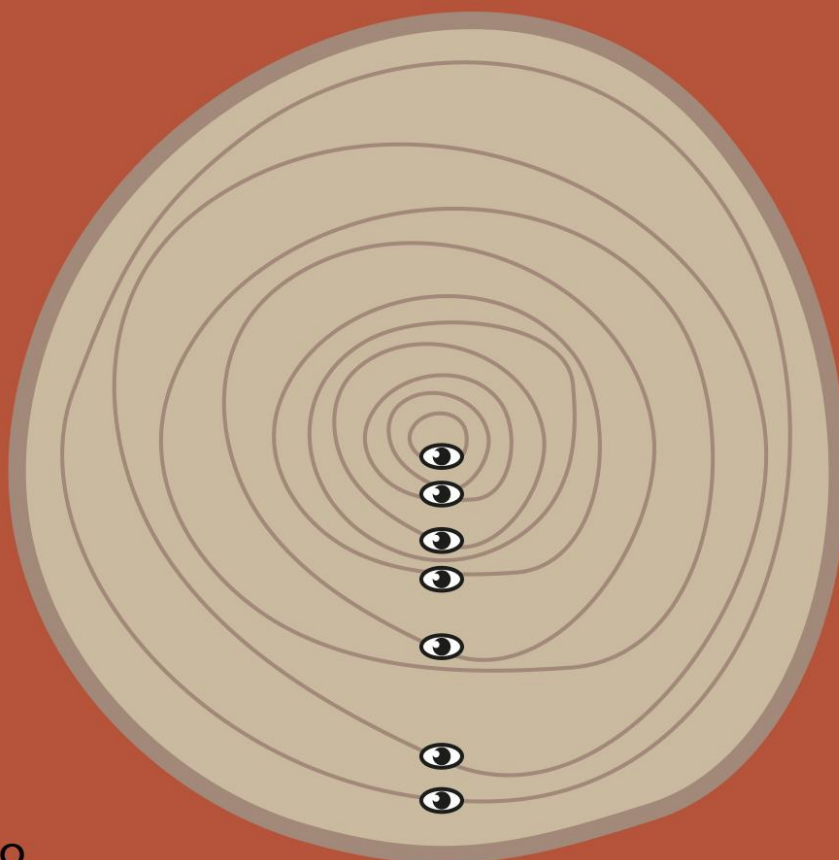


AFERIÇÃO *de* IDADE *no* ECA DIGITAL

CONTRIBUIÇÕES À TOMADA
DE SUBSÍDIOS ANPD



Juliano
MARANHÃO
Bernardo
FICO
Ana Laura
AZEVEDO
Thiago
POLONI

Sobre o Legal Wings Institute

O Legal Wings Institute é um instituto independente, com atuação autônoma na produção de conhecimento, pesquisa, análise regulatória e promoção de debates públicos sobre direito, tecnologia, inovação, ética e regulação. Sua atuação se desenvolve com independência intelectual e metodológica, por meio da elaboração de estudos, relatórios, eventos, conteúdos e iniciativas de interlocução com diferentes setores.

O Instituto trabalha de forma colaborativa com atores do setor público, privado, acadêmico e da sociedade civil e conta com apoios institucionais, parcerias e patrocínios, que não implicam qualquer compromisso interesses específicos dos parceiros, nem condicionam suas agendas, métodos, análises ou conclusões.

Para conhecer mais sobre o Legal Wings e consultar as informações disponibilizadas em seus canais oficiais, incluindo os sponsors/apoiadores do Instituto, acesse o site oficial: <https://www.legalwings.com.br>.

O Instituto Legal Wings parabeniza a iniciativa da Autoridade Nacional de Proteção de Dados na elaboração do Guia Orientativo sobre mecanismos de aferição de idade no âmbito do ECA Digital. Trata-se de esforço relevante para conferir maior previsibilidade regulatória à aplicação da Lei nº 15.211/2025 e para orientar a implementação de medidas de proteção de crianças e adolescentes em ambientes digitais. Não obstante, identificamos pontos que merecem maior densificação, a fim de aprimorar a segurança jurídica, a coerência regulatória e a utilidade prática do documento.

Objeto da contribuição

A presente contribuição tem por objetivo auxiliar no aprimoramento das orientações do Guia quanto aos mecanismos de aferição etária, especialmente em contextos de risco moderado e alto. Sustenta-se que **a aferição de idade não deve ser compreendida apenas como providência pontual**, realizada no momento do cadastro, do primeiro acesso ou da obtenção inicial de um sinal etário, mas como processo contínuo de preservação da confiabilidade desse sinal ao longo da utilização do serviço.

A lacuna identificada está na possibilidade de a minuta ainda ser interpretada a partir de uma lógica predominantemente estática da aferição etária. Essa leitura pode ser insuficiente em serviços digitais dinâmicos, nos quais o risco pode se alterar ao longo do tempo em razão de mudanças de funcionalidade, recomendação algorítmica, integração com terceiros, alteração do catálogo de conteúdos, compartilhamento de contas, uso por terceiros, criação de múltiplas contas, tentativas de burla ou inconsistência entre diferentes sinais disponíveis.

Nesse contexto, a contribuição propõe que o Guia explicita a possibilidade de adoção de modelos dinâmicos, graduais e proporcionais de aferição etária, inclusive com o uso responsável de sistemas de inteligência artificial, para preservar, revisar ou reforçar o grau de confiança atribuído ao sinal etário quando houver elementos que indiquem possível inadequação da classificação inicial.

O objetivo é oferecer parâmetros para que a aferição etária seja tratada como mecanismo efetivo de proteção de crianças e adolescentes no ambiente digital, sem que isso resulte em coleta excessiva de dados, vigilância permanente, perfilamento indevido ou fricções desproporcionais para os usuários.

Para desenvolver esse argumento, a contribuição está organizada em três eixos: **(1)** a aferição etária como processo contínuo, com a distinção entre aferição pontual e reavaliação posterior da confiabilidade do sinal etário; **(2)** a compatibilização dessa reavaliação com os princípios da minimização de dados, da proporcionalidade, da gradação por níveis de risco e da baixa fricção; e **(3)** o papel da inteligência artificial como ferramenta complementar de manutenção da confiabilidade do sinal etário, bem como as salvaguardas necessárias para evitar vieses, usos secundários, vigilância excessiva e perfilamento indevido.

1. Aferição etária como processo contínuo e diferentes formas de verificação

Inicialmente, é importante reconhecer que o Guia reconhece adequadamente a necessidade de reavaliação periódica dos mecanismos de aferição etária, especialmente para identificar obsolescências, limitações e oportunidades de aprimoramento.¹ Essa orientação poderia, contudo, ser aprofundada para abranger não apenas a revisão técnica dos mecanismos utilizados, mas também a reavaliação da confiabilidade do sinal etário atribuído ao usuário no momento do cadastro, a fim de verificar se essa classificação permanece adequada ao longo da utilização do serviço e se continua correspondendo à pessoa que efetivamente acessa a plataforma.

Sob essa perspectiva, a aferição etária não deve ser tratada como providência isolada, concluída com a criação da conta ou com o primeiro acesso ao serviço. Embora a aferição inicial seja etapa relevante para obtenção de uma declaração, estimativa, verificação ou outro sinal de idade, ela não elimina a necessidade de preservar, ao longo da relação de uso, grau adequado de confiança quanto à correspondência entre a faixa etária atribuída à conta e a idade da pessoa que efetivamente utiliza a plataforma.

Isso permite distinguir a aferição pontual da aferição contínua. A primeira ocorre em momento determinado, como o cadastro, o acesso a uma área restrita ou a realização de determinada transação. A segunda compreende medidas posteriores destinadas a confirmar, atualizar ou revisar a confiança atribuída ao sinal inicial, seja em intervalos compatíveis com as características do serviço, seja diante de circunstâncias que indiquem erro, desatualização, burla, compartilhamento de conta ou utilização por pessoa diversa.

A necessidade dessa distinção decorre do fato de que mesmo mecanismos iniciais robustos podem ser contornados. Subsistem riscos de uso de dados de terceiros, compartilhamento de contas ou dispositivos, criação de múltiplas contas, alteração de informações cadastrais e outras estratégias de evasão. Por isso, a aferição inicial não deve ser considerada suficiente por si só, sobretudo em contextos de risco moderado ou alto.

Essa necessidade de preservação da confiabilidade da classificação inicial encontra respaldo na orientação do *Office of Communications* (Ofcom), autoridade reguladora independente do setor de comunicações e responsável pela supervisão da segurança online no Reino Unido, segundo a qual a repetição da aferição pode reforçar a robustez do método, especialmente em situações de compartilhamento de contas ou dispositivos e nos casos em que crianças tenham sido inicialmente classificadas como adultas.²

A aferição contínua, contudo, não exige repetição integral da verificação inicial. Não se trata de submeter o usuário, a cada acesso, ao reenvio de documentos, à repetição de procedimentos biométricos ou a novas etapas invasivas de confirmação. A reavaliação deve ser gradual e proporcional, pois, ainda que o procedimento realizado no cadastro seja tecnicamente robusto, subsistem riscos de fraude, uso de dados de terceiros, compartilhamento de contas, erro de classificação e adoção de estratégias destinadas a contornar o controle inicial. Pesquisa realizada pela *Internet Matters* em 2025 com 1.270 crianças e adolescentes de 9 a 16 anos constatou que 32% dos participantes haviam burlado controles etários nos dois meses

¹ Cf. p. 25-26 do referido guia.

² OFFICE OF COMMUNICATIONS. **Guidance on highly effective age assurance: for Part 3 services.** Londres: Office of Communications, 24 abr. 2025, p. 16

anteriores à coleta dos dados, inclusive mediante a inserção de data de nascimento falsa, o uso de contas, dispositivos ou documentos de terceiros e o emprego de imagens destinadas a enganar mecanismos de estimativa facial.³ Nesse contexto, os dados evidenciam que a etapa inicial de aferição pode ser burlada e, por isso, não deve ser tratada como suficiente por si só.

Essa questão reforça a necessidade da aferição contínua, entendida como a possibilidade de reavaliar a classificação etária ao longo do uso do serviço quando houver elementos que coloquem em dúvida a confiabilidade do sinal inicialmente obtido. Ademais, essa lógica encontra apoio nas orientações da *eSafety Commissioner*, que recomenda medidas destinadas a prevenir, detectar e responder à burla, como exigir nova aferição em caso de alteração da idade autodeclarada, monitorar mudanças cadastrais que possam indicar transferência indevida da conta, identificar múltiplas contas associadas ao mesmo dispositivo ou endereço IP e utilizar sinais técnicos ou comportamentais para detectar atividades irregulares.⁴

Um exemplo de como essa reavaliação pode ser operacionalizada sem se converter em verificação permanente é apresentado no relatório da *Age Assurance Technology Trial*, conduzida pela *Age Check Certification Scheme*, organismo independente de avaliação da conformidade especializado em tecnologias de aferição etária e contratado pelo governo australiano para executar o estudo. O relatório registra, com base em fontes públicas, que grandes plataformas digitais, especialmente redes sociais, podem adotar modelos de validação sucessiva nos quais sinais observados durante o uso são confrontados com a idade anteriormente declarada ou atribuída. Nesses modelos, uma nova avaliação tende a ser acionada apenas quando surgem contraindícios relevantes, como alterações nas informações declaradas, padrões de linguagem, conexões ou formas de utilização aparentemente incompatíveis com a idade registrada e inconsistências entre dispositivos ou serviços. A plataforma pode, então, iniciar um processo gradual, começando pela reavaliação dos sinais disponíveis, pela solicitação de confirmação no próprio aplicativo ou pela consulta a informações alternativas, e recorrer a documentos, envolvimento parental ou restrições temporárias somente quando a dúvida persistir, especialmente nas proximidades de um limiar etário juridicamente relevante⁵ e reservando-se os métodos mais intrusivos às situações em que as alternativas anteriores se mostrem insuficientes e em que o risco associado à decisão justifique a obtenção de grau mais elevado de certeza.

Desse modo, o objetivo da aferição contínua consiste em manter, ao longo do tempo, grau de confiança compatível com a finalidade e com o risco da decisão etária, sem exigir padrão uniforme para todos os serviços, conteúdos e funcionalidades. Evidências menos intrusivas podem ser suficientes para decisões de menor impacto, enquanto o acesso a conteúdos, produtos ou atividades vedados a menores pode justificar verificação mais robusta ou a combinação de diferentes mecanismos. A forma de aferição deve, portanto, acompanhar a relevância da decisão e as consequências de eventual classificação incorreta, sem converter a proteção etária em instrumento de vigilância permanente.

³ INTERNET MATTERS. **The Online Safety Act: are children safer online?** Londres: Internet Matters, maio 2026, p. 6 e 16.

⁴ AUSTRÁLIA. eSafety Commissioner. **Social Media Minimum Age Regulatory Guidance**. Canberra: eSafety Commissioner, set. 2025, seção 2.4.3, p. 40.

⁵ AGE CHECK CERTIFICATION SCHEME. **Age Assurance Technology Trial: Part F: Successive Validation**. Age Check Certification Scheme, 2025, p. 43-45.

2. Minimização de dados, proporcionalidade, múltiplos níveis de risco e baixa fricção

A compreensão da aferição etária como processo contínuo exige definir de que modo a confiabilidade de um sinal já atribuído ao usuário pode ser revista sem produzir tratamento desproporcional de dados. O Guia oferece bases importantes para essa análise ao estabelecer que a solução de aferição deve ser proporcional ao risco associado ao serviço e que a escolha do mecanismo deve considerar, conjuntamente, os riscos do produto ou serviço, os impactos do próprio método de aferição e o contexto, a natureza e as funcionalidades do ambiente digital⁶. A presente contribuição propõe aplicar essa mesma lógica também às reavaliações realizadas após o ingresso do usuário na plataforma.

A aplicação dessa lógica às reavaliações exige que a minimização prevista no art. 6º, III, da Lei Geral de Proteção de Dados (LGPD) seja compreendida como a limitação do tratamento aos dados adequados, pertinentes e necessários à finalidade concreta, e não como a adoção automática do mecanismo que utilize o menor volume absoluto de dados.⁷ Na aferição etária contínua, isso significa que a plataforma não deve repetir, por rotina, procedimentos invasivos quando o sinal já disponível permanece confiável. A minimização, contudo, também não impede nova aferição quando fatos posteriores reduzam de forma relevante a confiança na classificação existente.

Quando a reavaliação envolver dados pessoais de crianças e adolescentes, o agente deverá justificar de forma mais rigorosa o uso de dados adicionais e demonstrar que o tratamento permanece limitado ao que seja indispensável à finalidade pretendida.⁸ A escolha deve considerar, ao mesmo tempo, a eficácia do mecanismo e seus efeitos sobre a privacidade, a proteção de dados e os demais direitos envolvidos, de modo que, entre soluções de eficácia comparável, seja adotada a menos intrusiva.⁹ O recurso a uma medida mais rigorosa somente se justifica quando a dúvida que motivou a reavaliação persistir ou quando o risco de uma classificação incorreta exigir grau superior de confirmação, isto é, em situações como acesso a conteúdo destinado ao público adulto.

Esse juízo de necessidade e menor intrusividade deve orientar também a intensidade da reavaliação posterior, eis que a resposta adotada deve guardar correspondência com a natureza da dúvida identificada e com os riscos decorrentes da manutenção de uma classificação possivelmente incorreta. Por isso, nem toda inconsistência justifica a repetição integral do procedimento realizado no cadastro. Indícios relevantes de burla, compartilhamento de conta, uso por terceiros, divergência entre sinais ou perda de validade de uma credencial podem reduzir o grau de confiança anteriormente estabelecido e exigir confirmação adicional. Ainda assim, a medida escolhida deve limitar-se ao necessário para esclarecer a incerteza concreta,

⁶ Ibidem, p. 16-17.

⁷ MARTINS, Guilherme Magalhães. **A Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018) e a sua principiologia**. Revista dos Tribunais, São Paulo, v. 1027, ano 110, p. 203-243, maio 2021, p. 217.

⁸ ZANATTA, Rafael; VALENTE, Jonas; MENDONÇA, Júlia. Entre o abusivo e o excessivo: novos contornos jurídicos para o tratamento de dados pessoais de crianças e adolescentes na LGPD. In: LATERÇA, Priscilla et al. (coord.). **Privacidade e proteção de dados de crianças e adolescentes**. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro; Obliq, 2021, p. 396-426, especialmente p. 410 e 415.

⁹ LUEKS, Wouter et al. **Assessing age assurance technologies: effectiveness, side-effects, and acceptance**. arXiv, 2026, p. 7.

escalonando-se a intervenção apenas quando alternativas menos intrusivas forem insuficientes ou quando o risco associado à decisão exigir grau superior de certeza.

Nesse sentido, o próprio Guia já define de forma clara e adequada os parâmetros para esse escalonamento, ao distinguir contextos de baixo, moderado e alto risco e relacioná-los a diferentes graus de exigência e exemplos de mecanismos de aferição¹⁰. Essa estrutura, coerente, flexível e compatível com a proporcionalidade, pode orientar tanto a escolha inicial do mecanismo quanto as reavaliações realizadas ao longo do uso. Aplicada à aferição contínua, essa lógica permite que inconsistências surgidas em serviços ou funcionalidades de baixo risco sejam tratadas, em primeiro lugar, por medidas de menor impacto, como a confirmação da validade de uma credencial, a atualização de um sinal já disponível ou a solicitação de esclarecimento complementar ao usuário. Métodos mais intrusivos, como nova verificação documental ou biométrica, ficam reservados às hipóteses em que essas alternativas se mostrem insuficientes e em que o risco decorrente de uma classificação incorreta exija grau superior de confiança.

A necessidade de reavaliação pode surgir não porque a aferição inicial tenha sido inadequada, mas porque o nível de certeza exigido se altera conforme o uso do serviço. Em funcionalidades de baixo risco, é legítimo adotar mecanismos menos intrusivos e, por consequência, com menor grau de robustez, desde que suficientes para aquele contexto. Se, posteriormente, o usuário passa a acessar conteúdos, interações, transações ou funcionalidades de maior risco, a classificação etária antes suficiente pode deixar de oferecer o grau de confiança necessário para a nova decisão. Nessa hipótese, a revisão do sinal não corrige necessariamente um erro anterior, mas adapta a aferição à mudança de contexto, permitindo que mecanismos adicionais ou mais robustos sejam acionados apenas quando o uso efetivo do serviço passe a exigir maior certeza quanto à idade.

Essa dinâmica, contudo, não autoriza o acompanhamento permanente e indiferenciado da atividade do usuário, pois a inferência baseada em comportamento pode exigir o tratamento de informações muito mais amplas do que aquelas estritamente necessárias à aferição da idade e acabar incorporada a sistemas já utilizados para formar perfis comerciais.¹¹ A reavaliação deve, portanto, estar ligada a circunstâncias que tornem a classificação existente insuficiente para uma decisão concreta, como a expiração de uma credencial, a divergência entre sinais ou o acesso a uma funcionalidade sujeita a restrição etária. Em vez de monitorar continuamente o comportamento do usuário, a plataforma deve limitar a nova aferição ao momento e aos dados necessários para esclarecer a inconsistência identificada.

A incorporação da reavaliação à experiência do usuário deve observar os princípios da necessidade e da proporcionalidade, de modo que revisões motivadas por circunstâncias concretas não resultem, como regra, em interrupções, etapas adicionais ou novas coletas de dados. Nesse contexto, a baixa fricção decorre da própria minimização, pois contribui para reduzir verificações repetidas, evitar novos pontos de coleta e limitar a exposição desnecessária de dados pessoais. Deve-se, por isso, priorizar o reaproveitamento seguro do resultado já

¹⁰ Ibidem, p. 17-19, Tabela 3.

¹¹ SHAFFIQUE, Mohammed Raiz; VAN DER HOF, Simone. Behavioural profiling for age assurance: do the ends justify the means? *International Data Privacy Law*, v. 16, n. 1, mar. 2026, p. 9-11.

obtido, especialmente mediante credenciais etárias que permitam confirmações posteriores sem nova apresentação de documentos ou compartilhamento reiterado dos dados utilizados na etapa inicial¹².

Enquanto a credencial permanecer válida e adequada ao contexto de uso, a repetição integral do procedimento tende a ser dispensável. Uma nova aferição, mais abrangente, deve ficar restrita às situações em que o sinal tenha expirado, sido revogado ou deixado de oferecer grau de confiança suficiente para a decisão a ser tomada. Esse escalonamento permite preservar a confiabilidade da classificação etária e, ao mesmo tempo, reduzir obstáculos desnecessários ao usuário.

Para compreender esse escalonamento, pode-se recorrer à experiência dos mecanismos de prevenção a fraudes empregados pelo setor financeiro, nos quais, após a identificação e a autenticação do cliente, as operações habituais seguem o fluxo ordinário, enquanto transações atípicas ou incompatíveis com o perfil de uso podem acionar controles adicionais. Nessa linha, o Regulamento do Pix prevê soluções capazes de identificar situações dessa natureza e autoriza, conforme o risco verificado, a ampliação da análise, a rejeição da operação ou o bloqueio cautelar dos recursos.¹³ A intensidade da verificação acompanha, portanto, os elementos concretos de risco associados a cada operação.

Essa mesma estrutura de controles graduais pode orientar a aferição etária contínua, de modo que a reutilização do sinal existente permaneça adequada enquanto ele for válido e compatível com o contexto de uso. A ocorrência de circunstâncias que reduzam a confiança anteriormente estabelecida, como divergências entre sinais, expiração da credencial ou acesso a funcionalidade de maior risco, pode justificar o reforço gradual da confirmação. A analogia restringe-se ao escalonamento das medidas conforme o risco identificado, sem transpor para a aferição etária as formas de monitoramento próprias das operações financeiras.

A partir dessa perspectiva, a minimização deve orientar a definição das medidas de reavaliação, o momento de sua adoção e o grau de intensidade adequado, preservando-se o sinal inicial enquanto ele oferecer confiança suficiente, com o emprego de mecanismos de baixa fricção diante das primeiras inconsistências e a reserva de procedimentos mais robustos para as hipóteses em que a dúvida persista ou a relevância da decisão exija maior grau de certeza. A aferição contínua configura, assim, um processo gradual de manutenção da confiabilidade da classificação etária, capaz de confirmá-la, atualizá-la ou corrigi-la conforme as circunstâncias verificadas ao longo do uso.

3. Inteligência Artificial como Instrumento de Aferição Contínua do Sinal Etário

Conforme desenvolvido nos tópicos anteriores, a aferição etária, especialmente em contextos de risco moderado e alto, não deve ser compreendida como uma medida que se esgota no momento do cadastro ou na obtenção inicial de um sinal etário. Isso porque a finalidade desses mecanismos não consiste apenas em atribuir uma determinada faixa etária ao usuário em um momento específico, mas em assegurar, ao longo de toda a utilização do serviço, que o

¹² POH, Norman; BURNS, Daryl. **Biometric bound credentials for age verification**. In: INTERNATIONAL CONFERENCE OF THE BIOMETRICS SPECIAL INTEREST GROUP, 24., 2025, Darmstadt. 2025, p. 4 e 6.

¹³ BANCO CENTRAL DO BRASIL. **Resolução BCB nº 403, de 22 de julho de 2024**. Altera o Regulamento do Pix, especialmente o art. 89, § 1º. Brasília, DF: Banco Central do Brasil, 2024.

acesso a conteúdos, funcionalidades e experiências digitais permaneça compatível com o seu estágio de desenvolvimento. Em outras palavras, a efetividade da proteção conferida pela legislação depende não apenas da obtenção inicial de um sinal etário confiável, mas também da capacidade de preservar esse grau de confiança ao longo do tempo, diante de mudanças de contexto, uso compartilhado de contas, utilização por terceiros, criação de múltiplas contas, manipulação de dados cadastrais ou outras formas de evasão.

3.1 IA como ferramenta complementar de manutenção da confiabilidade do sinal etário

A preocupação com a preservação da confiabilidade do sinal etário ao longo do tempo é coerente com a própria lógica regulatória adotada pelo Decreto nº 12.880/2026 e pelo Guia. Isso porque ambos adotam uma concepção ampla de aferição de idade¹⁴, reconhecendo a existência de diferentes mecanismos e métodos de aferição que podem ser utilizados de forma isolada ou combinada, conforme o risco associado ao serviço, produto ou funcionalidade específica. A experiência comparada (e.g. UK-ICO) também sustenta que a escolha do método de *age assurance* deve depender da avaliação do risco que o serviço gera para crianças e adolescentes, da necessidade dessa aferição, e da proporcionalidade do mecanismo escolhido.¹⁵ Conforme a Ofcom, a aferição etária efetiva deve observar critérios de acurácia técnica, robustez, confiabilidade e justiça, razão pela qual mecanismos baseados em IA ou aprendizado de máquina devem ser avaliados por meio de testes, monitoramento, indicadores de desempenho e investigação de resultados inesperados.¹⁶

A utilização de ferramentas baseadas em inteligência artificial pode desempenhar papel relevante na construção de modelos dinâmicos de aferição etária¹⁷. Sua função não deve ser a de substituir, em todos os casos, mecanismos mais robustos de verificação documental, biométrica ou baseada em credenciais confiáveis, mas a de operar como camada complementar de manutenção da confiabilidade do sinal etário. Em serviços de risco moderado ou alto, a simples verificação inicial pode não ser suficiente para enfrentar hipóteses posteriores de fraude, compartilhamento de contas ou burla deliberada. Ao mesmo tempo, a reaplicação constante de mecanismos documentais ou biométricos pode gerar fricção excessiva, exclusão injustificada e coleta desproporcional de dados. A IA pode, nesse intervalo, auxiliar na identificação de inconsistências, padrões de uso incompatíveis com a faixa etária declarada ou

¹⁴ BRASIL. Decreto nº 12.880, de 18 de março de 2026, art. 2º, IV. Para fins do disposto neste Decreto, considera-se: [...] IV - aferição de idade - 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;

¹⁵ Information Commissioner's Office (ICO). Expectations for age assurance and data protection compliance. In: Age Assurance for the Children's Code. Disponível em: <https://ico.org.uk/about-the-ico/what-we-do/information-commissioners-opinions/age-assurance-for-the-children-s-code/6-expectations-for-age-assurance-and-data-protection-compliance/>

¹⁶ OFCOM. *Age assurance duties under the Online Safety Act*. Disponível em: <https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/age-assurance>

¹⁷ A utilização de IA para apoio à aferição etária já vem sendo adotada por grandes plataformas digitais. A Meta, por exemplo, informou utilizar sistemas de IA para identificar possíveis inconsistências entre a idade declarada pelo usuário e outros sinais disponíveis na plataforma. Segundo a empresa, a tecnologia analisa elementos contextuais presentes no perfil e na atividade do usuário, além de indícios visuais extraídos de fotos e vídeos. Quando esses sinais sugerem que o usuário pode pertencer a uma faixa etária diversa da informada, a plataforma pode aplicar proteções compatíveis com a idade estimada ou exigir etapas adicionais de verificação. Cf. META. New AI-Powered Age Assurance Measures to Place Teens in Age-Appropriate Experiences (2026)

sinais que indiquem a necessidade de revalidação, escalonamento ou revisão do grau de confiança atribuído ao usuário.

A literatura técnica e os modelos regulatórios recentes têm tratado esse tipo de abordagem como uma lógica de “aferição em camadas”, “validação sucessiva” ou “step-up assurance”. No teste australiano de tecnologias de aferição etária,¹⁸ a validação sucessiva foi descrita como a combinação de dois ou mais métodos para alcançar uma decisão mais precisa, proporcional ao risco ou capaz de aumentar o nível de confiança quando um método isolado não for suficiente. O mesmo relatório descreve modelos em que a plataforma inicia a análise etária por sinais comportamentais ou métodos de menor fricção, escalando para estimativa biométrica ou verificação documental apenas quando o resultado é incerto ou quando o usuário está próximo de um limiar etário relevante. Essa lógica é particularmente útil para o Guia, pois permite compatibilizar a proteção de crianças e adolescentes, a minimização de dados e a boa experiência do usuário.

3.2 Salvaguardas para utilização de IA em mecanismos de aferição etária

A utilização de IA nesse contexto, contudo, exige salvaguardas específicas. A adoção de modelos inferenciais ou de estimativa etária deve ocorrer de forma proporcional, transparente e alinhada aos princípios da proteção de dados, especialmente finalidade, necessidade, minimização, qualidade dos dados, prevenção, segurança e responsabilização. A ICO¹⁹ orienta que dados coletados para *age assurance* não sejam reutilizados para finalidades incompatíveis, como perfilamento publicitário, e que a coleta se limite ao mínimo necessário para alcançar o nível adequado de certeza sobre a idade do usuário; a mesma conclusão pode ser tida em relação às proibições de perfilamento mercadológico no ECA Digital, e às orientações de minimização de dados provenientes da LGPD. No mesmo sentido, a declaração internacional sobre *age assurance*²⁰ afirma que os provedores devem demonstrar que suas soluções são proporcionais, efetivas, preservam privacidade e observam o melhor interesse da criança, sem transformar a proteção em barreira indevida de acesso à internet. Isso porque os mecanismos de aferição etária devem ser utilizados como uma forma de alcançar a proteção de crianças e adolescentes *no* ambiente digital, e não *do* ambiente digital.

A efetividade do sistema depende diretamente da qualidade, diversidade e representatividade dos dados empregados. O relatório técnico do NIST sobre estimativa e verificação de idade demonstra que a acurácia de algoritmos de estimativa facial é influenciada por variáveis como algoritmo, sexo, qualidade da imagem, região de nascimento, *idade* e interações entre esses fatores, inexistindo um algoritmo uniformemente superior em todos os

¹⁸ AGE CHECK CERTIFICATION SCHEME (ACCS). *Age Assurance Technology Trial – Part F: Successive Validation*. Stockport, UK: ACCS, 2025. Disponível em: https://ageassurance.com.au/wp-content/uploads/2025/08/AATT_Part_F_DIGITAL.pdf

¹⁹ Information Commissioner's Office (ICO). Expectations for age assurance and data protection compliance. In: Age Assurance for the Children's Code. Disponível em: <https://ico.org.uk/about-the-ico/what-we-do/information-commissioners-opinions/age-assurance-for-the-children-s-code/6-expectations-for-age-assurance-and-data-protection-compliance/>

²⁰ Information Commissioner's Office (ICO) et al. Joint Statement on a Common International Approach to Age Assurance. 6 set. 2024. Disponível em: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/joint-statement-on-a-common-international-approach-to-age-assurance/principles/>

recortes.²¹ O mesmo relatório aponta que a estimativa etária envolve desafios técnicos relacionados a iluminação, foco, distorção, apresentação do sujeito, óculos, pelos faciais, cosméticos, características fenotípicas e diferenças demográficas associadas a sexo e etnia.

Estudo recente do governo britânico²² sobre acesso a dados para *age assurance* observa que ferramentas de estimativa facial ainda enfrentam limitações para distinguir usuários em faixas etárias estreitas, como menores de 13 ou de 18 anos, e podem apresentar vieses relacionados a gênero, tom de pele e etnia; o mesmo **estudo associa parte dessas limitações à escassez de bases de treinamento e teste suficientemente representativas, especialmente envolvendo crianças**. Portanto, o Guia poderia reconhecer expressamente que a construção de modelos confiáveis de aferição etária pode demandar bases de dados amplas, diversas e representativas dos grupos etários que se pretende proteger, inclusive com dados de menores de idade, desde que observadas bases legais adequadas, salvaguardas éticas, limitação de finalidade, minimização, segurança, avaliação de impacto e mecanismos de auditoria.

A utilização de dados de crianças e adolescentes para treinamento, validação ou teste de sistemas de IA não é, contudo, trivial. Ainda que a LGPD não classifique dados de menores como sensíveis *per se*, a condição peculiar de desenvolvimento dos titulares impõe ônus argumentativo reforçado ao controlador, especialmente quanto à demonstração de necessidade, adequação, proporcionalidade e compatibilidade com o melhor interesse da criança e do adolescente. Ao mesmo tempo, a ausência de bases de dados adequadas pode gerar vieses, erros sistemáticos de classificação e redução da efetividade protetiva que o sistema busca alcançar. O problema regulatório, portanto, não deve ser formulado como uma oposição abstrata entre proteção de dados e uso de dados para treinamento, mas como uma questão de governança. Quando o tratamento for necessário para desenvolver modelos destinados à proteção infantojuvenil, ele deve ocorrer sob salvaguardas reforçadas, controle de acesso, documentação técnica, avaliação de impacto, testes de paridade de erro e mecanismos de supervisão.

A experiência comparada oferece parâmetros úteis para essa orientação. A Ofcom²³ exige que componentes baseados em IA ou aprendizado de máquina sejam treinados e testados com bases que reflitam a diversidade da população-alvo, além de avaliados quanto à paridade de resultados e de erros para evitar vieses ou impactos discriminatórios. O padrão ISO/IEC 27566-1:2025²⁴, por sua vez, estrutura a aferição etária como conjunto de processos e métodos

²¹ HANAOKA, Kayee K. et al. Face Analysis Technology Evaluation: Age Estimation and Verification. Gaithersburg, MD: National Institute of Standards and Technology (NIST), 2024. (NIST Interagency/Internal Report - NIST IR 8525). Disponível em: <https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8525.pdf>

²² UNITED KINGDOM. Department for Science, Innovation and Technology (DSIT). Age Assurance Data Access Study. Londres: DSIT, 2026. Disponível em: <https://www.gov.uk/government/publications/age-assurance-data-access-study/age-assurance-data-access-study>

²³ Ofcom. Age assurance duties under the Online Safety Act. Londres: Office of Communications, 2024. Disponível em: <https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/age-assurance>

²⁴ International Organization for Standardization (ISO); International Electrotechnical Commission (IEC). ISO/IEC 27566-1:2025 — Information security, cybersecurity and privacy protection — Age assurance systems — Part 1: Framework. Genebra: ISO/IEC, 2025. Disponível em: https://assets.vde-verlag.de/iec-normen/preview-pdf/info_isoiec27566-1%7Bed1.0%7Den.pdf

para verificar, estimar ou inferir idade ou faixa etária, com diferentes graus de certeza, e destaca características como funcionalidade, desempenho, privacidade, segurança e aceitabilidade.

Além das salvaguardas relacionadas à qualidade e representatividade dos dados utilizados no treinamento dos modelos, a adoção de IA para aferição contínua deve ser acompanhada de limites claros contra vigilância excessiva ou perfilamento indevido. Conforme observado no relatório australiano de tecnologias de *age assurance*²⁵, modelos de inferência contínua utilizados por plataformas baseadas em contas (e.g., redes sociais) podem contribuir para a identificação de inconsistências etárias ao longo do tempo, mas também apresentam riscos acrescidos de monitoramento comportamental constante, reutilização de sinais para finalidades distintas da aferição etária e expansão progressiva da pegada digital dos usuários. Assim, embora modelos contínuos ou sucessivos possam preservar a confiabilidade do sinal etário, sua adoção pode gerar riscos cumulativos de monitoramento comportamental, inferências secundárias e ampliação indevida de finalidade.

Diante desses riscos, mecanismos inferenciais de aferição etária deveriam ser estruturados de modo compatível com os princípios da ISO/IEC FDIS 27566-1²⁶, privilegiando o uso contextual dos dados, evitando a expansão desnecessária da pegada digital dos usuários e estabelecendo limites claros para a reutilização das informações coletadas. Além disso, a governança desses sistemas deve contemplar mecanismos de transparência, supervisão e revisão das conclusões inferenciais produzidas, de modo a assegurar que a aferição etária permaneça vinculada à sua finalidade específica e não se converta em instrumento de monitoramento permanente do comportamento dos usuários.²⁷

Por essa razão, o Guia deveria recomendar que reavaliações automatizadas sejam acionadas apenas por critérios previamente definidos, proporcionais ao risco e explicáveis ao usuário; que os dados utilizados para aferição etária sejam segregados de sistemas de publicidade, recomendação ou perfilamento comercial; que sinais de idade sejam preferencialmente armazenados como faixas, níveis de confiança ou respostas binárias, e não como dados brutos; que haja prazo de retenção limitado; e que usuários disponham de mecanismos acessíveis de contestação, revisão e correção de classificações incorretas. O relatório australiano²⁸ sobre validação sucessiva aponta precisamente a necessidade de governança clara, critérios transparentes de escalonamento, minimização, separação entre dados usados para inferência etária e sistemas gerais de perfilamento, e auditabilidade granular para assegurar aplicação justa e consistente.

Conclusão

A utilização de inteligência artificial em mecanismos de aferição etária deve ser compreendida como ferramenta complementar relevante para preservar a confiabilidade do

²⁵ Age Check Certification Scheme (ACCS). Age Assurance Technology Trial – Part E: Age Inference. Stockport: ACCS, 2025.

²⁶ International Organization for Standardization (ISO). ISO/IEC 27566-1: Age assurance systems — Part 1: Framework. Geneva: ISO, 2025. Disponível em: <https://www.iso.org/standard/88143.html>

²⁷ Age Check Certification Scheme (ACCS). Age Assurance Technology Trial – Part E: Age Inference. Op. cit.

²⁸ Age Check Certification Scheme (ACCS). Age Assurance Technology Trial - Part F: Successive Validation. Op cit.

sinaleário ao longo da utilização do serviço, especialmente em contextos de risco moderado e alto. Essa tecnologia pode reforçar a proteção de crianças e adolescentes contra conteúdos, produtos e serviços incompatíveis com sua faixa etária, reduzir a dependência de verificações documentais repetidas e contribuir para a prevenção de burla. Sua adoção, contudo, deve estar condicionada a salvaguardas específicas de transparência, proporcionalidade, governança de dados, representatividade das bases de treinamento, mitigação de vieses, acurácia, robustez, confiabilidade, segurança, auditabilidade e mecanismos de contestação. Por essa razão, seria recomendável que o Guia tratasse expressamente da IA como camada possível de aferição contínua e validação sucessiva, oferecendo parâmetros mínimos para sua utilização responsável no contexto da proteção infantojuvenil.

Bibliografia

AGE CHECK CERTIFICATION SCHEME. **Age Assurance Technology Trial: Part E: Age Inference.** [S. l.]: ACCS, 2025. Disponível em: <https://ageassurance.com.au/publications/report-e/>. Acesso em: 9 jul. 2026.

AGE CHECK CERTIFICATION SCHEME. **Age Assurance Technology Trial: Part F: Successive Validation.** [S. l.]: ACCS, 2025. Disponível em: https://ageassurance.com.au/wp-content/uploads/2025/08/AATT_Part_F_DIGITAL.pdf. Acesso em: 9 jul. 2026.

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS. **Guia orientativo: mecanismos de aferição de idade.** Versão preliminar submetida à tomada de subsídios. Brasília, DF: ANPD, maio 2026. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/eca-digital/>. Acesso em: 9 jul. 2026.

AUSTRÁLIA. 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: 9 jul. 2026.

BANCO CENTRAL DO BRASIL. **Resolução BCB nº 403, de 22 de julho de 2024.** Altera a Resolução BCB nº 1, de 12 de agosto de 2020, que institui o arranjo de pagamentos Pix e aprova o seu regulamento, e o regulamento anexo. Brasília, DF: Banco Central do Brasil, 2024. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?numero=403&tipo=Resolu%C3%A7%C3%A3o+BCB>. Acesso em: 9 jul. 2026.

BRASIL. **Decreto nº 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 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: 9 jul. 2026.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais. Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 9 jul. 2026.

BRASIL. **Lei nº 15.211, de 17 de setembro de 2025.** Dispõe sobre a proteção de crianças e adolescentes em ambientes digitais — Estatuto Digital da Criança e do Adolescente. Brasília, DF: Presidência da República, 2025. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/l15211.htm. Acesso em: 9 jul. 2026.

HANAOKA, Kayee K.; GROTH, Patrick J.; NGAN, Mei Lee; YANG, Joyce; QUINN, George W.; HOM, Austin. **Face Analysis Technology Evaluation: Age Estimation and Verification.** Gaithersburg, MD: National Institute of Standards and Technology, 2024. NIST Interagency/Internal Report 8525. DOI: 10.6028/NIST.IR.8525. Disponível em: <https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8525.pdf>. Acesso em: 9 jul. 2026.

INFORMATION COMMISSIONER'S OFFICE. **Age assurance for the Children's Code: expectations for age assurance and data protection compliance.** Wilmslow: ICO, [s. d.]. Disponível em: <https://ico.org.uk/about-the-ico/what-we-do/information-commissioners-opinions/age-assurance-for-the-children-s-code/6-expectations-for-age-assurance-and-data-protection-compliance/>. Acesso em: 9 jul. 2026.

INFORMATION COMMISSIONER'S OFFICE et al. **Joint Statement on a Common International Approach to Age Assurance.** 6 set. 2024. Disponível em: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/joint-statement-on-a-common-international-approach-to-age-assurance/>. Acesso em: 9 jul. 2026.

INTERNET MATTERS. **The Online Safety Act: Are Children Safer Online?** Londres: Internet Matters, maio 2026. Disponível em: <https://www.internetmatters.org/wp-content/uploads/2026/04/Internet-Matters-Online-Safety-Act-Report-May-2026.pdf>. Acesso em: 9 jul. 2026.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. **ISO/IEC 27566-1:2025: Information security, cybersecurity and privacy protection — Age assurance systems — Part 1: Framework.** Genebra: ISO, 2025. Disponível em: <https://www.iso.org/standard/88143.html>. Acesso em: 9 jul. 2026.

LUEKS, Wouter; DREYER, Stephan; FEDERRATH, Hannes; SIMON, Judith. **Assessing Age Assurance Technologies: Effectiveness, Side-Effects, and Acceptance.** arXiv, 26 mar. 2026. arXiv:2603.25695. DOI: 10.48550/arXiv.2603.25695. Disponível em: <https://arxiv.org/abs/2603.25695>. Acesso em: 9 jul. 2026.

MARTINS, Guilherme Magalhães. A Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018) e a sua principiologia. **Revista dos Tribunais**, São Paulo, ano 110, v. 1027, p. 203-243, maio 2021. Disponível em:

<https://www.mprj.mp.br/documents/20184/2668029/artigoaleigeraldeprotecaodedadospessoais.pdf>. Acesso em: 9 jul. 2026.

META. **New AI-Powered Age Assurance Measures to Place Teens in Age-Appropriate Experiences**. 5 maio 2026. Disponível em: <https://about.fb.com/news/2026/05/ai-age-assurance-teens/>. Acesso em: 9 jul. 2026.

OFFICE OF COMMUNICATIONS. **Age Assurance Duties under the Online Safety Act**. Londres: Ofcom, 23 fev. 2024. Disponível em: <https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/age-assurance>. Acesso em: 9 jul. 2026.

OFFICE OF COMMUNICATIONS. **Guidance on Highly Effective Age Assurance: for Part 3 Services**. Londres: Ofcom, 24 abr. 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: 9 jul. 2026.

POH, Norman; BURNS, Daryl. Biometric Bound Credentials for Age Verification. In: INTERNATIONAL CONFERENCE OF THE BIOMETRICS SPECIAL INTEREST GROUP, 24., 2025. **Proceedings of the 24th International Conference of the Biometrics Special Interest Group — BIOSIG 2025**. Darmstadt: IEEE, 2025. p. 1-5. DOI: 10.1109/BIOSIG65492.2025.11358017. Disponível em: <https://dl.gi.de/bitstreams/e8ee6a62-2bce-4a98-963c-f32729266216/download>. Acesso em: 9 jul. 2026.

SHAFFIQUE, Mohammed Raiz; VAN DER HOF, Simone. Behavioural profiling for age assurance: do the ends justify the means? **International Data Privacy Law**, Oxford, v. 16, n. 1, p. 1-13, mar. 2026. DOI: 10.1093/idpl/ipaf012. Disponível em: <https://academic.oup.com/idpl/article/16/1/ipaf012/8327959>. Acesso em: 9 jul. 2026.

UNITED KINGDOM. Department for Science, Innovation and Technology. **Age Assurance Data Access Study**. Londres: DSIT, 26 mar. 2026. Disponível em: <https://www.gov.uk/government/publications/age-assurance-data-access-study/age-assurance-data-access-study>. Acesso em: 9 jul. 2026.

ZANATTA, Rafael; VALENTE, Jonas; MENDONÇA, Júlia. Entre o abusivo e o excessivo: novos contornos jurídicos para o tratamento de dados pessoais de crianças e adolescentes na LGPD. In: LATERÇA, Priscilla Silva; FERNANDES, Elora; TEFFÉ, Chiara de; BRANCO, Sérgio (coord.). **Privacidade e proteção de dados de crianças e adolescentes**. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro; Obliq, 2021. p. 396-426. Disponível em: https://www.dataprivacybr.org/wp-content/uploads/2021/11/ppd_crianças_its_compressed-1.pdf. Acesso em: 9 jul. 2026.