Mecanismos de aferição de idade: proporcionalidade, minimização e governança

Autores:

Beatriz Fazan

| Advogada da área de Governança de Dados do b/luz

Thiago Xavier Peregrino

| Advogado da área de Governança de Dados do b/luz

Revisores:

Felipe Gabriades

| Sócio da área de Governança de Dados do b/luz

Fernando Bousso

| Sócio coordenador das áreas de Tecnologia, Governança de Dados e Mídia e Entretenimento do b/luz

b/luz

b/luz

Sumário

Introdução

A proteção de crianças e adolescentes em meios digitais vem ganhando cada vez mais relevância no Brasil. Conforme abordado em nosso último material sobre o tema, a publicação de Lei nº 15.211/2025 (Estatuto Digital da Criança e do Adolescente ou "ECA Digital") consolidou alguns pontos relevantes sobre medidas de preservação do melhor interesse de crianças e adolescentes na internet. A entrada em vigor do ECA Digital e a publicação do Decreto nº 12.880/2026 ("Decreto Regulamentador") nos dias 17 e 18 de março de 2026, respectivamente, indicam a necessidade de discussão sobre termos chave da regulamentação. Neste material, nos dedicaremos aos mecanismos de aferição de idade.

Para fins de clareza terminológica, adotaremos as definições previstas no Decreto Regulamentador e pela ANPD[1] ao considerar "aferição de idade" como um termo geral que abrange os procedimentos destinados a verificar, estimar ou inferir, direta ou indiretamente, a idade ou a faixa etária de um usuário, por meio de diferentes métodos e tecnologias; e a "verificação de idade" como uma modalidade específica de aferição, caracterizada pela confirmação da idade ou da faixa etária com base em evidências diretas (a estimativa e a inferência, por sua vez, operam por aproximação ou dedução indireta a partir de dados biométricos, comportamentais ou contextuais).

Ao final deste material, apresentamos dois anexos com caráter complementar: o Anexo I, com um resumo dos próximos passos para empresas no contexto aqui explorado, e o Anexo II, com um guia estruturado para avaliação de mecanismos de aferição de idade, consolidando os critérios discutidos ao longo do texto. Importante destacar, contudo, que os mecanismos de aferição de idade representam apenas um dos eixos regulatórios introduzidos pelo ECA Digital, de modo que a norma também contempla outras frentes relevantes voltadas à proteção de crianças e adolescentes no ambiente digital, como medidas de controle parental, design seguro e limitações à oferta de determinados conteúdos e funcionalidades.

A restrição do acesso de crianças e adolescentes a situações inapropriadas parte da mesma lógica existente no mundo offline. Para garantir que somente adultos tenham participação em certos contextos, devem ser estabelecidas barreiras no acesso a determinados locais, conteúdos ou produtos. Essas barreiras, no mundo digital, são materializadas nos denominados mecanismos de aferição de idade. Existem diversas possibilidades que permitem verificar de idade dos usuários online, ao contrário do que temos no mundo físico, em que, no geral, a forma de aferição é limitada à checagem de documentos de identidade.

1 BRASIL. Agência Nacional de Proteção de Dados. **Radar Tecnológico 5 - Mecanismos de aferição de idade**. Versão 1.0. Brasília, DF, 2025. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/radar-tecnologico-5-mecanismos-de-afericao-de-idade.pdf/view. Acesso em: 20 abr. 2026.

No cenário em que pessoas geralmente encarregadas de fazer a aferição de idade são substituídas por softwares, APIs e empresas, esses mecanismos trazem consigo uma preocupação com relação à proteção dos dados pessoais coletados para a aferição de idade. Ao contrário de uma pessoa, que tem capacidade relativamente limitada de armazenamento e possibilidade reduzida de uso posterior dos dados pessoais checados (como nome, CPF e data de nascimento), sistemas tecnológicos têm capacidade praticamente ilimitada de guardar essas informações e de reutilizá-las para finalidades posteriores – o que costuma depender de simples configurações. Por isso, quando pensamos no ambiente digital, as preocupações de privacidade se intensificam.

No próximo tópico serão explorados os princípios que orientam a implementação dos mecanismos de aferição de idade, conforme indicado pelo ECA Digital e no Decreto Regulamentador.

1. Princípios para adoção de soluções de aferição de idade

Antes de avançar na análise dos mecanismos de aferição de idade, é importante destacar que a ANPD, em suas orientações preliminares[2], sistematiza o tema a partir de seis requisitos fundamentais que devem orientar a implementação dessas soluções:

Proporcionalidade	O mecanismo adotado deve ser compatível com o nível de risco do serviço, evitando soluções insuficientes e excessivamente intrusivas.
Acurácia, robustez e confiabilidade	Refere-se ao grau de precisão com que o mecanismo consegue identificar corretamente a idade ou a faixa etária do usuário, a capacidade do sistema de resistir a tentativas de fraude, e a consistência dos resultados ao longo do tempo e em diferentes contextos de uso.
Privacidade e proteção de dados pessoais	A aferição deve ser realizada com o mínimo possível de dados, com segurança e vedação de usos indevidos, em linha com os princípios da LGPD.
Inclusão e não discriminação	Os mecanismos não devem criar barreiras desproporcionais de acesso ou gerar efeitos discriminatórios entre diferentes grupos.
Transparência e auditabilidade	Os processos devem ser compreensíveis para os usuários e passíveis de inspeção, inclusive por autoridades e terceiros independentes.
Interoperabilidade	Diferentes sistemas devem poder se comunicar de forma segura e eficiente, evitando redundâncias e reduzindo a necessidade de coleta repetitiva de dados.

2 BRASIL. Agência Nacional de Proteção de Dados. **Mecanismos confiáveis de aferição de idade: orientações preliminares**. Versão 1.0. Brasília, DF, 2026. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/eca-digital/mecanismos-confiaveis-de-afericao-de-idade-orientacoes-preliminares.pdf/view. Acesso em: 6 de abril de 2026.

2. Debate atual: os mecanismos mais relevantes

Os mecanismos de aferição de idade evoluíram paralelamente ao desenvolvimento das tecnologias digitais e à sofisticação dos modelos de negócio baseados em dados. Atualmente, é possível agrupá-los em diferentes categorias, cada qual com características próprias, distintos níveis de confiabilidade e diferentes impacto sob a perspectiva de proteção de dados pessoais.

Abaixo, abordamos exemplos de mecanismos já reconhecidos, incluindo hipóteses de uso dentro do cenário digital.

2.1. Autodeclaração e mecanismos declaratórios

A forma mais simples e historicamente difundida de aferição de idade consiste na autodeclaração do usuário, normalmente operacionalizada por meio da disponibilização de campo para inserção de data de nascimento ou confirmação de maioridade (como o botão de *"declaro que sou maior de 18 anos"*).

Trata-se de mecanismo de baixa fricção na jornada de interação com o usuário e custo reduzido. Contudo, sua eficácia é limitada, uma vez que depende exclusivamente da veracidade da informação prestada pelo próprio usuário, sem qualquer elemento de validação adicional.

Em linha com o já disposto no ECA Digital, o Decreto Regulamentador reitera que a autodeclaração não configura mecanismo válido de aferição de idade, vedando sua utilização tanto para desbloqueio de acesso quanto para conclusão de operações envolvendo conteúdos, produtos ou serviços restritos a adultos. O texto regulamentar exige a adoção de mecanismos "efetivos" de aferição de idade, reforçando que a simples declaração do usuário pode ser insuficiente.

> **Exemplo 1 – Confirmação do usuário:** Ao acessar uma página com conteúdo restrito, o usuário visualiza um aviso informando que o ambiente é destinado apenas a maiores de 18 anos. Para prosseguir, deve clicar em um botão com a mensagem *"Confirmo que tenho mais de 18 anos"*. Depois do clique, o sistema libera imediatamente o acesso ao conteúdo. Nesse caso, como o acesso depende apenas da informação fornecida pelo próprio usuário, sem qualquer validação adicional, trata-se de autodeclaração.
>
> **Exemplo 2 – Cadastro com CPF e data de nascimento:** Durante a criação de uma conta, a plataforma exige que o usuário informe seu CPF e sua data de nascimento em campos obrigatórios. A partir das informações inseridas, o sistema apenas valida se o CPF existe e utiliza a data de nascimento para definir se a conta poderá ser criada e quais funcionalidades ficarão disponíveis.
>
> Embora haja coleta do CPF, a plataforma apenas valida sua existência, sem que haja qualquer consulta ou validação da veracidade da data de nascimento em bases externas, de modo que o sistema considera como verdadeiros os dados fornecidos pelo próprio usuário. Como a classificação depende apenas da informação fornecida pelo próprio usuário, sem qualquer validação independente, trata-se de autodeclaração.

2.2. Verificação documental

Outra categoria de mecanismos de afeição de idade baseia-se na validação de informações de fontes externas estruturadas, associadas à identidade civil do usuário. Nesses casos, ocorre a verificação de idade, decorrente de um dado previamente estabelecido, como a data de nascimento constante em documentos oficiais ou em bases de dados confiáveis.

O exemplo mais comum consiste no envio de documento de identificação, como RG ou CNH, por meio de captura de imagem ou upload. A partir dessas informações, o sistema extrai os dados para confirmar que o usuário é o mesmo do documento fornecido, e verifica suas informações de idade através da data de nascimento. Esse método funciona como uma adaptação da verificação de documento físico, como tradicionalmente utilizado para permitir a entrada em determinados estabelecimentos ou viabilizar a compra de produtos destinados a maiores de idade.

Em comparação com a autodeclaração, o mecanismo de verificação documental aumenta significativamente o nível de segurança e confiabilidade da verificação. Por outro lado, implica tratamento de mais dados pessoais e a participação de terceiros, o que demanda atenção em relação a temas como necessidade, minimização e segurança.

> **Exemplo 3 – Captura de documento via câmera:** Durante o cadastro, o usuário é instruído a utilizar a câmera do dispositivo para fotografar seu documento de identidade. O sistema orienta o posicionamento do documento e realiza a leitura automatizada dos dados. A data de nascimento extraída é utilizada para determinar a idade do usuário e permitir a continuidade do fluxo. Como a aferição etária se baseia em dados obtidos a partir de documento oficial apresentado pelo usuário, trata-se de verificação documental.

2.3. Biometria

Outra categoria relevante compreende os mecanismos baseados no uso de características biométricas do usuário. Diferentemente da verificação documental, essas soluções operam a partir de atributos físicos do próprio indivíduo e podem ser utilizadas tanto para fins de identificação quanto para estimativa de idade.

Como será exposto a seguir, os mecanismos biométricos podem assumir diferentes níveis de confiabilidade a depender da forma como são implementados. Enquanto técnicas de comparação biométrica são utilizadas para autenticação de identidade, soluções baseadas em inferência apresentam natureza probabilística e, em geral, menor grau de robustez.

2.3.1. Biometria com comparação prévia

Uma primeira modalidade consiste na utilização de biometria para validação de identidade, por meio de técnicas de reconhecimento biométrico, como a comparação facial. Nesses casos, a biometria é utilizada para confirmar que o indivíduo que realiza

o procedimento corresponde a uma identidade previamente fornecida, normalmente vinculada a um documento ou cadastro validado.

Essa abordagem é frequentemente utilizada em combinação com mecanismos de verificação documental, nos quais o usuário submete um documento de identidade e realiza uma captura biométrica, que é comparada com a imagem previamente registrada. Essa imagem pode ter sido obtida no próprio fluxo de verificação ou estar armazenada em bases de dados previamente constituídas. A aferição da idade, nesse modelo, não decorre da biometria em si, mas da informação constante no documento ou registro validado. Assim, a biometria atua como mecanismo de autenticação, assegurando que o usuário corresponde ao titular da identidade previamente verificada.

Esse método surge, por exemplo, em sistemas e plataformas que demandam maior nível de precisão na detecção e confirmação de identidade do usuário que tenta acessá-la, como em aplicativos bancários. Nesses casos, os dados biométricos são coletados para validação da identidade do usuário, que não deve ser confundida com verificação de idade. Quando utilizados com propósito único de identificação da idade do titular, o recomendado é que os dados biométricos sejam descartados após a verificação e não utilizados para identificar o usuário quando não necessário.

2.3.2. Inferência de idade por sinais biométricos e comportamentais

Outra abordagem consiste na estimativa da idade a partir de inferências baseadas em características do usuário, como análise facial para estimativa etária, padrões de voz ou até comportamento de navegação (por exemplo, velocidade de digitação ou histórico de consumo de conteúdo). O objetivo é estimar a idade provável do indivíduo com base em modelos estatísticos, sem necessariamente identificar de forma direta a pessoa. Esses modelos são desenvolvidos a partir de grandes bases de dados, compostas por milhares de imagens, áudios e registros comportamentais previamente rotulados com as respectivas idades dos usuários. Assim, a abordagem não depende de uma identidade previamente validada, baseando-se na inferência de atributos a partir de modelos estatísticos.

Um dos principais desafios dessa abordagem é a acurácia. Em termos práticos, a acurácia diz respeito à probabilidade de o sistema classificar corretamente um indivíduo dentro de uma faixa etária relevante. Esse aspecto é particularmente crítico em idades limítrofes.

Outro ponto sensível diz respeito à possibilidade de discriminação algorítmica. Sistemas de inferência de idade podem apresentar desempenho desigual entre diferentes grupos populacionais. Por exemplo, no caso de pessoas com deficiência, pessoas não brancas, idosos ou pessoas em situações de vulnerabilidade socioeconômica, características biométricas ou comportamentais podem divergir dos padrões dos datasets de treinamento dos sistemas e cálculo dos modelos estatísticos, aumentando a probabilidade de classificações incorretas.

Ainda, mecanismos baseados em sinais comportamentais pressupõem que o dispositivo utilizado seja de uso individual, refletindo padrões consistentes de um único usuário. No entanto, em cenários de acesso limitado e compartilhamento de terminais de acesso, os padrões coletados podem comprometer a confiabilidade das inferências realizadas. Nesse contexto, é especialmente relevante a implementação de mecanismos de contestação e revisão de decisões automatizadas, permitindo que o usuário questione classificações incorretas e tenha acesso a alternativas razoáveis para comprovação de sua idade.

Vale destacar que além dos métodos atualmente implementados de forma mais ampla relacionados à aferição biométrica, outras metodologias estão surgindo com base em novos estudos científicos e avanço tecnológico. Por exemplo, no cenário internacional há empresas[3] que oferecem tecnologias de aferição de idade na análise do movimento e fisionomia das mãos de um titular[4]. Essas tecnologias promissoras ainda são recentes e, portanto, não há difusão acerca de sua eficácia e viabilidade.

Exemplo 4 – Comparação facial com documento: Durante o processo de verificação, o usuário é solicitado a enviar a imagem de um documento de identidade e, em seguida, realizar uma captura facial. O sistema compara a imagem capturada com a foto constante no documento apresentado. Após a confirmação de correspondência entre as imagens, a data de nascimento presente no documento é utilizada para verificar a idade do usuário. Como a biometria é utilizada em conjunto com o documento para confirmar que o indivíduo é o titular da identidade apresentada, e a idade decorre da informação constante no documento validado, trata-se de identificação biométrica combinada com verificação documental.

Exemplo 5 – Estimativa de idade por análise facial: Ao acessar determinada funcionalidade, o usuário autoriza o uso da câmera do dispositivo. O sistema captura a imagem do rosto e aplica um modelo de análise facial para estimar a idade provável do indivíduo. Com base na estimativa gerada, o sistema classifica o usuário em uma faixa etária e permite ou restringe o acesso. Como a aferição da idade ocorre diretamente a partir da análise de características biométricas, sem utilização de documento ou base externa, trata-se de inferência de estimativa de idade por análise biométrica.

Exemplo 6 – Aferição de idade por perfil comportamental: Um usuário já logado em determinada rede é submetido à aferição de idade através de tecnologia automatizada, com base no seu comportamento de uso da plataforma. Os perfis que o usuário segue, como ele interage com outros usuários, a velocidade de digitação e suas publicações determinam, com base na comparação com uma base de dados de outros usuários, se seu perfil comportamental é compatível com o de um usuário maior de idade. Como os dados comportamentais são utilizados para indicar a idade do usuário, trata-se de aferição de idade por sinais comportamentais.

3 MCCONVEY, J. **BorderAge promises 100% anonymous age assurance with hand gesture modality**. Biometric Update. Web, 2026. Disponível em: <https://www.biometricupdate.com/202501/borderage-promises-100-anonymous-age-assurance-with-hand-gesture-modality>. Acesso em: 9 de abril de 2026.

4 ABDERRAHMANE, M. et al. **Human Age Prediction Based on Hand Image using Multiclass Classification**. International Conference on Data Analytics for Business and Industry: Way Towards a Sustainable Economy. Bahrein, 2020. Disponível em: <https://www.researchgate.net/publication/348637921_Human_Age_Prediction_Based_on_Hand_Image_using_Multiclass_Classification>. Acesso em: 9 de abril de 2026.

2.4. Aferição por uso de meios de pagamento

Possível também mencionar os mecanismos baseados na autenticação de meios de pagamento. Nesses casos, a utilização de instrumentos financeiros, como cartões de crédito, funciona como indicador indireto de maioridade, diante da presunção de que um usuário que possui meio próprio de pagamento é maior de idade.

Esse mecanismo pode também ser compreendido como indício de supervisão ou consentimento de pais ou responsáveis, já que ainda que um menor de idade tenha acesso ao meio de pagamento de um pai ou responsável, há uma presunção de ciência da parte deles sobre os gastos realizados pelo menor. Esse tipo de solução é frequentemente adotado em serviços digitais pagos, como forma de introduzir uma camada adicional de controle de acesso, ainda que criticado diante da possibilidade de exclusão de camadas mais vulneráveis da sociedade, da falta de precisão e do potencial de fraude.

> **Exemplo 7 – Validação por meio de cartão de crédito:** Para acessar determinado conteúdo, o usuário deve inserir os dados de um cartão de crédito válido. O sistema realiza a autorização do meio de pagamento junto ao emissor, validando assim os dados de pagamento inseridos. A existência de um instrumento financeiro válido vinculado ao usuário é utilizada para permitir o acesso à funcionalidade. Como a aferição se apoia em um elemento externo associado a um instrumento financeiro, trata-se de aferição por meio de pagamento.

2.5. Tokens, credenciais e provas criptográficas de idade

Mais recentemente, surgiram soluções baseadas em credenciais digitais e mecanismos criptográficos que permitem comprovar atributos, como “ser maior de 18 anos”, em que o compartilhamento de dados pessoais é, em tese, limitado. Embora amplamente discutidos no plano teórico e em iniciativas internacionais, esses modelos ainda apresentam baixa adoção prática no mercado, especialmente em aplicações de larga escala.

Trata-se dos modelos baseados em provas de zero conhecimento (zero-knowledge proofs – “ZKP”) e arquiteturas de duplo cego (double-blind). Em linhas gerais, as ZKP permitem que um usuário prove a veracidade de uma informação sem revelar qualquer dado subjacente. Já os modelos de duplo cego estruturam a interação de modo que nenhuma das partes envolvidas tenha visibilidade completa sobre a transação: o emissor da credencial não sabe onde ela será utilizada, e o provedor do serviço não tem acesso à identidade do usuário.

Embora ambos os modelos tenham como objetivo central a preservação da privacidade, há distinções relevantes. As ZKP são um mecanismo criptográfico específico que viabiliza a prova sem revelação, enquanto o duplo cego refere-se a uma arquitetura de fluxo de informações, que pode ou não incorporar técnicas como ZKP para reforçar garantias de não rastreabilidade. Em conjunto, essas abordagens buscam assegurar que apenas o atributo necessário seja compartilhado, sem exposição de dados adicionais.

No entanto, a implementação envolve desafios relevantes. Do ponto de vista técnico e

operacional, trata-se de soluções complexas e, em geral, custosas, tanto em termos de desenvolvimento quanto de integração com sistemas existentes.

Outro ponto importante é que esses modelos não eliminam, por completo, a necessidade de mecanismos prévios de aferição de identidade ou idade. Em regra, a emissão inicial da credencial ou token depende da utilização de outros métodos, como validação documental ou biométrica, para assegurar que a maioridade foi corretamente atribuída ao usuário. A diferença central está na arquitetura: uma vez emitida, a credencial pode ser utilizada de forma dissociada desses dados originais.

> **Exemplo 8 – Emissão e uso de credencial digital de maioridade:** Antes de acessar um serviço com restrição etária, o usuário realiza um processo de verificação de idade junto a um provedor confiável. Nesse fluxo, o usuário envia a imagem de um documento de identidade e, em seguida, realiza uma captura facial em tempo real, conforme instruções do sistema. A imagem capturada é comparada com a fotografia constante no documento, com o objetivo de confirmar que o usuário é o titular da identidade apresentada. Após a validação da correspondência, o sistema extrai a data de nascimento do documento e confirma que o usuário atende ao requisito de maioridade. ***Nessa etapa, há verificação documental combinada com autenticação biométrica por comparação facial.***
>
> Após a validação, o provedor emite uma credencial digital associada ao usuário, contendo apenas a informação necessária, como a confirmação de que é maior de 18 anos, sem incluir dados como nome, CPF ou data de nascimento. Essa credencial é armazenada em carteira digital ou aplicação sob controle do usuário. ***Nessa etapa, há minimização de dados e separação entre identidade civil e atributo etário.***
>
> Ao acessar um serviço com restrição de idade, o usuário apresenta a credencial. O sistema solicita apenas a comprovação do atributo etário, sem acesso aos dados originais utilizados na verificação inicial. ***Nessa etapa, há dissociação entre o dado verificado e o dado compartilhado.***
>
> A validação da credencial pode ocorrer por meio de protocolos criptográficos que permitem comprovar a maioridade sem revelação de dados adicionais. Nesse fluxo, o provedor da credencial não tem visibilidade sobre qual serviço está sendo acessado, e o serviço não tem acesso à identidade do usuário. ***Nessa etapa, observam-se características de provas criptográficas e arquitetura de duplo cego.***
>
> Como a verificação ocorre a partir de um atributo previamente certificado, com compartilhamento limitado de informações e sem exposição da identidade do usuário, trata-se, em uma análise global, de modelo baseado em credenciais digitais.

2.6. Ambientes de teste e integração sistêmica no ecossistema digital

Mecanismos de aferição vêm também sendo inseridos em ecossistemas mais amplos, como ambientes de testes regulatórios (testbeds) e soluções integradas a infraestruturas digitais, como identidades digitais governamentais, carteiras digitais e sistemas operacionais.

Destaca-se, nesse contexto, a experiência da União Europeia com a implementação da *European Digital Identity Wallet*[5], que prevê um modelo interoperável de identidade

5 COMISSÃO EUROPEIA. **European Digital Identity Wallet**. Bruxelas, 2024. Disponível em: <https://digital-strategy.ec.europa.eu/en/factpages/european-digital-identity-wallet>. Acesso em: 9 de abril de 2026.

digital no qual usuários poderão armazenar e compartilhar atributos verificados, incluindo prova de idade, de forma seletiva e segura. Esse método, apesar de elogiado no cenário internacional, apresenta uma dificuldade de adoção no Brasil, considerando o desafio de letramento digital[6] e acesso à internet em diversas regiões do país[7].

Nessa lógica, a aferição de idade deixa de ser uma funcionalidade isolada e passa a compor uma arquitetura mais ampla de identidade e confiança digital. Isso permitiria maior consistência na aplicação de controles etários, além de potencial redução de redundâncias na coleta de dados.

Por outro lado, esses sistemas não operam de forma autônoma. Os mecanismos integrados ao ecossistema digital dependem de outros processos de aferição, como validação documental, biométrica ou outros métodos robustos, para assegurar a confiabilidade dos atributos que serão posteriormente compartilhados. A inovação sendo testada, portanto, não reside na eliminação dessas etapas, mas na forma como elas são organizadas e reutilizadas dentro de uma infraestrutura interoperável.

2.7. Momento da aferição de idade no fluxo do usuário

Além da escolha do mecanismo, outro aspecto relevante diz respeito ao momento em que a aferição de idade é realizada no fluxo de interação com o usuário. A aferição pode ocorrer em diferentes etapas, como no primeiro acesso ao serviço, no momento de criação de conta, na conclusão de uma compra ou no ingresso em áreas específicas da plataforma.

A definição desse momento impacta diretamente a experiência do usuário, o nível de fricção do serviço e a efetividade do controle implementado, devendo ser considerada em conjunto com o nível de risco associado à atividade.

2.8. Confiabilidade dos mecanismos de aferição de idade

Os mecanismos de aferição de idade podem ser organizados conforme o grau de dependência da informação prestada pelo usuário, a existência de validação externa e a capacidade de resistir a tentativas de burla.

Em uma ponta, situam-se os mecanismos declaratórios, que dependem exclusivamente da autodeclaração. Em seguida, encontram-se modelos baseados em inferência, que estimam a idade a partir de características do usuário. Em níveis intermediários, estão soluções que se apoiam em elementos externos indiretos, como meios de pagamento e mecanismos de verificação documental. Em patamares mais elevados de confiabilidade, destacam-se modelos que combinam verificação documental com autenticação biométrica.

6 BRASIL. Agência Nacional de Telecomunicações. **Boletim de Diagnóstico: Habilidades Digitais no Brasil e no Mundo**. Brasília, 2024. Disponível em: <https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?8-74Kn1tDR89f1Q7RjX8EYU46IzCFD26Q9Xx5QNDbqbl-GuBQvTrV78dFpuB7IKQqoNrnZCOZ3jtE5kL3VAa5556cOPI5SUdQPc8loctKVzQanQNRvcIh1XFEKYys8Yfr>. Acesso em: 9 de abril de 2026.

7 CNN. **Mais de 20 milhões de brasileiros ainda não têm acesso à internet, diz IBGE**. Web, 2026. Disponível em: <https://www.cnnbrasil.com.br/tecnologia/mais-de-20-milhoes-de-brasileiros-ainda-nao-tem-acesso-a-internet-diz-ibge/>. Acesso em: 9 de abril de 2026.

Vale destacar, contudo, que, a maior confiabilidade técnica não implica automaticamente maior adequação regulatória, devendo a escolha do mecanismo observar o princípio da proporcionalidade.

3. Eficácia e impacto

A eficácia dos mecanismos de aferição de idade deve considerar também seus impactos sobre a experiência do usuário, incluindo o acesso legítimo à internet. Em primeiro lugar, é importante reconhecer que a eficácia de um mecanismo depende da sua taxa de adesão pelos usuários. Nesse sentido, mecanismos mais rigorosos podem, paradoxalmente, ser menos eficazes caso gerem barreiras excessivas ao uso. Estudo recente conduzido pela Carnegie Mellon University[8] demonstrou que métodos mais intrusivos, como envio de documento oficial, apresentaram taxas significativamente menores de conclusão (entre 17% e 28%), enquanto mecanismos mais simples, como autodeclaração, atingiram taxas próximas a 99%. Isso evidencia que há uma tensão estrutural entre segurança e usabilidade: quanto maior o nível de exigência, maior tende a ser a resistência do usuário.

Essa discussão também deve ser considerada sob a perspectiva de desigualdade digital. A complexidade da tecnologia pode afetar desproporcionalmente determinados grupos, como pessoas com menor letramento digital, acesso limitado a dispositivos, conexão precária ou mesmo restrições documentais. A depender da solução adotada, o sistema de aferição pode, na prática, criar barreiras adicionais para populações já vulneráveis.

Diante desse cenário, a definição de mecanismos de aferição de idade no âmbito do ECA Digital exige uma abordagem de ponderação entre diferentes vetores normativos e práticos, isso porque mecanismos excessivamente permissivos são insuficientes, mas soluções excessivamente restritivas também podem falhar. O desafio está, portanto, em encontrar soluções proporcionais, que cumpram sua finalidade, sem gerar novos riscos ou discriminações no ambiente digital, conforme será aprofundado no próximo item.

8 LIN, Y., et al. **User (Non-)Compliance with Age Verification: Preliminary Evidence from a Deceptive Web Experiment**. Carnegie Mellon University CyLab Security and Privacy Institute. Pittsburgh, Estados Unidos, 2026. Disponível em: https://www.cs.cmu.edu/~sscheffl/docs/2026/AgeVerif2026.pdf. Acesso em: 6 de abril de 2026.

4. Proporcionalidade como critério estruturante

A análise dos mecanismos de aferição de idade evidencia que não há solução única capaz de atender todos os contextos de aplicação. Nesse cenário, o princípio da proporcionalidade emerge como critério estruturante para a interpretação e implementação das obrigações previstas no ECA Digital.

A proporcionalidade pode ser compreendida como um critério de calibragem das medidas de aferição de idade em relação aos riscos que se pretende mitigar. Trata-se, assim, de definir a solução mais apropriada diante das circunstâncias concretas de cada serviço ou atividade.

Na prática, a aplicação da proporcionalidade pode ser orientada por duas perguntas centrais que devem guiar a tomada de decisão pelos fornecedores:

PROPORCIONALIDADE	
Quais são os riscos inerentes ao serviço ou produto oferecido para crianças e adolescentes?	**Quais são os riscos associados ao mecanismo de verificação de idade adotado?**
Essa análise diz respeito aos potenciais impactos do próprio ambiente digital, a depender do tipo de funcionalidade disponibilizada.	Certos mecanismos podem implicar tratamento de dados sensíveis, criar barreiras de acesso e riscos de discriminação e potencializar incidentes de segurança.

A proporcionalidade, portanto, exige uma análise combinada desses dois vetores de risco. Por exemplo, mecanismos mais intrusivos podem ser justificáveis em contextos de maior potencial de dano, mas tendem a ser desproporcionais quando aplicados a serviços de menor risco.

A correta aplicação do princípio da proporcionalidade é essencial para evitar a ineficácia das medidas e a imposição de ônus excessivos, garantindo que o ECA Digital produza efeitos compatíveis com a realidade brasileira.

Nesse contexto, é relevante reconhecer a própria lógica do ECA Digital reflete não apenas a preocupação com a mitigação de riscos, mas também o objetivo mais amplo de viabilizar um ambiente digital seguro e acessível para todos. Esse ponto é particularmente relevante quando se considera o papel central que a internet desempenha - o ambiente digital é essencial para acesso à informação, educação, cultura, participação cívica e

desenvolvimento econômico. Para crianças e adolescentes, a internet pode representar importante ferramenta de aprendizado, socialização e inclusão. Nesse sentido, a limitação desproporcional do acesso ao ambiente digital pode aprofundar desigualdades, restringir oportunidades e comprometer o pleno desenvolvimento de indivíduos.

Assim, a proporcionalidade se apresenta como elemento central para a implementação de soluções que sejam, ao mesmo tempo, juridicamente adequadas, tecnicamente viáveis e efetivas na proteção de crianças e adolescentes, sem comprometer o acesso seguro e sustentável ao ambiente digital. Essa lógica de análise combinada de riscos e proporcionalidade também orienta o conjunto de critérios consolidados no Anexo II, que traduz esses elementos em parâmetros de avaliação aplicáveis a diferentes contextos.

5. Minimização de dados e riscos associados à aferição etária

O art. 24, § 3º, do Decreto Regulamentador[9] veda, de forma expressa, o armazenamento, a retenção ou qualquer forma de conservação da imagem, da cópia do documento ou das informações extraídas, as quais devem ser eliminadas de forma imediata e irreversível após a captura do dado necessário.

Essa limitação é especialmente relevante considerando a natureza dos dados frequentemente envolvidos nos processos de verificação de idade, de modo que a minimização de dados não deve se restringir apenas à fase de coleta, devendo abranger todo o ciclo de vida do tratamento. Os mecanismos adotados devem privilegiar soluções que reduzam a quantidade de dados tratados e que evitem a retenção de informações após a verificação. De forma geral, deve-se evitar que os próprios mecanismos de controle se tornem fontes autônomas de risco.

6. Governança como elemento central

A efetiva implementação das obrigações previstas no ECA Digital exige a estruturação de modelos de governança capazes de sustentar, documentar e demonstrar a adequação dos mecanismos de verificação de idade adotados.

Nesse sentido, o próprio ECA Digital reforça a centralidade da governança ao prever a necessidade de elaboração de instrumentos formais de avaliação e monitoramento, como relatórios de impacto que devem estar disponíveis para compartilhamento com a ANPD, mediante requisição.

9 Art. 24, § 3º: O tratamento de dados decorrente da coleta de documentos deverá limitar-se ao dado relativo à idade ou à confirmação da faixa etária, vedado o armazenamento, a retenção ou qualquer forma de conservação da imagem, da cópia do documento ou da informação, que deverá ser eliminada de modo imediato e irreversível após a captura da informação necessária, nos termos do disposto na Lei nº 13.709, de 14 de agosto de 2018.

Nesse contexto, a governança permite que os agentes demonstrem não apenas que adotaram medidas de proteção, mas que essas medidas foram escolhidas de forma proporcional e adequada ao contexto específico de suas atividades.

Ainda, a estruturação de uma governança adequada contribui não apenas para o cumprimento das obrigações legais, mas também para a construção de confiança junto a usuários, reguladores e demais stakeholders. Em um contexto de crescente escrutínio sobre práticas digitais, a capacidade de demonstrar responsabilidade e compromisso com a proteção de crianças e adolescentes tende a se tornar um diferencial relevante. A estruturação desses elementos de governança encontra correspondência prática nos próximos passos sugeridos no Anexo I, bem como nos critérios de avaliação consolidados no Anexo II.

7. Cronograma de monitoramento e fiscalização: implementação gradual e orientada por risco

A publicação das orientações preliminares pela ANPD foi acompanhada da definição de um cronograma de monitoramento e fiscalização . A estratégia regulatória adota uma abordagem escalonada e predominantemente preventiva, voltada, inicialmente, à compreensão dos desafios técnicos e operacionais enfrentados pelos agentes regulados.

O cronograma de atuação da ANPD pode ser compreendido nas seguintes etapas:

01 **Monitoramento inicial com foco em agentes estruturantes (início imediato).**	A primeira fase, já em curso, prioriza o acompanhamento de lojas de aplicativos e sistemas operacionais, considerados atores com papel central no ecossistema digital. A escolha por esse grupo reflete uma estratégia regulatória de alto impacto: a atuação sobre um número reduzido de agentes pode gerar efeitos sistêmicos relevantes para a proteção de crianças e adolescentes.
02 **Ampliação do monitoramento com base em risco (a partir de agosto de 2026).**	Em um segundo momento, previsto para agosto de 2026, a ANPD ampliará o escopo de fiscalização para incluir outros setores. Essa expansão será orientada por critérios como o nível de risco associado aos serviços oferecidos e as informações coletadas na fase inicial.
03 **Consolidação regulatória e eventual aplicação de sanções (etapas subsequentes).**	O cronograma também prevê a atualização dos regulamentos de fiscalização e de aplicação de sanções administrativas para adequação às novas disposições do ECA Digital, o que deve ocorrer a partir de novembro de 2026. O início de ações de fiscalizações está programado para janeiro de 2027.

Relevante destacar, no entanto, que a estipulação de um cronograma por parte da ANPD não impede que outros órgãos com poder fiscalizador, como aqueles voltados à proteção de consumidores, iniciem, por iniciativa própria, ações para avaliar a conformidade legal de determinador atores regulados, inclusive com a aplicação de penalidades em casos de descumprimento.

8. Considerações finais

A implementação de mecanismos de aferição de idade no contexto do ECA Digital representa aspecto central na proteção de crianças e adolescentes no ambiente digital. No entanto, como demonstrado ao longo deste material, trata-se de tema que não pode ser reduzido a uma escolha técnica isolada.

A aferição de idade deve ser compreendida como um elemento de governança baseada em risco, que envolve a análise integrada de múltiplos fatores. Nesse cenário, a adoção de abordagens proporcionais e orientadas pela minimização de dados é instrumento essencial para o desenho de soluções sustentáveis.

Como forma de sistematizar as discussões desenvolvidas, os Anexos I e II apresentam, respectivamente, um conjunto de próximos passos para empresas e um guia de avaliação de mecanismos de aferição de idade, permitindo a aplicação prática dos conceitos de proporcionalidade, minimização e governança aqui discutidos.

Em última análise, o desafio colocado pelo ECA Digital não é apenas o de restringir o acesso indevido, mas o de estruturar um ambiente digital que seja simultaneamente seguro, acessível e sustentável.

ANEXO I

Próximos passos para empresas

Diante da entrada em vigor do ECA Digital e da publicação das orientações preliminares pela ANPD, empresas que ofertam produtos ou serviços digitais acessíveis a crianças e adolescentes devem iniciar, ou aprimorar, seus processos de adequação, com base em uma abordagem estruturada e multidisciplinar.

Nesse contexto, alguns passos práticos se destacam:

01	**Mapeamento de riscos e casos de uso**	Identificar quais produtos, funcionalidades ou fluxos de usuário apresentam risco potencial para crianças e adolescentes, considerando aspectos como interação entre usuários, acesso a conteúdo sensível e exposição a terceiros.
02	**Avaliação e seleção de mecanismos de vaferição de idade**	Analisar as alternativas de mecanismos de aferição de idade disponíveis considerando os critérios de proporcionalidade, eficácia, impacto na experiência do usuário e riscos associados ao tratamento de dados pessoais, evitando abordagens padronizadas e descontextualizadas.
03	**Revisão de práticas de tratamento de dados pessoais**	Garantir que a coleta e o uso de dados para aferição de idade estejam estritamente limitados à finalidade específica, com implementação de medidas de minimização, segurança e segregação de dados.
04	**Estruturação de governança e documentação**	Desenvolver políticas que indiquem quando e como devem ser produzidos relatórios de impacto, avaliações de risco e demais registros de decisão que demonstrem a adequação das medidas adotadas, em linha com as exigências do ECA Digital e boas práticas de proteção de dados.
05	**Implementação de mecanismos de transparência e contestação**	Assegurar que os usuários tenham acesso a informações claras sobre o funcionamento dos mecanismos e possam contestar decisões automatizadas ou classificações incorretas.
06	**Monitoramento regulatório e evolução contínua**	Acompanhar a evolução das orientações e regulamentações da ANPD e estabelecer rotinas de revisão periódica das soluções adotadas, considerando avanços tecnológicos e mudanças no perfil de risco.

ANEXO II

Guia para Avaliação de Mecanismos de Aferição de Idade

A partir das discussões desenvolvidas ao longo do material, reunimos abaixo os principais pontos de avaliação que devem ser considerados por empresas no momento de definição, implementação ou revisão de mecanismos de aferição de idade.

Este checklist reflete as orientações preliminares da ANPD e deve ser revisado assim que diretrizes definitivas forem publicadas.

01. Proporcionalidade e Riscos

- ☑ **Riscos do Produto/Serviço**: Foram identificados os potenciais efeitos adversos sobre privacidade, segurança e saúde de crianças e adolescentes ao utilizarem o produto (ex: interação entre usuários, uso compulsivo etc.)?
- ☑ **Riscos do Mecanismo**: Foi avaliado se a própria solução de verificação gera riscos, como o tratamento de dados sensíveis ou a criação de barreiras indevidas?
- ☑ **Equilíbrio**: A solução técnica escolhida é proporcional ao nível de risco do serviço, equilibrando acurácia com a proteção à privacidade?
- ☑ **Instrumentos de Apoio**: Foi considerada a elaboração de um Relatório de Impacto à Proteção de Dados Pessoais?

02. Acurácia, Robustez e Confiabilidade

- ☑ **Métricas de Acurácia**: A precisão do método em determinar a faixa etária é mensurada e documentada periodicamente?
- ☑ **Resistência a Fraudes (Robustez)**: O sistema passou por testes para resistir a tentativas de burla ou manipulação?
- ☑ **Fontes de Dados (Confiabilidade)**: As fontes utilizadas são íntegras e independentes? Lembre-se: a autodeclaração pura tem baixo grau de confiabilidade.

03. Privacidade e Proteção de Dados

- ☑ **Minimização**: O sistema trata apenas o dado ou atributo etário estritamente necessário, evitando coletar dados desnecessários?
- ☑ **Vedação de Uso Secundário**: Está garantido que os dados coletados não serão usados para outras finalidades que não a aferição de idade?

04. Transparência e Auditabilidade

- ☑ **Informação Clara**: O usuário recebe informações em linguagem simples e acessível sobre a finalidade da verificação e quais dados são usados?
- ☑ **Contestação**: Existe um canal para o usuário contestar ou retificar o resultado?
- ☑ **Registros de Auditoria (Logs)**: A empresa mantém registros das operações para fins de auditoria?

05. Interoperabilidade

- ☑ **Segurança de Fluxo**: Estão definidos os limites de fluxo de dados, agentes autorizados e salvaguardas contra o compartilhamento irrestrito?

b/luz

www.baptistaluz.com.br/