no momento da criação de conta, independentemente da localização geográfica do usuário. Para todos os demais, a aferição *ex ante*, quando existente, é acionada seletivamente: em determinadas jurisdições; para acesso a funcionalidades específicas (como transmissões ao vivo, monetização ou comunicação com desconhecidos); ou quando há indicativo de que o usuário não atende à idade mínima. A autodeclaração, por digitação de data de nascimento ou marcação de uma caixa confirmando maioridade, é o mecanismo mais frequente nessa fase.

Mecanismos de aferição *ex post* **(após o cadastro).** A maioria dos serviços que implementa alguma forma de aferição o faz após o cadastro, como condição para desbloqueio de funcionalidades restritas ou em resposta a atividade considerada suspeita. Os métodos de verificação de idade identificados incluem: documento oficial de identidade (com ou sem *selfie* para correspondência facial); cartão de crédito; conta vinculada a outro serviço (como Google ou Apple); e consentimento parental verificado. Entre os métodos de estimativa de idade identificados, o uso de *selfie*, em foto ou vídeo, como insumo para análise biométrica é o mais difundido. Algumas plataformas combinam mais de um método ou adotam tecnologias diferentes conforme a jurisdição.

Salvaguardas por faixa etária. A maioria dos serviços com público de idades mistas adota salvaguardas escalonadas por faixa etária (*age-tiered safeguards*), respondendo a riscos de conteúdo, contato, privacidade, publicidade e transações comerciais. Essas salvaguardas incluem funcionalidades obrigatórias e opcionais, sendo que, frequentemente, as configurações mais restritivas podem ser desativadas pelos próprios usuários ou dependem de ativação ativa por parte dos responsáveis. Crianças mais velhas tendem a ter configurações mais permissivas.

Mecanismos de identificação proativa de usuários crianças e adolescentes. Apenas 34% dos serviços analisados dispõem de ferramentas para identificar proativamente usuários que possam ser crianças e adolescentes, conforme a sua idade. Cerca de 40% possuem canal dedicado para denúncias de usuários crianças e adolescentes, e apenas três publicam informações sobre a aplicação de suas políticas de idade em relatórios de transparência.

II. O estudo nacional do Cetic.br: práticas identificadas em 25 serviços no Brasil

O Cetic.br, com assistência técnica da OCDE e adotando a mesma referência metodológica do estudo global, publicou em março de 2026 o levantamento "Práticas de Aferição de Idade em 25 Serviços Digitais Usados por Crianças no Brasil"[122]. A pesquisa analisou 550 páginas de documentos de governança coletados entre 10 e 30 de janeiro de 2026, em 25 plataformas distribuídas entre as categorias de lojas de aplicativos, relacionamento, serviços infantis, jogos, IA generativa, mensageria, pornografia, redes sociais, apostas e *marketplace*, observando dez dimensões analíticas: idade mínima para uso, mecanismos de aferição *ex ante* e *ex post*, supervisão parental, sanções por descumprimento e transparência.

Mecanismos de aferição *ex ante*. A pesquisa identificou que 21 dos 25 serviços não realizavam aferição no momento do cadastro, inclusive aqueles voltados ao público adulto. Os quatro serviços que realizavam alguma forma de aferição *ex ante* incluíam, entre os métodos identificados: documento oficial de identidade (o mais frequente, presente em 13 dos 25 serviços quando considerado o conjunto completo de mecanismos); cartão de crédito; endereço de e-mail; e consentimento parental.

Mecanismos de aferição *ex post*. A aferição em momento posterior ao cadastro era o padrão dominante: concentrava-se na liberação de funcionalidades específicas, como *chat* ao vivo, transmissões e recompensas financeiras, ou era acionada diante de atividade considerada suspeita. Quase metade das plataformas (11 de 25), especialmente redes sociais e ferramentas de IA generativa, recorria a prestadores terceirizados especializados para realizar a aferição em algum momento da jornada do usuário. Entre os métodos identificados, a *selfie* em foto ou vídeo era o mais comum (presente em 12 das plataformas).

Supervisão parental. A maioria dos serviços (15 de 25) oferecia mecanismos de supervisão parental, mas sua ativação era, na maioria dos casos, facultativa e dependia de iniciativa ativa dos responsáveis.

III. Práticas das plataformas: relatos das entrevistas do GT-6

As entrevistas conduzidas pelo GT-6 com plataformas e provedores que atuam no Brasil permitem detalhar abordagens concretas de *age assurance* no contexto nacional.

Uma **empresa de jogos eletrônicos** descreve arquitetura baseada em contas com restrições automáticas por padrão (*cabined accounts*): contas que não passaram por processo de expansão de permissões recebem, automaticamente, restrições abrangentes

[122] CGI.br; NIC.br; CETIC.BR. *Práticas de Aferição de Idade em 25 Serviços Digitais Usados por Crianças no Brasil*. São Paulo: Cetic.br, março de 2026. Disponível em: https://cetic.br/media/analises/Ceticbr_Estudo_Afericao_Idade_Servicos_Digitais_Criancas.pdf.

de funcionalidades (impossibilidade de adicionar amigos, receber mensagens de não amigos, criar perfil público ou participar de transmissões). Para a expansão das permissões, a empresa utiliza ferramenta de verificação de responsáveis legais com mecanismo de aferição etária. Descreve ainda painel centralizado de controles parentais com configurações diferenciadas por faixa etária, limites automáticos de comunicação para crianças mais novas, desativação de *marketing* por padrão para crianças e adolescentes de até 13 anos e relatório semanal para responsáveis.

Uma **plataforma de jogos e experiências interativas** descreve seu modelo como sistema em camadas: para liberar funcionalidades específicas ou conteúdo restrito, recorre a verificação documental via fornecedor terceirizado especializado, com comparação entre documento oficial e imagem facial; para modular o acesso a ferramentas de comunicação, utiliza estimativa facial de idade por faixas etárias (*age bucket*), que aloca o usuário em uma categoria a partir de características faciais, sem identificação civil. A plataforma indica que o modelo é recente, está em calibração e conta com mecanismos de recurso com participação dos responsáveis legais quando a conta da criança ou adolescente está vinculada a uma conta parental.

Uma **plataforma de rede social e serviços de comunicação** descreve, para uma de suas aplicações, o uso de tecnologia de análise de texto e predição de idade alimentada por inteligência artificial como mecanismo de inferência da faixa etária do usuário. A empresa defende que a aferição de idade deve ocorrer primariamente na camada dos sistemas operacionais e lojas de aplicativos, com repasse de um sinal mínimo padronizado de faixa etária às aplicações. Para funcionalidades de maior risco, propõe aferição adicional por carteira digital ou documento de identidade.

Uma **empresa especializada em soluções de *age assurance*** com atuação em 180 países e mais de um bilhão de aferições realizadas descreve modelo baseado em estimativa facial de idade sem retenção de imagem após o processamento, com precisão média de 0,9 ano para a faixa dos 17 anos. O sistema é submetido a avaliação independente pelo benchmarking do NIST e às certificações iBeta nível 2 e 3. A empresa destaca que, no Brasil, documentos de identidade estaduais e carteiras de habilitação apresentam taxas de aprovação em verificação automatizada entre 29% e 35%, em razão de deterioração física decorrente do uso cotidiano, enquanto passaportes atingem aproximadamente 90%, mas com penetração significativamente menor na população.

Uma **empresa de tecnologia de identidade digital** apresenta modelo de identidade descentralizada baseado em credenciais verificáveis no padrão W3C e provas de conhecimento zero (ZKP): o verificador recebe apenas uma resposta binária sem acesso

a dados pessoais identificáveis, e o ato de verificação é registrado de forma imutável e auditável. A empresa descreve também rede de adultos previamente verificados que permite a reutilização do resultado de uma verificação já realizada em outros serviços que utilizem a mesma infraestrutura, sem necessidade de nova apresentação de documentos.

Uma **associação representativa do setor de *streaming* audiovisual** descreve modelo em que a proteção parte do fluxo de contratação: a conta principal é criada por um adulto, titular da relação contratual, e em alguns serviços do setor a validação do CPF perante base de dados externa ou pelo intermediário de pagamento constitui camada adicional de verificação da maioridade do titular.

IV. O Age Assurance Technology Trial australiano

O *Age Assurance Technology Trial*[123], conduzido entre 2024 e 2025 com financiamento do governo federal australiano e coordenação do *Age Check Certification Scheme*, é uma abrangente avaliação independente de tecnologias de *age assurance* disponíveis. Avaliou 45 provedores de tecnologia segundo padrões internacionais, em especial a série ISO/IEC 27566, o IEEE 2089.1 e a série ISO/IEC 25000, e produziu relatório de 1.150 páginas estruturado em dez volumes (Parts A a K), com dados abertos e estudos de caso individualizados por provedor.

Part C — Verificação de Idade (Age Verification)

De acordo com o Relatório, a verificação de idade é o processo de comprovação da idade real do usuário por referência a uma data de nascimento validada, sendo a forma de maior nível de garantia de *age assurance*. O Trial concluiu que a verificação de idade é tecnicamente viável e operacionalmente implementável de forma privada, segura e efetiva, sem limitações tecnológicas substanciais. Não existe solução única: há uma diversidade de modelos válidos, moldados por necessidades setoriais, perfis de risco, disponibilidade de dados e expectativas de privacidade. O setor é dinâmico e inovador, com provedores desenvolvendo formas mais eficientes de recuperar, vincular e comunicar a informação de idade verificada. Os sistemas performaram de forma consistente entre grupos demográficos distintos, inclusive populações indígenas. Os provedores avaliados nesta categoria foram:

- **AgeChecked**: combina correspondência de dados cadastrais, consulta a agências de crédito e listas eleitorais, estimativa facial de idade, verificação documental com

[123] AGE CHECK CERTIFICATION SCHEME. *Age Assurance Technology Trial — Report (Parts A to K)*. Australian Government, agosto de 2025. Disponível em: https://ageassurance.com.au/report.

detecção de vivacidade e verificação por cartão de crédito vinculado a adulto em processo em cascata.

- **APP ConnectID** (Australian Payments Plus): baseia-se na data de nascimento verificada pelos bancos via *KYC* para retornar apenas asserções binárias de idade (por exemplo, "maior de 18 anos: sim/não"); o modelo de troca ponto a ponto garante que nenhuma informação pessoal identificável transite pelo sistema intermediário, e somente o dado mínimo consentido é compartilhado.
- **Austroads**: gestora do sistema nacional australiano de informações sobre veículos e habilitações (NEVDIS), pioneira nos padrões de Carteira de Habilitação Digital (*Mobile Driver Licence* — mDL); viabiliza credenciais verificadas e atestações seletivas de faixa etária por meio de identificadores emitidos pelo governo e registros seguros, com design conforme a ISO.
- **DigiChek**: provedor de verificação de idade que combina técnicas documentais e de dados para avaliar a idade do usuário, com alinhamento às normas internacionais de verificação. *(Erratum: o nível de maturidade tecnológica — TRL — havia sido classificado como TRL 5 no momento da avaliação; o provedor informa que a solução está agora em produção, equivalente ao TRL 9.)*
- **EarthID**: verificação descentralizada baseada em *blockchain*, com ênfase em privacidade do usuário, segurança de dados e compartilhamento orientado por consentimento, alinhada às normas internacionais para sistemas de identidade digital confiáveis.
- **Eden Game Development Centre**: voltada a ambientes de jogos para jovens; realiza verificação manual de identidade em eventos presenciais e planeja lançar sistema tokenizado com resistência a fraudes por gestos, retenção mínima de dados e princípios de confiança comunitária para usuários crianças e adolescentes.
- **Frankie One**: agrega serviços de *age assurance* de múltiplos provedores, habilitando inferência por meio de integrações com terceiros e suportando lógica de orquestração para *fallback*, limiares de confiança e decisões de identidade com múltiplos fornecedores.
- **GBG**: sistema de verificação multicamadas em tempo real, combinando verificação documental, biometria facial, dados de agências de crédito e detecção de vivacidade; inclui opções de verificação presencial e suporta estimativa facial de idade para usuários a partir de seis anos, sem retenção de informações pessoais identificáveis, com aplicabilidade em múltiplos setores regulados.
- **IDmission**: verificação biométrica de identidade e idade via correspondência de *selfie*, escaneamento de documentos e verificação por vouching como alternativa; oferece SDK global orientado a dispositivos móveis com opções inclusivas para usuários sem documentos de identidade tradicionais.

- **IDVerse**: utiliza IA avançada para verificação de idade em tempo real por correspondência biométrica facial, detecção de vivacidade e OCR; oferece proteção robusta contra fraudes e conformidade com normas globais para grupos de usuários diversos.
- **One Click Group**: entrega identidade descentralizada e orientada a dispositivos móveis com tokens criptográficos vinculados ao dispositivo; utiliza reconhecimento facial e detecção de vivacidade para associar a idade ao usuário de forma segura sem armazenamento de dados em servidores.
- **PRIVO**: combina estimativa facial, verificação documental e fluxos de aprovação parental; certificada pela COPPA e voltada à proteção de crianças em serviços *online* e contextos educacionais. *(Erratum: o relatório publicado sugeriu que a solução era "centrada nos EUA"; o provedor esclarece que, embora desenvolvida para o mercado americano e a COPPA em particular, a solução é configurável para outras jurisdições, incluindo a Austrália.)*
- **Right Crowd**: eficaz para fluxos de acesso físico e segurança corporativa; não projetada para verificação *online* ou voltada ao consumidor; melhor adequada a ambientes empresariais com infraestrutura de identificação existente.
- **Sedicii**: realiza escaneamento de documento com correspondência biométrica por *selfie* ou, na ausência de documento, provas de conhecimento zero; emite credenciais binárias de uso único não vinculáveis (por exemplo, "maior de 18 anos") sem exposição da identidade civil.
- **ShareRing**: utiliza *blockchain* para gerenciar identidade e verificação de idade com prioridade à privacidade, via OCR, biometria e *ePassports*; opera por meio do aplicativo ShareRing Me com armazenamento descentralizado de credenciais verificáveis.
- **TruAnon**: vincula contas existentes do usuário, acesso escolar, prontuário de saúde ou e-mail estudantil, para comprovar a idade sem exposição de dados privados; transfere a responsabilidade das plataformas para o próprio indivíduo, eliminando riscos associados ao armazenamento de dados privados e à coleta biométrica.
- **Yoti**: verificação de baixa fricção e alta confiança com tokens de uso único ou reutilizáveis; utiliza identificadores com *hash* não vinculáveis, sem perfis de identidade persistentes; o sistema registrou Taxas de Verdadeiro Positivo consistentemente acima de 94% a partir dos 13 anos e Erro Médio Absoluto (MAE) abaixo de dois anos para a faixa de 13 a 20 anos nos testes automatizados em laboratório; 80% dos usuários relataram satisfação ou alta satisfação com a experiência.

Part D — Estimativa de Idade (Age Estimation).

De acordo com o Relatório, a estimativa de idade é um método de determinação da faixa etária provável do usuário por análise de características físicas ou comportamentais mediante inteligência artificial ou modelos de aprendizado de máquina, sem necessidade de documentos de identidade. O Trial identificou que a estimativa de idade está em uso ativo e é implementável na Austrália, sem limitações tecnológicas substanciais, com alinhamento às normas ISO/IEC FDIS 27566-1 e IEEE 2089.1. Não existe abordagem única: os provedores ofertam diferentes modelos de implantação (tempo real ou assíncrono), com limiares configuráveis e métodos de *fallback* ajustáveis ao perfil de risco. O setor está em rápida evolução, com introdução de IA *on-device*, augmentação de dados sintéticos e modelos de menor latência. A consistência demográfica está melhorando, embora a sub-representação de populações indígenas permaneça um desafio em processo de endereçamento. Os provedores avaliados nesta categoria foram:

- **IDmission**: verificação biométrica via correspondência de *selfie* e documentos com opções inclusivas para usuários sem documentos tradicionais; orientado a dispositivos móveis com SDK global.
- **Needemand**: solução *BorderAge*, estimativa de faixa etária não facial e não biométrica, baseada na dinâmica de gestos manuais capturada pela câmera do dispositivo para determinar se o usuário é provavelmente adulto ou criança, sem qualquer análise de traços faciais ou outros dados biométricos tradicionais.
- **Persona**: estimativa facial de idade com *fallback* para verificação documental; inclui métricas de equidade com auditoria, processo governado de atualização de modelos e design com preservação de privacidade e controles de exclusão (*opt-out*).
- **Privately**: sistema leve de estimativa facial *on-device*, projetado para implantações com privacidade por concepção, especialmente em contextos voltados a jovens, como educação e ambiente familiar.
- **PRIVO**: *(ver descrição na Part C acima.)*
- **Rigr AI**: utiliza estimativa facial com arquitetura *on-device* ou de borda (*edge*) com IA, entregando *age assurance* em tempo real sem armazenamento de dados biométricos, para contextos digitais diversos e de baixa fricção.
- **Unissey**: provedor de estimativa de idade por análise facial avaliado no Trial. *(Informações detalhadas de desempenho disponíveis no relatório individual do provedor.)*
- **Verifymy**: soluções integradas com carteiras digitais, verificação documental e bases de dados transjurisdicionais; suporta divulgação seletiva e verificações de idade com prioridade à privacidade, entregando resultados binários (por exemplo, "maior de 18 anos: sim") via APIs e credenciais reutilizáveis para setores como apostas, e-commerce e educação.

- **Yoti**: *(ver descrição na Part C acima; adicionalmente, na estimativa de idade, o sistema não retém a imagem após o processamento e publica métricas de desempenho desagregadas por sexo e tom de pele, com certificações iBeta nível 2 e 3.)*

Part E — Inferência de Idade (Age Inference).

De acordo com o Relatório, a inferência de idade é um método de determinação da faixa etária provável com base em sinais contextuais, comportamentais, transacionais ou ambientais verificáveis, sem recorrer a dados biométricos ou documentos de identidade (por exemplo, matrícula escolar, transações financeiras, configurações de controle de conteúdo, padrão de uso do serviço ou participação em atividades específicas de determinada faixa etária). O Trial identificou que a inferência de idade é viável e efetiva na Austrália, especialmente quando usada para sinalizar acesso provável por crianças e adolescentes, apoiar intervenções de segurança precoces ou acionar mecanismos de *fallback*. Os métodos mais precisos baseiam-se em sinais com modelagem clara: complexidade de linguagem, padrões de sessão, acesso a funcionalidades específicas. O setor está evoluindo com técnicas como modelagem de gestos, análise de complexidade narrativa e síntese de metadados contextuais. Os provedores avaliados nesta categoria foram:

- **Equifax**: utiliza inferência de idade como camada complementar, integrável em processos de validação sucessiva.
- **Frankie One**: *(ver descrição na Part C acima.)*
- **Luciditi**: combina estimativa facial, verificação documental por correspondência *selfie*-ID, leitura NFC de passaporte e registros de *open banking* ou telecomunicações, com *fallback* para aplicativo de identidade digital reutilizável.
- **MyMahi**: verificação de idade a partir da data de nascimento registrada em sistemas escolares. *(Erratum: a solução foi incluída no volume de Inferência de Idade por equívoco — a determinação da idade baseia-se em data de nascimento registrada em prontuários escolares, não em inferência comportamental; trata-se, tecnicamente, de verificação de idade.)*
- **PRIVO**: *(ver descrição na Part C acima.)*
- **Verifymy**: *(ver descrição na Part D acima.)*
- **Yoti**: *(ver descrição na Part C acima.)*

Part F — Validação Sucessiva (Successive Validation).

De acordo com o estudo, a validação sucessiva é o processo de combinação de dois ou mais métodos de *age assurance*, como inferência, estimativa e verificação, para alcançar

uma decisão mais precisa, adequada ao risco ou com maior nível de confiança. Definida na ISO/IEC FDIS 27566-1, sustenta o princípio de que a aferição deve ser proporcional ao risco, viabilizando abordagens em camadas onde nenhum método isolado é suficiente ou contextualmente adequado. O Trial identificou que a validação sucessiva é tecnicamente viável e alinhada às normas internacionais, com provedores articulando lógicas de escalonamento bem definidas, gatilhos de *fallback* e limiares de confiança, sustentados por tratamento de dados com preservação de privacidade. Não existe configuração única: os modelos variam conforme o contexto de risco e o caso de uso, de modelos com estimativa como primeira camada e *fallback* para verificação documental, a escalonamento em tempo real acionado por contra-indicadores comportamentais. O setor está em processo de maturação, com exploração de jornadas dinâmicas de usuário, verificações baseadas em dispositivo e reutilização de identidades previamente validadas. Os provedores avaliados nesta categoria foram:

- **AgeChecked**: *(ver descrição na Part C acima — processo em cascata com múltiplos métodos.)*
- **Equifax**: *(ver descrição na Part E acima.)*
- **Luciditi**: *(ver descrição na Part E acima.)*
- **Persona**: *(ver descrição na Part D acima.)*
- **Right Crowd**: *(ver descrição na Part C acima — aplicável a fluxos de acesso físico.)*
- **Verifymy**: *(ver descrição na Part D acima.)*
- **Yoti**: *(ver descrição na Part C acima.)*

Part G — Controle Parental (Parental Control).

De acordo com o Relatório, os sistemas de controle parental são ferramentas, configurações e funcionalidades de supervisão que permitem que pais ou responsáveis gerenciem o acesso de crianças a conteúdo, serviços, dispositivos ou funções digitais. Diferem do consentimento parental por serem pré-configurados e contínuos, em vez de acionados pontualmente. O Trial concluiu que esses sistemas são efetivos em muitos contextos, mas concentram-se em restrição em vez de participação, com limitada acomodação da autonomia progressiva da criança e do adolescente. Quando bem projetados, podem gerar sinais contextuais de faixa etária úteis para moderação de conteúdo e controle de acesso, embora não devam ser tratados como dados de idade verificada. A eficácia depende de configuração precisa e engajada pelos responsáveis. O Trial identificou demanda crescente das plataformas por formatos padronizados que permitam integrar sinais de controle parental em lógicas de acesso. Os provedores avaliados nesta categoria foram:

- **Apple**: controles parentais integrados ao sistema operacional (*Screen Time*), com vinculação de contas familiares, configuração de limites de conteúdo e tempo de uso, e sinal de faixa etária emitido ao nível do dispositivo e da loja de aplicativos; avaliada também na Part J.
- **Assure ID**: sistema de controle parental digital avaliado no Trial. *(Informações detalhadas disponíveis no relatório individual do provedor.)*
- **Epic Games Kids Web Services (KWS)**: fluxo completo de aferição e consentimento parental com validação de CPF/data de nascimento, configurações granulares por faixa etária, limites automáticos de comunicação e relatório de atividade periódico para responsáveis.
- **K-ID**: especializada em sistemas de controle e gerenciamento parental para contextos digitais. *(Informações detalhadas disponíveis no relatório individual do provedor.)*
- **Qoria**: especializada em controle e consentimento parental; avaliada também na Part H.

Part H — Consentimento Parental (Parental Consent).

De acordo com o Relatório, no consentimento parental uma mãe, um pai ou a pessoa responsável confirma o acesso de uma criança ou de um adolescente a bens, serviços ou conteúdo com restrição etária. Diferentemente dos controles parentais, que são pré-configurados e contínuos, o consentimento parental é acionado em pontos específicos de acesso, sem determinar diretamente a idade da criança ou do adolescente. O Trial identificou que esses sistemas são funcionais e implementáveis, mas variam significativamente em design: de verificação leve por *e-mail* a modelos formalizados com verificação de identidade e tokens de consentimento criptográficos. A maioria assume estruturas familiares convencionais e não acomoda arranjos de guarda mais complexos. O consentimento é geralmente tratado como evento pontual, sem adaptação ao longo do desenvolvimento da criança ou do adolescente. Modelos emergentes com tokens de consentimento com escopo limitado e prazo de validade mostram potencial para fluxos mais dinâmicos. Os provedores avaliados nesta categoria foram:

- **PRIVO**: *(ver descrição na Part C acima.)*
- **Qoria**: *(ver descrição na Part G acima.)*
- **R2 Labs**: provedor de consentimento parental e integração em pilha tecnológica; avaliado também na Part J. *(Informações detalhadas disponíveis no relatório individual do provedor.)*

- **Sedicii**: *(ver descrição na Part C acima — inclui modelo de consentimento com credenciais binárias não vinculáveis.)*
- **Trust Elevate**: provedor de consentimento parental avaliado no Trial. *(Informações detalhadas disponíveis no relatório individual do provedor.)*

Part J — Integração

O Part J examina como os mecanismos de *age assurance*, consentimento e controle parental podem ser incorporados de forma sistêmica na infraestrutura digital, ao nível de dispositivos, navegadores, redes, lojas de aplicativos e serviços de *backend*, superando a implementação fragmentada serviço a serviço. O Trial concluiu que essa abordagem oferece potencial para proteções interoperáveis e transversais, mas os modelos ainda estão em estágio inicial, com muitas soluções em fase conceitual ou de prototipagem e Níveis de Maturidade Tecnológica (*TRL*) muitas vezes superestimados pelos provedores. Os modelos baseados em lojas de aplicativos são os mais desenvolvidos, mas atualmente dependem de informações autodeclaradas ou definidas pelos responsáveis, sem verificação independente, e a adoção pelos principais operadores é necessária para que funcionem em escala. A implantação no nível de rede ou dispositivo levanta considerações de privacidade, autonomia e proteção de dados. A responsabilidade pela integração permanece difusa sem marcos regulatórios ou contratuais claros. O Trial identificou também que serviços de geolocalização podem contribuir para detectar circunvenção via VPN. Os provedores avaliados nesta categoria foram:

- **Apple**: *(ver descrição na Part G acima, avaliada pela integração de controles parentais e sinal de faixa etária ao nível de dispositivo e loja de aplicativos.)*
- **euCONSENT** (*Age Aware*): sistema de consentimento e *age assurance* desenvolvido no contexto europeu, com arquitetura de interoperabilidade entre plataformas. *(Informações detalhadas disponíveis no relatório individual do provedor.)*
- **GeoComply**: especializada em serviços de geolocalização; avaliada pela capacidade de detectar e prevenir circunvenção por VPN em sistemas de *age assurance* baseados em localização.
- **General Identity Protocol**: protocolo de identidade de propósito geral avaliado pela capacidade de integração em pilha tecnológica. *(Informações detalhadas disponíveis no relatório individual do provedor.)*
- **Google**: avaliada pelas ferramentas de controle parental (*Family Link*) e APIs de sinal de faixa etária disponíveis ao nível do sistema operacional Android e da loja de aplicativos. *(Informações detalhadas disponíveis no relatório individual do provedor.)*

- **ID Exchange**: sistema de interoperabilidade de identidade digital avaliado pela capacidade de integração em pilha tecnológica. *(Informações detalhadas disponíveis no relatório individual do provedor.)*
- **Meta**: avaliada pelas ferramentas de supervisão parental (*Family Center*) e pelo modelo de repasse de sinal de faixa etária via infraestrutura de plataforma. *(Informações detalhadas disponíveis no relatório individual do provedor.)*
- **Netsweeper**: provedor de filtragem de conteúdo ao nível de rede, avaliado pela capacidade de implementar restrições baseadas em faixa etária na camada de infraestrutura de ISP. *(Informações detalhadas disponíveis no relatório individual do provedor.)*
- **Opale**: sistema de *age assurance* para pilha tecnológica avaliado no Trial. *(Informações detalhadas disponíveis no relatório individual do provedor.)*
- **Privately**: *(ver descrição na Part D acima, avaliada aqui pela arquitetura de estimativa* on-device *integrável à pilha tecnológica sem dependência de servidor remoto.)*
- **R2 Labs**: *(ver descrição na Part H acima.)*
- **Shayype Solutions**: sistema de *age assurance* baseado em pilha tecnológica avaliado no Trial. *(Informações detalhadas disponíveis no relatório individual do provedor.)*
- **Snap Inc.**: avaliada pelo mecanismo de inferência de faixa etária por análise comportamental integrado à pilha da plataforma. *(Erratum: o relatório publicado incorretamente afirmava que a tecnologia de estimativa de idade da Snap considera informações biométricas, a referência correta é a informações comportamentais.)*

3.5. Implementação de Sinais de Idade: Conceito e Desafios Práticos

I. O sinal de idade no ECA Digital e no Decreto nº 12.880/2026

O ECA Digital e o Decreto nº 12.880/2026 introduziram no ordenamento brasileiro um regime estruturado de aferição de idade organizado em torno de conceitos operacionais distintos. Para os fins deste capítulo, interessa especificamente o *sinal de idade,* definido pelo art. 2º, VI, do Decreto como a informação ou credencial indicativa que atesta a idade ou a faixa etária de um usuário aos fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e adolescentes ou de acesso provável por eles, sem revelar dados pessoais adicionais.

O sinal de idade ocupa posição específica dentro de um espectro mais amplo de mecanismos de aferição. O Decreto distingue a aferição de idade em sentido geral,

procedimentos destinados a verificar, estimar ou inferir a idade ou faixa etária por qualquer método tecnicamente idôneo (art. 2º, IV), da verificação de idade em sentido estrito, procedimento de alto grau de confiabilidade baseado na conferência da veracidade do atributo etário mediante mecanismos técnicos ou documentais, cujos parâmetros serão estabelecidos pela ANPD (art. 2º, V), e da autodeclaração, método limitado à indicação da idade pelo próprio usuário, sem evidências adicionais (art. 2º, VII). O sinal de idade não se confunde com nenhum desses conceitos isoladamente: ele é o produto de uma aferição prévia realizada pela loja de aplicativos ou pelo sistema operacional que é transmitido, de forma minimizada e sem revelar dados pessoais adicionais, aos fornecedores de aplicações para que estes possam cumprir suas próprias obrigações legais.

A obrigação de emissão do sinal está prevista no art. 12, III, da Lei nº 15.211/2025, que determina aos provedores de lojas de aplicações de internet e de sistemas operacionais de terminais que possibilitem, por meio de API segura e pautada pela proteção da privacidade desde o padrão, o fornecimento do sinal de idade aos provedores de aplicações de internet, exclusivamente para o cumprimento das finalidades da Lei e com salvaguardas técnicas adequadas. O art. 25 do Decreto regulamenta essa obrigação e acrescenta três elementos centrais: a gratuidade do fornecimento; a limitação do sinal aos dados estritamente necessários à confirmação da idade mínima exigida para acesso ao produto ou serviço, com expressa vedação ao envio de data de nascimento exata, da identidade civil ou de dados de perfilamento do usuário (§1º); e a obrigação de que a loja ou o sistema operacional solicite ao titular a declaração da idade ou faixa etária no momento da criação da conta e a afira mediante método confiável, preferencialmente com a adoção de credenciais verificáveis (§2º, I e II).

Do lado receptor, os fornecedores de produtos ou serviços de tecnologia da informação que disponibilizem conteúdo impróprio, inadequado ou proibido para crianças e adolescentes são obrigados a receber o sinal e a adequar a experiência do produto ou serviço em conformidade com a Lei (art. 26 do Decreto). Independentemente do recebimento do sinal, mantêm a obrigação de implementar mecanismos próprios de proteção. Em caso de divergência entre o resultado de aferição própria e o sinal recebido da loja ou do sistema operacional, o fornecedor deve adotar a alternativa mais protetiva a crianças e adolescentes (art. 25, §4º, do Decreto). O recebimento do sinal não isenta o fornecedor de responsabilidade pela efetividade das medidas de proteção adotadas (art. 26, §3º, do Decreto).

II. Legislações estrangeiras com sistemática equivalente

A obrigação de emissão de sinal de idade por lojas de aplicativos ou sistemas operacionais constitui inovação regulatória recente, adotada de forma expressa em apenas cinco jurisdições até o momento: Califórnia, Utah, Texas e Louisiana (Estados Unidos) e Singapura (trazida para esse estudo de maneira pontual no tema, muito embora não faça parte do benchmark mais abrangente). A análise dessas experiências busca subsidiar o processo regulatório brasileiro por meio do exame do direito comparado, com o objetivo de verificar o que tem sido desenvolvido em outras jurisdições e avaliar em que medida conceitos, sistemáticas, relações entre atores e soluções técnicas já testadas podem ser aproveitados nas escolhas regulatórias ainda em aberto no âmbito do ECA Digital.

III.1 Califórnia, Digital Age Assurance Act (Assembly Bill No. 1043, Chapter 675, Statutes of 2025)

Conceito de sinal de idade. A lei define *signal* na seção 1798.500, alínea (h) como os dados de faixa etária (*age bracket data*) enviados por uma API segura em tempo real ou pelo sistema operacional a uma aplicação. *Age bracket data* é definido no §1798.500(b) como dados não pessoalmente identificáveis derivados da data de nascimento ou da idade do usuário, para fins de compartilhamento com desenvolvedores de aplicações, indicando a faixa etária do usuário em ao menos quatro categorias: abaixo de 13 anos; de 13 a menos de 16 anos; de 16 a menos de 18 anos; 18 anos ou mais.

Atores relevantes. O §1798.500(g) define *operating system provider* como a pessoa ou entidade que desenvolve, licencia ou controla o software do sistema operacional de um computador, dispositivo móvel ou qualquer outro dispositivo de computação de uso geral[124]. O §1798.500(e) define *covered application store* como o sítio, aplicação ou plataforma publicamente disponível que distribui e facilita o download de aplicações de desenvolvedores terceiros. O §1798.500(f) define *developer* como a pessoa que possui, mantém ou controla uma aplicação. O §1798.500(a) define *account holder* como o indivíduo com ao menos 18 anos ou o pai, mãe ou responsável legal do usuário com menos de 18 anos. O §1798.500(i) define *user* como a criança ou o adolescente que é o usuário primário do dispositivo.

[124] A amplitude da definição de *operating system provider* adotada pelo AB 1043 que abrange expressamente computadores, dispositivos móveis e "qualquer outro dispositivo de computação de uso geral" gerou debate nos Estados Unidos sobre os limites do escopo da lei. A principal controvérsia diz respeito à possível incidência da obrigação sobre distribuições Linux e sistemas BSD de código aberto, que não operam por meio de entidade corporativa centralizada e não impõem camada uniforme de criação de conta ao usuário. Em março de 2026, o projeto MidnightBSD declarou publicamente que planejava excluir residentes da Califórnia do uso de seu sistema a partir de janeiro de 2027 como medida de mitigação de risco. A autora da lei, Buffy Wicks, sinalizou abertura para trabalhar em ajustes na sessão legislativa de 2026, mas até maio de 2026 nenhuma emenda havia sido introduzida para endereçar a questão.

Obrigações dos atores relevantes. O provedor de SO é o agente primariamente obrigado pela emissão do sinal. O §1798.501(a) determina que deve: disponibilizar interface acessível no momento de configuração da conta que exija do titular a indicação da data de nascimento ou da idade do usuário; fornecer ao desenvolvedor que o solicitar um sinal digital via API em tempo real razoavelmente consistente identificando a faixa etária do usuário; e enviar apenas o mínimo de informação necessário para cumprimento da lei, sendo vedado o compartilhamento com terceiros para finalidades não exigidas pelo diploma. O desenvolvedor, nos termos do §1798.501(b), deve: solicitar o sinal no momento do download e do lançamento do aplicativo; tratá-lo como indicador primário da faixa etária do usuário, cedendo apenas diante de informação interna clara e convincente em sentido contrário; e não compartilhá-lo com terceiros para finalidades não exigidas pela lei.

Como o sinal é obtido. Por autodeclaração. O §1798.501(a)(1) exige que o provedor de SO disponibilize, no momento de configuração da conta do dispositivo, uma interface acessível que exija do titular da conta a indicação da data de nascimento, da idade ou de ambas do usuário. A lei não exige qualquer método adicional de aferição da veracidade da informação declarada.

Como o sinal é transmitido ao provedor de aplicações. O §1798.501(a)(2) determina que o provedor de SO forneça ao desenvolvedor que o solicitar um sinal digital via API em tempo real razoavelmente consistente (*reasonably consistent real-time application programming interface*), identificando a faixa etária do usuário. O §1798.501(b)(1) impõe ao desenvolvedor a obrigação de solicitar o sinal no momento do download e do lançamento do aplicativo.

Gratuidade. A lei não trata do tema.

Obrigações e requisitos adicionais. O desenvolvedor que recebe o sinal é considerado detentor de conhecimento efetivo (*actual knowledge*) da faixa etária, mesmo que o ignore deliberadamente (§1798.501(b)(2)(A)). O provedor de SO e a loja de aplicativos estão proibidos de usar dados coletados de terceiros no curso do cumprimento da lei para competir contra esses terceiros ou para fins anticoncorrenciais (§1798.504(c)(2)). A lei não cria obrigação de consentimento parental para download. O §1798.504(b) veda a coleta de informações pessoais adicionais além do estritamente necessário para cumprimento do §1798.501. O descumprimento sujeita o infrator a penalidade civil de até USD 2.500 por criança afetada por violação negligente e até USD 7.500 por violação intencional, aplicada pelo Procurador-Geral (§1798.503(a)).

Status. Sancionada em 13 de outubro de 2025, com vigência a partir de 1º de janeiro de 2027. O Governador Newsom, ao assiná-la, reconheceu a necessidade de ajustes legislativos na sessão de 2026, especialmente em relação a serviços de streaming e contas compartilhadas entre membros da família[125]. Até maio de 2026, nenhuma emenda havia sido introduzida, e não há ação judicial em curso contestando a lei. O prazo principal de cumprimento permanece 1º de janeiro de 2027, com prazo complementar de 1º de julho de 2027 para dispositivos cuja conta tenha sido configurada antes da entrada em vigor da lei.

III.2 Utah, App Store Accountability Act (Senate Bill 142, 2025 General Session, Utah Code Annotated 1953, §§ 13-75-101 et seq.)

Conceito de sinal de idade. A lei opera com o conceito de *age category data*, definido no §13-75-101(2) como a informação sobre a categoria etária do usuário que é coletada pelo provedor de loja de aplicativos e compartilhada com o desenvolvedor. As categorias etárias (*age category*) são definidas no §13-75-101(1): *child* (abaixo de 13 anos), *younger teenager* (de 13 a menos de 16 anos), *older teenager* (de 16 a menos de 18 anos) e *adult* (18 anos ou mais).

Atores relevantes. O §13-75-101(6) define *app store provider* como a pessoa que possui, opera ou controla uma loja de aplicativos que permite a usuários do estado fazer download de aplicativos em dispositivos móveis. O §13-75-101(8) define *developer* como a pessoa que possui ou controla um aplicativo disponibilizado por meio de uma loja de aplicativos no estado. O §13-75-101(15) define *parent* como o indivíduo com autoridade legal para tomar decisões em nome do usuário com menos de 18 anos, incluindo pai ou mãe com relação parental reconhecida, tutor legal ou detentor de custódia legal. O sistema operacional é definido no §13-75-101(14) mas não figura como agente obrigado pela emissão do sinal.

Obrigações dos atores relevantes. A loja de aplicativos é o agente obrigado pela aferição de idade e pela emissão do sinal. O §13-75-201(1) determina que deve: solicitar e aferir a categoria etária do usuário no momento da criação da conta; vincular a conta daquele que tem menos de 18 anos a uma conta parental e obter consentimento parental verificável antes de permitir download, compra de aplicativo ou compra no aplicativo; fornecer ao desenvolvedor, em resposta a solicitação autorizada, os dados de categoria etária e o status do consentimento parental para crianças e adolescentes; notificar o desenvolvedor quando o consentimento parental for revogado; e proteger os dados

[125] CALIFORNIA (Estado). Signing Message for Assembly Bill 1043. Sacramento: Office of Governor Gavin Newsom, 2025. Disponível em: https://www.gov.ca.gov/wp-content/uploads/2025/10/AB-1043-Signing-Message.pdf. Acesso em: 25 maio 2026.

pessoais de verificação de idade com protocolos de criptografia de padrão industrial. O desenvolvedor, nos termos do §13-75-202(1), deve: verificar pelos métodos de compartilhamento de dados da loja a categoria etária dos usuários e, para crianças e adolescentes, o status do consentimento parental; notificar a loja de alterações significativas no aplicativo; e usar os dados de categoria etária recebidos para fazer cumprir restrições etárias, assegurar conformidade legal e implementar recursos de segurança.

Como o sinal é obtido. O §13-75-201(1)(a) exige que a loja, no momento da criação da conta pelo usuário localizado no estado, solicite informações de idade e as afira utilizando métodos comercialmente disponíveis razoavelmente concebidos para assegurar precisão, ou método estabelecido por norma da Division of Consumer Protection. A lei não se contenta com mera autodeclaração, mas não especifica os métodos de aferição admitidos, delegando essa definição à Division of Consumer Protection.

Como o sinal é transmitido ao provedor de aplicações. O §13-75-201(1)(d) determina que a loja forneça ao desenvolvedor, em resposta a solicitação autorizada pelo §13-75-202, os dados de categoria etária do usuário localizado no estado e o status do consentimento parental verificado para crianças e adolescentes. Os dados devem ser transmitidos com protocolos de criptografia de padrão industrial que assegurem integridade e confidencialidade (§13-75-201(1)(f)(ii)).

Gratuidade. A lei não trata do tema.

Obrigações e requisitos adicionais. O compartilhamento de dados pessoais de aferição de idade é vedado exceto entre loja e desenvolvedor conforme exigido pelo capítulo ou por determinação legal (§13-75-201(2)(c)). A coleta e o tratamento de dados ficam limitados ao mínimo necessário para verificação de idade, obtenção de consentimento parental e manutenção de registros de conformidade (§13-75-201(1)(f)(i)). O §13-75-202(3) estabelece que, ao implementar recursos ou configurações padrão de segurança, o desenvolvedor deve utilizar a faixa etária mais baixa indicada pelos dados recebidos da loja ou pelos dados coletados de forma independente. A lei cria direito de ação privada para pais de crianças e adolescentes prejudicados por violação (§13-75-401), com indenização mínima de USD 1.000 por violação, honorários advocatícios e custas. O desenvolvedor que agir de boa-fé com base nos dados recebidos da loja está protegido por *safe harbor* (§13-75-402).

Status. A lei entrou em vigor em 7 de maio de 2025, com obrigações principais originalmente fixadas para 6 de maio de 2026. Em fevereiro de 2026, a Computer & Communications Industry Association (CCIA) ajuizou ação federal contestando a

constitucionalidade da lei com fundamento na Primeira Emenda[126]. Enquanto o litígio estava pendente, Utah emendou a lei por meio do HB 498, sancionado em 18 de março de 2026, que: adiou a data de vigência das obrigações principais de 6 de maio de 2026 para 6 de maio de 2027; eliminou a competência do Procurador-Geral do estado para executar a lei, restringindo o enforcement exclusivamente à ação privada; expandiu o escopo da lei para cobrir aplicativos pré-instalados; e ajustou a definição de significant change e os requisitos de aferição de idade[127]. Em 21 de abril de 2026, a CCIA desistiu voluntariamente da ação após as emendas terem removido o principal mecanismo de enforcement governamental[128]. A lei permanece vigente com as modificações do HB 498, com obrigações principais a partir de 6 de maio de 2027[8] e direito de ação privada a partir de 31 de dezembro de 2026[129].

III.3 Texas, App Store Accountability Act (Senate Bill 2420, 89th Legislature, Texas Business & Commerce Code, Chapter 121)

Conceito de sinal de idade. A lei opera com o conceito de *age category*, estruturado na Seção 121.021(b) em quatro faixas: *child* (abaixo de 13 anos), *younger teenager* (de 13 a menos de 16 anos), *older teenager* (de 16 a menos de 18 anos) e *adult* (18 anos ou mais). A informação sobre essa categoria é transmitida da loja ao desenvolvedor nos termos da Seção 121.024.

Atores relevantes. A Seção 121.002 define *app store* como a plataforma que distribui aplicativos de software para dispositivos móveis. O proprietário da loja (*owner of an app store*) é o agente obrigado pela aferição e pela transmissão das informações ao desenvolvedor. O sistema operacional não figura como agente obrigado. Pais e responsáveis (*parent or guardian*) figuram como titulares do consentimento parental necessário para que crianças e adolescentes façam download de aplicativos.

126 COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION. CCIA Challenges Unconstitutional App Store Law in Utah. Washington, D.C., 5 fev. 2026. Disponível em: https://ccianet.org/news/2026/02/ccia-challenges-unconstitutional-app-store-law-in-utah/. Acesso em: 25 maio 2026.

127 FOLKS, Andrew. Utah First State to Amend its App Store Accountability Act. FKKS Technology Law, 10 abr. 2026. Disponível em: https://technologylaw.fkks.com/post/102mpap/utah-first-state-to-amend-its-app-store-accountability-act. Acesso em: 25 maio 2026.

128 ALSTON & BIRD. Challenge to Utah's App Store Accountability Act Voluntarily Dismissed Following Statutory Amendments. Atlanta, abr. 2026. Disponível em: https://www.alstonprivacy.com/challenge-to-utahs-app-store-accountability-act-voluntarily-dismissed-following-statutory-amendments/. Acesso em: 25 maio 2026.

129 ALSTON & BIRD. Challenge to Utah's App Store Accountability Act Voluntarily Dismissed Following Statutory Amendments. Atlanta, abr. 2026. Disponível em: https://www.alstonprivacy.com/challenge-to-utahs-app-store-accountability-act-voluntarily-dismissed-following-statutory-amendments/. Acesso em: 25 maio 2026.

Obrigações dos atores relevantes. O proprietário da loja, nos termos das Seções 121.021 a 121.027, deve: aferir a categoria etária de cada usuário do estado no momento da criação da conta por método comercialmente razoável; vincular a conta daquele que tem menos de 18 anos a uma conta parental e obter consentimento dos pais ou responsáveis antes de permitir download, compra de aplicativo ou compra no aplicativo; exibir a classificação etária e a descrição de conteúdo de cada aplicativo disponível; permitir ao desenvolvedor o acesso às informações de categoria etária e status de consentimento parental de cada usuário; e notificar o titular do consentimento parental quando houver alteração significativa no aplicativo, obtendo novo consentimento. O desenvolvedor, nos termos das Seções 121.051 a 121.056, deve: atribuir classificação etária a cada aplicativo e a cada compra disponível no aplicativo e fornecê-las à loja; notificar a loja antes de realizar alteração significativa nos termos de serviço ou política de privacidade do aplicativo; criar e implementar sistema para usar as informações recebidas da loja na verificação da categoria etária e do status de consentimento de cada usuário; e utilizar os dados recebidos exclusivamente para fazer cumprir restrições etárias, assegurar conformidade legal e implementar recursos de segurança, excluindo-os após a conclusão da verificação.

Como o sinal é obtido. A Seção 121.021(a) exige que o proprietário da loja, quando um indivíduo no estado cria uma conta, utilize método comercialmente razoável para aferir a categoria etária do usuário. A lei qualifica esse método como *commercially reasonable method of verification*, sem especificar quais métodos são admitidos.

Como o sinal é transmitido ao provedor de aplicações. A Seção 121.024 determina que o proprietário da loja permita ao desenvolvedor o acesso, por método comercialmente disponível, às informações atuais relativas à categoria etária atribuída a cada usuário e ao status do consentimento parental para cada usuário com menos de 18 anos. A Seção 121.054(a) exige que o desenvolvedor crie e implemente um sistema para usar essas informações na verificação da categoria etária e do status de consentimento de cada usuário.

Gratuidade. A lei não trata do tema.

Obrigações e requisitos adicionais. A Seção 121.025 limita a coleta e o tratamento de dados pessoais ao mínimo necessário para aferição de idade, obtenção de consentimento e manutenção de registros de conformidade, com transmissão por protocolos de criptografia de padrão industrial. A Seção 121.055(b) impõe ao desenvolvedor a exclusão dos dados após a conclusão da verificação. A Seção 121.026(b) prevê *safe harbor* para o proprietário da loja que aplicar padrões amplamente adotados pela indústria de forma consistente e de boa-fé. A Seção 121.056(c) prevê *safe harbor*

equivalente para o desenvolvedor que agir de boa-fé com base nas informações recebidas da loja. A lei foi suspensa por liminar federal em 23 de dezembro de 2025; o litígio está em curso.

Status. A lei foi suspensa por liminar federal em 23 de dezembro de 2025, um dia antes de sua entrada em vigor prevista para 1º de janeiro de 2026. O tribunal federal identificou probabilidade de violação da Primeira Emenda, considerando a lei excessivamente ampla e com disposições constitucionalmente vagas[130]. O litígio está em curso, com apelação pendente[131].

III.4 Louisiana, Protection of Children on Applications Act (House Bill 570, Act No. 481, 2025 Regular Session, Louisiana Revised Statutes, §§ R.S. 51:1771–51:1775)

Conceito de sinal de idade. A lei opera com o conceito de *age category data*, definido como a informação sobre a categoria etária do usuário coletada pela loja e compartilhada com o desenvolvedor. As categorias etárias seguem a mesma estrutura das demais leis americanas: *child* (abaixo de 13 anos), *younger teenager* (de 13 a menos de 16 anos), *older teenager* (de 16 a menos de 18 anos) e *adult* (18 anos ou mais).

Atores relevantes. A lei define *covered application store provider* como o agente obrigado pela aferição de idade e pela transmissão das informações ao desenvolvedor. O *developer* é o agente receptor, obrigado a utilizar as informações recebidas. O sistema operacional não figura como agente obrigado. Pais e responsáveis figuram como titulares do consentimento parental para download por crianças e adolescentes.

Obrigações dos atores relevantes. A loja deve: aferir a categoria etária dos usuários no momento da criação da conta; vincular a conta daquele que tem menos de 18 anos a uma conta parental e obter consentimento parental verificável antes de permitir download, compra ou transação no aplicativo; fornecer ao desenvolvedor, mediante solicitação, os dados de categoria etária e o status do consentimento parental para crianças e adolescentes; e notificar o desenvolvedor quando o consentimento parental for revogado. O desenvolvedor deve: verificar a categoria etária e o status de consentimento parental dos usuários pelos dados compartilhados pela loja; utilizar esses dados para

130 TEXAS TRIBUNE. Federal judge temporarily blocks Texas law restricting kids from app stores. Austin, 23 dez. 2025. Disponível em: https://www.texastribune.org/2025/12/23/texas-app-store-child-ban-age-verification/. Acesso em: 25 maio 2026.

131 TEXAS POLICY RESEARCH. Federal Court Blocks Texas App Store Accountability Act. Austin, dez. 2025. Disponível em: https://www.texaspolicyresearch.com/federal-court-blocks-texas-app-store-accountability-act/. Acesso em: 25 maio 2026.

implementar restrições e proteções etárias, assegurar conformidade legal e adotar recursos de segurança adequados à faixa etária; e notificar a loja de alterações significativas no aplicativo.

Como o sinal é obtido. A loja deve aferir a categoria etária dos usuários no momento da criação da conta mediante métodos comercialmente confiáveis (*reliable methods*). A lei não especifica os métodos de aferição admitidos.

Como o sinal é transmitido ao provedor de aplicações. A loja deve fornecer ao desenvolvedor, mediante solicitação, os dados de categoria etária do usuário e o status do consentimento parental para crianças e adolescentes, por método comercialmente disponível.

Gratuidade. A lei não trata do tema.

Obrigações e requisitos adicionais. O uso dos dados pelo desenvolvedor é restrito às finalidades previstas em lei, vedado o compartilhamento com terceiros. A lei prevê enforcement pelo Procurador-Geral do estado mediante ação civil. A vigência está fixada para 1º de julho de 2026.

Status. Sancionada em 30 de junho de 2025, com vigência fixada para 1º de julho de 2026. Não há registro de ação judicial em curso contestando a lei até maio de 2026. O Procurador-Geral do estado é o agente de enforcement, com previsão de multa civil de até USD 10.000 por violação e período de cura de 45 dias para infrações iniciais[132].

III.5 Singapura, Code of Practice for Online Safety for App Distribution Services (IMDA, Broadcasting Act 1994, seção 45L; vigência: 31 de março de 2025; obrigações de age assurance: 1º de abril de 2026)

Conceito de sinal de idade. O Código não define um conceito equivalente a *signal* ou *sinal de idade*, nem prevê uma API de transmissão de faixa etária da loja ao desenvolvedor. O instrumento opera com o conceito de *age assurance*, descrito nos parágrafos 19 e 20 como sistemas e processos, incluídos verificação e estimativa de idade,

[132] DIGITAL POLICY ALERT. Protection of Children on Applications Act (Act No. 481 / HB 570) was signed by Governor of Louisiana. Genebra, 30 jun. 2025. Disponível em: https://digitalpolicyalert.org/event/32433-protection-of-children-on-applications-act-act-no-481-hb-570-was-signed-by-governor-of-louisiana. Acesso em: 25 maio 2026. Ver também: FASTDEMOCRACY. HB 570 — Louisiana 2025. Disponível em: https://fastdemocracy.com/bill-search/la/2025/bills/LAB00024814/. Acesso em: 25 maio 2026.

pelos quais a idade ou faixa etária do usuário de uma conta no serviço pode ser estabelecida com razoável precisão.

Atores relevantes. Os agentes obrigados são as lojas de aplicativos (App Distribution Services) designadas pela IMDA nos termos da seção 45K(1) do Broadcasting Act 1994. Por meio de ato de designação publicado conjuntamente com o Código em 15 de janeiro de 2025, a IMDA designou cinco serviços com significativo alcance ou impacto em Singapura: Apple App Store, Google Play Store, Huawei AppGallery, Microsoft Store e Samsung Galaxy Store[133].Os *app providers*, desenvolvedores que distribuem aplicativos por meio das lojas designadas, não são diretamente obrigados pelo Código a receber ou processar informações de faixa etária. Crianças (*children*), definidas no Código como indivíduos abaixo de 18 anos, e seus pais ou responsáveis figuram como destinatários das medidas de proteção.

Obrigações dos atores relevantes. As lojas designadas devem, nos termos dos parágrafos 19 a 23 do Código: implementar sistemas e processos de *age assurance* que permitam estabelecer a idade ou faixa etária do usuário com razoável precisão, em conformidade com a PDPA e as diretrizes da PDPC; disponibilizar contas diferenciadas para crianças com configurações mais restritivas por padrão, salvo se o serviço restringir integralmente o acesso de crianças; fornecer a crianças e seus responsáveis informações e ferramentas para gerenciar a segurança online, incluindo controles parentais e restrições de busca; e restringir o acesso ou o download de aplicativos inadequados conforme a faixa etária aferida do usuário. Os *app providers* não são diretamente obrigados pelo Código a receber ou processar informações de faixa etária, mas estão sujeitos às diretrizes de conteúdo das lojas designadas e às restrições de acesso por faixa etária que estas imponham.

Como o sinal é obtido. O Código não especifica o método de aferição de idade a ser utilizado. O parágrafo 20 exige que as lojas implementem sistemas e processos de *age assurance* em conformidade com a Personal Data Protection Act 2012 e as diretrizes da PDPC, com ênfase em minimização de dados.

Como o sinal é transmitido ao provedor de aplicações. O Código não prevê obrigação de transmissão de informação de faixa etária da loja ao desenvolvedor. A

[133] INFOCOMM MEDIA DEVELOPMENT AUTHORITY. List of Designated App Distribution Services. Singapura, 15 jan. 2025. Disponível em: https://www.imda.gov.sg/-/media/imda/files/regulations-and-licensing/regulations/codes-of-practice/code-of-practice-app-distribution-services/list-of-designated-app-distribution-services.pdf. Acesso em: 25 maio 2026.

proteção opera no nível da própria loja, que restringe o acesso ou o download de aplicativos inadequados conforme a faixa etária aferida do usuário.

Gratuidade. O Código não trata do tema.

Obrigações e requisitos adicionais. O parágrafo 20 exige que a *age assurance* seja implementada em conformidade com a PDPA e as diretrizes da PDPC, com ênfase em minimização de dados. As lojas devem submeter à IMDA relatórios anuais de segurança online a serem publicados no sítio da IMDA, contendo informações e métricas sobre as medidas adotadas e sua efetividade (parágrafo 28). O descumprimento pode implicar determinação da IMDA de desabilitação do acesso de usuários de Singapura a conteúdo nos termos da seção 45K(1) do Broadcasting Act 1994.

Status. Instrumento infralegal em vigor desde 31 de março de 2025, com obrigações de age assurance vigentes desde 1º de abril de 2026.Não há registro de contestação judicial[134].

III. Ferramentas disponibilizadas pelas empresas

III.1 Estados Unidos - Texas, Utah e Louisiana

Em 8 de outubro de 2025, a Apple publicou comunicado na Apple Developer News anunciando que, com a entrada em vigor do SB 2420 no Texas a partir de 1º de janeiro de 2026, usuários no estado que criassem uma nova Apple Account seriam obrigados a confirmar se têm 18 anos ou mais. Todas as novas contas de usuários crianças e adolescentes de 18 anos passariam a ser vinculadas a um grupo de Family Sharing, exigindo consentimento de pais ou responsáveis para todos os downloads, compras na App Store e transações via In-App Purchase. Para atender a essas obrigações, a Apple anunciou a disponibilização da Declared Age Range API para implementação imediata, com previsão de atualização para fornecer as categorias etárias exigidas para novos usuários no Texas[135].

134 INFOCOMM MEDIA DEVELOPMENT AUTHORITY. New Online Safety Code of Practice for App Distribution Services Enhances Protection for Singapore Users. Singapura, 15 jan. 2025. Disponível em: https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2025/online-safety-code-of-practice-for-app-distribution-services. Acesso em: 25 maio 2026. Ver também: ALLEN & GLEDHILL. New Code of Practice for Online Safety for App Distribution Services effective 31 March 2025. Singapura, mar. 2025. Disponível em: https://www.allenandgledhill.com/publication/articles/30237/new-code-of-practice-for-online-safety-for-app-distribution-services-effective-31-mar2025. Acesso em: 25 maio 2026.

135 APPLE INC. *New requirements for apps available in Texas*. Apple Developer News, 8 out. 2025. Disponível em: https://developer.apple.com/news/?id=btkirlj8. Acesso em: 25 maio 2026.

Em 4 de novembro de 2025, a Apple publicou comunicado técnico detalhando o conjunto completo de ferramentas disponíveis em versão beta no iOS 26.2 e iPadOS 26.2[136]:

- A *Declared Age Range API* permite ao desenvolvedor obter a categoria etária do usuário nas faixas definidas pelo SB 2420 (abaixo de 13, 13–15, 16–17 e acima de 18). A API retorna ainda um sinal sobre o método de aferição de idade utilizado pela Apple para aquela conta, como cartão de crédito ou documento de identidade governamental, e uma indicação sobre se é necessário consentimento parental em razão de alteração significativa no aplicativo. As categorias etárias de usuários com novas Apple Accounts no Texas a partir de 1º de janeiro de 2026 são compartilhadas com o aplicativo do desenvolvedor quando solicitadas.

- A *Significant Change API*, integrada ao framework PermissionKit, é chamada pelo desenvolvedor quando este determina ter realizado uma alteração significativa no aplicativo. Ao ser invocada, a API exibe ao usuário com menos de 18 anos um diálogo do sistema para solicitar o consentimento do pai ou responsável, podendo o desenvolvedor restringir o acesso ao aplicativo ou à nova funcionalidade até que o consentimento seja obtido. O SB 2420 considera alteração no *age rating* do aplicativo uma alteração significativa; a Apple disponibilizou nova propriedade em StoreKit para que o desenvolvedor verifique automaticamente quando o *age rating* do aplicativo foi alterado no dispositivo do usuário e acione a Significant Change API.

- As *App Store Server Notifications* permitem ao desenvolvedor receber notificações do servidor da App Store sobre a revogação de consentimento parental para seu aplicativo em dispositivo de pessoas com menos de 18 anos.

Após a liminar federal suspender a lei do Texas, a Apple publicou novo comunicado informando que as ferramentas permaneceriam disponíveis para testes em sandbox e seriam utilizadas para cumprimento das leis de Utah e Louisiana em 2026[137].

Em 24 de fevereiro de 2026, a Apple publicou comunicado expandindo a cobertura para Utah (a partir de 6 de maio de 2026) e Louisiana (a partir de 1º de julho de 2026), além de Brasil, Austrália e Singapura. O comunicado informou que novos sinais passariam a estar disponíveis via Declared Age Range API, incluindo indicação sobre se os requisitos regulatórios da jurisdição aplicável incidem sobre o usuário e se é necessário obter

136 APPLE INC. Next steps for apps distributed in Texas. Apple Developer News, 4 nov. 2025. Disponível em: https://developer.apple.com/news/?id=2ezb6jhj. Acesso em: 25 maio 2026.

137 APPLE INC. *Update on age requirements for apps distributed in Texas*. Apple Developer News. Disponível em: https://developer.apple.com/news/?id=8jzbigf4. Acesso em: 25 maio 2026.

autorização de pai ou responsável para atualizações significativas do aplicativo no caso de crianças e adolescentes. Para Utah e Louisiana, as categorias etárias são compartilhadas com o aplicativo do desenvolvedor quando solicitadas via API para usuários com novas contas a partir das respectivas datas de vigência[138].

O Google publicou comunicado na central de suporte para desenvolvedores do Google Play descrevendo as três ferramentas a serem disponibilizadas[139]:

- A *Play Age Signals API* (beta) permite ao aplicativo receber, em tempo de execução via chamada de API no lado do cliente, o status de verificação ou supervisão de idade do usuário, a faixa etária e outros sinais aplicáveis. A API retorna dados apenas para usuários em regiões onde o Google Play é legalmente obrigado a fornecê-los; as faixas etárias retornadas correspondem àquelas definidas pela legislação da jurisdição aplicável. A API não requer que o desenvolvedor a integre obrigatoriamente, o Google a disponibiliza como ferramenta de conformidade, cabendo ao desenvolvedor determinar suas próprias obrigações legais.

- As *Play Console features* permitem ao desenvolvedor notificar o Google Play de uma alteração significativa no aplicativo sem necessidade de publicar nova versão, e acessar relatório no Play Console exibindo quando um pai ou responsável revogou a aprovação de seu aplicativo. Para aplicativos que utilizam o Play Billing Library, é possível atribuir classificações etárias aos SKUs de compras.

- As *trust & safety requirements* estabelecem os requisitos de uso dos dados recebidos via API: o desenvolvedor deve cumprir as políticas do Google Play sobre como os dados da API devem ser tratados.

O comunicado informou ainda que, em razão da liminar federal, a Play Age Signals API não retornaria respostas para usuários no Texas até nova comunicação, e que o Google continuaria desenvolvendo soluções para Utah (7 de maio de 2026) e Louisiana (1º de julho de 2026).

III.2 Singapura

[138] APPLE INC. Age requirements for apps distributed in Brazil, Australia, Singapore, Utah, and Louisiana. Apple Developer News, 24 fev. 2026. Disponível em: https://developer.apple.com/news/?id=f5zj08ey. Acesso em: 25 maio 2026.

[139] GOOGLE. Changes to Google Play for upcoming app store bills for users in applicable US states. Google Play Console Help. Disponível em: https://support.google.com/googleplay/android-developer/answer/16569691. Acesso em: 25 maio 2026.

O comunicado de 24 de fevereiro de 2026 informou que a partir daquela data a Apple passaria a bloquear automaticamente o download de aplicativos classificados como 18+ para usuários em Singapura, Brasil e Austrália, salvo confirmação de maioridade por métodos razoáveis, realizada automaticamente pela App Store. A Declared Age Range API foi disponibilizada como ferramenta complementar para que desenvolvedores obtenham sinal sobre a faixa etária do usuário sem acesso à data de nascimento exata.

A Samsung publicou comunicado no Samsung Newsroom Singapore em 30 de março de 2026 informando que a Galaxy Store em Singapura implementaria medidas de *age assurance* a partir de 27 de março de 2026, em conformidade com as diretrizes da IMDA[140]. A empresa publicou também documento de suporte ao usuário detalhando o funcionamento da medida: todos os usuários que acessem a Galaxy Store em Singapura devem completar a etapa de *age assurance*. O método adotado é a vinculação de cartão de crédito à conta Samsung. Usuários com cartão já cadastrado não precisam reinserir os dados e podem desvinculá-lo após a conclusão do processo. Usuários que optarem por não concluir a verificação de maioridade podem continuar utilizando a Galaxy Store, mas sem acesso a aplicativos e conteúdos classificados como 18+[141].

A Microsoft publicou comunicado no Microsoft Source Asia em 17 de março de 2026 descrevendo as medidas implementadas no Microsoft Store e nas plataformas Xbox em Singapura. Para download e acesso a aplicativos e jogos classificados como 18+, os usuários serão solicitados a confirmar a maioridade por uma das seguintes opções: verificação via Singpass; estimativa de idade por análise facial de selfie; ou envio de documento oficial de identidade governamental, como documento de identidade nacional, carta de condução, passaporte ou autorização de residência. O comunicado indicou que a verificação é uma etapa única (*one-time*) e que as atualizações começariam a ser implementadas nas semanas seguintes[142].

O Google não publicou comunicado de imprensa específico para Singapura. As informações sobre a implementação constam da documentação técnica da Play Age Signals API na central de desenvolvedores Android.

---

140 SAMSUNG ELECTRONICS SINGAPORE. *Building a Trusted Galaxy Experience for Singapore*. Samsung Newsroom Singapore, 30 mar. 2026. Disponível em: https://news.samsung.com/sg/building-a-trusted-galaxy-experience-for-singapore. Acesso em: 25 maio 2026.

141 SAMSUNG ELECTRONICS SINGAPORE. FAQs for Galaxy Store Singapore Age Assurance. Samsung Support Singapore, 18 mar. 2026. Disponível em: https://www.samsung.com/sg/support/apps-services/sg-age-assurance/. Acesso em: 25 maio 2026.

142 MICROSOFT CORPORATION. *Microsoft to introduce age assurance measures in Singapore*. Microsoft Source Asia, 17 mar. 2026. Disponível em: https://news.microsoft.com/source/asia/2026/03/17/microsoft-to-introduce-age-assurance-measures-in-singapore/. Acesso em: 25 maio 2026.

Não foi identificado comunicado oficial da Huawei sobre suas medidas de *age assurance* em Singapura.

3.6. Face Estimation: Ponderações sobre a Tecnologia e Considerações sobre Uso de Dados Biométricos

O avanço de mecanismos de aferição de idade no ambiente digital tem ampliado o debate sobre o uso de tecnologias voltadas à estimativa da idade dos usuários, e seus potenciais impactos sobre a privacidade e proteção de dados. Primeiramente, cumpre destacar que o conceito de "aferição de idade" se refere aos procedimentos destinados a verificar, estimar ou inferir, direta ou indiretamente, a idade ou a faixa etária de um usuário, por meio de um conjunto de métodos, tecnologias e processos[143]. A própria ideia de "aferição" está associada aos variados níveis de confiança e precisão que diferentes soluções podem oferecer para determinar se um indivíduo possui determinada idade, pertence a certa faixa etária ou está acima ou abaixo de um limite mínimo previamente estabelecido[144].

Dentro desse guarda-chuva conceitual, é importante diferenciar mecanismos de "verificação de idade" e "estimativa de idade", que operam sob lógicas técnicas distintas. A verificação de idade busca comprovar a exatidão da idade declarada ou a faixa etária do usuário, normalmente mediante documentos oficiais, autenticação, bases cadastrais, entre outros. Já a "estimativa de idade" funciona de maneira diversa: trata-se de um processo de inferência probabilística destinado a estimar a provável faixa etária de um indivíduo a partir de determinados atributos, sem a finalidade de identificá-lo. Em vez de estabelecer quem é o usuário, o objetivo é apenas avaliar se ele aparenta estar acima, abaixo ou dentro de determinada faixa etária[145]. Essa distinção é central para evitar que diferentes tecnologias de aferição etária sejam tratadas indistintamente, ignorando diferenças substanciais de funcionamento técnico, finalidade e impacto regulatório.

Nesse cenário, as tecnologias de estimativa de idade passaram a ocupar posição central nas discussões regulatórias relacionadas à proteção de crianças e adolescentes no ambiente digital, especialmente diante da crescente busca por mecanismos proporcionais, escaláveis e menos intrusivos. O tema ganhou ainda mais tração diante do avanço das

[143] Art. 2º, inciso IV, Decreto nº 12.880/2026

[144] CENELEC. CWA 18016:2023 — Age-appropriate digital services framework. Brussels: European Committee for Electrotechnical Standardization, 2023. Disponível em: https://www.cencenelec.eu/media/CEN-CENELEC/CWAs/ICT/cwa18016_2023.pdf. Acesso em: 01 jun. 2026.

[145] FUTURE OF PRIVACY FORUM (FPF). Unpacking Age Assurance: Technologies and Tradeoffs. Washington, DC: Future of Privacy Forum, 2026. Disponível em: https://fpf.org/wp-content/uploads/2026/02/FPF-Age-Assurance-v2.0.pdf. Acesso em: 01 jun. 2026.

discussões internacionais sobre aferição de idade e da consolidação de normas específicas voltadas à proteção de crianças e adolescentes em ambientes digitais. O Comitê Europeu de Proteção de Dados (EDPB), por exemplo, passou a distinguir expressamente modelos de autodeclaração, verificação de idade e estimativa etária, justamente para evidenciar que diferentes mecanismos produzem diferentes níveis de intrusão, riscos e impactos sobre direitos fundamentais[146].

No caso específico da estimativa facial de idade, as soluções operam por meio da detecção da presença de uma face e da conversão de determinados elementos faciais em padrões matemáticos analisados por modelos estatísticos treinados para produzir inferências probabilísticas sobre idade. O tratamento é direcionado exclusivamente à caracterização facial necessária para gerar uma estimativa etária, sem depender de autenticação documental, comparação com bases biométricas ou criação de perfis individualizados[147]. Em outras palavras, diferentemente de modelos baseados em reconhecimento facial tradicional, a estimativa de idade facial não tem como finalidade identificar civilmente o usuário, autenticar sua identidade ou vinculá-lo a um perfil persistente. Seu objetivo consiste exclusivamente em inferir uma faixa etária provável a partir da análise de características faciais por modelos estatísticos e sistemas de inteligência artificial.

Apesar disso, ainda é comum que as soluções de estimativa de idade facial sejam interpretadas como modalidades de reconhecimento facial. Essa aproximação conceitual, contudo, exige cautela. A discussão transcende uma questão meramente terminológica e demanda uma análise mais aprofundada acerca das diferenças técnicas e funcionais existentes entre sistemas voltados à identificação de indivíduos e modelos destinados apenas à inferência de atributos etários.

A preocupação com tecnologias de reconhecimento facial não é infundada. Autoridades regulatórias, organizações da sociedade civil e especialistas em proteção de dados têm alertado reiteradamente para os riscos associados à utilização indiscriminada do reconhecimento facial em contextos de aferição etária. Entre as principais preocupações estão os riscos de vigilância massiva, reutilização indevida de dados biométricos, compartilhamento excessivo de informações, perfilamento comportamental, opacidade algorítmica, vieses discriminatórios, incidentes de segurança e criação de

[146] EUROPEAN DATA PROTECTION BOARD (EDPB). Statement 1/2025 on Age Assurance. Brussels: EDPB, 2025. Disponível em: https://www.edpb.europa.eu/system/files/2025-04/edpb_statement_20250211ageassurance_v1-2_en.pdf. Acesso em: 01 jun. 2026.

[147] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Face Analysis Technology Evaluation: Age Estimation and Verification (FATE AEV). Gaithersburg, MD: NIST, 2024. Disponível em: https://pages.nist.gov/frvt/reports/aev/fate_aev_report.pdf. Acesso em: 01 jun. 2026.

mecanismos persistentes de rastreamento de usuários. Em especial, chama atenção o risco de que políticas legítimas de proteção de crianças e adolescentes acabem, na prática, fomentando a consolidação de infraestruturas permanentes de identificação biométrica no ambiente digital.

Nesse contexto, o principal ponto de atenção reside justamente na desproporção potencial entre finalidade e meio empregado. Em muitos casos, a finalidade regulatória consiste apenas em verificar se determinado usuário está acima ou abaixo de certo limite etário. Para atingir esse objetivo, nem sempre é necessário coletar documentos oficiais, dados cadastrais extensivos, autenticação civil persistente ou biometria facial identificadora. A adoção indiscriminada de mecanismos tradicionais de reconhecimento facial para fins de aferição etária pode transformar uma política de proteção infantojuvenil em uma arquitetura permanente de vigilância biométrica, ampliando significativamente os riscos aos direitos fundamentais dos usuários.

Sob essa perspectiva, torna-se essencial diferenciar tecnologias de reconhecimento facial de mecanismos de estimativa etária estruturados exclusivamente para inferência contextual de idade. Embora ambas possam utilizar imagens faciais como insumo técnico, tratam-se de soluções funcionalmente distintas, com objetivos, arquiteturas e impactos regulatórios diversos. A distinção central reside justamente no funcionamento técnico das soluções e, consequentemente, na finalidade do tratamento de dados.

Em sistemas tradicionais de reconhecimento facial, o objetivo é identificar, autenticar ou individualizar uma pessoa natural, seja por meio de verificação 1:1 (confirmar se alguém é quem afirma ser) ou identificação 1:N (comparar uma face contra bases biométricas amplas)[148]. Já nos sistemas de estimativa de idade facial, a finalidade é distinta: busca-se exclusivamente estimar a idade aproximada do usuário a partir de padrões faciais, sem determinar sua identidade civil ou estabelecer mecanismos persistentes de rastreamento individual.

Nesses modelos, a imagem facial pode operar apenas como insumo transitório para geração de uma inferência probabilística limitada ao atributo etário necessário, sem autenticação civil, interoperabilidade entre bases ou retenção permanente de templates biométricos. Assim, a estimativa etária facial pode representar alternativa significativamente menos intrusiva em comparação a mecanismos tradicionais de reconhecimento facial ou verificação documental extensiva. Esses aspectos técnicos dialogam diretamente com a própria recomendação da ANPD, no sentido de que as

[148]EUROPEAN DATA PROTECTION BOARD (EDPB). Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement. Brussels: EDPB, 2023. Disponível em: https://www.edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf. Acesso em: 01 jun. 2026.

soluções de aferição sejam estruturadas para tratar apenas o “dado ou atributo etário necessário”, com limitação de coleta, retenção e uso compatíveis com a finalidade da aferição. A Agência também ressalta que mecanismos de aferição etária não devem criar meios adicionais para identificação, localização, perfilamento ou rastreamento dos usuários, reforçando a necessidade de estruturas compatíveis com os princípios da necessidade, proporcionalidade e minimização de dados[149].

Essa diferenciação técnica possui profunda relevância jurídica e dialoga diretamente com os princípios, bases legais e critérios de tratamento de dados pessoais previstos na LGPD. Nem toda tecnologia que utiliza imagem facial opera com finalidade identificadora. Para que um tratamento de dados biométricos seja caracterizado como um tratamento de dados pessoais sensíveis, não basta que os dados decorram de características físicas de um indivíduo; é necessário que seja empregado em uma atividade de tratamento voltada à identificação única ou individualização da pessoa natural. Em soluções de estimativa etária que operam de forma contextual, sem retenção de imagens, sem criação de templates biométricos persistentes e sem interoperabilidade entre serviços, os riscos tradicionais de vigilância contínua ou rastreamento são drasticamente reduzidos. Assim, questiona-se a possível interpretação de equiparar indistintamente toda análise facial como tratamento de dados pessoais sensíveis, ignorando as especificidades e arquiteturas das tecnologias utilizadas.

Naturalmente, a ausência de identificação civil não afasta a necessidade de estruturas adequadas de governança. A credibilidade e a legitimidade dessas soluções dependem da adoção de salvaguardas robustas e de mecanismos efetivos de mitigação de riscos. Questões relacionadas à acurácia dos modelos, potenciais vieses discriminatórios, transparência, segurança da informação e proporcionalidade do tratamento permanecem centrais nesse debate. Nesse contexto, tornam-se especialmente relevantes medidas como auditorias independentes, testes contínuos de precisão, sistemas de detecção de fraude, ferramentas anti-spoofing e buffers de segurança, capazes de reduzir riscos operacionais e evitar que a estimativa etária seja automaticamente equiparada, de forma simplificada e contraproducente, ao reconhecimento biométrico tradicional.

Uma interpretação excessivamente abrangente dessas tecnologias pode, inclusive, desincentivar o desenvolvimento e a adoção de soluções menos invasivas voltadas à proteção de crianças e adolescentes no ambiente digital. Em determinados contextos, mecanismos de estimativa etária podem representar alternativa mais proporcional e

[149] AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Mecanismos confiáveis de aferição de idade: orientações preliminares. Brasília, DF: ANPD, 2026. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/eca-digital/mecanismos-confiaveis-de-afericao-de-idade-orientacoes-preliminares.pdf. Acesso em: 01 jun. 2026.

menos intrusiva à privacidade do que modelos baseados na coleta massiva de documentos oficiais, integração com bases governamentais ou autenticação civil persistente dos usuários. Entre essas alternativas, destacam-se modelos baseados em credenciais verificáveis, tokens criptográficos e arquiteturas de prova de conhecimento zero[150], capazes de confirmar apenas o atributo etário necessário sem revelar identidade civil, histórico de navegação ou outros dados excessivos.

Portanto, o debate regulatório deve focar em uma análise contextual, funcional e baseada em risco, reconhecendo que as tecnologias em torno de age estimation não envolvem o tratamento de dados biométricos em si e podem ser mecanismos eficazes de se buscar a proteção de crianças e adolescentes no ambiente digital. A questão central deixa de ser simplesmente a existência de tratamento de dados biométricos em si e passa a envolver a verificação acerca da efetiva identificação do indivíduo e da eventual formação de mecanismos persistentes de individualização.

Nesse cenário, a estimativa etária facial desponta como ferramenta potencialmente relevante para políticas de proteção de crianças e adolescentes no ambiente digital, sobretudo quando estruturada em conformidade com os princípios da privacidade e proteção de dados. Portanto, evitar a transposição de problemáticas e preocupações legítimas envolvendo reconhecimento facial as discussões de age estimation mostra-se essencial para conciliar proteção infantojuvenil, inovação tecnológica e preservação de direitos fundamentais.

3.7. Reações à Implementação de Mecanismos de Aferição de Idade

Nas jurisdições que avançaram com obrigações concretas de aferição de idade, a implementação foi acompanhada por reações relevantes que revelam dimensões práticas do tema às quais o processo regulatório precisa estar atento. Essas reações não são, em sua maioria, contrárias ao objetivo de proteger crianças e adolescentes em ambientes digitais, mas dizem respeito à forma como os mecanismos de aferição são desenhados, implementados e operados. Conhecer esse repertório é insumo relevante para que o processo regulatório brasileiro possa antecipar tensões e calibrar suas escolhas com base em experiências concretas de outras jurisdições.

I. Evasão para ambientes não regulados

[150] O Ministério da Justiça e Segurança Pública (MJSP), por meio da Secretaria Nacional de Direitos Digitais (SEDIGI), publicou o relatório "Mecanismos de Aferição de Idade: análise das contribuições à consulta pública e subsídios para regulamentação da Lei nº 15.211/2025", que sistematizou as 70 contribuições recebidas em consulta pública realizada na plataforma Participa + Brasil, com o objetivo de subsidiar a regulamentação da Lei nº 15.211/2025, que institui o ECA Digital, abordou o uso de tais mecanismos.

Um dos fenômenos mais documentados no período pós-implementação de obrigações de aferição de idade tem sido o deslocamento de parcela dos usuários para mecanismos de circunvenção, notadamente redes privadas virtuais (VPNs), e para plataformas que recusam conformidade. Do ponto de vista regulatório, esse deslocamento é relevante porque pode representar a transferência de usuários de ambientes onde alguma proteção existe para ambientes sem qualquer salvaguarda. Tal constatação reforça a necessidade de a ANPD estar ciente deste movimento e considera-lo na edição de seus normativos.

No Reino Unido, a OFCOM registrou, em seu relatório anual Online Nation 2025 e no Summary of the Technology Sector's Response to Our Rules, que a entrada em vigor das obrigações de aferição de idade altamente eficaz (highly effective age assurance — HEAA) para conteúdo adulto, em 25 de julho de 2025, nos termos do Online Safety Act 2023, foi imediatamente seguida de aumento expressivo no uso de VPNs.[151] Segundo os dados reportados pela autoridade reguladora britânica, o número de usuários diários de VPN mais que dobrou no período, saltando de aproximadamente 650 mil antes de 25 de julho para um pico de 1,4 milhão em meados de agosto de 2025, estabilizando-se posteriormente em torno de 900 mil em novembro, ainda significativamente acima do nível pré-lei. A própria Ofcom observou que seus dados não permitem distinguir com precisão se o aumento de uso de VPN está associado prioritariamente a adultos que buscam contornar os controles de privacidade ou a crianças e adolescentes que tentam acessar o conteúdo restrito.[152]

Nos documentos em questão, a OFCOM registrou queda de aproximadamente um terço no número de visitantes de sites de conteúdo adulto no Reino Unido após a entrada em vigor das aferições em 25 de julho de 2025, ressalvando estar ainda avaliando em que medida essa redução resultou em menor exposição de crianças ao conteúdo.[153] A Aylo, empresa controladora do Pornhub, ao anunciar o encerramento do acesso de novos usuários britânicos ao serviço, afirmou publicamente que, com base em seus próprios "dados e experiência", a aferição de idade teria "tornado a internet mais perigosa para

---

[151] OFCOM. Online Nation Report 2025. Londres: Ofcom, 10 dez. 2025. Disponível em: https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/online-research/online-nation/2025/online-nations-report-2025.pdf. Acesso em: 27 maio 2026. Ver também: OFCOM. Online Safety in 2025: A Summary of the Technology Sector's Response to Our Rules. Londres: Ofcom, 2025. Disponível em: https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/research-statistics-and-data/os-standards/online-safety-in-2025-summary-of-the-technology-sectors-response-to-our-rules.pdf. Acesso em: 27 maio 2026.

[152] Ibid. A ressalva da Ofcom sobre a impossibilidade de distinguir o perfil dos usuários de VPN foi amplamente citada pela imprensa britânica; ver: The Independent. UK porn site traffic plunges since age checks – but VPN use up. Dez. 2025. Disponível em: https://www.independent.co.uk/news/uk/home-news/uk-porn-site-traffic-down-age-checks-vpn-up-b2881714.html. Acesso em: 27 maio 2026.

[153] OFCOM. Online Nation Report 2025, op. cit.

crianças e adolescentes e adultos" e "colocado em risco a privacidade e os dados pessoais dos cidadãos britânicos", argumentando que usuários que recusaram a aferição teriam migrado para serviços não regulados sem qualquer salvaguarda.[154] A Ofcom avaliou, por sua vez, que os dez principais serviços de conteúdo adulto no país haviam se ajustado às regras.[155]

Em contraponto, pesquisa do Childnet, publicada em conjunto com os dados da Ofcom, identificou que, embora cerca de 24% dos jovens britânicos declarassem ter começado a usar VPNs nos três meses anteriores à pesquisa, esse número era consistente com o observado no ano anterior, sugerindo que o aumento de uso de VPN não decorreu de um salto repentino entre crianças e adolescentes, mas de um padrão comportamental mais difuso.[156]

Na Austrália, segundo dados citados pela Reuters, os downloads de VPNs praticamente triplicaram no período que antecedeu a vigência da Social Media Minimum Age Act.[157] Estudo acadêmico de pesquisadores das Universidades de Stanford, Georgia, Georgia State e da New York University (NYU Center for Social Media & Politics), submetido ao Journal of Law, Economics & Policy em dezembro de 2025, analisou os efeitos comportamentais das leis estaduais de aferição de idade nos Estados Unidos por meio de metodologia de controle sintético pré-registrada e análise multiverso sobre dados do Google Trends. Os resultados indicaram que, nos três meses seguintes à entrada em vigor das leis, as buscas pela principal plataforma conforme caíram 51%, enquanto as buscas pela principal plataforma não conforme cresceram 48,1% e as buscas por VPNs aumentaram 23,6%.[158]

Na França, a implementação da Lei nº 2024-449, de 21 de maio de 2024, que conferiu à autoridade reguladora de comunicação audiovisual e digital (Arcom) poderes para impor

---

[154] CNN. Pornhub shuts off access to new UK users, citing age verification constraints. Dez. 2025. Disponível em: https://edition.cnn.com/2026/02/02/uk/uk-pornography-restricted-access-intl Acesso em: 27 maio 2026.

[155] OFCOM. Online Nation Report 2025, op. cit.

[156] CHILDNET; NOMINET. New research from Childnet shows that the 'surge' in VPN use following the introduction of age verification in the summer is not attributable to children. Londres: Childnet / UK Safer Internet Centre, 1 dez. 2025. Pesquisa conduzida com 2.018 crianças de 8 a 17 anos no Reino Unido, amostra representativa nacionalmente. Relatório completo disponível em: https://www.childnet.com/wp-content/uploads/2025/12/Young-peoples-use-of-VPNs.pdf. Acesso em: 27 maio 2026.

[157] REUTERS. Australians reach for VPNs, find porn sites blocked as online age restrictions take effect. Reuters, Sydney, 9 mar. 2026. Disponível em: https://www.reuters.com/world/asia-pacific/vpns-up-porn-websites-down-australia-brings-new-online-age-restrictions-2026-03-09/. Acesso em: 29 maio 2026.26.

[158] LANG, David; LISTYG, Benjamin; ROSS, Brennah V.; MUSQUERA, Anna V.; SANDERSON, Zeve. Age Verification and Public Adaptation: A Pre-Registered Synthetic Control Multiverse. JLEA Resubmission, dez. 2025. Pesquisadores vinculados ao Polarization and Social Change Lab (Stanford University), Department of Psychology (University of Georgia e Georgia State University) e Center for Social Media & Politics / Center on Technology Policy (New York University). Disponível em: https://osf.io/vp9z6/.

sanções e ordenar o bloqueio de sites pornográficos que não implementassem aferição de idade, registrou reação análoga: a Aylo optou por suspender o acesso ao serviço no país a partir de abril de 2025, em vez de conformar com as exigências, afirmando que havia tentado, por anos, "trabalhar com Paris para encontrar uma forma de verificar a idade dos usuários sem expor os dados de milhões de franceses a violações de privacidade e ataques".[159] A secretária de Estado digital da França, Clara Chappaz, respondeu publicamente, afirmando que se a empresa "preferia deixar a França a aplicar a lei, estava livre para fazê-lo".[160]

II. Preocupações com privacidade e manifestações cívicas

A exigência de que usuários se identifiquem para acessar determinadas plataformas ou conteúdos gerou, em diversas jurisdições, debate público sobre as implicações para a privacidade e para o exercício anônimo da expressão e do acesso à informação online.

No Reino Unido, esse debate ganhou expressão cívica direta e de grande escala. A petição ao Parlamento britânico solicitando a revogação do Online Safety Act, disponível no portal oficial petition.parliament.uk, atingiu 550.136 assinaturas, superando o limiar de 100.000 assinaturas que obriga o Comitê de Petições a considerar o tema para debate parlamentar.[161] O debate foi realizado na Câmara dos Comuns em 15 de dezembro de 2025, tendo o deputado responsável pela introdução observado que as preocupações dos signatários envolviam "privacidade, segurança de dados e liberdade de expressão", ao mesmo tempo em que reconheceu os dados da Comissária da Infância britânica indicando que 70% das crianças relataram ter visto pornografia online.O governo britânico respondeu formalmente à petição afirmando que não havia planos de revogar a lei e que continuaria trabalhando com a Ofcom para sua implementação.[162]

A pesquisa do Ipsos, conduzida com amostra representativa de 2.196 adultos britânicos entre 1 e 5 de agosto de 2025, capturou uma assimetria significativa na percepção pública: 69% dos respondentes declararam apoiar as aferições de idade para

[159]REUTERS / Yahoo Finance. Pornhub exits France, its second-biggest market, over age verification law. Abr. 2025. Disponível em: https://www.yahoo.com/news/pornhub-exits-france-over-age-115558131.html. Acesso em: 27 maio 2026. Ver também: BETTER INTERNET FOR KIDS / Comissão Europeia. Law No 2024-449 of May 21 2024 aimed at securing and regulating the digital space. Disponível em: https://better-internet-for-kids.europa.eu/en/rules-guidelines/law-no-2024-449-may-21-2024-aimed-securing-and-regulating-digital-space. Acesso em: 27 maio 2026.

[160]Yahoo News. Porn sites block access in protest against new French restrictions. Abr. 2025. Disponível em: https://www.yahoo.com/news/porn-sites-block-access-protest-171229283.html. Acesso em: 27 maio 2026. Declaração de Clara Chappaz, secretária de Estado digital da França.

[161]UK PARLIAMENT. Petition: Repeal the Online Safety Act (nº 722903). Disponível em: https://petition.parliament.uk/petitions/722903. Acesso em: 27 maio 2026.

[162]TECHRADAR. “No plans to repeal the Online Safety Act” – UK government responds to age verification backlash. TechRadar, 1 ago. 2025. Disponível em: TechRadar. Acesso em: 29 maio 2026.

acesso a plataformas que possam hospedar conteúdo prejudicial, mas apenas 48% afirmaram ser provável que submetessem prova de identidade para acessar um site, e apenas 14% afirmaram estar dispostos a fazê-lo especificamente para sites de conteúdo pornográfico.[163] O Ipsos descreveu esse resultado como "um paradoxo significativo na opinião pública": há desejo claro e amplo de proteger crianças online, refletido no apoio à aferição de idade, mas isso é acompanhado de "ceticismo arraigado sobre se a lei pode cumprir suas promessas", com preocupações sobre violações de dados e potencial de censura destacadas pelos respondentes.[164]

O estudo internacional da PRophet/Stagwell, publicado em outubro de 2025 e abrangendo múltiplas jurisdições, identificou que, no Reino Unido, 69% das publicações online sobre aferição de idade tinham tom negativo, o índice mais alto dentre todos os países analisados, com usuários descrevendo frequentemente as medidas como "orwellianas" ou "distópicas", questionando os motivos por trás das iniciativas governamentais.[165]

Nos Estados Unidos, a Age Verification Providers Association (AVPA) e organizações de direitos digitais têm documentado, de perspectivas distintas, os efeitos práticos das exigências de aferição sobre o comportamento dos usuários e sobre o acesso a conteúdo legalmente protegido, em contexto no qual a metade dos estados norte-americanos havia adotado, até o final de 2025, alguma forma de exigência de aferição de idade para conteúdo adulto ou redes sociais.[166]

Na CNIL, autoridade de proteção de dados francesa, um relatório sobre sistemas de aferição de idade online concluiu que os sistemas então existentes eram "contornáveis e intrusivos" e conclamou a implementação de modelos "mais respeitosos da privacidade".[167]

---

[163] IPSOS. Britons back Online Safety Act's age checks, but are sceptical of effectiveness and unwilling to share ID. 27 ago. 2025. Disponível em: https://www.ipsos.com/en-uk/britons-back-online-safety-acts-age-checks-are-sceptical-effectiveness-and-unwilling-share-id. Acesso em: 27 maio 2026. Dados completos em: IPSOS. Online Safety Act — Tabelas de dados públicas. Ago. 2025. Disponível em: https://www.ipsos.com/sites/default/files/ct/news/documents/2025-08/Ipsos_Aug%202025_Online%20Safety%20Act_V1%20PUBLIC.pdf. Acesso em: 27 maio 2026.

[164] IPSOS, op. cit.

[165] PROPHET / STAGWELL. Freedom or Protection? New Study Reveals Global Skepticism Toward Online Age Verification. 8 out. 2025. Disponível em: https://finviz.com/news/186540/freedom-or-protection-new-study-by-prophet-a-stagwell-stgw-company-reveals-global-skepticism-toward-online-age-verification. Acesso em: 27 maio 2026.

[166] EFF. The Year States Chose Surveillance Over Safety: 2025 in Review. 9 jan. 2026. Disponível em: https://www.eff.org/deeplinks/2025/12/year-states-chose-surveillance-over-safety-2025-review. Acesso em: 27 maio 2026.

[167] CNIL — Commission Nationale de l'Informatique et des Libertés. Vérification de l'âge en ligne : trouver l'équilibre entre protection des mineurs et respect de la vie privée. Paris: CNIL, jul. 2022. Disponível em: https://www.cnil.fr/fr/verification-de-lage-en-ligne-trouver-lequilibre-entre-protection-des-mineurs-et-respect-de-la-vie. Acesso em: 27 maio 2026.

III. Possíveis impactos sobre grupos em situação de vulnerabilidade

Pesquisadores e organizações que trabalham com proteção de infância e adolescência em contextos de vulnerabilidade têm identificado que mecanismos de aferição de idade baseados em identificação civil ou em documentação padrão podem produzir efeitos diferenciados sobre determinados grupos de usuários.

A TechPolicy Press, em análise publicada em julho de 2024, documentou que adolescentes LGBTQ+, migrantes sem documentação padronizada e jovens em situações de vulnerabilidade familiar tendem a depender de forma mais intensa do anonimato online como condição de acesso a comunidades de apoio, informações de saúde e redes de suporte não disponíveis em seus contextos físicos imediatos.[168] Segundo essa análise, exigências de identificação civil para acesso a determinados serviços podem criar barreiras desproporcionais precisamente para os usuários cujo acesso depende mais da possibilidade de participação anônima ou pseudônima.

A Australian and New Zealand Children's Commissioners, Guardians and Advocates (ANZCCGA) manifestou preocupação com os potenciais impactos adversos da restrição ampla sobre "grupos já marginalizados, como crianças e jovens LGBTQIA+ e aqueles que vivem em áreas regionais e remotas, muitos dos quais dependem das redes sociais para apoio, conexão social e aprendizagem"[169]. Em contraponto, eSafety sinalizou, em sua página sobre restrições de idade para redes sociais, que segurança e privacidade devem ser tratadas de forma complementar, e que sua abordagem regulatória incentiva os serviços a incorporar a segurança do usuário desde a concepção, em conformidade com o Online Safety Act.[170]

Nesse sentido, o olhar atento da ANPD para o incentivo de tecnologias que sejam confiaveis em termos de aferição etária mas que o façam sem necessariamente coletar dados de identificação da usuário se mostra indispensável para o sucesso da implementação do ECA Digital e da garantia das proteções e direitos nele assegurados.

IV. Litigância nos Estados Unidos

[168] TECHPOLICY PRESS. Considering Age Verification and Impacts on LGBTQ+ Youth. 9 jul. 2024. Disponível em: https://www.techpolicy.press/age-verification-and-lgbtq-youth/. Acesso em: 27 maio 2026.

[169] AUSTRALIAN AND NEW ZEALAND CHILDREN'S COMMISSIONERS, GUARDIANS AND ADVOCATES (ANZCCGA). Top children's officials call for a rethink of social media ban. Disponível em: https://www.acyp.nsw.gov.au/info/media-releases/top-childrens-officials-call-for-a-rethink-of-social-media-ban. Acesso em: 27 maio 2026.

[170] eSAFETY COMMISSIONER. Social media age restrictions. Disponível em: https://www.esafety.gov.au/about-us/industry-regulation/social-media-age-restrictions. Acesso em: 27 maio 2026.

Nos Estados Unidos, a proliferação de leis estaduais de aferição de idade deu origem a um ciclo expressivo de contestações judiciais que têm moldado o ritmo e o escopo da implementação dessas obrigações.

A decisão mais relevante no período foi proferida pela Suprema Corte dos Estados Unidos no caso Free Speech Coalition v. Paxton, julgado em junho de 2025, no qual a Corte sustentou, por maioria, que os estados podem exigir aferição de idade para acesso a conteúdo considerado obsceno para crianças e adolescentes, rejeitando a impugnação com base na Primeira Emenda da Constituição.[171] A decisão foi descrita pela EFF como "um golpe direto aos direitos de liberdade de expressão dos adultos", na medida em que permitiria que estados introduzissem "onerosas regras de aferição de idade que bloqueiam adultos de acessar discurso lícito, cerceiam sua capacidade de permanecerem anônimos e colocam em risco sua segurança de dados e privacidade".[172]

Em paralelo, diversas leis estaduais específicas foram alvo de impugnações judiciais que resultaram em liminares de suspensão. O App Store Accountability Act do Texas (SB 2420) foi suspenso por tribunal federal em 23 de dezembro de 202, um dia antes de sua entrada em vigor , com o tribunal identificando probabilidade de violação da Primeira Emenda, por considerar a lei "excessivamente ampla e com disposições constitucionalmente vagas".[173] A Computer & Communications Industry Association (CCIA) ajuizou ação federal contra a lei equivalente do estado de Utah (App Store Accountability Act, SB 142/2025) em fevereiro de 2026; houve desistência voluntária da ação após o estado promover emendas que modificaram o mecanismo de enforcement da lei em março de 2026.[174] A lei da Califórnia Age-Appropriate Design Code Act (AB 2273) enfrenta contestação judicial desde 2022, com liminares que suspenderam sua aplicação integral com base em

[171] UNITED STATES SUPREME COURT. Free Speech Coalition, Inc., et al. v. Ken Paxton, Attorney General of Texas. No. 23-1122. Argued January 15, 2025 — Decided June 27, 2025. 606 U.S. 461 (2025). Opinião majoritária do Justice Thomas, acompanhado pelos Chief Justice Roberts e pelos Justices Alito, Gorsuch, Kavanaugh e Barrett (6-3). Dissidência da Justice Kagan, acompanhada pelas Justices Sotomayor e Jackson. Texto integral disponível em: https://www.supremecourt.gov/opinions/24pdf/23-1122_3e04.pdf. Acesso em: 27 maio 2026.

[172] EFF. The Supreme Court's Decision on Age Verification Tramples Free Speech and Undermines Privacy. Dez. 2025. Disponível em: https://www.eff.org/pages/supreme-courts-decision-age-verification-tramples-free-speech-and-undermines-privacy. Acesso em: 27 maio 2026.

[173] TEXAS TRIBUNE. Federal judge temporarily blocks Texas law restricting kids from app stores. 23 dez. 2025. Disponível em: https://www.texastribune.org/2025/12/23/texas-app-store-child-ban-age-verification/. Acesso em: 27 maio 2026.

[174] ALSTON & BIRD. Challenge to Utah's App Store Accountability Act Voluntarily Dismissed Following Statutory Amendments. Abr. 2026. Disponível em: https://www.alstonprivacy.com/challenge-to-utahs-app-store-accountability-act-voluntarily-dismissed-following-statutory-amendments/. Acesso em: 27 maio 2026. Ver também: CCIA. CCIA Challenges Unconstitutional App Store Law in Utah. 5 fev. 2026. Disponível em: https://ccianet.org/news/2026/02/ccia-challenges-unconstitutional-app-store-law-in-utah/. Acesso em: 27 maio 2026.

potencial conflito com a Primeira Emenda, permanecendo pendente de decisão definitiva no momento de elaboração deste Relatório.[175]

Essas contestações refletem tensões constitucionais específicas do sistema jurídico norte-americano, centradas na proteção da liberdade de expressão conferida pela Primeira Emenda, que não têm correspondência direta no ordenamento brasileiro. Ainda assim, a litigância americana é relevante como registro das categorias de argumentos que emergem quando regulações de aferição de idade são submetidas a escrutínio judicial, incluindo questões de proporcionalidade, vagueza normativa, impacto sobre expressão lícita e atribuição de responsabilidades entre diferentes camadas da cadeia digital.

V. Tensões entre segurança da informação e proteção de dados pessoais

A implementação de mecanismos de aferição de idade tem sido acompanhada de debate relevante sobre suas implicações para a segurança da informação e para a proteção de dados pessoais dos próprios usuários que se pretende proteger. Esse debate não questiona a legitimidade do objetivo regulatório, mas aponta para dimensões práticas da implementação que precisam ser cuidadosamente endereçadas para que os mecanismos adotados sejam, ao mesmo tempo, eficazes e compatíveis com os direitos fundamentais dos usuários.

O ponto central desse debate diz respeito principalmente às informações tratadas para fazer a aferição, que podem incluir identificadores fortes, como documentos de identidade, dados biométricos, registros governamentais ou combinações dessas categorias. O Center for Democracy and Technology (CDT) observou que propostas de segurança online frequentemente exigem ou incentivam o uso de mecanismos de aferição sem salvaguardas suficientes para governar o uso secundário, a retenção e o compartilhamento com terceiros dos dados coletados, abrindo caminho para o risco de vinculação da identidade do usuário à sua atividade online[176]. Não se trata de uma tensão intransponível, mas de uma variável que precisa ser antecipada e gerenciada, o volume e a sensibilidade dos dados tratados para fins de aferição não podem ser ignorados.

Incidentes concretos ocorridos em jurisdições que avançaram com obrigações de aferição ilustram esse risco. Em outubro de 2025, uma plataforma de comunicação registrou incidente de segurança que resultou no vazamento de aproximadamente 70.000

[175] Sobre a AB 2273 californiana, ver seção II.1 do Benchmarking Internacional (Parte II deste Relatório).

[176] CENTER FOR DEMOCRACY AND TECHNOLOGY (CDT). *Mitigating risk to rights with age verification: Privacy-preserving guardrails that should accompany deployments of age verification approaches*. Washington, D.C.: CDT, 10 out. 2025. Disponível em: https://cdt.org/insights/mitigating-risk-to-rights-with-age-verification-privacy-preserving-guardrails-that-should-accompany-deployments-of-age-verification-approaches/. Acesso em: 29 maio 2026.

imagens de documentos de identidade de usuários submetidos a processo de verificação etária[177]. Em 2024, um serviço de verificação de idade expôs credenciais administrativas internas por cerca de um ano, com potencial acesso não autorizado a documentos de usuários[178]. Esses casos não demonstram que a aferição de idade não deve ser realizada, mas evidenciam que sua realização enseja riscos que precisam ser considerados no regime regulatório.

Essa preocupação ganhou expressão institucional relevante em março de 2026, quando mais de 400 pesquisadores e acadêmicos de segurança e privacidade de mais de 30 países subscreveram carta aberta dirigida a governos e reguladores. Os signatários foram explícitos em compartilhar as preocupações com os efeitos negativos da exposição de crianças e adolescentes a conteúdos nocivos, mas alertaram que a implementação de sistemas de aferição de idade em escala sem consideração cuidadosa dos riscos tecnológicos e do impacto social poderia produzir consequências não intencionais relevantes, concluindo que a implantação de infraestruturas de aferição de identidade em larga escala sem compreensão adequada de seus efeitos sobre segurança, autonomia e liberdade dos usuários seria perigosa[179]. Estudo acadêmico ofereceu avaliação técnica estruturada das diferentes tecnologias de aferição disponíveis, concluindo que cada categoria apresenta combinações distintas de limitações em termos de precisão, disponibilidade, privacidade e resistência à circunvenção[180]. A conclusão dos autores não é de que a aferição seja inviável, mas de que a escolha do mecanismo mais adequado exige análise contextualizada e proporcional ao tipo de serviço e ao perfil de risco envolvido.

A experiência recente da União Europeia ilustra bem essa complexidade. Conforme registro acima, em abril de 2026, a Comissão Europeia lançou um aplicativo de verificação etária baseado em provas de conhecimento zero (zero-knowledge proofs), desenvolvido no contexto das medidas associadas ao Digital Services Act e concebido como precursor das

---

177 WEEK IN SECURITY. Discord says users' government IDs used for age checks stolen by hackers. 4 out. 2025. Disponível em: https://this.weekinsecurity.com/discord-says-users-government-ids-used-for-age-checks-stolen-by-hackers/. Acesso em: 29 maio 2026.

178 COX, Joseph. ID verification service for TikTok, Uber, X exposed driver licenses. *404 Media*, 26 jun. 2024. Disponível em: https://www.404media.co/id-verification-service-for-tiktok-uber-x-exposed-driver-licenses-au10tix/. Acesso em: 29 maio 2026.

179 CYBERNEWS. 400+ experts urge governments to rethink online age verification laws. 5 mar. 2026. Disponível em: https://cybernews.com/privacy/scientists-slam-brakes-age-verification-laws-teens/. Acesso em: 29 maio 2026. O texto integral da carta aberta encontra-se disponível em: https://chilleffects.au/open-letter/. Ver também: TECHDIRT. 438 experts said age verification is dangerous. Legislators are moving forward with it anyway. 14 abr. 2026. Disponível em: https://www.techdirt.com/2026/04/14/438-experts-said-age-verification-is-dangerous-legislators-are-moving-forward-with-it-anyway/. Acesso em: 29 maio 2026.

180 LUEKS, Wouter; DREYER, Stephan; FEDERRATH, Hannes; SIMON, Judith. Assessing Age Assurance Technologies. CISPA Helmholtz Center for Information Security; Leibniz Institute for Media Research | Hans-Bredow-Institut; Universität Hamburg. Versão de 26 mar. 2026. Disponível em: https://arxiv.org/pdf/2603.25695. Acesso em: 29 maio 2026.

carteiras digitais europeias previstas no eIDAS 2.0, com comprometimento expresso com os princípios de minimização de dados e privacidade por design[181]. A solução foi apresentada como uma tentativa de deslocar a responsabilidade pela coleta direta de dados pessoais das plataformas para uma infraestrutura pública. No entanto, horas após o lançamento público, facilitado pela disponibilização do código-fonte em repositório aberto, pesquisadores de segurança identificaram e demonstraram publicamente vulnerabilidades que permitiam contornar o sistema de autenticação em menos de dois minutos[182].

A análise técnica revelou fragilidades de implementação que os próprios pesquisadores descreveram como falhas de design fundamentais: o mecanismo de limitação de tentativas de PIN estava armazenado em arquivo editável pelo usuário; a autenticação biométrica era controlada por variável que podia ser desabilitada; e uma análise arquitetural anterior havia identificado que o componente emissor do sistema era incapaz de verificar se a validação documental havia de fato ocorrido no dispositivo do usuário[183]. A Comissão Europeia sinalizou que as vulnerabilidades seriam corrigidas, e o caso foi encerrado sem comprometimento de dados de usuários em larga escala[184]. Ainda assim, o episódio é pedagogicamente relevante: demonstra que mesmo soluções desenvolvidas sob forte compromisso regulatório com privacidade e proteção de dados permanecem sujeitas a desafios técnicos de implementação que somente uma auditoria independente prévia ao lançamento em larga escala poderia ter antecipado. Como observou a TechPolicy Press, a realidade da implementação é frequentemente mais complexa do que a narrativa oficial, e sistemas baseados em dispositivo apresentam vulnerabilidades específicas que precisam ser endereçadas com soluções técnicas distintas daquelas aplicáveis a sistemas baseados em servidor[185].

O balanço entre proteção de crianças e adolescentes, proteção de dados e segurança da informação não configura, portanto, uma escolha entre objetivos incompatíveis, mas um desafio de design regulatório que exige atenção simultânea a essas três dimensões. A New America Foundation, em análise sobre mecanismos de aferição de

181 EU PERSPECTIVES. Hackers shred EU's age app hours after launch. 18 abr. 2026. Disponível em: https://euperspectives.eu/2026/04/hackers-shred-eus-age-app-hours-after-launch/. Acesso em: 29 maio 2026

182 CYBERSECURITY NEWS. EU's New Age Verification App Can Be Hacked Within 2 Minutes, Researchers Claim. 17 abr. 2026. Disponível em: https://cybersecuritynews.com/eus-age-verification-app/amp/. Acesso em: 29 maio 2026.

183 CYBERSECURITY NEWS, op. cit.; PROTON. EU age verification app hacked in 2 minutes – now what? 20 abr. 2026. Disponível em: https://proton.me/blog/eu-age-verification-app-hacked. Acesso em: 29 maio 2026.

184 CYBERNEWS. New EU age verification app hacked in minutes. 21 abr. 2026. Disponível em: https://cybernews.com/security/eu-age-verification-app-hack/. Acesso em: 29 maio 2026.

185 TECHPOLICY PRESS. The EU's Age Verification Fix May Create More Problems Than it Solves. 22 abr. 2026. Disponível em: https://www.techpolicy.press/the-eus-age-verification-fix-creates-more-problems-than-it-solves/. Acesso em: 29 maio 2026.

idade com preservação de privacidade, observou que métodos mais rigorosos de aferição tendem a oferecer maior precisão, mas ao custo de exigir identificadores fortes como documentos governamentais ou dados biométricos, o que torna as escolhas de arquitetura e as salvaguardas associadas componentes centrais, e não periféricos, do modelo regulatório[186]. O artigo acadêmico publicado nos anais da ICISSP 2025 sobre a eficácia de métodos de aferição etária em redes sociais documentou lacunas nos níveis intermediários de garantia etária e concluiu que atualizações periódicas dos processos de aferição são essenciais para adaptação a novas ameaças e vulnerabilidades[187].

[186] NEW AMERICA. Exploring Privacy-Preserving Age Verification: A Close Look at Zero-Knowledge Proofs. 17 fev. 2026. Disponível em: https://www.newamerica.org/insights/exploring-privacy-preserving-age-verification/. Acesso em: 29 maio 2026.

[187] ELTAHER, Fatmaelzahraa; GAJULA, Rahul Krishna; MIRALLES-PECHUÁN, Luis; THORPE, Christina; MCKEEVER, Susan. The Digital Loophole: Evaluating the Effectiveness of Child Age Verification Methods on Social Media. In: International Conference on Information Systems Security and Privacy (ICISSP 2025), 11., 2025. Proceedings... Porto: SCITEPRESS, 2025. p. 213–222. DOI: 10.5220/0013248300003899. Disponível em: https://www.scitepress.org/Papers/2025/132483/132483.pdf. Acesso em: 29 maio 2026.

PARTE IV – Diagnóstico Nacional

4.1. Síntese das Entrevistas com Stakeholders Nacionais

O GT-6 realizou, ao longo de seu período de funcionamento, entrevistas com representantes do setor privado, do poder público e da academia, abrangendo empresas de jogos eletrônicos, plataformas de entretenimento audiovisual, prestadores de soluções de identidade digital, entidades do setor financeiro, órgãos governamentais e especialistas acadêmicos. As entrevistas tiveram como objetivo coletar perspectivas diversas sobre os desafios concretos da implementação do ECA Digital e subsidiar as análises e proposições do grupo. A síntese a seguir organiza os principais achados por eixo temático, sem prejuízo do relato individualizado constante do Anexo 4.

I. Aferição de idade: pluralidade de métodos e limites da autodeclaração

Os entrevistados convergiram para o diagnóstico desenvolvido na Parte III deste Relatório de que nenhum método único é suficiente. Empresa especializada em identidade digital e aferição de idade acrescentou dado relevante sobre o contexto brasileiro: documentos de identidade estaduais e carteiras de habilitação apresentam taxas de aprovação em verificações automatizadas entre 29% e 35%, ao passo que passaportes atingem cerca de 90%, mas com penetração limitada na população. Representante do setor de streaming indicou que, em serviços com contratação restrita a maiores de idade, a validação do CPF perante base externa já representa etapa adicional de aferição além da mera autodeclaração.

II. Infraestrutura pública de identidade digital e o papel do Gov.br

As práticas do setor público, incluindo a solução Gov.br e o projeto Govinho, são descritas na Parte III, seção 3.3.

III. Credenciais verificáveis, provas de conhecimento zero e identidade descentralizada

O estado da arte tecnológico nesse campo é examinado na Parte III. Os entrevistados trouxeram perspectiva prática complementar: empresa de proteção ao crédito apresentou modelo baseado em blockchain e ZKP como solução de privacidade por concepção; empresa pública de tecnologia vinculada ao poder público federal descreveu proposta baseada em software livre com credencial emitida pelo Gov.br e armazenada localmente no dispositivo; representante do setor acadêmico, por sua vez, alertou que a

execução técnica dos protocolos de duplo-cego na EUDI Wallet europeia ainda é objeto de críticas severas de criptógrafos, matizando o entusiasmo regulatório com soluções análogas.

IV. Biometria facial: distinção entre estimação de idade e reconhecimento facial

A distinção técnica entre estimativa facial de idade e reconhecimento facial e suas implicações regulatórias são abordadas na Parte III, seção 3.6. Os entrevistados trouxeram posições divergentes: empresa especializada em identidade digital e aferição de idade defendeu a estimativa facial como método proporcional e de menor fricção, destacando que a autoridade de proteção de dados do Reino Unido reconheceu formalmente que ela não constitui identificação única de indivíduo; empresa do setor de jogos eletrônicos e empresa de proteção ao crédito manifestaram rejeição a usos que impliquem coleta e armazenamento remoto de imagens de crianças e adolescentes.

V. Interoperabilidade entre sinais etários de diferentes fontes

Os desafios de interoperabilidade entre sinais etários são examinados na Parte III, seção 3.5. Plataforma digital voltada a jogos e experiências virtuais identificou incerteza regulatória sobre como tratar sinais divergentes provenientes de fontes distintas. Plataforma de redes sociais e serviços de comunicação acrescentou que, diferentemente de estados norte-americanos que receberam meses de aviso prévio e acesso a APIs estruturadas, o mercado brasileiro enfrenta comunicações escassas às vésperas da vigência da lei, e propôs que a ANPD estabeleça semântica padronizada de sinal etário.

VI. Supervisão parental e autonomia progressiva

O tema é abordado comparativamente na Parte II, seção 2.2.2 (II.2). Empresa do setor de jogos eletrônicos descreveu soluções já implementadas no Brasil, incluindo integração com a base do SERPRO para verificação de vínculo parental por CPF. Plataforma digital voltada a jogos e experiências virtuais alertou para os riscos de leituras regulatórias que tratem todos os menores de 18 anos como grupo homogêneo, defendendo que a ANPD reforce expressamente a compatibilidade dos deveres de supervisão parental com o princípio da autonomia progressiva.

VII. Moderação de conteúdo e denúncias

O tema é abordado comparativamente na Parte II. Empresa do setor de jogos eletrônicos descreveu arquitetura de moderação em três pilares: pré-moderação humana obrigatória, monitoramento proativo por IA e mecanismo permanente de denúncia com

análise contextual abrangente. Plataforma digital voltada a jogos e experiências virtuais propôs que a regulamentação brasileira incorpore critérios de priorização inspirados no modelo europeu de trusted flaggers, com credenciamento formal de entidades qualificadas.

VIII. Classificação indicativa e design compulsivo

Plataforma digital voltada a jogos e experiências virtuais identificou dois problemas operacionais sem paralelo no benchmarking: a ausência de coordenação clara entre ANPD e ClassInd sobre funcionalidades tecnicamente bloqueadas para crianças dentro de plataformas, e a ausência de definição regulatória sobre o que caracteriza design compulsivo no contexto específico de jogos, cuja natureza depende estruturalmente de engajamento e recorrência. Entidade do setor de streaming alertou para os riscos da equiparação indevida entre conteúdo impróprio e conteúdo pornográfico.

IX. Proteção de dados e minimização no contexto da aferição

O tema é transversal à Parte III. Empresa pública de tecnologia vinculada ao poder público federal reforçou o paradoxo já identificado no benchmarking: modelos excessivamente intrusivos tendem a empurrar usuários para ambientes não regulados.

X. Escopo do ECA Digital: realidade onlife[188] e lacunas interpretativas

O conceito de acesso provável é examinado na Parte II. Representante do setor acadêmico acrescentou preocupação específica com categorias que podem ficar fora de leitura restritiva do escopo: brinquedos conectados integrados em hardware físico e tecnologias educacionais de adoção sistêmica obrigatória. A entrevistada propôs interpretação sistemática que integre o ECA Digital ao Código de Defesa do Consumidor e ao artigo 227 da Constituição Federal. Entidade do setor financeiro apontou incerteza quanto à extensão da incidência da lei sobre instituições bancárias que operam como intermediárias em transações que podem envolver crianças de forma indireta.

XI. Custos de observância e atribuição de responsabilidade em ecossistemas distribuídos

Entidade do setor financeiro identificou como lacuna relevante a ausência de critério claro de atribuição de responsabilidade em ecossistemas de múltiplos agentes, ilustrando com

188 Ver: FLORIDI, Luciano (ed.). The Onlife Manifesto: Being Human in a Hyperconnected Era. Springer, 2015. Disponível em: https://link.springer.com/book/10.1007/978-3-319-04093-6. Acesso em: 1 jun. 2026.

o exemplo de menor que utiliza cartão de crédito em aplicativo de delivery para adquirir produto restrito, cadeia que envolve responsável legal, aplicativo, estabelecimento, instituição de pagamento, emissor do cartão e bandeira, sem que a lei ofereça critério de atribuição. A mesma entidade apontou assimetria de custo regulatório entre bancos tradicionais e outros players do ecossistema financeiro sujeitos a menor escrutínio.

XII. Governança institucional e articulação intergovernamental

Representante do Ministério dos Direitos Humanos e da Cidadania (MDHC) descreveu a pasta como ponto focal de articulação política sobre direitos de crianças no ambiente digital, diferenciando seu papel do dos órgãos com competência técnico-regulatória, notadamente MJSP e ANPD, e relatou a instituição de comitê interministerial para formulação da Política Nacional, com coordenação executiva atribuída ao CONANDA. O representante posicionou a ANPD como ator indispensável e estruturante da implementação e destacou o interesse suscitado pelo marco regulatório brasileiro em foros como o G20.

XIII. Comunicação pública e risco de desinformação sobre o alcance da lei

Representante do MDHC alertou para o risco de que o ECA Digital seja indevidamente responsabilizado por medidas que não decorrem de seu texto, gerando desgaste político e desinformação, e defendeu a construção de estratégia comunicacional clara e pedagógica. Empresa especializada em identidade digital e aferição de idade recomendou, com base em experiência internacional, o uso consistente da terminologia "estimação facial de idade" em detrimento de "reconhecimento facial", e o envolvimento antecipado de organizações da sociedade civil como forma de mitigar resistência baseada em desinformação.

XIV. Melhor interesse da criança: conceito aberto versus definição normativa fechada

O princípio é examinado comparativamente na Parte II, seção 2.2.2 (I.2). Representante do setor acadêmico manifestou preocupação específica com a tentativa de transformar o melhor interesse em definição normativa fechada, argumentando que o conceito é inerentemente aberto e deve ser preenchido por análise casuística à luz do artigo 227 da Constituição Federal e da Convenção sobre os Direitos da Criança.

XV. Inteligência artificial generativa e princípio da precaução

Representante do setor acadêmico propôs a adoção do princípio da precaução como vetor interpretativo em contextos de incerteza sobre os efeitos da IA generativa para crianças e adolescentes, e recomendou avaliações de impacto holísticas inspiradas nos Children Rights Impact Assessments (CRIAs), que considerem de forma integrada proteção, participação e liberdade de expressão.

XVI. Participação de crianças e adolescentes na formulação de políticas

Representante do setor acadêmico defendeu a materialização do direito à participação de crianças e adolescentes no desenvolvimento de políticas públicas e produtos digitais, propondo que a exigência seja calibrada pelo porte da empresa e pelo risco sistêmico do produto: quanto maior o poder econômico do controlador e mais elevado o risco sistêmico, maior deve ser o esforço de envolvimento desse público. A entrevistada ressaltou que essa inclusão não pode ser figurativa, devendo ocorrer por meio de metodologias qualitativas reais, como entrevistas e grupos focais, e citou o caso do banimento de redes sociais para crianças e adolescentes na Austrália como exemplo de política implementada sem consulta direta às crianças e aos adolescentes afetados, com impactos práticos não antecipados.

XVII. Dispositivos compartilhados e limites da solução tecnológica

Empresa pública de tecnologia vinculada ao poder público federal contextualizou a dimensão do problema com dados do CETIC: a incidência de compartilhamento de dispositivos no Brasil é inferior ao senso comum, abaixo de 20%, concentrada em comunidades rurais e de baixa renda. O MGI adotou posição equivalente, optando por garantir o dispositivo como proxy do titular sem impor validação biométrica adicional recorrente, reconhecendo a margem para burla mas avaliando que essa não é a prioridade do primeiro momento.

XVIII. O papel do setor bancário e financeiro como terceiro confiável

Entidade do setor financeiro demonstrou abertura à discussão sobre a possibilidade de bancos disponibilizarem sinal de maioridade em ambiente interoperável, em analogia a modelos de open banking, sem que haja iniciativa concreta em andamento. Empresa de proteção ao crédito descreveu o sistema Age Graph, integrado ao Kids Web Services, como rede de identidade reutilizável que reduz fricção em ecossistemas distribuídos ao dispensar nova verificação de usuários adultos já previamente validados.

XIX. Benchmarking internacional como insumo regulatório para a ANPD

Empresa pública de tecnologia vinculada ao poder público federal recomendou acompanhamento próximo do eIDAS 2.0 e da integração da identidade Aadhaar ao Google Wallet como cases de escalabilidade em países de alta densidade demográfica. Empresa especializada em identidade digital e aferição de idade destacou o modelo alemão de coexistência entre órgão estatal de normatização (KJM) e organismo co-regulatório de certificação (FSM) como referência de arranjo institucional que confere segurança jurídica a provedores.

XX. Experiência do usuário, fricção e risco de evasão para ambientes não regulados

O tema é examinado na Parte III, seção 3.7. Os entrevistados reforçaram o diagnóstico do benchmarking: empresa pública de tecnologia vinculada ao poder público federal alertou para o efeito rebote de modelos excessivamente intrusivos; empresa de proteção ao crédito apresentou a identidade digital reutilizável como alternativa que combina segurança e fluidez; plataforma de redes sociais e serviços de comunicação desaconselhou bloqueios genéricos, sugerindo que restrições sejam aplicadas apenas a recursos de alto risco.

4.2. Mapeamento de Pontos de Convergência, Desafios a serem Superados e Tensões entre Atores

A análise transversal das entrevistas realizadas pelo GT-6 permite identificar, para além das perspectivas setoriais individuais, um conjunto de pontos de convergência, de desafios e de tensões não resolvidas entre os diferentes atores. O mapeamento a seguir organiza esses achados com o objetivo de subsidiar as proposições do grupo e orientar a atuação regulatória da ANPD.

I. Pontos de convergência

A pluralidade de métodos como condição de cobertura adequada foi reconhecida de forma transversal entre os entrevistados que abordaram o tema. Empresa especializada em identidade digital e aferição de idade, a partir de experiência acumulada em 180 países, afirmou categoricamente não ter encontrado nenhuma jurisdição em que um único método seja suficiente. Esse diagnóstico foi compartilhado pelos demais interlocutores que descreveram suas arquiteturas de aferição, todos apresentando modelos em camadas em vez de soluções únicas.

A necessidade de proporcionalidade regulatória em função do nível de risco do serviço foi outro ponto de convergência entre os atores que se manifestaram sobre o tema. Empresas de streaming audiovisual, de jogos e do setor financeiro convergiram na percepção de que obrigações uniformes, indiferentes ao perfil de risco e às salvaguardas já existentes, gerariam custos de observância desproporcionais sem ganho correspondente em proteção efetiva. Esse entendimento encontra respaldo no próprio artigo 39 do ECA Digital, que prevê modulação de obrigações por critérios de adequação etária e nível de risco.

A privacidade por concepção como princípio orientador dos mecanismos de aferição foi defendida pelos interlocutores do setor privado e do poder público que abordaram a arquitetura técnica das soluções. A rejeição à coleta desnecessária de dados pessoais identificáveis no processo de verificação etária foi posição recorrente entre esses atores, ainda que com diferentes propostas técnicas para operacionalizá-la.

O reconhecimento de que segurança e minimização de dados não são objetivos contraditórios perpassou as falas de múltiplos interlocutores que abordaram a arquitetura técnica. Empresa especializada em identidade digital e aferição de idade ao defender a estimação facial como método que descarta a imagem imediatamente após o processamento, a empresa de proteção ao crédito e empresa pública de tecnologia vinculada ao poder público federal ao propor ZKP e atributo binário como resposta ao problema, e o MGI ao se opor à entrega da data de nascimento ao verificador na minuta do Decreto, todos partiram do pressuposto de que a solução técnica ideal é aquela que maximiza a acurácia da verificação com o menor volume de dados coletados e armazenados. Essa convergência de princípio, contudo, não se traduziu em consenso sobre qual método específico melhor realiza esse equilíbrio na prática.

A inadequação da biometria facial com armazenamento remoto de imagens infantis foi posição compartilhada explicitamente por empresa de proteção ao crédito, por empresa do setor de jogos eletrônicos e por empresa pública de tecnologia vinculada ao poder público federal, ainda que por fundamentos ligeiramente distintos: minimização de dados, imaturidade técnica e risco de vigilância em massa, respectivamente.

A centralidade da infraestrutura pública de identidade para a implementação do ECA Digital foi reconhecida tanto pelo poder público quanto pelos interlocutores do setor privado que trataram do tema. Empresa de proteção ao crédito, e empresa pública de tecnologia vinculada ao poder público federal e o MGI convergiram no diagnóstico de que o Brasil dispõe de vantagem comparativa relevante em relação a outras jurisdições, em razão da universalidade do CPF e da base instalada do Gov.br, e de que essa infraestrutura

deve ser aproveitada como alicerce dos mecanismos de verificação etária, ainda que com arquiteturas técnicas distintas entre si.

A vinculação parental como elemento estruturante do controle de acesso de crianças e adolescentes foi abordada pela empresa do setor de jogos eletrônicos, pela plataforma digital voltada a jogos, desenvolvimento de jogos e experiências virtuais, por empresa de proteção ao crédito e pelo MGI, todos descrevendo mecanismos que dependem de alguma forma de vínculo verificável entre responsável e criança ou adolescente como condição para o funcionamento efetivo dos controles parentais.

A necessidade de coordenação entre a ANPD e outros órgãos foi reconhecida por múltiplos atores. A plataforma digital voltada a jogos, desenvolvimento de jogos e experiências virtuais apontou a necessidade de alinhamento entre ANPD e ClassInd sobre o tratamento de funcionalidades bloqueadas para crianças e adolescentes. O MDHC descreveu o comitê interministerial como resposta institucional a essa necessidade de articulação. O MGI sinalizou que a obrigatoriedade de uso da solução pública de verificação dependerá das diretrizes que a ANPD vier a fixar. Há convergência entre esses interlocutores de que a implementação do ECA Digital não pode ser conduzida por um único órgão de forma isolada.

A necessidade de regulamentação secundária clara e tempestiva por parte da ANPD foi apontada de forma recorrente como condição para que os agentes regulados possam planejar e implementar suas soluções com segurança jurídica. A plataforma de redes sociais e serviços de comunicação, a plataforma digital voltada a jogos, desenvolvimento de jogos e experiências virtuais e a entidade do setor de streaming foram explícitas nesse ponto, indicando que a incerteza regulatória quanto a prazos, critérios e semântica dos sinais etários compromete a capacidade de conformidade do mercado.

II. Desafios a serem superados

A principal questão trazida pelos atores empresariais foi a insegurança jurídica decorrente da abertura textual do ECA Digital e da ausência de regulamentação secundária no momento das entrevistas. Empresas de diferentes setores relataram dificuldade em identificar, com segurança, qual é o exato conteúdo dos deveres impostos, quem é o agente responsável em cadeias multifatoriais e até que ponto determinadas medidas são realmente exigíveis. Essa incerteza foi descrita não como resistência à lei em si, mas como obstáculo prático à conformidade.

A atribuição de responsabilidade em ecossistemas distribuídos foi apontada pela entidade do setor financeiro como questão especialmente problemática. O exemplo da criança ou adolescente que utiliza cartão de crédito em aplicativo de delivery para adquirir produto restrito ilustrou que a cadeia de agentes potencialmente responsáveis pode ser extensa e que a lei não oferece critério claro de atribuição. Essa questão não é exclusiva do setor financeiro: a plataforma digital voltada a jogos, desenvolvimento de jogos e experiências virtuais identificou problema estruturalmente semelhante na interface com as lojas de aplicativos, em que a responsabilidade pelo sinal etário transmitido ao aplicativo não está claramente delimitada.

O custo de observância foi apontado pela entidade do setor financeiro como fator de preocupação relevante, especialmente para conglomerados que operam em larga escala com grande volume de produtos, serviços e inovações constantes. A preocupação manifestada não foi de incapacidade de conformidade, mas de que determinadas obrigações resultem em expansão burocrática de controles sem correspondência com redução real de riscos para crianças e adolescentes. A assimetria entre bancos tradicionais e outros players do ecossistema financeiro, sujeitos a menor escrutínio regulatório, foi apontada como fator agravante.

A divergência entre sinais etários de diferentes fontes foi identificada por agentes do setor privado fornecedores de serviços como questão técnica sem solução regulatória clara. O cenário em que o sinal proveniente da loja de aplicativos diverge do sinal da conta do usuário na plataforma ou do sinal associado ao dispositivo não encontra orientação interpretativa no texto da lei nem na regulamentação existente, gerando risco regulatório para as plataformas independentemente da escolha técnica que façam.

A comunicação escassa das lojas de aplicativos e sistemas operacionais sobre as APIs de sinal etário foi apontada como um desafio operacional relevante.

O risco de evasão para ambientes não regulados foi identificado por representante de empresa pública de tecnologia vinculada ao poder público federal como problemática associada a modelos de verificação excessivamente intrusivos. A imposição de identificação plena para acesso a plataformas legalizadas tende a empurrar parte do público para serviços sem qualquer salvaguarda, produzindo efeito inverso ao pretendido pela regulação. Essa preocupação foi compartilhada implicitamente pela empresa especializada em identidade digital e aferição de idade ao defender a estimação facial como método de menor fricção, e pela plataforma de redes sociais e serviços de comunicação ao desaconselhar bloqueios genéricos que criem experiências excessivamente restritivas.

A interface entre o ECA Digital e a classificação indicativa foi identificada como área de sobreposição regulatória disfuncional ainda não equacionada. A ausência de coordenação clara entre a ANPD e o ClassInd sobre o tratamento de funcionalidades tecnicamente bloqueadas para crianças e adolescentes gera insegurança sobre as consequências classificatórias de decisões de design que as plataformas já implementaram unilateralmente como medidas protetivas.

O caráter excessivamente fluido de determinados conceitos do ECA Digital foi apontado como fonte de insegurança por múltiplos interlocutores do setor privado. Ademais, a ausência de definição clara sobre design compulsivo foi apontada como obstáculo ao planejamento regulatório. Entidade do setor de streaming alertou para os riscos da equiparação entre conteúdo impróprio e conteúdo pornográfico. Entidade do setor financeiro apontou a subjetividade das obrigações de prevenção como geradora de zona relevante de incerteza interpretativa.

III. Tensões entre atores

A tensão mais estrutural identificada nas entrevistas opõe a lógica de maximização da proteção, que tende a demandar métodos de aferição mais robustos e potencialmente mais intrusivos, à lógica de minimização de dados, que impõe restrições à coleta e ao armazenamento de informações pessoais no processo de verificação. Essa tensão percorre todas as discussões sobre aferição de idade e não encontrou solução consensual entre os entrevistados, que propuseram respostas técnicas distintas, cada uma com vantagens e limitações próprias.

A tensão entre uniformidade regulatória e proporcionalidade por risco também permanece não resolvida. O setor privado, de forma ampla, defendeu modulação das obrigações em função do perfil de risco do serviço e das salvaguardas já existentes. A academia, por outro lado, alertou para os riscos de interpretações restritivas que criem vácuos regulatórios, especialmente em relação a tecnologias emergentes e ambientes híbridos. O equilíbrio entre esses dois vetores caberá à ANPD definir na regulamentação secundária.

A tensão entre autonomia progressiva e proteção uniforme de crianças e adolescentes de até 18 anos foi identificada por alguns, que alertaram para os riscos de leituras regulatórias que tratem o grupo de forma homogênea. A ausência de orientação regulatória clara sobre como calibrar obrigações em função de faixas etárias internas ao grupo de crianças e adolescentes de 18 anos foi apontada como lacuna relevante, com

implicações diretas para o design de produtos e para a implementação de controles parentais.

Por fim, a tensão entre a visão acadêmica de um conceito de melhor interesse da criança aberto e de preenchimento casuístico e a demanda do setor privado por definições normativas mais precisas e operacionalizáveis ilustra o dilema estrutural da regulação de direitos fundamentais em ambientes tecnológicos: a abertura conceitual que garante adaptabilidade da norma ao longo do tempo é a mesma que pode em circunstâncias específicas gerar insegurança jurídica para os agentes que precisam planejar e implementar conformidade no curto prazo. Essa tensão pode, contudo, ser potencialmente mitigada por meio da análise contextual orientada pelo Comentário Geral nº 14 do Comitê dos Direitos da Criança da ONU, que consagra a tridimensionalidade do melhor interesse (direito substantivo, princípio jurídico interpretativo fundamental e regra de procedimento), e pelas soluções desenvolvidas por jurisdições que já enfrentaram o desafio de operacionalizar o conceito em contextos regulatórios digitais.

4.3. Elementos Adicionais Identificados pelos Membros do GT-6

Ao longo dos trabalhos do GT-6, e especialmente nas reuniões finais dedicadas à consolidação do relatório, os membros do Grupo identificaram dois temas que, embora não decorram diretamente do benchmarking internacional ou das entrevistas com stakeholders, emergiram como pontos de atenção relevantes para a implementação do ECA Digital pela ANPD. O primeiro diz respeito ao papel do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD) nesse processo, e à importância de que a Agência utilize de forma contínua e estruturada essa instância multisetorial como espaço de subsídio qualificado. O segundo trata da interface com o Poder Judiciário e do sistema de justiça como um todo, cuja capacitação e articulação com a Agência os membros do GT-6 identificaram como condição para a efetividade do regime sancionatório e protetivo instituído pelo Estatuto. Esses dois temas são desenvolvidos nas subseções a seguir.

I. O Papel do CNPD na Implementação do ECA Digital

A Lei nº 15.352, de 25 de fevereiro de 2026, resultado da conversão da Medida Provisória nº 1.317/2025, consolidou juridicamente a transformação da ANPD em autarquia de natureza especial, dotada de autonomia funcional, técnica, decisória, administrativa e financeira, e formalizou as competências da Agência para atuar na implementação do Estatuto Digital da Criança e do Adolescente. A mesma lei fixou expressamente a data de 17 de março de 2026 como marco de entrada em vigor do ECA Digital, tendo em vista a redução

da vacatio legis da referida lei para seis meses após sua publicação[189]. Com isso, a ANPD passou a ser a entidade central responsável pela regulamentação, orientação e fiscalização do cumprimento do ECA Digital, acumulando esse novo mandato a suas já relevantes atribuições no campo da proteção de dados pessoais.

Diante desse redesenho institucional, é natural e recomendável que a ANPD utilize de forma plena as estruturas que já possui, em vez de construir novos arranjos a partir do zero. Nesse sentido, o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD) representa um ativo institucional de valor imediato. Composto por 23 representantes titulares e suplentes, o CNPD reúne, nos termos do art. 58-A da LGPD, representantes do Poder Executivo federal, do Senado Federal, da Câmara dos Deputados, do Conselho Nacional de Justiça, do Conselho Nacional do Ministério Público, do Comitê Gestor da Internet no Brasil, de entidades da sociedade civil com atuação em proteção de dados, de instituições científicas, tecnológicas e de inovação, de confederações sindicais representativas do setor produtivo, de entidades do setor empresarial ligado ao tratamento de dados pessoais e de entidades representativas do setor laboral[190]. Trata-se de um fórum genuinamente multisetorial e plural, cuja composição já o credencia como espaço privilegiado de construção democrática de políticas públicas voltadas à infância e à adolescência no ambiente digital. Nos termos do art. 58-B da LGPD, compete ao CNPD propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados e para a atuação da ANPD; elaborar relatórios anuais de avaliação; sugerir ações a serem realizadas pela Agência; realizar estudos, debates e audiências públicas; e disseminar o conhecimento sobre proteção de dados à população.[5] Cada uma dessas atribuições encontra correspondência direta com os desafios colocados pela implementação do ECA Digital.

A experiência acumulada pelo CNPD no trabalho por meio de grupos temáticos reforça ainda mais esse potencial. Desde abril de 2022, o Conselho vem operando por meio de grupos de trabalho temporários, inaugurados pelas Portarias CNPD nºs 01 a 05, de 1º de

[189] BRASIL. Lei nº 15.352, de 25 de fevereiro de 2026. Transforma cargos no âmbito do Poder Executivo federal; altera a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), para dispor sobre a Agência Nacional de Proteção de Dados (ANPD), a Lei nº 10.871, de 20 de maio de 2004, para criar a Carreira de Regulação e Fiscalização de Proteção de Dados, a Lei nº 15.211, de 17 de setembro de 2025 (Estatuto Digital da Criança e do Adolescente), para dispor sobre o início da vigência da referida Lei; altera as Leis nºs 9.008, de 21 de março de 1995, 11.890, de 24 de dezembro de 2008, 13.326, de 29 de julho de 2016, 13.848, de 25 de junho de 2019, e 14.600, de 19 de junho de 2023; revoga a Medida Provisória nº 1.319, de 17 de setembro de 2025; e dá outras providência. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/lei/l15352.htm.

[190] BRASIL. Lei nº 13.709, de 14 de agosto de 2018.Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

abril de 2022, que estabeleceram a metodologia de aprofundamento temático por meio de oitivas, estudos comparados e elaboração de recomendações dirigidas à ANPD e aos demais órgãos competentes[191]. Ao longo dos anos seguintes, esses grupos foram prorrogados e ajustados por sucessivas portarias[192], demonstrando a capacidade do Conselho de sustentar ciclos de trabalho especializados com produção técnica consistente. Mais recentemente, essa metodologia foi aplicada diretamente à temática do ECA Digital: em novembro de 2025, foi instituído o Grupo de Trabalho 6 (GT-6) do CNPD[193], por meio da Portaria nº 6/2025, com o objetivo específico de acompanhar e subsidiar a regulamentação do Estatuto Digital da Criança e do Adolescente, bem como o Grupo de Trabalho 2 (GT-2) do CNPD, dedicado à temática de proteção de dados de crianças e adolescentes[194].

Esse histórico demonstra que o modelo de grupos temáticos é não apenas viável, mas comprovadamente eficaz no âmbito do CNPD. Por essa razão, recomenda-se que o Conselho mantenha, de forma permanente, grupos de trabalho dedicados à proteção de crianças e adolescentes no ambiente digital. A urgência dessa medida é acentuada pelo prazo exíguo com que o ECA Digital entrou em vigor e pelo cronograma regulatório extremamente comprimido a que a ANPD está submetida. A Agenda Regulatória para o biênio 2025-2026, aprovada pela Resolução CD/ANPD nº 31, de 22 de dezembro de 2025, incorporou três iniciativas específicas relacionadas ao ECA Digital: a elaboração de guia orientativo sobre o escopo e as obrigações gerais dos fornecedores de produtos ou serviços de tecnologia da informação (item 13); a revisão dos regulamentos de fiscalização e aplicação de sanções administrativas para incorporar as novas competências da Agência (item 14); e a regulamentação dos mecanismos de aferição de idade (item 15)[195]. O cronograma de implementação é igualmente exigente: a Etapa I, iniciada em março de 2026, compreende a divulgação de orientações preliminares sobre mecanismos de aferição de idade, a criação de página virtual dedicada ao ECA Digital e o monitoramento da implantação de soluções pelas lojas de aplicativos e sistemas operacionais; a Etapa II, prevista para o segundo semestre de 2026, inclui a publicação de parâmetros normativos

191 BRASIL. Agência Nacional de Proteção de Dados. Portarias CNPD nºs 01 a 05, de 1º de abril de 2022. Disponível em: https://www.gov.br/anpd/pt-br/cnpd-2/portarias-gts-2.pdf.

192 As atividades dos grupos de trabalho foram prorrogadas e ajustadas pelas Portarias CNPD nºs 06 a 10 (15 jun. 2022), 11 (4 jul. 2022), 12 (8 ago. 2022), 13 (8 ago. 2022), 14 (14 out. 2022) e 15 (13 dez. 2022). Disponível em: https://www.gov.br/anpd/pt-br/cnpd-2.

193 BRASIL. Conselho Nacional de Proteção de Dados Pessoais e da Privacidade. Portaria CNPD nº 6, de 5 de novembro de 2025. Institui o Grupo de Trabalho 6 (GT-6) no âmbito do CNPD.

194 BRASIL. Conselho Nacional de Proteção de Dados Pessoais e da Privacidade. Portaria CNPD nº 2, de 5 de novembro de 2025. Institui o Grupo de Trabalho 2 (GT-2) no âmbito do CNPD.

195 BRASIL. Agência Nacional de Proteção de Dados. Resolução CD/ANPD nº 31, de 22 de dezembro de 2025. Diário Oficial da União, ed. 245, seção 1, p. 858, 24 dez. 2025. Itens 13, 14 e 15 do Anexo.

detalhados e a atualização dos regulamentos de fiscalização e sanção; e a Etapa III, a partir de janeiro de 2027, inaugura o ciclo efetivo de ações fiscalizatórias[196].

Essa dimensão fiscalizatória ganha contornos ainda mais concretos no Mapa de Temas Prioritários para Fiscalização 2026-2027 da ANPD, aprovado pela Resolução CD/ANPD nº 30/2025. O Tema 2 , "Proteção de crianças e adolescentes no ambiente digital, nos termos da LGPD e da Lei nº 15.211/2025" ,estabelece três eixos de atuação: o monitoramento, no primeiro semestre de 2026, da adequação dos fornecedores às exigências legais do ECA Digital; a realização de 15 atividades de fiscalização, no primeiro semestre de 2027, para verificar a configuração, por design e por padrão, do modelo mais protetivo disponível em relação à privacidade e à proteção de dados, incluindo ferramentas de supervisão parental; e a realização de outras 15 atividades de fiscalização, também no primeiro semestre de 2027, voltadas a verificar a adoção de medidas para impedir o acesso de crianças e adolescentes a conteúdos impróprios, inadequados ou proibidos por lei, incluindo mecanismos de aferição de idade[197]. Trata-se de um roteiro denso e sem precedentes na história regulatória brasileira de proteção de dados, que exigirá da ANPD não apenas capacidade técnica interna, mas suporte qualificado de seus órgãos consultivos, entre os quais o CNPD ocupa posição de destaque.

Para que esse ciclo regulatório e fiscalizatório seja bem-sucedido, a ANPD precisará contar também com uma rede qualificada de cooperação institucional. O Decreto nº 12.880/2026, que regulamentou o ECA Digital e instituiu a Política Nacional de Promoção e Proteção dos Direitos da Criança e do Adolescente no Ambiente Digital, já aponta nessa direção ao garantir a participação, no comitê intersetorial de coordenação da Política Nacional, de órgãos como o Ministério da Justiça e Segurança Pública, o Ministério da Saúde, o Ministério da Educação, o Ministério da Ciência, Tecnologia e Inovação, a Secretaria de Comunicação Social da Presidência da República, o Conselho Nacional dos Direitos da Criança e do Adolescente (Conanda) e a própria ANPD. O Decreto prevê ainda a articulação, em conjunto com a ANPD, com o Ministério Público, o Poder Judiciário e as organizações da sociedade civil, bem como, em coordenação com o Ministério das Relações Exteriores, com organismos internacionais e autoridades estrangeiras[198]. Além dessas parcerias normativamente previstas, a efetividade da implementação demandará

196 BRASIL. Agência Nacional de Proteção de Dados. Cronograma de implementação do ECA Digital. Etapas I, II e III. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-orientacoes-preliminares-e-cronograma-para-afericao-de-idade-no-ambiente-digital .

197 BRASIL. Agência Nacional de Proteção de Dados. Resolução CD/ANPD nº 30, de 22 de dezembro de 2025. Mapa de Temas Prioritários para Fiscalização 2026-2027. Tema 2, itens i, ii e iii.

198 BRASIL. Decreto nº 12.880, de 18 de março de 2026. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/decreto/d12880.htm.

cooperação ativa com outros atores governamentais relevantes: o Conselho Nacional de Justiça (CNJ), com sua capilaridade no sistema de justiça; o Conselho Nacional dos Direitos da Criança e do Adolescente (Conanda), com sua experiência na proteção de crianças e adolescentes; e o Comitê Gestor da Internet no Brasil (CGI.br), que acumula expertise técnica e de governança multissetorial da internet, são alguns exemplos.

A necessidade de engajamento permanente do CNPD com todas essas dimensões é uma recomendação de boa governança que parte da própria experiência acumulada por esse Grupo de Trabalho. O presente relatório final, em seu item 1.5, destaca explicitamente que o grupo operou sob uma dinâmica de "alvo em movimento", dada a velocidade com que o cenário regulatório evoluiu entre o início dos trabalhos, em novembro de 2025, e a consolidação do relatório, em meados de 2026, período que compreendeu a entrada em vigor da lei, a publicação do decreto regulamentador, a divulgação das orientações preliminares sobre aferição de idade e a abertura da tomada de subsídios sobre o guia orientativo da Agência. Essa experiência demonstra, com precisão, que a proteção digital de crianças e adolescentes é um campo em permanente construção, que exige do CNPD não manifestações pontuais, mas presença institucional contínua.

II. Intersecção com o Poder Judiciário

O Poder Judiciário e o sistema de justiça como um todo ocupam posição estrutural insubstituível na arquitetura de proteção instituída pelo ECA Digital. Diferentemente do modelo regulatório-administrativo, que se estrutura a partir de uma lógica de fiscalização sistêmica, padronização de condutas e aplicação de sanções em escala, o sistema de justiça opera com a especificidade do caso concreto, a tutela de direitos individuais e coletivos e a garantia do acesso à reparação, funções que nenhum arranjo administrativo, por mais robusto que seja, tem condições de substituir.

Essa complementaridade não é implícita: está expressa no próprio texto do ECA Digital. O caput do art. 35 é explícito ao ressalvar que as sanções nele previstas se aplicam "sem prejuízo das demais sanções cíveis, criminais ou administrativas", afirmando que o modelo sancionatório construído pelo Estatuto não exclui, e não poderia excluir, as vias judiciais já disponíveis. Mais do que isso, o legislador optou por reservar ao Poder Judiciário a aplicação das penalidades mais gravosas previstas no dispositivo. Nos termos do §5º do art. 35, as sanções dos incisos I e II, de natureza administrativa, serão aplicadas pela autoridade administrativa autônoma de proteção dos direitos de crianças e adolescentes no ambiente digital, ao passo que as dos incisos III e IV, compreendendo a suspensão parcial ou total das atividades e a proibição de exercício de atividades, serão aplicadas pelo Poder Judiciário. Trata-se de uma escolha deliberada de arquitetura normativa: as

intervenções mais severas, com maior potencial de impacto econômico e operacional sobre os fornecedores, ficam reservadas à apreciação judicial, com todas as garantias processuais que lhe são inerentes, inclusive a garantia do princípio do devido processo legal, que possui status constitucional (art. 5º, LIV da CF/88).

Essa divisão de competências sancionatórias exige, por sua vez, um diálogo institucional fluido entre a autoridade administrativa e o Poder Judiciário. O Decreto nº 12.880/2026, que regulamentou o ECA Digital, já reconhece essa necessidade: o art. 34, §3º, determina que o Ministério da Justiça e Segurança Pública atue em articulação com o Conselho Nacional de Justiça (CNJ) e com o Conselho Nacional do Ministério Público (CNMP) para a elaboração de normas, procedimentos, orientações e soluções técnicas destinados à operacionalização das medidas ali previstas. Essa articulação normativa entre instâncias administrativas e de justiça é o reconhecimento explícito de que a efetividade do ECA Digital depende de uma atuação coordenada e intersetorial e não de compartimentos estanques.

Nesse cenário, o CNJ e o CNMP assumem papel de protagonismo. Ao CNJ compete, entre outras atribuições, a padronização de procedimentos judiciais, a orientação de magistrados e a formulação de políticas judiciárias nacionais — funções que se revelam decisivas em um campo como o da proteção digital de crianças e adolescentes, marcado por rápida evolução tecnológica, pluralidade de atores e necessidade de respostas uniformes em escala nacional. Ao CNMP cabe papel equivalente no âmbito do Ministério Público, instituição que, por sua vocação constitucional de tutela dos interesses difusos, coletivos e individuais indisponíveis, tem competência natural para a promoção de ações civis públicas e para o controle externo dos direitos fundamentais de crianças e adolescentes no ambiente digital. A ambos — CNJ e CNMP — recomenda-se o desenvolvimento de referenciais técnicos específicos sobre o ECA Digital, incluindo enunciados interpretativos, orientações procedimentais e programas de formação continuada voltados a magistrados, membros do Ministério Público, da Defensoria Pública e demais operadores do direito.

A OAB e o Sistema Nacional de Defesa do Consumidor integram essa rede de forma igualmente estratégica, sobretudo do ponto de vista da territorialização do acesso à justiça. A rede de Procons, presente em centenas de municípios brasileiros, constitui um dos vetores mais capilarizados de recepção de denúncias e orientação de consumidores no país — e o histórico de êxito dessa experiência no campo consumerista é um modelo que merece ser adaptado e replicado para o domínio da proteção digital infantojuvenil. A OAB, por sua vez, pode desempenhar papel relevante tanto na formação dos operadores do

direito quanto na orientação da sociedade civil sobre os direitos assegurados pelo ECA Digital e os meios disponíveis para sua efetivação. A lógica subjacente a essas propostas é a de territorialização: assim como a proteção do consumidor ganhou escala e efetividade no Brasil a partir da distribuição capilar de pontos de atendimento e orientação, a proteção digital de crianças e adolescentes também requer que os mecanismos de denúncia, escuta e resposta estejam geograficamente próximos das famílias e das comunidades.

A formação e a capacitação de magistrados, membros do Ministério Público, da Defensoria Pública e demais profissionais do direito constituem, nesse quadro, uma demanda imediata e de natureza estruturante. Compreender o ECA Digital exige, necessariamente, compreender o ECA em sua integralidade e, em particular, a doutrina da proteção integral que lhe é fundante. Não é possível aplicar adequadamente o Estatuto Digital sem um domínio sólido dos princípios que regem o Estatuto da Criança e do Adolescente como um todo, da jurisprudência que o consolida e dos mecanismos do Sistema de Garantia de Direitos (SGD) que lhe dão suporte. Por essa razão, recomenda-se que o ECA Digital seja incorporado como conteúdo obrigatório em disciplinas de direito da criança e do adolescente e direito digital dos cursos de graduação em Direito, com abordagem que articule as dimensões protetivas tradicionais com as especificidades do ambiente digital, um campo que, pela sua natureza, requer a interseção entre proteção integral, proteção de dados pessoais e regulação de plataformas.

Essa perspectiva formativa conecta-se diretamente ao cruzamento entre duas culturas que precisam ser construídas em paralelo e em diálogo: a cultura de proteção de dados, promovida pela LGPD e pelas ações da ANPD, e a cultura de proteção integral dos direitos de crianças e adolescentes, enraizada no ECA e no SGD. No ambiente digital, essas duas culturas convergem e se reforçam mutuamente. Iniciativas de letramento sobre privacidade, consentimento e tratamento de dados pessoais de crianças encontram solo fértil quando articuladas com a sensibilização sobre os riscos digitais, os direitos de participação, a proteção contra conteúdos prejudiciais e a responsabilidade dos fornecedores de tecnologia. O cruzamento dessas agendas, hoje ainda tratadas de forma relativamente isolada por seus respectivos atores institucionais, representa uma oportunidade concreta de ampliar o alcance e o impacto de ambas.

Também é fundamental que o sistema de justiça compreenda o ECA Digital não como uma ruptura com o ordenamento jurídico preexistente, mas como uma camada protetiva adicional que se soma a um arcabouço já consolidado. O Código Civil, o Código de Defesa do Consumidor, a LGPD, o Marco Civil da Internet e o próprio ECA seguem integralmente vigentes e aplicáveis. O ECA Digital não substitui nenhum desses

instrumentos: reforça-os, especifica-os e os articula no contexto do ambiente digital, funcionando como um cinto de segurança adicional em um veículo normativo que já estava em movimento. A perspectiva correta é, portanto, a do diálogo das fontes, conceito consolidado na doutrina jurídica brasileira, e da harmonia interpretativa entre normas que, embora provenientes de diferentes matrizes, compartilham o objetivo comum de garantir a dignidade, o desenvolvimento e a proteção de crianças e adolescentes. Para o Poder Judiciário, essa perspectiva de soma e complementaridade é o horizonte a partir do qual deverá construir sua jurisprudência sobre o tema.

A cooperação com a sociedade civil organizada constitui boa prática indispensável nesse processo. Organizações especializadas em proteção de dados, direitos digitais e direitos da infância acumulam expertise técnica e experiência prática que o sistema de justiça não produz internamente — e que podem ser mobilizadas por meio de parcerias formais, convênios de cooperação técnica, participação em instâncias consultivas e colaboração na elaboração de materiais formativos. Um exemplo concreto dessa contribuição é o curso ECA Digital e Sistema de Justiça[199], desenvolvido pela Data Privacy Brasil, com apoio do Instituto Alana, CONDEGE, Procon Brasil e MPCON, voltado especificamente à capacitação de operadores do direito sobre o Estatuto Digital e suas implicações para a prática jurídica. Iniciativas dessa natureza, produzidas por atores da sociedade civil com competência técnica reconhecida, merecem ser referenciadas, apoiadas e integradas às estratégias de formação continuada do CNJ, do CNMP e da OAB.

O mesmo vale para a cooperação com universidades, centros de pesquisa e instituições de ensino jurídico. A produção acadêmica sobre proteção digital de crianças e adolescentes ainda é incipiente no Brasil, e seu fortalecimento depende de parcerias entre o sistema de justiça, a ANPD, o CNPD e a academia, seja por meio de editais de pesquisa, clínicas jurídicas, grupos de trabalho conjuntos ou participação de pesquisadores em processos regulatórios e formativos.

Por fim, qualquer sistema de proteção de crianças e adolescentes no ambiente digital será incompleto se não observar, de forma rigorosa, os princípios da não revitimização e do acolhimento. A Lei nº 13.431/2017, conhecida como Lei da Escuta Protegida, estabelece o sistema de garantia de direitos de crianças e adolescentes vítimas ou testemunhas de violência, definindo protocolos de escuta especializada e depoimento especial que impedem a exposição repetida da criança a situações traumáticas. Quando a

[199] DATA PRIVACY BRASIL. ECA Digital e Sistema de Justiça: design responsável e responsabilidade civil. São Paulo, 2026. Curso on-line destinado a integrantes do Sistema de Justiça e do Sistema Nacional de Defesa do Consumidor, com apoio do Instituto Alana e parceria institucional do Condege, MPCON e Procons Brasil. Disponível em: https://dataprivacy.com.br/cursos/eca-digital-e-sistema-de-justica/. Acesso em: 29 maio 2026.

violação de direitos ocorre no ambiente digital, seja por exposição a conteúdos prejudiciais, exploração, assédio ou tratamento ilegal de dados , os danos emocionais e psicológicos são reais e frequentemente invisíveis. O sistema de justiça deve estar preparado para receber, escutar e acolher essas crianças com a metodologia adequada, prevenindo que o próprio processo de apuração se torne uma nova fonte de sofrimento. A integração entre os protocolos da Lei da Escuta Protegida e os fluxos de atendimento relacionados ao ECA Digital é, portanto, uma exigência de coerência sistêmica, e um compromisso que o CNJ, o CNMP e os órgãos do SGD devem assumir de forma coordenada.

PARTE V – Considerações Finais e Proposições

A elaboração das recomendações do GT-6 deve ser lida à luz do contexto institucional em que os trabalhos se desenvolveram. Como detalhado na Seção 1.5, o grupo operou sob uma dinâmica de "alvo em movimento": o benchmarking internacional foi consolidado antes da entrada em vigor do ECA Digital, da edição do Decreto nº 12.880/2026, da publicação das Orientações Preliminares sobre Mecanismos Confiáveis de Aferição de Idade e da abertura da tomadas de subsídios sobre os Guia Orientativos[200] da ANPD. Esse descasamento temporal implica que determinadas análises que se mostravam urgentes no início dos trabalhos já foram, em alguma medida, endereçadas pela produção normativa superveniente, ao passo que outras discussões ganharam relevância renovada para as próximas etapas regulatórias da Agência.

Além disso, cabe ressaltar que, mais do que formular orientações prescritivas que anteciparam ou substituiriam o juízo regulatório da Agência, o GT-6 concentrou seus esforços em elaborar estudos e realizar debates a fim de subsidiá-la na implementação do ECA Digital, em consonância com as competências do CNPD previstas no art. 58-B da LGPD. As recomendações ora apresentadas situam-se, portanto, nesse registro: o de contribuição técnica multisetorial que o CNPD oferece à Agência como insumo qualificado, e não como diretriz vinculante.

Em relação à Parte II, que se debruçou sobre a paisagem normativa nacional e o benchmarking internacional comparado, a recomendação central do GT-6 é de natureza instrumental: que a ANPD utilize o benchmarking elaborado como fonte de estudo e subsídio. Esse aproveitamento pode se dar em diferentes dimensões: o estudo aprofundado de jurisdições ou fontes normativas específicas identificadas no documento; o uso do mapeamento como ponto de partida para investigações complementares; o aprofundamento de orientações ou revisão de interpretações firmadas em instrumentos normativos da Agência; e, sobretudo, a utilização do material como subsídio para a regulamentação de temas que ainda aguardam norma da ANPD.

Em relação à Parte III, que se debruçou sobre o desafio da aferição de idade, o GT-6 recomenda que a ANPD igualmente aproveite os subsídios reunidos como insumo para o aprofundamento de sua atuação sobre o tema. Isso se justifica com particular força dado que, por mais que certos aspectos já tenham sido endereçados pela lei, pelo Decreto nº 12.880/2026 e pelas Orientações Preliminares publicadas em março de 2026, a regulamentação definitiva da matéria permanece em aberto, visto que a Agenda

[200] Cabe destacar que durante a finalização do presente Grupo de Trabalho, a Agência iniciou Tomada de Subsídios sobre o Guia Orientativo "Mecanismos de Aferição de Idade", disponível no seguinte link: <https://brasilparticipativo.presidencia.gov.br/processes/Guia-orientativo-mecanismos-de-afericao-idade>.

Regulatória 2025–2026 contempla expressamente a regulamentação dos mecanismos de aferição de idade como iniciativa prioritária. Além disso, o Mapa de Temas Prioritários para Fiscalização para o biênio 2026–2027 igualmente sinaliza a centralidade do tema para as próximas etapas de atuação da Agência.

Em relação à Parte IV, o GT-6 recomenda que a ANPD a examine com atenção particular. Diferentemente das partes anteriores, ela apresenta um panorama de maior proximidade com a realidade brasileira: reúne a visão de atores pertencentes a diversos setores da sociedade nacional sobre temas de extrema relevância para a implementação do ECA Digital. O material permite à Agência compreender o que esses atores já fazem e têm feito na matéria, mas também quais são suas preocupações e perspectivas, e identificar os pontos de convergência, os desafios compartilhados e as tensões que persistem entre eles.

Além do diagnóstico nacional, a Parte IV contempla duas recomendações específicas formuladas pelos próprios membros do GT-6 ao final da condução dos trabalhos. A primeira, constante da Seção 4.3.I, diz respeito ao papel do CNPD na implementação do ECA Digital: diante do redesenho institucional decorrente da transformação da ANPD em autarquia especial e da atribuição a ela da centralidade regulatória e fiscalizatória do Estatuto, os membros do GT-6 recomendam que o Conselho mantenha, de forma permanente, grupos de trabalho dedicados à proteção de crianças e adolescentes no ambiente digital, aproveitando a composição multisetorial e plural do CNPD como ativo institucional imediato para subsidiar a Agência. A segunda, constante da Seção 4.3.II, trata da intersecção com o Poder Judiciário, os membros do GT-6 recomendam à ANPD que promova e fomente a articulação com o CNJ, o CNMP e os demais atores do sistema de justiça, reconhecendo que a efetividade do ECA Digital depende de atuação coordenada entre a Agência e essas instâncias, inclusive para fins de desenvolvimento de referenciais técnicos, enunciados interpretativos e programas de formação continuada voltados a magistrados, membros do Ministério Público, da Defensoria Pública e demais operadores do direito, de modo a preparar o sistema de justiça para exercer com efetividade o papel que a arquitetura normativa do Estatuto lhe reserva, incluindo a aplicação das sanções mais graves previstas no art. 35.

Anexos

Anexo 1 – Mapeamento de Temas

Encaminhado por e-mail à Agência.

Anexo 2 – Benchmarking Internacional

Encaminhado por e-mail à Agência.

Anexo 3 – Relato das Entrevistas

Encaminhado por e-mail à Agência.

Anexo 4 – Atas de Reunião

Encaminhado por e-mail à Agência.