

Mecanismos confiáveis de aferição de idade

ORIENTAÇÕES PRELIMINARES





Mecanismos confiáveis de aferição de idade

ORIENTAÇÕES PRELIMINARES

Brasília, DF
março / 2026

Presidente da República

Luiz Inácio Lula da Silva

Agência Nacional de Proteção de Dados · ANPD

Diretor-Presidente

Waldemar Gonçalves Ortunho Junior

Diretores

Iagê Zendron Miola

Lorena Giuberti Coutinho

Miriam Wimmer

Autores

Davi Teofilo Nunes Oliveira

Diego Carvalho Machado

Jeferson Dias Barbosa

Lucas Borges de Carvalho

Projeto gráfico, editoração e capa

André Scofano Maia Porto

Gráficos

Ana Luisa Schiavo Leite

Bruna Assi Hernandes

Versão 1.0

Publicação digital – PDF (março / 2026)

Agência Nacional de Proteção de Dados

SCN, Qd. 6, Conj. A

Ed. Venâncio 3000, Bl. A, 9º andar

Brasília, DF · Brasil · 70716-900

www.gov.br/anpd

Introdução

O presente documento tem por objetivo apresentar orientações preliminares para a implementação de mecanismos confiáveis de aferição de idade¹ por fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e adolescentes, ou de acesso provável por esse público. Tais orientações destinam-se a guiar os agentes regulados até que sejam editadas orientações definitivas, conforme previsto na Agenda Regulatória 2025-2026 e após consulta à sociedade, podendo ser modificadas ao longo desse processo.²

Até a publicação das orientações definitivas, este documento reflete a posição institucional da ANPD sobre os cuidados a serem observados na implementação dos referidos mecanismos e servirá de referência para as atividades de monitoramento da Agência. Nesse contexto, as orientações buscam delinear parâmetros que permitam aos agentes regulados interpretar, neste momento inicial de aplicação da nova legislação, os princípios e regras estabelecidos na Lei nº 15.211/2025 (Estatuto Digital da Criança e do Adolescente – “ECA Digital”) e no Decreto nº 12.880, de 18 de março de 2026 (Decreto regulamentador do ECA digital – “Decreto”). Mais precisamente, em cumprimento ao art. 49, parágrafo único, II, do Decreto, pretende-se emitir “recomendações e orientações acerca das práticas relevantes para a implementação de mecanismos confiáveis de aferição de idade, observado o disposto no art. 24 do mesmo Decreto.

Inicialmente, deve-se considerar que o ECA Digital adota um modelo regulatório orientado à prevenção de riscos e à proteção integral de crianças e adolescentes no ambiente digital. Essa diretriz se expres-

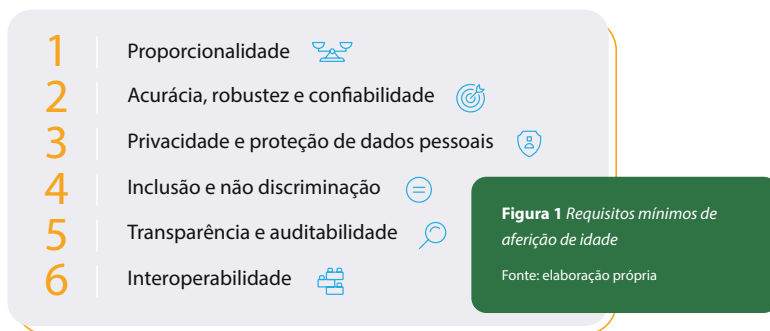
1 Nos termos do art. 2º, IV, do Decreto, aferição de idade é o “termo geral referente aos procedimentos destinados a verificar, estimar ou inferir, direta ou indiretamente, a idade ou a faixa etária de um usuário, por meio de um conjunto de métodos, tecnologias e processos, incluídos análise documental, biométrica e de padrões de uso, e outros meios tecnicamente idôneos”.

2 A presente versão está sujeita a comentários e contribuições pela sociedade de forma contínua, de maneira que as orientações preliminares poderão ser atualizadas, a critério da ANPD, à medida que novas regulamentações e entendimentos forem publicados. Sugestões podem ser enviadas para a Ouvidoria da ANPD, pela Plataforma Fala. BR: <https://falabr.cgu.gov.br>

sa, por exemplo, no art. 3º, que determina que produtos e serviços de tecnologia da informação direcionados a esse público, ou de acesso provável por ele, adotem medidas adequadas e proporcionais para assegurar nível elevado de privacidade, proteção de dados e segurança, tomando como parâmetro o melhor interesse da criança e do adolescente. No mesmo sentido, o art. 5º vincula os fornecedores aos deveres de prevenção, proteção, informação e segurança, em articulação com os referenciais do Estatuto da Criança e do Adolescente (Lei nº 8.069, de 13 de julho de 1990) e do Código de Defesa do Consumidor (Lei nº 8.078, de 11 de setembro de 1990).

É com base nesse modelo regulatório que se deve compreender o comando do art. 9º, caput e § 1º, do ECA Digital, que determina que os mecanismos de aferição de idade adotados sejam “confiáveis”. Trata-se, nesse sentido, de uma obrigação que decorre do dever geral imposto aos fornecedores de serviços e produtos de atuar de forma proativa e diligente para prevenir e mitigar riscos a crianças e adolescentes no ambiente digital. O mesmo dispositivo estabelece, ainda, que devem ser adotadas medidas “eficazes” para impedir o acesso de crianças e adolescentes a conteúdo, produtos ou serviços cuja oferta ou acesso seja impróprio, inadequado ou proibido para menores de dezoito anos.

Estas determinações gerais de confiabilidade e eficácia previstas no ECA Digital foram detalhadas no art. 24 do Decreto, que estabelece requisitos mínimos para a implementação de soluções de aferição de idade. Para fins didáticos e de sintetização, os onze incisos do art. 24 podem ser agrupados em seis conjuntos de requisitos: (i) proporcionalidade; (ii) acurácia, robustez e confiabilidade; (iii) privacidade e proteção de dados pessoais; (iv) inclusão e não discriminação; (v) transparência e auditabilidade; e (vi) interoperabilidade.



Esses seis requisitos mínimos serão examinados nas seções seguintes deste documento. Cada seção apresenta conceitos, fundamentos legais e regulamentares aplicáveis, bem como recomendações e boas práticas destinadas a apoiar a implementação dessas soluções pelos fornecedores. Ao final do documento, o Anexo traz um quadro sintético com as principais recomendações associadas a cada um desses requisitos.

1



Proporcionalidade

O ECA Digital consagra, em diversos dispositivos, uma abordagem baseada em risco, isto é, a concepção de que os fornecedores devem adotar medidas de prevenção e mitigação proporcionais aos riscos inerentes aos seus conteúdos, produtos e serviços. Tal abordagem se traduz, por exemplo, nos deveres de prevenção, proteção, informação e segurança previstos na Lei. Assim, por exemplo, o art. 6º determina que fornecedores adotem medidas razoáveis desde a concepção e ao longo da operação de suas aplicações, com o objetivo de prevenir e mitigar riscos associados ao acesso, à exposição, à recomendação ou à facilitação de contato com conteúdo, produtos ou práticas capazes de violar direitos de crianças e adolescentes. Na mesma linha, o art. 8º, I, estabelece a obrigação de realizar gerenciamento de riscos de recursos, funcionalidades e sistemas e de seus impactos direcionados à segurança e à saúde de crianças e adolescentes.

Partindo desse modelo regulatório, o art. 24, I, do Decreto incorpora a abordagem baseada em risco também no âmbito específico das soluções de aferição de idade, ao estabelecer que estas deverão observar “a proporcionalidade entre a solução adotada e o nível de risco associado ao serviço”.

Este requisito orienta a aplicação dos demais parâmetros previstos no Decreto, na medida em que impõe aos fornecedores o dever de buscar equilíbrio entre, de um lado, a acurácia, a robustez e a confiabilidade exigidas em um determinado contexto e, de outro, a probabilidade e a gravidade dos efeitos adversos que a própria solução de aferição de idade pode gerar sobre direitos dos usuários, em especial sobre a privacidade e a proteção de dados pessoais.

Assim, recomenda-se, portanto, que a definição, pelo fornecedor, da solução técnica mais adequada seja precedida de identificação e avaliação dos riscos inerentes:

- (i) uso do serviço ou do produto; e
- (ii) ao próprio mecanismo de aferição de idade a ser adotado.

No primeiro caso, relacionado aos riscos do serviço ou produto, recomenda-se que sejam considerados especialmente os efeitos adversos sobre a privacidade, a segurança e a saúde de crianças e adolescentes. O ECA Digital indica diversas situações que podem ser consideradas de maior risco do serviço ou produto, a depender do contexto em que utilizadas, a exemplo de serviços com funcionalidades que permitam interação entre usuários, que contenham conteúdos proibidos para menores de dezoito anos ou que possam levar ao uso compulsivo, entre outras hipóteses apontadas em seus artigos 1º, parágrafo único, III; 6º; 8º, III e IV; 9º; 17, § 4º; 21; 27 e 29. Ressalta-se, de qualquer forma, que a avaliação de risco é sempre contextual e deve levar em consideração as circunstâncias relevantes de cada situação concreta.

No segundo caso, relacionado à solução de aferição de idade adotada, recomenda-se atenção aos riscos decorrentes do próprio mecanismo de aferição implementado, em especial, em relação ao tratamento de dados sensíveis, à ampliação de compartilhamento de dados, ao eventual estabelecimento de barreiras indevidas de acesso a usuários e à possibilidade de reprodução de vieses discriminatórios ou de aumento da exposição a incidentes de segurança. Deve-se considerar, ainda, que os efeitos adversos da solução de aferição de idade adotada podem alcançar tanto usuários crianças e adolescentes quanto adultos, uma vez que estes também serão submetidos a mecanismos de aferição etária.



A escolha do método mais adequado, portanto, não deve ser orientada apenas pela precisão do mecanismo de aferição de idade, mas também pela sua compatibilidade com os direitos de usuários e com as exigências de proteção de dados pessoais. Nesse sentido, o relatório do Ministério da Justiça e Segurança Pública (MJSP) “*Mecanismos de aferição de idade*” registra convergência multissetorial quanto à preferência por soluções que “minimizam a exposição de dados”, bem como cautela em relação a métodos baseados em biometria facial, em razão de “riscos de vigilância, vieses algorítmicos e coleta excessiva de dados sensíveis”³

Quando a solução de aferição de idade adotada envolver o tratamento de dados biométricos, devem ser adotadas medidas de segurança apropriadas e específicas, considerando sua qualificação como dado pessoal sensível (art. 5º, II LGPD). Nessas hipóteses, sua utilização tende a exigir fundamentação mais robusta quanto à adequação e necessidade da medida no contexto específico, especialmente quando existirem alternativas menos intrusivas à privacidade capazes de alcançar resultado equivalente. Logo, o uso desses mecanismos deve ser acompanhado de salvaguardas compatíveis com a natureza e a sensibilidade dos dados envolvidos.

O Relatório de Impacto à Proteção de Dados Pessoais (RIPD) pode ser um instrumento relevante para identificação e avaliação dos riscos associados à aferição de idade do ponto de vista da privacidade e da proteção de dados pessoais, bem como das medidas e salvaguardas destinadas à sua mitigação, nos termos do art. 38 da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD) e do art. 16, parágrafo único, do ECA Digital, especialmente quando o tratamento associado à aferição de idade puder acarretar alto risco às liberdades civis e aos direitos fundamentais dos titulares.

Outro instrumento relevante à avaliação de proporcionalidade das soluções adotadas é a avaliação de impacto de riscos à segurança e à saúde de crianças prevista no art. 47 do Decreto.

3 Ministério da Justiça e Segurança Pública. Secretaria Nacional de Direitos Digitais. *Mecanismos de aferição de idade. Análise das Contribuições à Consulta Pública e Subsídios para Regulamentação da Lei nº 15.211/2025*. Brasília: MJSP, janeiro de 2026, p. 3. Disponível em: <https://www.gov.br/mj/pt-br/assuntos/noticias/relatorio-sedigi-consulta-de-afericao-de-idade.pdf>.

Nesse contexto, recomenda-se que os fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável por esse público:

- + Identifiquem e avaliem os riscos associados ao produto ou serviço digital, especialmente os potenciais efeitos adversos sobre a privacidade, a segurança e a saúde de crianças e adolescentes;*
- + Identifiquem e avaliem os riscos decorrentes do próprio mecanismo de aferição de idade a ser implementado, com atenção aos seus impactos na privacidade e proteção de dados pessoais, especialmente quando envolver o tratamento de dados biométricos; e*
- + Avaliem a proporcionalidade entre os riscos do produto ou serviço e os riscos decorrentes do mecanismo de aferição de idade a ser implementado.*

2



Acurácia, robustez e confiabilidade

Para que os mecanismos de aferição de idade cumpram adequadamente seu propósito de determinar a idade ou a faixa etária dos usuários de produtos e serviços de tecnologia da informação e distinguir usuários adultos de crianças e adolescentes, a solução adotada deve observar parâmetros de acurácia, robustez e confiabilidade.

Essa diretriz preliminar decorre do art. 9º, § 1º, do ECA Digital, bem como do art. 24, II, do Decreto, que exigem a adoção de mecanismos confiáveis de aferição de idade e a observância de sua efetividade.

Acurácia refere-se ao grau de precisão com que determinado método é capaz de determinar a idade ou a faixa etária do usuário. Trata-se de um indicador do desempenho do método ou técnica de aferição de idade, que pode ser avaliado, por exemplo, por meio de testes, estudos técnicos ou outras formas de validação utilizadas no desenvolvimento ou na avaliação da solução. Caso um método apresente baixo desempenho nessas avaliações, é provável que produza resultados insatisfatórios em contextos reais de implementação. Nessas hipóteses, recomenda-se a adoção de método alternativo ou, ainda, a integração de técnicas adicionais capazes de aumentar a precisão da solução adotada.

A *robustez* corresponde à capacidade de resistir a tentativas de burla ou fraude por parte dos usuários, considerando a faixa etária predominante da base de usuários do produto ou serviço de tecnologia da informação e os meios técnicos razoavelmente disponíveis. Soluções facilmente contornáveis são pouco robustas. Por essa razão, é imprescindível que os mecanismos de aferição de idade sejam capazes de manter seu desempenho em situações reais de uso, reduzindo a probabilidade de acessos indevidos por meio de manipulação ou fraude.

A *confiabilidade* (em sentido estrito)⁴, por sua vez, refere-se à capacidade do mecanismo de produzir resultados corretos e adequados de modo constante e verificável em diferentes contextos de uso. Nesse sentido, um mecanismo confiável não é apenas aquele que produz bom desempenho em situações pontuais ou em avaliações realizadas durante seu desenvolvimento ou validação, mas aquele que demonstra funcionamento estável e verificável em condições reais de operação. A avaliação da confiabilidade envolve, entre outros aspectos, a integridade e a independência das fontes de dados utilizadas para o funcionamento do mecanismo. Neste sentido, soluções baseadas exclusivamente em autodeclaração do próprio usuário possuem baixo grau de confiabilidade, uma vez que dependem de informações facilmente manipuláveis e carecem de fontes de dados íntegras e independentes.⁵

Nesse contexto, recomenda-se que os fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável:

- + *Mensurem e documentem a acurácia dos mecanismos de aferição de idade por eles empregados, utilizando métricas claras e adequadas, com reavaliações periódicas de acordo com o estado da arte da tecnologia para identificar obsolescências e potenciais de aprimoramento;*

4 A noção de *confiabilidade* em sentido estrito se relaciona, ao lado da acurácia e robustez, ao desempenho do(s) método(s) de aferição de idade de acordo com métricas de ordem técnica, como explicitado no item 2 abaixo. Desse modo, não se pode confundir esta noção inscrita no art. 24, II, do Decreto, com a noção mais ampla de mecanismo de aferição de idade *confiável*.

5 De acordo com estudo da ANPD: “A previsibilidade e a facilidade de manipular datas de nascimento tornam esse tipo de informação pouco confiável para fins de verificação de idade. Como resultado, é muito mais fácil criar múltiplas contas usando dados falsos, pois a informação não é única o suficiente para impedir a fraude. Em outras palavras, por ser um dado facilmente dedutível e de simples falsificação, a data de nascimento favorece a criação de múltiplos cadastros com informações inverídicas. Além disso, a ausência de mecanismos de vinculação à identidade civil e de camadas adicionais de comprovação, como biometria ou verificação documental, limita a confiabilidade desse método”. ANPD. *Mecanismos de aferição de idade*. Brasília, DF: ANPD, 2025, p. 41. (Radar Tecnológico, n. 5). Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-5a-edicao-do-radar-tecnologico>.

- + *Avaliem, previamente à adoção de uma solução de aferição de idade, a confiabilidade das fontes de dados utilizados no processo, bem como monitorá-las continuamente e documentar eventuais falhas e as medidas corretivas adotadas.*

3



Privacidade e proteção de dados pessoais

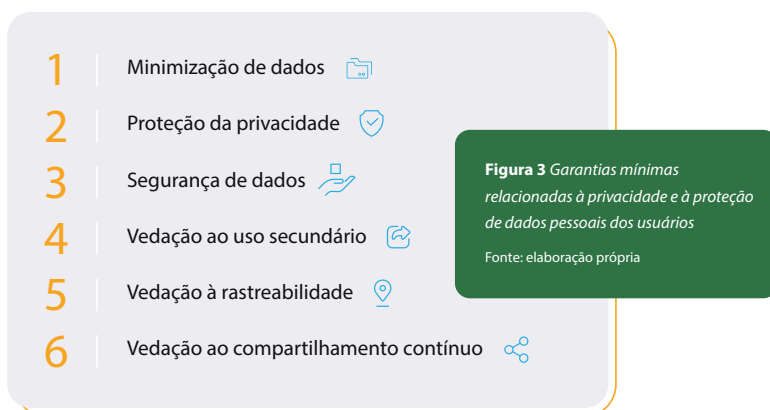
A privacidade e a proteção de dados pessoais constituem direitos fundamentais de essencial observância na implementação de mecanismos de aferição de idade que envolvem, em maior ou menor grau, o tratamento de dados pessoais. Por essa razão, a análise da adequação dessas soluções deve abranger a avaliação e mitigação dos potenciais impactos produzidos sobre os titulares de dados.

No âmbito do ECA Digital, essa obrigação aparece de forma expressa, por exemplo, no art. 12, inciso I, ao atribuir às lojas de aplicações de internet e sistemas operacionais a obrigação de adotar medidas proporcionais, auditáveis e tecnicamente seguras para aferir a idade ou a faixa etária dos usuários, observados os princípios previstos no art. 6º da LGPD. O inciso III do mesmo artigo dispõe que o fornecimento de sinal de idade deverá ocorrer por meio de Interface de Programação de Aplicações (API) segura e pautada pela proteção da privacidade por padrão, exclusivamente para o cumprimento das finalidades da lei e com salvaguardas técnicas adequadas. Já o § 1º estabelece que esse fornecimento deverá observar o princípio da minimização de dados, vedado qualquer compartilhamento contínuo, automatizado e irrestrito de dados pessoais de crianças e adolescentes. O art. 13, por sua vez, determina que os dados coletados para aferição de idade só poderão ser utilizados para essa finalidade, vedado seu tratamento para qualquer outro propósito.

A mesma lógica é reforçada pelo art. 37, parágrafo único, ao estabelecer que a regulamentação do ECA Digital a ser realizada pelo Po-

der Executivo não poderá, em nenhuma hipótese, impor, autorizar ou resultar na implantação de mecanismos de vigilância massiva, genérica ou indiscriminada, nem em práticas que comprometam os direitos fundamentais à liberdade de expressão, à privacidade, à proteção integral e ao tratamento diferenciado dos dados pessoais de crianças e adolescentes, nos termos da Constituição Federal, do Estatuto da Criança e do Adolescente e da LGPD.

O Decreto, em seu art. 24, prevê que as soluções de aferição de idade devem observar as seguintes garantias mínimas relacionadas à privacidade e à proteção de dados pessoais dos usuários: (i) minimização de dados; (ii) proteção da privacidade; (iii) segurança de dados; (iv) vedação ao uso secundário; (v) vedação à rastreabilidade; e (vi) vedação ao compartilhamento contínuo, automatizado e irrestrito de dados pessoais. Em conjunto, essas garantias indicam que a proteção de dados pessoais constitui dimensão inerente ao próprio desenvolvimento, à implementação e ao funcionamento de soluções de aferição de idade. O cumprimento desses requisitos deve ser orientado por definições já consolidadas na LGPD. Ressalta-se, ainda, que embora o ECA Digital e o Decreto confirmem especial destaque a essas salvaguardas, permanece aplicável, sempre que houver tratamento de dados pessoais em uma atividade, todo o conjunto de disposições previstos na LGPD.



Nessa perspectiva, o princípio da *minimização de dados* (ou da necessidade) - conforme definido no Art. 6º, inciso III da LGPD - impõe que o tratamento de dados pessoais se limite ao mínimo necessário para a realização de suas finalidades, com abrangência apenas dos dados pertinentes, proporcionais e não excessivos. No âmbito da aferição de idade, o respeito a tal princípio demanda que a solução adotada se restrinja, tanto quanto possível, ao tratamento dos dados necessários à confirmação da idade ou da faixa etária do usuário relevante para o contexto de uso, evitando a coleta excessiva de dados pessoais ou o tratamento de informações que extrapolem o necessário para a finalidade específica de aferição etária. Essa avaliação deve considerar não apenas os dados tratados após a implementação da solução, mas também as decisões adotadas durante sua fase de desenvolvimento, que devem ser estruturadas de modo a reduzir o tratamento de dados pessoais.

DICA

Algumas soluções tecnológicas permitem verificar se um usuário atende a determinado requisito etário, como ser maior de 18 anos ou pertencer a determinada faixa etária, sem que seja necessário revelar ou armazenar dados pessoais adicionais.

Entre essas abordagens estão mecanismos baseados em credenciais verificáveis e técnicas criptográficas de prova de conhecimento zero (*Zero-Knowledge Proofs – ZKP*).

Essas tecnologias permitem que um usuário comprove um atributo específico, por exemplo “é maior de idade”, a partir de uma credencial emitida por fonte fidedigna, sem que o serviço receba ou retenha informações adicionais, como data de nascimento completa, número de documento ou outros dados identificáveis. Dessa forma, a verificação ocorre com exposição mínima de dados pessoais, contribuindo para a observância dos princípios de minimização de dados e proteção da privacidade desde a concepção. Embora não constituam solução única ou obrigatória, abordagens desse tipo ilustram como o desenho técnico das soluções de aferição de idade pode incorporar mecanismos que reduzam a coleta e a circulação de dados pessoais.

A *proteção da privacidade dos usuários*, nesse contexto, também se relaciona à necessidade de que os mecanismos adotados sejam compatíveis com a garantia constitucional da inviolabilidade da intimidade, da vida privada, da honra e da imagem dos usuários, nos termos do art. 5º, X, da Constituição Federal. Da mesma forma, devem igualmente ser observadas outras garantias previstas em normas como o Marco Civil da Internet (Lei nº 12.965/2014), que assegura a inviolabilidade e sigilo do fluxo das comunicações realizadas pela internet, salvo por ordem judicial, na forma da lei. Assim, mecanismos de aferição de idade não podem gerar, direta ou indiretamente, violações à privacidade dos usuários em suas mais diversas dimensões.

No âmbito da proteção de dados pessoais, o princípio da *segurança*, por sua vez, previsto no Art. 6º, VII da LGPD, pressupõe a adoção de medidas técnicas e administrativas aptas a proteger os dados pessoais tratados. No contexto da aferição de idade, é especialmente relevante prevenir acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão de dados. Dessa forma, os dados utilizados no processo de aferição de idade devem permanecer protegidos ao longo de todas as etapas do procedimento, evitando acessos indevidos, incidentes de segurança, reutilizações não autorizadas, conservação por prazo superior ao necessário ou qualquer outro tratamento dissociado da finalidade que justificou sua coleta. Por essa razão, recomenda-se a adoção de salvaguardas técnicas e organizacionais concretamente ajustadas à natureza e à sensibilidade dos dados tratados, às vulnerabilidades do mecanismo de aferição de idade empregado e aos riscos aos titulares.

A *vedação de uso secundário* constitui desdobramento do princípio da finalidade previsto no art. 6º, I da LGPD, que exige que o tratamento de dados pessoais ocorra para propósitos legítimos, específicos, explícitos e informados ao titular, vedando-se tratamentos posteriores incompatíveis com as finalidades que justificaram a coleta. Essa diretriz é expressamente reforçada pelo art. 13 do ECA Digital e pelo art. 24, III, do Decreto, ao dispor que os dados coletados para a verificação de idade de crianças e adolescentes poderão ser utilizados unicamente para essa finalidade, “vedado seu tratamento para qualquer outro propósito”. Disso decorre a vedação à reutilização dos dados para outras finalidades, inclusive publicidade comportamental, perfilamento,

classificação de usuários, enriquecimento cadastral ou extração de informações sobre hábitos, preferências e padrões de navegação.

Em conexão com essa diretriz, a *vedação à rastreabilidade* da identidade e do histórico de acessos, solicitações ou verificações busca impedir que a solução de aferição de idade seja estruturada de modo a permitir a vinculação da identidade do usuário ao seu histórico de navegação ou interações. O mecanismo adotado deve limitar-se ao resultado necessário para a finalidade de proteção, sem permitir o monitoramento continuado da atividade do usuário, a correlação entre acessos ou a formação de histórico de navegação.

Da mesma forma, a *vedação ao compartilhamento contínuo, automatizado e irrestrito* afasta a possibilidade de que a aferição de idade resulte em fluxos permanentes e generalizados de dados pessoais entre múltiplos agentes. Ainda que algum grau de compartilhamento possa ser necessário à operacionalização da solução de aferição de idade, o compartilhamento deve permanecer pontual, delimitado, proporcional e estritamente vinculado à finalidade que o justifica, sem abrir espaço para circulação excessiva de dados pessoais.

Nesse contexto, recomenda-se que os fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável:

- + Incorporem, no desenho do mecanismo de aferição de idade, as obrigações gerais da LGPD e a lógica de privacidade e proteção de dados desde a concepção e por padrão;*
- + Estruturem a solução para tratar apenas o dado ou atributo etário necessário, com limitação de coleta, retenção e uso compatíveis com a finalidade da aferição; e*
- + Implementem salvaguardas técnicas e organizacionais para prevenir usos e tratamentos indevidos de dados, incluindo medidas capazes de atender às vedações de rastreabilidade, uso secundário e compartilhamento contínuo e automatizado de dados pessoais.*

4

⊖ Inclusão e não discriminação

A implementação de mecanismos de aferição de idade deve ser inclusiva e não discriminatória. Essa diretriz decorre do art. 24, X, do Decreto, que estabelece a inclusão e a não discriminação como parâmetros a serem considerados na adoção de técnicas de aferição de idade.

O requisito da *inclusão* implica que os métodos adotados em mecanismos de aferição de idade e sua implementação em produtos e serviços de tecnologia da informação devem considerar “a diversidade de contextos socioeconômicos brasileiros” (art. 10, caput, ECA Digital) e a garantia de “acesso significativo às tecnologias digitais” (art. 5º, § 2º, ECA Digital), além de contribuir para a “redução das desigualdades estruturais nos ambientes digitais que impactem crianças e adolescentes” (art. 4º, IX, Decreto).

Nesse contexto, a implementação desses mecanismos não deve resultar, direta ou indiretamente, na exclusão de usuários da vida digital ou no impedimento desproporcional de acesso a produtos e serviços digitais legítimos, especialmente quando se trata de crianças e adolescentes, que merecem proteção integral e prioritária.

Cabe destacar, ainda em caráter preliminar, que as diferentes arquiteturas de mecanismos de aferição de idade apresentam exigências tecnológicas e materiais distintas, bem como diferentes possibilidades de uso. Soluções baseadas exclusivamente na avaliação de documentos oficiais, por exemplo, podem impor barreiras de acesso indevidas a refugiados ou outras pessoas em situação de vulnerabilidade social que não possuem tais documentos. Da mesma forma, fatores como limitações motoras ou cognitivas, bem como dificuldades de acesso à internet por meio de dispositivos próprios, também devem ser considerados no design dessas soluções.

Assim, mecanismos que imponham obstáculos excessivos ao exercício de direitos ou ao acesso legítimo a produto ou serviço podem não se mostrar compatíveis com a finalidade protetiva que justifica sua adoção. Nesse sentido, recomenda-se que os possíveis obstáculos à inclusão sejam avaliados na escolha da solução adotada e, sempre que cabível, que sejam disponibilizados métodos alternativos de aferição de idade e múltiplas formas de comprovação etária, de modo a contemplar diferentes contextos de uso e reduzir o risco de exclusão indevida.

O requisito da *não discriminação*, por sua vez, possui relação direta com o princípio inscrito no art. 6º, IX, da LGPD, que veda a realização do tratamento para fins discriminatórios ilícitos ou abusivos. Nesse sentido, recomenda-se que os fornecedores de produtos ou serviços de tecnologia da informação adotem medidas para prevenir e mitigar vieses discriminatórios nos mecanismos de aferição de idade para não incorrerem em resultados que impliquem discriminação ilícita ou abusiva.

Determinados métodos podem apresentar diferenças de desempenho entre grupos populacionais distintos. Por exemplo, vieses em mecanismos de aferição de idade, com níveis diferentes de acurácia entre gêneros ou entre grupos raciais e étnicos em métodos de biometria facial, tem o potencial de produzir efeitos discriminatórios.

Nesse contexto, recomenda-se que os fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável:

- + Avaliem previamente se o método adotado pode gerar barreiras desproporcionais de acesso ou produzir efeitos discriminatórios sobre determinados grupos; e*
- + Considerem a adoção de meios alternativos ou complementares de aferição de idade quando a solução principal impuser obstáculos relevantes de acesso ou uso, especialmente sobre pessoas pertencentes a grupos vulneráveis.*

5



Transparência e auditabilidade

Os mecanismos de aferição de idade adotados pelos fornecedores de produtos e serviços de tecnologia da informação devem ser transparentes e auditáveis, conforme art. 24, XI, do Decreto. Especificamente em relação aos provedores de lojas de aplicações de internet e de sistemas operacionais de terminais, o ECA Digital determina que devem tomar medidas auditáveis para aferir a idade ou a faixa etária dos usuários (art. 12, I)⁶.

Considerando que os mecanismos de aferição de idade envolvem, em alguma medida, o tratamento de dados pessoais, sob o prisma da LGPD, os requisitos da transparência e da auditabilidade também estão relacionados com os princípios da transparência e da responsabilização e prestação de contas (art. 6º, VI e X), e com regras relativas aos deveres de informar acerca do tratamento de dados pessoais (art. 9º) e de registro das operações de tratamento (art. 37).

A *transparência*, nesse contexto, implica a necessidade de disponibilização de informações claras, precisas e facilmente acessíveis sobre o funcionamento e a finalidade do mecanismo de aferição de idade, os dados utilizados na atividade, os agentes envolvidos no tratamento e as consequências práticas da aferição de idade. Para atender ao requisito da transparência não se exige o fornecimento de documentos de natureza técnica, contendo quantidades excessivas de informação e de difícil compreensão por pessoas comuns. Embora possa ser útil para a comunidade técnica ou acadêmica e atender a obrigações re-

6 A ANPD disporá oportunamente sobre os requisitos mínimos de transparência dos mecanismos de aferição de idade a serem implementados por lojas de aplicativos e sistemas operacionais, conforme Art. 12, § 3º do ECA Digital.



gulatorias, esse tipo de documento não cumpre o objetivo mais amplo de reduzir assimetrias informacionais e empoderar o usuário. Por isso, é recomendável disponibilizar as informações mais essenciais sobre o funcionamento do mecanismo de aferição de idade, preferencialmente em linguagem simples e em formatos acessíveis, incluindo recursos interativos e visualmente atrativos. Especial atenção deve ser destinada às informações relacionadas ao exercício dos direitos dos titulares previstos no art. 18 da LGPD e à possibilidade de contestação e retificação da idade ou faixa etária aferida, nos termos previstos no art. 25, § 2º, III e 27 do Decreto. Em relação a usuários crianças e adolescentes, é importante levar em consideração a sua autonomia progressiva e as suas características físico-motoras, perceptivas, sensoriais, intelectuais e mentais (art. 14, § 6º, da LGPD).

Por *auditabilidade*, entende-se a capacidade de que o mecanismo de aferição de idade possa ser examinado, inclusive de forma independente, quanto aos seus componentes, procedimentos, operações e registros ao longo do seu ciclo de funcionamento. Para que este requisito seja respeitado, recomenda-se que os fornecedores de produto ou serviço de tecnologia da informação documentem adequadamente o processo de implementação do mecanismo de aferição de idade adotado, incluindo, por exemplo, os testes e dados empíricos utilizados na avaliação da acurácia, robustez e confiabilidade do(s) método(s) escolhido(s).

Uma vez implementado o mecanismo de aferição, recomenda-se, ainda, manter um registro de auditoria (*audit logs*) relacionados ao funcionamento da solução, como registros de acessos concedidos ou acessos negados. Para fins de manutenção dos registros de auditoria, recomenda-se evitar o armazenamento de dados pessoais biométricos, imagens ou dados extraídos de documentos de identidade.

Sempre que possível, os registros de auditoria devem conter apenas metadados funcionais associados ao processo de aferição etária, como o resultado da aferição, o momento do acesso e o método empregado, sem reproduzir os dados pessoais que serviram de insumo ao processo.

Nesse contexto, recomenda-se que os fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável:

- + Informem de forma clara, precisa e acessível a finalidade do mecanismo de aferição utilizado, quais dados são utilizados para tal finalidade, quem são os agentes envolvidos no tratamento e as consequências da aferição de idade;*
- + Disponibilizem canais e procedimentos para contestação e retificação da idade ou faixa etária aferida;*
- + Mantenham registros das ações e decisões associadas ao mecanismo;*
- + Evitem o armazenamento de dados pessoais biométricos, imagens ou dados extraídos de documentos de identidade para fins de audibilidade; e*
- + Garantam integridade, rastreabilidade e possibilidade de auditoria independente de componentes, operações e registros associados ao mecanismo de aferição de idade.*

6



Interoperabilidade

A interoperabilidade refere-se à capacidade de sistemas tecnológicos se comunicarem entre si por meio de formatos e padrões comuns, possibilitando a integração entre diferentes soluções e reduzindo, quando adequado, a necessidade de repetição de procedimentos. No contexto da aferição de idade, trata-se de diretriz relevante para possibilitar a integração e a coordenação do ecossistema tecnológico, inclusive entre sistemas e soluções públicas e privadas.

Cabe destacar que os requisitos mínimos de transparência, segurança e *interoperabilidade* serão objetivo de regulamentação específica da ANPD, nos termos do art. 12, § 3º do ECA Digital. Neste sentido, as orientações apresentadas neste documento possuem caráter preliminar e buscam estabelecer balizas mínimas até a edição da regulamentação posterior, notadamente em relação a especificidades técnicas sujeitas a aprofundamento regulatório.

A diretriz da interoperabilidade pode se concretizar, por exemplo, por meio de arquiteturas baseadas em protocolos padronizados e interfaces de comunicação, aptas a permitir o funcionamento articulado de diferentes métodos de aferição etária, como verificação documental, biometria, credenciais verificáveis, tokens criptográficos, entre outros.⁷

No âmbito do ECA Digital, a interoperabilidade está prevista no art. 12, III. De acordo com este dispositivo, os provedores de lojas de aplicações de internet e sistemas operacionais de terminais deverão possibilitar, por meio de Interface de Programação de Aplicações (API) segura e pautada pela proteção da privacidade desde o padrão, o fornecimento de sinal de idade aos provedores de aplicações de internet, exclusivamente para o cumprimento das finalidades da lei e com sal-

7 AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Mecanismos de aferição de idade*. Brasília, DF: ANPD, 2025. (Radar Tecnológico, n. 5). Disponível em: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/radar-tecnologico-5-mecanismos-de-afericao-de-idade.pdf>. Acesso em: 11 mar. 2026.

vaguadas técnicas adequadas. Por sua vez, o § 3º do mesmo artigo prevê que ato do Poder Executivo regulamentará os requisitos mínimos de transparência, segurança e interoperabilidade para os mecanismos de aferição de idade e de supervisão parental adotados pelos sistemas operacionais e pelas lojas de aplicativos.

No contexto do Decreto, a interoperabilidade também é apresentada como requisito relevante a ser observado na implementação de mecanismos confiáveis de aferição de idade. O art. 24, IX, menciona expressamente a possibilidade de articulação entre sistemas e soluções públicas e privadas, o que se relaciona diretamente com o art. 11 do ECA Digital, que prevê o papel do poder público na promoção de soluções técnicas de aferição de idade.

Para a aferição de idade, a interoperabilidade assume especial relevância uma vez que a repetição sucessiva de procedimentos de verificação pode ampliar a exposição de dados pessoais do usuário, gerar fricções desnecessárias na experiência de uso e multiplicar os pontos de coleta e tratamento de dados. Uma arquitetura interoperável adequadamente estruturada pode contribuir para reduzir esses efeitos, permitindo que o sistema receptor acesse apenas ao resultado estritamente necessário para a finalidade pretendida, sem exigir nova coleta de dados pessoais a cada acesso a produto ou serviço.

Nesse mesmo sentido, o art. 12 do ECA Digital indica que a interoperabilidade não deve ser confundida com a formação de bases integradas extensas, tampouco com transmissão permanente de dados pessoais entre diferentes fornecedores de produto ou serviço de tecnologia da informação. A referência, na própria lei, a APIs seguras, à privacidade por padrão, à minimização de dados e à vedação ao compartilhamento contínuo indicam que o arranjo interoperável deve ser estruturado para transmitir, sempre que possível, apenas o resultado ou atributo étário necessário para aferição de idade.

Entre os exemplos de tecnologias que podem contribuir para esse objetivo estão soluções baseadas em intermediários confiáveis, credenciais verificáveis ou tokens criptográficos. Nessas arquiteturas, o provedor do serviço recebe apenas a confirmação da condição etária necessária para o acesso ou para configuração da experiência do usuário, sem acesso aos dados utilizados no processo de aferição.

Em relação a soluções baseadas em tokens etários criptográficos, embora esses mecanismos possam reduzir a identificação direta do usuário, a transmissão do sinal de idade por API entre verificadores e provedores de serviços pode, em determinadas circunstâncias, introduzir riscos adicionais à privacidade e à segurança. Esse arranjo pode revelar a identidade do provedor destinatário, indicar a finalidade da verificação ou, dependendo do desenho do sistema, ampliar a possibilidade de rastreamento das atividades do usuário.

Para mitigar esse tipo de risco, alguns modelos técnicos utilizam arquitetura duplo-cego (*double-blind*), na qual nenhuma das partes envolvidas no processo de aferição detém conhecimento completo sobre as demais. Nesses arranjos, o verificador terceirizado realiza a aferição de idade sem ter acesso à identidade do provedor de serviços que solicitou a verificação ou ao histórico de acessos do usuário. O provedor de serviços, por sua vez, recebe apenas o resultado da aferição, sem acesso aos dados utilizados pelo verificador para produzi-lo. Esse isolamento mútuo é operacionalizado por meio de mecanismos criptográficos destinados a impedir que o provedor de serviços e o verificador terceirizado tenham conhecimento recíproco um do outro.⁸

A interoperabilidade entre soluções públicas e privadas pode envolver o reaproveitamento do resultado de uma aferição de idade em diferentes serviços, inclusive com o compartilhamento dessa informação entre diferentes soluções e sistemas. Em tese, isso pode reduzir a quantidade de informações que o usuário precisa fornecer novamente quando já houver comprovado sua idade em outro contexto, além de diminuir etapas desnecessárias de verificação.

As estruturas de interoperabilidade podem também potencializar a minimização do tratamento de dados e a redução da exposição do titular, mas exigem atenção quanto à governança, à distribuição de responsabilidades entre os agentes envolvidos, às condições de segurança dos fluxos de informação e aos riscos de concentração excessiva de dados ou o poder informacional em determinados pontos da arquitetura.

8 AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Mecanismos de aferição de idade*. Brasília, DF: ANPD, 2025. (Radar Tecnológico, n. 5). Página 44. Disponível em: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/radar-tecnologico-5-mecanismos-de-afericao-de-idade.pdf>. Acesso em: 11 mar. 2026.

Em termos gerais, a interoperabilidade pode constituir elemento relevante para a construção de soluções mais eficientes e menos onerosas. Sua implementação, contudo, deve permanecer estritamente vinculada à finalidade de aferição etária e ser estruturada em bases compatíveis com a privacidade e a proteção de dados pessoais.

Para que contribua efetivamente para a redução de fricções e da repetição de procedimentos, é importante que sua adoção observe princípios como limitação da finalidade do tratamento, minimização dos dados, segurança dos fluxos informacionais e prevenção de usos indevidos, excessivos ou desvinculados da finalidade que justificou o compartilhamento.

Nesse contexto, recomenda-se que os fornecedores de produtos ou serviços de tecnologia da informação observem as seguintes orientações:

- + Estruturem soluções interoperáveis de modo a permitir apenas a comunicação do atributo etário estritamente necessário para a finalidade pretendida, evitando a circulação do conjunto ampliado de dados pessoais empregado para produzir essa confirmação; e*
- + Definam previamente de forma clara os limites dos fluxos de dados entre os sistemas, incluindo finalidade do compartilhamento, agentes autorizados, salvaguardas de segurança e mecanismos destinados a impedir o compartilhamento contínuo, automatizado e irrestrito de dados pessoais.*

Anexo

Mecanismos confiáveis de aferição de idade Síntese – Orientações Preliminares

Requisitos Mínimos	Fundamentação	Recomendações
Proporcionalidade	Arts. 24, I; e 47 do Decreto. Arts. 6º; 8º, III; 16, parágrafo único, ECA Digital Art. 38, LGPD	<ul style="list-style-type: none">+ Identifiquem e avaliem os riscos associados ao produto ou serviço digital, especialmente os potenciais efeitos adversos sobre a privacidade, a segurança e a saúde de crianças e adolescentes;+ Identifiquem e avaliem os riscos decorrentes do próprio mecanismo de aferição de idade a ser implementado, com atenção aos seus impactos na privacidade e proteção de dados pessoais, especialmente quando envolver o tratamento de dados biométricos; e+ Avaliem a proporcionalidade entre os riscos do produto ou serviço e os riscos decorrentes do mecanismo de aferição de idade a ser implementado.

Requisitos Mínimos	Fundamentação	Recomendações
Acurácia, robustez e confiabilidade	Art. 9º, § 1º, do ECA Digital e art. 24, II, do Decreto.	<ul style="list-style-type: none"> <li data-bbox="573 357 964 656">+ Mensurem e documentem a acurácia dos mecanismos de aferição de idade por eles empregados, utilizando métricas claras e adequadas, com reavaliações periódicas de acordo com o estado da arte da tecnologia para identificar obsolescências e potenciais de aprimoramento; <li data-bbox="573 701 964 999">+ Realizem testes e avaliações de robustez antes e ao longo do uso do mecanismo, adotando medidas para identificar e mitigar riscos de burla e fraude conhecidos ou razoavelmente previsíveis, com atenção especial às formas de contorno que estejam ao alcance de crianças e adolescentes; <li data-bbox="573 1045 964 1272">+ Avaliem, previamente à adoção de uma solução de aferição de idade, a confiabilidade das fontes de dados utilizados no processo, bem como monitorá-las continuamente e documentar eventuais falhas e as medidas corretivas adotadas.

Requisitos Mínimos	Fundamentação	Recomendações
Proteção de dados pessoais	<p data-bbox="365 291 553 482">Arts. 12, I e III, § 1º; 13; e 37, parágrafo único, do ECA Digital. Art. 24, III, IV, V, VI, VII, VIII do Decreto.</p> <p data-bbox="365 531 553 588">Art. 5º, X, da Constituição Federal</p> <p data-bbox="365 637 553 692">Arts. 6º, I, III e VII, da LGPD</p> <p data-bbox="365 741 553 829">Lei nº 12.965/2014 (Marco Civil da Internet)</p>	<p data-bbox="573 291 967 453">+ Incorporem, no desenho do mecanismo de aferição de idade, as obrigações gerais da LGPD e a lógica de privacidade e proteção de dados desde a concepção e por padrão.</p> <p data-bbox="573 501 967 663">+ Estruturem a solução para tratar apenas o dado ou atributo etário necessário, com limitação de coleta, retenção e uso compatíveis com a finalidade da aferição; e</p> <p data-bbox="573 710 967 968">+ Implementem salvaguardas técnicas e organizacionais para prevenir usos e tratamentos indevidos de dados, incluindo medidas capazes de atender às vedações de rastreabilidade, uso secundário e compartilhamento contínuo e automatizado de dados pessoais.</p>
Inclusão e não discriminação	<p data-bbox="365 1029 553 1121">Arts. 5º, § 2º; e 10, caput, do ECA Digital</p> <p data-bbox="365 1170 553 1227">Arts. 4º, IX; e 24, X, do Decreto.</p> <p data-bbox="365 1275 553 1295">Art. 6º, IX, da LGPD</p>	<p data-bbox="573 1029 967 1190">+ Avaliem previamente se o método adotado pode gerar barreiras desproporcionais de acesso ou produzir efeitos discriminatórios sobre determinados grupos; e</p> <p data-bbox="573 1239 967 1468">+ Considerem a adoção de meios alternativos ou complementares de aferição de idade quando a solução principal impuser obstáculos relevantes de acesso ou uso, especialmente sobre pessoas pertencentes a grupos vulneráveis.</p>

Requisitos	Fundamentação	Recomendações
Transparência e auditabilidade	<p data-bbox="366 357 545 418">Arts. 12, I; e 12, § 3º, do ECA Digital</p> <p data-bbox="366 461 524 552">Arts. 24, XI; 25, § 2º, III; e 27, do Decreto.</p> <p data-bbox="366 595 545 690">Arts. 6º, VI e X; 9º; 14, § 6º; e 37, da LGPD</p>	<ul style="list-style-type: none"> <li data-bbox="573 357 967 591">+ Informem de forma clara, precisa e acessível a finalidade do mecanismo de aferição utilizado, quais dados são utilizados para tal finalidade, quem são os agentes envolvidos no tratamento e as consequências da aferição de idade; <li data-bbox="573 635 967 725">+ Disponibilizem canais e procedimentos para contestação e retificação da idade ou faixa etária aferida; <li data-bbox="573 769 967 829">+ Mantenham registros das ações e decisões associadas ao mecanismo; <li data-bbox="573 873 967 1038">+ Evitem o armazenamento de dados pessoais biométricos, imagens ou dados extraídos de documentos de identidade para fins de auditabilidade; e <li data-bbox="573 1081 967 1242">+ Garantam integridade, rastreabilidade e possibilidade de auditoria independente de componentes, operações e registros associados ao mecanismo de aferição de idade.

Requisitos	Fundamentação	Recomendações
Interoperabilidade	Arts. 11; 12, III e § 3º, do ECA Digital Arts. 24, IX, do Decreto.	<ul style="list-style-type: none"> <li data-bbox="573 357 961 621">+ Estruturem soluções interoperáveis de modo a permitir apenas a comunicação do atributo etário estritamente necessário para a finalidade pretendida, evitando a circulação do conjunto ampliado de dados pessoais empregado para produzir essa confirmação; e <li data-bbox="573 670 961 965">+ Definem previamente de forma clara os limites dos fluxos de dados entre os sistemas, incluindo finalidade do compartilhamento, agentes autorizados, salvaguardas de segurança e mecanismos destinados a impedir o compartilhamento contínuo, automatizado e irrestrito de dados pessoais.

www.gov.br/anpd



Agência Nacional de
Proteção de Dados