Guia Orientativo

Mecanismos de Aferição de Idade

TOMADA DE SUBSÍDIOS

Maio de 2026

ANPD

ANPD Agência Nacional de Proteção de Dados

GUIA ORIENTATIVO

Mecanismos de Aferição de Idade

(Versão Preliminar)

Brasília – Maio/2026

Presidente da República: Luiz Inácio Lula da Silva

Agência Nacional de Proteção de Dados

Diretor-Presidente: Waldemar Gonçalves Ortunho Junior

Diretores:

Miriam Wimmer
Iagê Zendron Miola
Lorena Giuberti Coutinho

Equipe de elaboração:

Adriano dos Santos Mello
Davi Teófilo Nunes Oliveira
Diego Carvalho Machado
Gabriela Simão Tavares
Guilherme Ferreira Machado
Jeferson Dias Barbosa
Jorge André Ferreira Fontelles de Lima
Leandro Rivelli Teixeira Nogueira
Lucas Borges de Carvalho
Luis Felipe Castilho Torres
Maria Carolina Ferreira da Silva
Marcus Vinicius Rossi da Rocha
Priscila Lini
Rodrigo Santana dos Santos

Sumário

INTRODUÇÃO

O presente Guia tem por objetivo apresentar orientações gerais para a implementação de mecanismos confiáveis de aferição de idade por fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e adolescentes, ou de acesso provável por esse público. O Guia consolida, sistematiza e aprofunda as "Orientações Preliminares – Mecanismos Confiáveis de Aferição de Idade"[1], documento divulgado pela ANPD em março de 2026, com ajustes e acréscimos, a fim de conferir maior operacionalidade e clareza interpretativa aos agentes regulados.

O objetivo é demonstrar os principais cuidados a serem observados na implementação desses mecanismos, bem como apresentar e discutir os conceitos e as regras mais relevantes previstos na Lei nº 15.211/2025 (Estatuto Digital da Criança e do Adolescente – "ECA Digital") e no Decreto nº 12.880, de 18 de outubro 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, à proteção do melhor interesse e à proteção integral de crianças e adolescentes no ambiente digital. Essa diretriz se expressa, por exemplo, no art. 3º, caput, 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, caput, 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 nisso que se deve compreender os comandos do art. 9º, caput e § 1º, do ECA Digital e art. 24, II e do art. 25, §2º, II, do Decreto, que determinam que os mecanismos de aferição de idade adotados sejam **"confiáveis".** Trata-se de uma obrigação que decorre do dever geral de atuar de forma proativa e diligente para prevenir e mitigar riscos a crianças e adolescentes no ambiente digital. O primeiro dispositivo destaca, ainda, que as medidas devem ser **"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.

Por isso, estas determinações gerais de confiabilidade e eficácia ganham importância. Elas são detalhadas no art. 24 do Decreto, que estabelece diretrizes para a implementação de soluções de aferição de idade. Conforme já havia sido feito nas Orientações Preliminares, para fins didáticos e de sintetização, os onze incisos do art. 24 foram agrupados em seis requisitos gerais: (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 serão examinados, com mais detalhes, na Seção III ("Requisitos Gerais") deste documento. Antes de abordar este ponto, a Seção I ("Aspectos Gerais") discute os principais conceitos relacionados à aferição de idade e a Seção II ("Cadeia Digital de Responsabilidades") é dedicada à exposição da divisão legal de responsabilidades entre os

[1] Disponível em: https://www.gov.br/anpd/pt-br/assuntos/eca-digital/mecanismos-confiaveis-de-afericao-de-idade-orientacoes-preliminares.pdf/@@display-file/file

fornecedores de produtos ou serviços de tecnologia da informação, com destaque para as lojas de aplicações e os sistemas operacionais. Já a Seção IV ("Requisitos Específicos"), apresenta garantias mínimas a serem observadas por soluções de aferição de idade baseadas em estimativa facial, verificação documental e credenciais verificáveis.

Cada seção apresenta conceitos, fundamentos legais e regulamentares aplicáveis, bem como recomendações destinadas a apoiar a implementação dessas soluções pelos fornecedores. Ao final do documento, o Anexo apresenta um quadro sintético com as principais recomendações associadas a cada um dos requisitos gerais indicados na Seção III.

I. ASPECTOS GERAIS

Nesta Seção, apresentam-se os principais conceitos que permeiam a legislação sobre aferição de idade e que serão utilizados neste Guia Orientativo.

O Decreto, em seu art. 2º, IV, estabelece que a **aferição de idade** é o *conjunto de procedimentos destinados a verificar, estimar ou inferir, direta ou indiretamente, a idade ou a faixa etária de um usuário*, o que pode incluir, dentre outros métodos tecnicamente idôneos, a análise documental, biométrica e de padrões de uso.[2]

Esse processo integra as condutas que garantem a adaptação das experiências no ambiente digital ao estágio de desenvolvimento em que a criança e o adolescente se encontram, de modo a assegurar espaços protegidos e interações saudáveis. Em razão disso, é fundamental compreender que a **aferição de idade não constitui um fim em si mesmo**, mas sim um eixo essencial na construção de um ecossistema seguro e condizente com a autonomia progressiva e a proteção integral do público infantojuvenil, do qual fazem parte outras garantias legais e medidas protetivas, em especial os mecanismos de supervisão parental – a vinculação de contas ao responsável legal em redes sociais –, a vedação ao perfilamento para fins de direcionamento de publicidade comercial e a prevenção do uso problemático, excessivo ou compulsivo. Dessa forma, **a aferição de idade não deve ser vista como a única forma de proteger crianças e adolescente no ambiente digital, mas uma obrigação legal que viabiliza, se integra e interage com as demais**.

O art. 10 do ECA Digital, que inaugura o capítulo dedicado aos mecanismos de aferição de idade, segue essa linha. O seu objetivo central é assegurar a adoção de medidas *para proporcionar experiências adequadas à idade*.[3] Nesse sentido, as regras relacionadas à aferição de idade **devem ser sempre interpretadas à luz de sua finalidade legal**: proteger crianças e adolescentes no ambiente digital, observados o princípio do melhor interesse e demais requisitos previstos na legislação e indicados neste Guia.

Outro aspecto relevante a se considerar é que a **aferição de idade não se confunde com a verificação de identidade**, mesmo quando são utilizados métodos que envolvam a análise documental do usuário. As finalidades jurídicas e operacionais das duas práticas se diferem.

---

[2] Art. 2º 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.

[3] Art. 10. Os fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável por eles deverão adotar mecanismos para proporcionar experiências adequadas à idade, nos termos deste Capítulo, respeitadas a autonomia progressiva e a diversidade de contextos socioeconômicos brasileiros.

A aferição de idade é um procedimento destinado a obter o conhecimento da idade ou da faixa etária (atributo etário) de um usuário, com o intuito único de saber se uma pessoa natural é menor de 18 (dezoito) anos de idade, sem necessidade de identificação do indivíduo. A verificação da identidade, por sua vez, exige o tratamento de outros dados pessoais que conduzem à individualização da pessoa natural. Esta, por exemplo, pode ser requerida para o exercício dos direitos dos titulares, no contexto da Lei Geral de Proteção de Dados Pessoais (LGPD).

A minimização do tratamento de dados constitui princípio geral de proteção de dados pessoais, nos termos do art. 6º, III, da LGPD, e é particularmente relevante quando o procedimento de aferição envolve dados pessoais sensíveis, como biometria. Existem meios técnicos que permitem que apenas a data de nascimento ou a idade sejam coletados, ou que compartilham informações de forma anonimizada ou pseudonimizada, como prova de conhecimento zero ou *tokens*, sem vinculação direta a nomes ou cadastros associados à determinada pessoa.

A utilização de tokens etários reduz significativamente a exposição de dados pessoais e limita a circulação de informações sensíveis entre diferentes sistemas. Por isso, as soluções de aferição de idade devem ser desenvolvidas e implementadas de forma compatível com as normas de proteção de dados pessoais, em particular com o princípio da necessidade.

Nessa concepção, o Decreto estrutura a aferição como um gênero, do qual decorrem três espécies: estimativa, verificação e inferência de idade. No âmbito dessas espécies, situam-se as soluções técnicas de aferição propriamente ditas, tais como estimativa por biometria, verificação documental, entre outras. Essa dinâmica pode ser sintetizada por meio do seguinte quadro:

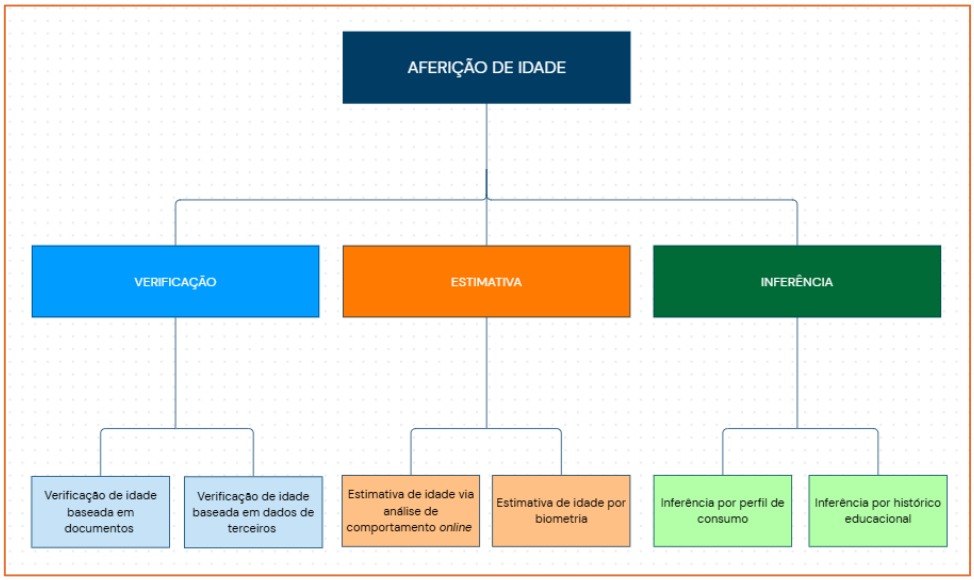

Figura 1 – Taxonomia dos mecanismos de aferição de idade.

É importante esclarecer que **existem diversos métodos de aferição de idade**, não se restringindo aos mecanismos contidos na Figura 1. Eles variam de acordo com a forma de coleta de dados, integração com sistemas e plataformas, armazenamento da informação, dentre outros aspectos. Além disso, os mecanismos de aferição de idade podem ser utilizados de forma isolada ou combinada, a depender do nível de risco associado ao conteúdo, produto ou serviço digital. A combinação de mecanismos, denominada **aferição em camadas**, permite ampliar a acurácia do processo e reduzir as margens de erro, na medida em que a limitação de um mecanismo pode ser compensada pela robustez de outro.

De acordo com o art. 2º, V, do Decreto, a **verificação de idade** é o *procedimento específico, de alto grau de confiabilidade, baseado na conferência da veracidade do atributo etário, com a finalidade de comprovar a exatidão da idade declarada ou a faixa etária.*[4] Os atributos que distinguem a verificação das demais espécies de aferição de idade são "o **alto grau de confiabilidade**" e a finalidade de comprovar a "**exatidão**" da idade declarada.

Por isso, **o Decreto prevê o uso de soluções de verificação de idade em contextos que podem ser considerados de maior risco**, como serviços que oferecem acesso a conteúdo pornográfico (art. 16, § 1º), redes sociais que disponibilizam conteúdos, serviços ou produtos proibidos (art. 19, II) e jogos eletrônicos com caixas de recompensa (art. 23). A verificação de idade também pode ser utilizada para complementar análises efetuadas por estimativa e inferência, ou até mesmo fornecer evidências adicionais sempre que necessário, especialmente quando o resultado da aferição não é conclusivo.[5] Igualmente, um mecanismo de verificação de idade poderá ser utilizado em casos de contestação do resultado inicial pelo usuário ou quando houver divergência entre a aferição de idade realizada pelo fornecedor de tecnologia da informação e o sinal de idade enviado pela loja de aplicações de internet ou sistema operacional.

Por sua vez, a **estimativa de idade** consiste no emprego de métodos para determinar a idade provável de uma pessoa, com base em características biométricas ou comportamentais. Já a **inferência de idade** compreende soluções técnicas que deduzem a idade de forma indireta, a partir do contexto, dados de consumo, histórico educacional ou preferências *online*.[6] Em ambos os casos, a solução **não apresenta um resultado com exatidão**, isto é, a idade de uma pessoa precisamente. Assim, por exemplo, uma solução de estimativa de idade pode determinar que há alto grau de probabilidade de que uma pessoa é maior de 18 anos, por integrar uma faixa etária específica – por exemplo, de 30 a 35 anos – mas não indica qual é a sua idade.

Finalmente, conforme o art. 2º, VI, do Decreto, a **autodeclaração de idade** consiste no *método limitado à indicação da idade, faixa etária ou outro dado pessoal fornecido pelo próprio usuário, sem evidências adicionais para confirmar a veracidade ou a titularidade da informação*. Por meio dela, o fornecedor solicita que o próprio usuário informe a sua idade ou faixa etária, sem qualquer confirmação posterior dessas informações. Ou seja, a aferição é feita exclusivamente com base no informado pelo usuário.

Dadas essas características, **a autodeclaração não constitui um mecanismo confiável de aferição de idade**, de modo que não pode ser utilizada em contextos de maior risco a crianças e adolescentes. Por isso, **a autodeclaração é vedada nos casos de produtos, serviços e conteúdos proibidos para crianças e adolescentes**. É o caso, por exemplo, de

---

[4] Art. 2º Para fins do disposto neste Decreto, considera-se: [...] V - verificação de idade - procedimento específico de aferição de idade de alto grau de confiabilidade, nos termos estabelecidos pela ANPD, baseado na conferência da veracidade do atributo etário, com a finalidade de comprovar a exatidão da idade declarada ou a faixa etária, mediante o emprego de mecanismos técnicos ou documentais;

[5] Conforme o disposto nos seguintes artigos, do Decreto: art. 25 [...] § 2º Para cumprimento do disposto no *caput*, as lojas de aplicações de internet e os sistemas operacionais de terminais deverão: III - permitir a contestação e a retificação da classificação etária mediante apresentação de evidência adicional, com decisão fundamentada em prazo razoável. [...] art. 27. O fornecedor de produtos ou serviços de tecnologia da informação que afira ou verifique a idade deverá possibilitar ao usuário meio adequado para contestar a idade ou a faixa etária aferida ou verificada.

[6] ANPD. *Mecanismos de aferição de idade*. Brasília, DF: ANPD, 2025. p. 16. (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/@@download/file.

serviços e redes sociais que disponibilizem conteúdo pornográfico ou de plataformas de *e-commerce* que vendem bebidas alcoólicas.[7]

Assim, o simples fornecimento do número de Cadastro de Pessoa Física (CPF) pelo usuário equipara-se à autodeclaração, na medida em que se trata de dado pessoal apresentado pela própria pessoa, sem evidências adicionais para confirmar a veracidade ou a titularidade da informação.

Além de poder ser implementada por diferentes técnicas e em diferentes contextos, importa destacar que **a obrigação de aferição de idade não incide de modo uniforme sobre todos os produtos ou serviços** de tecnologia da informação abrangidos pelo ECA Digital.

Nesse sentido, o Decreto estabelece uma **distinção baseada na categorização do conteúdo, produto ou serviço**: de um lado, os "impróprios ou inadequados" (art. 2º, I) e, de outro, os "proibidos" (art. 2º, II) para crianças e adolescentes. Os **impróprios ou inadequados** são aqueles que podem apresentar riscos às crianças e adolescentes, nos termos estabelecidos na classificação indicativa, quando aplicável. Já os **proibidos** são aqueles expressamente vedados para crianças e adolescentes por determinação legal específica.[8]

Em caso de disponibilização de conteúdos, produtos e serviços **proibidos**, os fornecedores devem, obrigatoriamente, implementar solução de verificação de idade (art. 15).[9] Portanto, **a verificação de idade é exigida e deve ser obrigatoriamente implementada caso o fornecedor disponibilize conteúdo, produto ou serviço proibido**. Trata-se, portanto, de medida protetiva essencial e obrigatória a ser adotada nestes casos.

Já no caso de conteúdos **impróprios ou inadequados**, é necessário cumprir, cumulativamente, três requisitos previstos no art. 14 do Decreto: (i) observar a política de classificação indicativa, (ii) a disponibilização de ferramentas efetivas de supervisão parental e (iii) a adoção, desde a concepção, de medidas técnicas e organizacionais de segurança por padrão.[10]

---

[7] É o que verifica nos artigos 17 a 19 do Decreto: art. 17. O fornecedor de produtos ou serviços de tecnologia da informação que permita a visualização de imagens ou vídeos de conteúdo pornográfico deverá, quando o usuário não estiver cadastrado, quando a idade não for verificada ou quando a conta for operada por criança ou adolescente: [...] II - exigir verificação de idade para desbloqueio, *vedada a mera autodeclaração*. Art. 18. O fornecedor que oferte ou intermedeie a compra e a venda de produtos e serviços proibidos para crianças e adolescentes a que se refere o art. 15, § 1º, incisos I a VII, deverá implementar mecanismos efetivos de verificação de idade, nos termos estabelecidos pela ANPD: I - no ato de cadastro dos usuários, com bloqueio da aquisição dos produtos e dos serviços, por padrão, por usuários crianças ou adolescentes, *vedado o desbloqueio por autodeclaração*; [...] Art. 19. O serviço de rede social deverá, caso disponibilize conteúdo, produto ou serviço proibido para crianças e adolescentes: [...] II - adotar mecanismos efetivos de verificação de idade, nos termos estabelecidos pela ANPD, *vedada a autodeclaração*.

[8] Art. 2º Para fins do disposto neste Decreto, considera-se: I - conteúdo, produto ou serviço impróprio ou inadequado - aquele que possa apresentar risco à privacidade, à segurança, ao desenvolvimento psicossocial, à saúde mental e física e ao bem-estar da criança e do adolescente, nos termos estabelecidos na classificação indicativa, quando aplicável; II - conteúdo, produto ou serviço proibido para crianças e adolescentes - aquele cujo acesso, cuja disponibilização, cuja aquisição ou cujo consumo seja expressamente vedado para crianças e adolescentes por determinação legal específica. [...] Os conteúdos, produtos e serviços considerados proibidos para crianças e adolescentes estão indicados no art. 15, § 1º, do Decreto.

[9] Art. 15. O fornecedor de produtos ou serviços de tecnologia da informação que disponibilize conteúdo, produto ou serviço proibido para crianças e adolescentes, nos termos do disposto nos art. 9º a art. 15 da Lei nº 15.211, de 17 de setembro de 2025, deverá: I - implementar mecanismos eficazes de verificação de idade; e II - impedir efetivamente o acesso, a fruição ou o consumo por crianças e adolescentes.

[10] Art. 14. A disponibilização de conteúdo, produto ou serviço impróprio ou inadequado a crianças e adolescentes, nos termos do disposto no art. 9º da Lei nº 15.211, de 17 de setembro de 2025, ficará condicionada, cumulativamente, à: I - observância à política de classificação indicativa, quando aplicável; II -

É importante destacar que, em alguns contextos, o último requisito ("medidas técnicas e organizacionais de segurança por padrão") pode incluir o dever de adotar mecanismos de aferição de idade, inclusive para fins de cumprimento de outros encargos legais. Portanto, **mesmo no caso de conteúdos impróprios ou inadequados, a aferição de idade pode ser uma medida de segurança necessária para assegurar a efetiva proteção de crianças ou adolescentes**, especialmente em contextos de maior risco.

A esse respeito, conforme art. 14, parágrafo único do ECA Digital, a ANPD pode determinar a adoção de medidas de proteção adicionais *quando identificar riscos relevantes à privacidade, à segurança, ao desenvolvimento psicossocial, à saúde mental e física e ao bem-estar, respeitados o melhor interesse e a autonomia progressiva da criança e do adolescente*, o que igualmente pode incluir a determinação da utilização de mecanismos de aferição de idade.

O contexto, a natureza do serviço, as funcionalidades e o ambiente de fornecimento desses produtos, conteúdos e serviços são, portanto, imprescindíveis para esta análise de risco e para proporcionar uma experiência de usuário adaptada à sua autonomia progressiva.[11] A título exemplificativo, redes sociais possuem obrigações especiais de supervisão parental para menores de 16 anos (art. 24, ECA Digital) e, portanto, têm de adotar medidas adicionais para assegurar sua efetividade e viabilidade na prática. No mesmo sentido, a viabilização do tratamento de dados no melhor interesse da criança e do adolescente (Art. 14, LGPD) e a vedação ao perfilamento de dados de crianças e adolescentes em redes sociais para fins de direcionamento de publicidade comercial (art. 26, ECA Digital) se tornam operacionalizáveis com aferição etária.

Em resumo, a verificação de idade é exigida em casos de conteúdos, produtos e serviços proibidos, enquanto para aqueles inadequados e impróprios podem ser adotados mecanismos de aferição de idade, considerando os riscos identificados de acordo com o contexto, a natureza do serviço, as funcionalidades e o ambiente de fornecimento, para: (i) adotar, por padrão e desde a concepção, medidas técnicas e organizacionais de segurança; e (ii) cumprir determinação da ANPD de medidas de proteção adicionais, em caso de riscos relevantes à criança e ao adolescente. Trata-se, portanto, da efetivação do dever geral de prevenção, em conformidade com o princípio do melhor interesse da criança e do adolescente e da sua proteção integral, especial e prioritária (art. 5º, caput, do ECA Digital).

II. CADEIA DIGITAL DE RESPONSABILIDADES

As obrigações de aferição de idade previstas no ECA Digital são distribuídas de forma distinta, de acordo com a posição em que o fornecedor ocupa no ambiente digital. Nesse sentido, o art. 15 do ECA Digital dispõe que as obrigações atribuídas aos agentes devem ser compreendidas à luz de uma **cadeia digital de responsabilidades compartilhadas**.[12]

---

adoção de medidas técnicas e organizacionais de segurança por padrão, desde a concepção, proporcionais aos riscos identificados para faixa etária; e III - disponibilização de ferramentas efetivas de supervisão parental, com funcionalidades de bloqueio configuráveis pelos responsáveis legais e demais métodos que visem a proporcionar segurança digital a crianças e adolescentes, nos termos do disposto nos art. 17 e art. 18 da Lei nº 15.211, de 17 de setembro de 2025.

[11] UK. ICO. Safety by design: Code of practice. Maio 2026. P. 22-23. Disponível em: https://www.onlinesafetyact.net/documents/1684/Safety_by_Design_-_Code_of_Practice.pdf.

[12] Art. 15. O cumprimento das obrigações previstas neste Capítulo não exime os demais agentes da cadeia digital das suas responsabilidades legais, cabendo a todos os envolvidos garantir de forma solidária a proteção integral de crianças e de adolescentes.

Por meio dessa alocação de responsabilidades, os deveres protetivos não podem ser vistos de maneira isolada. Pelo contrário, eles são interdependentes, de caráter sucessivo e encadeado, em conformidade com o princípio da proteção integral e prioritária de crianças e adolescentes. O Decreto reitera esse entendimento ao destacar a responsabilidade compartilhada entre Poder Público, famílias, sociedade civil e fornecedores de produtos ou serviços de tecnologia da informação na garantia e na efetivação dos direitos de crianças e adolescentes no ambiente digital.[13]

Isso implica a necessidade de atuação coordenada entre diversos agentes, de modo que as soluções de aferição de idade sejam implementadas de forma complementar e concatenada. Na maioria das vezes, a atuação de um agente influencia ou direciona a forma de cumprimento das obrigações por outro, de acordo com o modelo previsto no ECA Digital. Parte-se do pressuposto da existência de estrutura sequencial para acesso e uso de produtos e serviços no ambiente digital, o que forma uma integração entre diferentes plataformas.

Diante desse cenário, para fins de aferição de idade, o ECA Digital dividiu esses fornecedores em dois grupos: (i) lojas de aplicações de internet e sistemas operacionais; e (ii) demais fornecedores de produtos ou serviços de tecnologia da informação. O modelo legal prevê, portanto, um sistema protetivo de dois níveis, com a possibilidade de realização de duas aferições de idade diferentes, que são realizadas em momentos apartados: a primeira, feita pelas lojas de aplicações e sistemas operacionais, e uma segunda, realizada pelos demais fornecedores.

As **lojas de aplicações e os sistemas operacionais** atuam como infraestruturas essenciais de acesso a serviços e produtos digitais, na medida em que viabilizam a distribuição, a disponibilização e o funcionamento das aplicações de internet. Por isso, conforme art. 12, § 1º, do ECA Digital, têm o **dever de fornecer o sinal de idade** aos provedores de aplicação de internet, exclusivamente para o cumprimento das finalidades previstas na Lei e com salvaguardas técnicas adequadas.

O **sinal de idade** consiste em uma *informação ou credencial indicativa que atesta a idade ou a faixa etária de um usuário, sem revelar dados pessoais adicionais* (art. 2º, VI, Decreto), sendo *vedado o envio de data de nascimento exata, da identidade civil ou de dados de perfilamento do usuário* (art. 25, § 1º, Decreto). Ressalta-se que esses fornecedores devem mitigar eventuais riscos de rastreamento do usuário e de incidentes de segurança que exponham dados pessoais.

Nessa toada, o art. 25, §2º, do Decreto estabelece um modelo em etapas para a realização da aferição de idade pelas lojas de aplicações e sistemas operacionais.[14] A intenção é fortalecer a aferição feita na origem para gerar menos impactos nos outros fornecedores da cadeia e nos usuários finais. O fluxograma abaixo pode auxiliar na compreensão:

---

[13] Art. 4º São princípios da Política Nacional de Promoção e Proteção dos Direitos da Criança e do Adolescente no Ambiente Digital: [...] IV - a responsabilidade compartilhada entre Poder Público, famílias, sociedade civil e fornecedores de produtos ou serviços de tecnologia da informação na garantia e na efetivação dos direitos de crianças e adolescentes no ambiente digital;

[14] Art. 25. [...] § 2º Para cumprimento do disposto no caput, as lojas de aplicações de internet e os sistemas operacionais de terminais deverão: I - solicitar aos titulares a declaração da idade ou da faixa etária ao criar a conta; II - aferir a idade, mediante emprego de método confiável, nos termos estabelecidos pela ANPD, preferencialmente com a adoção de credenciais verificáveis, nos termos do disposto no art. 11 da Lei nº 15.211, de 17 de setembro de 2025; III - permitir a contestação e a retificação da classificação etária mediante apresentação de evidência adicional, com decisão fundamentada em prazo razoável; e IV - adotar medidas para evitar a criação de múltiplas contas ou outros artifícios com o objetivo de burlar os mecanismos de aferição de idade.

Figura 2 – Fluxograma de etapas na aferição de idade das lojas de aplicações/sistemas operacionais.

Como primeiro passo, o Decreto dispõe que será solicitada a autodeclaração do usuário, por meio da indicação da idade específica ou da faixa etária. A próxima fase é a aferição etária propriamente dita, que deve ser realizada por métodos confiáveis, preferencialmente com a adoção de credenciais verificáveis. Após a realização da aferição, o sinal etário deve ser compartilhado com outros atores por meio de interfaces de programação de aplicações (*Application Programming Interface* - API).

Essas interfaces devem ser projetadas de acordo com os princípios de privacidade desde a concepção e por padrão (*privacy by design* e *privacy by default*). Em função disso, a API deve permitir que esses fornecedores recebam apenas evidências da informação etária apurada, como a confirmação binária (sim/não) de que o usuário é ou não maior de 18 anos, sem acesso aos dados pessoais utilizados pelas lojas de aplicativo ou sistemas operacionais para gerar essa evidência, tais como documentos de identificação, data de nascimento ou dados biométricos.

Durante esse processo, deve ser assegurada a possibilidade de contestação pelo usuário, mediante a apresentação de informações adicionais. Essa medida contribui para a observância do princípio da qualidade dos dados (art. 6º, V, da LGPD),[15] mediante a correção de eventuais imprecisões, bem como para a garantia do direito fundamental do contraditório e da ampla defesa. Além disso, os agentes devem adotar medidas destinadas a prevenir a burla dos mecanismos de aferição de idade. Tais medidas estão relacionadas à robustez, à acurácia e à confiabilidade dos sistemas empregados.

Diante desse conjunto de obrigações, verifica-se que as lojas de aplicações e os sistemas operacionais desempenham papel central na cadeia digital de responsabilidades, ao realizarem a aferição inicial da idade e viabilizarem a circulação do sinal etário entre os agentes. Esse modelo reforça a lógica em camadas, baseada na combinação de métodos proporcionais, na validação contínua das informações e na possibilidade de revisão das decisões.

Por sua vez, os **demais fornecedores** de produtos e serviços de tecnologia da informação são responsáveis pela criação e disponibilização do conteúdo final ao usuário. Essa categoria abrange diferentes serviços e modelos de negócio, como provedores de jogos eletrônicos, redes sociais e serviços de conteúdo adulto.

[15] Art. 6º [...] V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

Em um primeiro plano, esses agentes devem garantir o adequado recebimento e processamento dos sinais de idade, nos termos do art. 14, *caput*, do ECA Digital.[16] Essa função não pode se limitar à simples recepção da informação, mas deve envolver a correta interpretação dos atributos etários e a tomada das providências correlatas, incluindo a implementação de medidas protetivas. Adicionalmente, os fornecedores devem prever mecanismos de contingência para hipóteses de falha ou indisponibilidade sistêmica na transmissão do sinal, bem como manter rotinas de auditoria e monitoramento contínuo do tratamento de dados, em aderência ao princípio da prevenção (art. 6º, inciso VIII, LGPD)[17]. Essas medidas favorecem a compatibilidade entre os sistemas e a integridade das decisões baseadas na idade dos usuários.

Como regra geral, **ao receber o sinal de idade** fornecido por lojas de aplicações e sistemas operacionais, **esses fornecedores devem adequar a experiência do produto ou serviço à faixa etária do usuário**. Não obstante, **o recebimento do sinal de idade não isenta a responsabilidade do fornecedor** pela efetividade da adequação etária e das medidas de proteção adotadas.[18]

Ademais, como já mencionado, **fornecedores de produtos, serviços ou conteúdos proibidos** para crianças e adolescentes **devem adotar mecanismos próprios de aferição de idade, na forma da verificação de idade** (ECA Digital, art. 9º; Decreto, art. 15). Em caso de divergência entre as informações – isto é, caso o sinal de idade divirja da aferição de idade realizada pelo próprio fornecedor – o Decreto estabelece que devem ser adotadas as medidas correspondentes à alternativa mais protetiva a crianças e adolescentes (art. 25, §4º).

Não obstante a necessidade de atuação coordenada, é importante esclarecer que a solidariedade prevista no art. 15 do ECA Digital não se confunde com aspectos jurídicos envolvendo a responsabilidade civil. Para o presente contexto, trata-se de diretriz de natureza regulatória, que orienta a interpretação das obrigações legais à luz do princípio da proteção integral estabelecido no art. 227, da Constituição Federal.[19] Com efeito, a solidariedade prevista no art. 15 do ECA Digital, sobre o ponto de vista regulatório, tem por objetivo principal assegurar a efetiva proteção de crianças e adolescentes no ambiente digital, em conformidade com o princípio do melhor interesse.

Ainda quanto à distribuição de responsabilidades, é importante considerar que o Decreto delimitou **obrigações gerais por categorias de fornecedores** de serviços ou produtos, e, ao mesmo tempo, **obrigações específicas por setores**. Há hipóteses específicas para o dever (ou a dispensa) de realizar aferição de idade, além de estabelecer obrigações acessórias, como a disciplina de etapas prévias, simultâneas ou posteriores à aferição, com a finalidade de reforçar a eficácia da proteção de crianças e adolescentes.

---

[16] Art. 14. Os fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável por eles deverão adotar medidas técnicas e organizacionais para garantir o recebimento das informações de idade de que trata o art. 12 desta Lei.

[17] Art. 6º. [...] VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

[18] Art. 26. [...] § 1º Após o recebimento de sinais de idade, caberá ao fornecedor adequar a experiência do produto ou do serviço de tecnologia da informação ao disposto na Lei nº 15.211, de 17 de setembro de 2025. [...] § 3º O recebimento de sinais de idade não isentará a responsabilidade do fornecedor de produtos ou serviços de tecnologia da informação pela efetividade da adequação etária e das medidas de proteção adotadas.

[19] Art. 227. É dever da família, da sociedade e do Estado assegurar à criança, ao adolescente e ao jovem, com absoluta prioridade, o direito à vida, à saúde, à alimentação, à educação, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária, além de colocá-los a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão.

As duas tabelas abaixo visam consolidar essas regras e facilitar o seu entendimento, dividindo as obrigações, respectivamente, por categorias gerais e por setores específicos. Vale ressaltar que um mesmo fornecedor pode estar enquadrado em uma determinada categoria de fornecedor na Tabela 1 (por exemplo, de conteúdo proibido) e, ao mesmo tempo, em um setor específico indicado na Tabela 2 (por exemplo, conteúdo pornográfico), devendo, portanto, atender a todas as obrigações legais indicadas.

Obrigações gerais por categorias de fornecedores			
Categorias	**Aferição de idade**	**Obrigações acessórias à aferição**	**Observações**
Lojas de aplicações e sistemas operacionais (art. 25)	Obrigatória, mediante emprego de método confiável, preferencialmente com a adoção de credenciais verificáveis.	Fornecimento gratuito de sinal de idade; Autorização dos responsáveis legais para *download* e instalação de aplicativos; e Informação quanto à classificação indicativa atribuída aos aplicativos antes da sua autorização.	N/A
Fornecedor de conteúdo, produto ou serviço impróprio ou inadequado (art. 14)	Pode ser uma medida necessária para assegurar a efetiva proteção de crianças ou adolescentes, especialmente em contextos de maior risco ou para fins de cumprimento de outros encargos legais (como supervisão parental).	Observância da classificação indicativa; Medidas técnicas e organizacionais, desde a concepção, de segurança por padrão, que podem incluir aferição de idade; e ferramentas efetivas de supervisão parental.	A ANPD poderá determinar a adoção de medidas de proteção adicionais, quando identificar riscos relevantes a crianças e adolescentes.
Fornecedor de conteúdo, produto ou serviço proibido (art. 15)	Mecanismos eficazes de verificação de idade, independentemente do sinal de idade recebido.	Impedir efetivamente o acesso, a fruição ou o consumo por crianças e adolescentes; Vedar a criação e identificar e remover contas e perfis de crianças e adolescentes (*no caso dos serviços indicados nos incisos VI a X do §*	N/A

		1º do art. 15, do Decreto)[20]	

Tabela 1 – Obrigações gerais de aferição de idade por categorias e suas obrigações acessórias.

Obrigações específicas por setores			
Setores	**Aferição de idade**	**Obrigações acessórias à aferição**	**Observações**
Conteúdo pornográfico (arts. 16 e 17)	Mecanismos próprios de verificação de idade que assegurem que não haja acesso por crianças e adolescentes, ainda que em forma de prévias, imagens, títulos ou legendas.	Nos casos de usuários não cadastrados, quando a idade não for verificada ou quando a conta for operada por criança ou adolescente deve-se ocultar, desfocar ou não exibir, por padrão, conteúdo pornográfico ou exigir a verificação de idade para desbloqueio.	O autoenquadramento do fornecedor quanto ao conteúdo pornográfico poderá ser revisto por determinação da ANPD, com base na natureza preponderante ou nos efeitos práticos do produto ou do serviço (art. 16, §3º, Decreto). Nessa situação, esses fornecedores estarão obrigados a proceder com a verificação etária de seus usuários.
Plataformas de comércio eletrônico e *marketplaces* (compra e venda serviços ou produtos proibidos) (art. 18)	Mecanismos efetivos de verificação de idade no ato do cadastro ou no momento de aquisição do produto.	Bloqueio à aquisição dos produtos e serviços, por padrão, por usuário criança ou adolescente ou por usuário não cadastrado ou não autenticado.	N/A
Redes sociais (art. 19)	Mecanismos efetivos de verificação de idade, caso disponibilize conteúdo, serviço ou produto proibido; e mecanismos de aferição de idade quando necessário para assegurar a efetiva proteção de crianças ou adolescentes ou para fins de cumprimento de outros encargos legais,	Devem vincular as contas dos menores de 16 (dezesseis) anos a dos seus respectivos responsáveis legais (art. 24, ECA Digital).	N/A

[20] Jogos de azar, apostas, loterias e equivalentes, jogos eletrônicos com caixas de recompensa, provedores de conteúdo pornográfico, serviços de acompanhantes ou com finalidade de marcar encontros ou relacionamentos de cunho sexual.

	especialmente efetivar as ferramentas de supervisão parental e demais obrigações que envolvam limitações de idade.		
Jogos de azar e casas de apostas	Mecanismos eficazes de verificação de idade, independentemente do sinal de idade recebido	Devem vedar a criação de contas e perfis por crianças e adolescentes, além de remover as existentes.	Lojas de aplicações e sistemas operacionais devem impedir a disponibilização do produto ou serviço, caso estes não adotem verificação de idade ou não possuam autorização de funcionamento emitida pelos órgãos competentes (art. 21).
Jogos eletrônicos com caixas de recompensa (art. 23)	Mecanismos eficazes de verificação de idade, independentemente do sinal de idade recebido, de modo a impedir o acesso à caixa de recompensa pelo usuário.	Deverão, por padrão, limitar as funcionalidades de interação a usuários, de modo a assegurar o consentimento dos pais ou responsáveis (art. 21, parágrafo único, ECA Digital).	A verificação de idade é dispensada nos casos de jogos sem caixas de recompensa ou com restrição completa, por padrão, do acesso a esta funcionalidade.
Serviços com controle editorial, de conteúdos protegidos por direitos autorais e de conteúdo musical ou literário (art. 22)	Dispensada, desde que implementadas as obrigações acessórias indicadas na coluna ao lado.	Devem disponibilizar conta ou perfil infantil e mecanismos de supervisão parental, sistemas de bloqueio ou restrição de acesso.	N/A
Provedores de conteúdo jornalístico e esportivo (art. 22, parágrafo único)	Dispensada, desde que o serviço não se sujeite à classificação indicativa e se submeta a controle editorial.	N/A	N/A

Tabela 2 – Obrigações de aferição de idade atribuídas a setores específicos e suas obrigações acessórias.

III. REQUISITOS GERAIS

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) ao uso do serviço ou do produto; e

(ii) ao próprio mecanismo de aferição de idade a ser adotado;

(iii) ao contexto, à natureza do serviço, às funcionalidades e ao ambiente de fornecimento.

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 18 (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”.[21]

Assim, para se alcançar o nível de proteção almejada, a indicação do mecanismo deve se orientar pela **gestão de riscos em múltiplas camadas**, dependendo da gravidade dos riscos e do contexto, à natureza do serviço, às funcionalidades e ao ambiente de fornecimento. Essa visão é aderente com a legislação brasileira e com abordagens internacionais voltadas à proteção de crianças e adolescentes em ambientes digitais. Isso parte da premissa de que métodos isolados de aferição etária podem ser incapazes de garantir com a precisão desejada a idade do usuário, podendo apresentar falhas, possibilidade de burla, vulnerabilidades ou limitações técnicas.

Essa visão privilegia o requisito da proporcionalidade e possibilita que a aferição de idade seja estruturada com a utilização sucessiva de diferentes mecanismos, aplicados progressivamente conforme o grau de incerteza do resultado obtido em etapas anteriores. Por exemplo, mecanismos com menor grau de impacto podem ser utilizados para aferição etária preliminar. Caso seja identificada incerteza quanto à acurácia, robustez ou confiabilidade do resultado, ou uma proximidade com os limiares de erros, deve ser acionado método adicional de aferição, mais robusto.

Por outro lado, sempre que a idade do usuário for confirmada por meio de um método de alta confiabilidade e que possa gerar impacto à proteção de dados pessoais, recomenda-se que seja emitida credencial verificável ou atributo etário reutilizável. Isso permite que o usuário comprove sua idade em acessos futuros sem necessidade de repetir todo o processo de aferição.

Identificados os riscos, a próxima etapa consiste na determinação do nível de risco associado ao produto ou serviço. A Tabela 3 apresenta uma matriz contendo esse nivelamento, elencado conforme as características do serviço ou produto de tecnologia da informação. O racional é que mecanismos de aferição etária com um grau maior de impacto à privacidade, à proteção de dados pessoais, à segurança, à saúde e ao bem-estar de crianças e adolescentes devem ser reservados para contextos de risco elevado no ambiente digital. Por outro lado, mecanismos com menor nível de impacto deve ser priorizados em cenários de baixo risco. Essa abordagem busca equilibrar a proteção de crianças e adolescentes no ambiente digital com os direitos à privacidade e à proteção de dados pessoais.

Para cada nível de risco identificado por meio da Tabela 3 é possível encontrar uma lista exemplificativa de mecanismos de aferição de idade. Destaca-se que a relação não é exaustiva, permitindo a adaptação às especificidades de cada caso concreto, respeitando os parâmetros estabelecidos no ECA Digital, no art. 24 do Decreto, bem como os explicitados neste Guia Orientativo. Ressalta-se que a avaliação de risco é sempre contextual e deve levar em consideração as circunstâncias relevantes de cada situação concreta.

A tabela abaixo esquematiza, exemplificadamente, uma matriz de risco de acordo com as características do serviço ou produto. Entretanto, esta classificação de risco deve também considerar a probabilidade do impacto, a gravidade e o contexto. Desta maneira, esta tabela não deve ser interpretada de maneira absoluta e estanque. Além disso, a classificação abaixo está sujeita à adequação por esta Agência em casos concretos e em conformidade com a evolução das tecnologias e sua regulação responsiva no decorrer da implementação da lei. Assim, os regulados têm de centrar a análise de risco no impacto biopsicossocial e aos direitos de crianças e adolescentes, considerando sua autonomia progressiva e as peculiaridades de cada situação específica.

Nível de risco	Características do serviço ou produto; considerada a probabilidade, a gravidade e o contexto	Aferição exigida	Exemplos de mecanismos	Observações
Baixo risco	Serviços digitais que, embora não ofereçam conteúdo, produto ou serviço considerados impróprios, inadequados ou proibidos para menores de 18 (dezoito) anos de idade, podem gerar impactos adversos, ainda que indiretos. Exemplos: plataformas de conteúdo educacional e cultural; aplicativos de produtividade e utilidade; serviços de *streaming* de conteúdo classificado como adequado para todas as idades; jogos eletrônicos com classificação indicativa livre; serviços de busca e navegação na internet de uso geral.	Aferição com **mínimo** grau de impacto à privacidade, à proteção de dados pessoais, à segurança, à saúde e ao bem-estar de crianças e adolescentes.	• Recebimento de sinal de idade enviados por lojas de aplicações e sistemas operacionais; • Adoção de credenciais verificáveis.	A implementação deve priorizar soluções que minimizem a coleta de dados pessoais e reduzam fricções de acesso.
Risco moderado	Serviços que possuam efeitos adversos sobre a privacidade, a segurança e a saúde de crianças e adolescentes; que permitam interação entre usuários; que permitam compartilhamento de conteúdo ou exposição a conteúdo, produto ou serviço impróprio ou inadequado para menores de 18 (dezoito) anos; que façam tratamento de dados pessoais sensíveis; entre outras hipóteses dispostas nos artigos 1º, parágrafo único, III; 6º; 8º, III e IV; 9º; 17, § 4º; 21; 27 e 29 do ECA Digital. Os fornecedores de produtos, serviços e conteúdos impróprios e inadequados deverão, obrigatoriamente, receber sinais de idade, nos termos do art. 26 do Decreto. Exemplos: redes sociais; plataformas de vídeo com conteúdo misto; jogos eletrônicos com funcionalidade de interação entre usuários; jogos eletrônicos com microtransações; plataformas de mensageria instantânea de uso geral; serviços de *streaming* de música e *podcasts* com conteúdo explícito disponível; serviços de IA generativa de uso geral; serviços de saúde digital e bem-estar mental; plataformas de *e-commerce* de uso geral.	Aferição **proporcional** ao risco à privacidade, à proteção de dados pessoais, à segurança, à saúde e ao bem-estar de crianças e adolescentes.	• Recebimento de sinal de idade enviados por lojas de aplicações e sistemas operacionais; • Adoção de credenciais verificáveis, com base em provas criptografadas. • Uso de mecanismos de estimação etária, incluindo análise biométrica, acompanhada de medidas robustas de segurança da informação, especialmente quanto à proteção de dados pessoais e à privacidade; e • Uso de verificação de idade como serviço.[22]	Recomenda-se a adoção do modelo multicamadas, onde há o emprego sucessivo de mecanismos, nos quais métodos com menor grau de impacto sejam utilizados inicialmente, sendo complementados por mecanismos de aferição mais robustos apenas quando necessário. Recomenda-se a elaboração do Relatório de Impacto à Proteção de Dados Pessoais para documentar os tratamentos de dados realizados, os riscos e as medidas de proteção adotadas.

[22] Segundo a ANPD, "a verificação de idade como serviço consiste na terceirização do processo de verificação para instituições públicas ou privadas confiáveis, que assumem a responsabilidade de identificar e garantir a idade do usuário. Esse mecanismo utiliza dados pessoais como nome e data de nascimento, comparando-os com informações obtidas em bases de dados oficiais de órgãos públicos, bancos ou serviços sociais. [...] Nesse processo de verificação de idade, há a possibilidade de se recorrer a intermediários confiáveis que emitem *tokens* de idade (*age tokens*) para os usuários se autenticarem, conferindo maior segurança aos seus dados pessoais. 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.

Alto risco	Serviços que oferecem conteúdos, produtos ou serviços proibidos para menores de 18 (dezoito) anos de idade, nos termos do art. 15, §1º do Decreto. Jogos eletrônicos com caixas de recompensa (*loot boxes*), nos termos do art. 23 do Decreto, os quais deverão, obrigatoriamente, implementar mecanismos efetivos de verificação de idade. Os fornecedores de produtos, serviços e conteúdos proibidos deverão, obrigatoriamente, receber sinais de idade, nos termos do art. 26 do Decreto.	**Verificação** com alto grau de robustez, acurácia e confiabilidade, de forma a assegurar a proteção à privacidade, aos dados pessoais, à segurança, à saúde e ao bem-estar de crianças e adolescentes.	• Recebimento de sinal de idade enviados por lojas de aplicações e sistemas operacionais; • Adoção de credenciais verificáveis; • Uso de mecanismos de estimação etária, incluindo análise biométrica, acompanhada de medidas robustas de segurança da informação, especialmente quanto à proteção de dados pessoais e à privacidade, complementado com mecanismo de verificação; • Uso de verificação de idade como serviço; e • Verificação etária, incluindo a realizada por meio de documentos e com prova de vivacidade.	Recomenda-se a adoção do modelo multicamadas, onde há o emprego sucessivo de mecanismos, nos quais métodos com menor grau de impacto sejam utilizados inicialmente, sendo complementados por mecanismos de aferição mais robustos apenas quando necessário, exceto naqueles casos em que a verificação seja obrigatória. Deve-se, ademais, priorizar soluções que combinem elevada acurácia, robustez e confiabilidade com mecanismos avançados de proteção da privacidade, como arquitetura baseada em atributos etários ou provas criptográficas, que confirmem a idade sem revelar dados pessoais adicionais. Também deve-se evitar que os mecanismos gerem qualquer tipo de rastreabilidade ou monitoramento contínuo dos usuários no ambiente digital. Recomenda-se a elaboração do Relatório de Impacto à Proteção de Dados Pessoais para documentar os tratamentos de dados realizados, os riscos e as medidas de proteção adotadas.

Tabela 3 - Matriz de risco de produtos e serviços.

Exemplo: Francisco possui dispositivo *tablet* que é acessado por todos da casa. Seu filho, João, um estudante de 10 (dez) anos, é apaixonado por futebol e utiliza o *tablet* para acessar um portal para verificar as estatísticas do seu time. O dispositivo possui as configurações de supervisão parental ativadas por seu pai, que restringe o *download* de aplicativos e monitora o histórico de navegação. Ao carregar a página do portal, João não é interrompido por formulários de cadastro ou pedidos de documentos. Em segundo plano, o portal realiza uma inferência de sinal de idade, detectando que o navegador está operando sob um perfil restrito de sistema operacional e que os sinais de outras funcionalidades são consistentes com um acesso doméstico padrão (fuso horário e idioma). Como o portal possui controle editorial estrito, João navega livremente pelas tabelas e notícias esportivas, sem encontrar salas de bate-papo ou anúncios de produtos restritos, usufruindo de uma experiência segura e adaptada ao seu estágio de desenvolvimento.

Análise: O caso de João ilustra a aplicação prática do enquadramento em Baixo Risco. Conforme o parágrafo único do art. 22 do Decreto, os provedores de conteúdo jornalístico e esportivo submetidos a controle editorial e não sujeitos à classificação indicativa são dispensados de adotar métodos de aferição de idade. A plataforma observa o princípio da proporcionalidade (art. 24, I, Decreto) ao optar por mecanismos de baixa fricção, como a aferição por sinais técnicos e o respeito às configurações de controle parental do sistema operacional.

Exemplo: Uma plataforma de vídeos curtos é lançada com classificação indicativa de 12 (doze) anos nas lojas de aplicativos. A plataforma possui uma estética vibrante e foca em

desafios musicais e de dança. No entanto, o algoritmo de recomendação começa a impulsionar, de forma orgânica, uma tendência denominada "Desafio do Balão", que utiliza áudios de frequência perturbadora e edições com imagens subliminares de suspense, visando gerar reações de susto. João, um jovem de 12 (doze) anos, acessa a plataforma em seu *smartphone*. O sistema operacional, já configurado com o perfil de criança sob supervisão parental, envia automaticamente um sinal de idade (*token* etário) informando que o usuário possui entre 12 e 14 anos. Com base nisso, a plataforma permite o cadastro de João em uma conta vinculada à de seu responsável legal. Após interagir com o "Desafio do Balão" e outros conteúdos similares, João desenvolve quadros de ansiedade aguda. Diante da repercussão deste e de outros casos envolvendo crianças, o fornecedor realiza uma nova gestão de riscos e identifica que a funcionalidade de recomendação automatizada expôs usuários a conteúdo impróprio ou inadequado. Como medida, a classificação da funcionalidade de "Desafios Virais" é alterada e a plataforma implementa um bloqueio automático via sinais de idade para usuários como João.

Análise: O cenário descreve um serviço de rede social que, conforme o art. 1º, parágrafo único, III, do ECA Digital, apresenta risco significativo ao desenvolvimento biopsicossocial devido à finalidade de interação e compartilhamento em massa. O conteúdo, embora não contenha violência explícita, enquadra-se como impróprio ou inadequado, nos termos do art. 2º, I, do Decreto, por gerar riscos à saúde mental e ao bem-estar da criança. Neste caso de Risco Moderado, o fornecedor falhou inicialmente no gerenciamento de riscos de suas funcionalidades e algoritmos (art. 8º, I, ECA Digital), mas agiu corretamente ao readequar a experiência após a identificação do dano.

Exemplo: Uma plataforma é lançada no mercado como uma plataforma de disponibilização de conteúdos audiovisuais, apresentando inicialmente apenas vídeos com classificação livre. Em razão do catálogo aparentemente inofensivo, a empresa não implementa qualquer mecanismo de aferição de idade no cadastro inicial. No entanto, após o primeiro mês de operação, o canal de denúncias da plataforma recebe inúmeros relatos de pais informando que, por meio de *links* de "parceiros" e aplicações integradas dentro da interface, era possível acessar conteúdos proibidos para crianças e adolescentes. Diante dessa constatação, a empresa passa a exigir mecanismo de verificação de idade, com elevado grau de robustez, acurácia e confiabilidade, sempre que o usuário tenta acessar as áreas de integração com terceiros que disponibilizam conteúdos proibidos.

Análise: O cenário ilustra a aplicação do princípio da proporcionalidade diante da descoberta de riscos não mapeados inicialmente. A falha inicial ocorreu na subestimação do risco das "funcionalidades de integração", em razão da disponibilização de conteúdos ofertados por terceiros. Dada a existência de conteúdos proibidos, a verificação de idade é medida obrigatória, corretamente implementada pela empresa.

Uma vez identificados os riscos e seus níveis respectivos, é necessário elencar as medidas de segurança técnicas e administrativas aptas a mitigá-los. Elas devem ser compatíveis com a natureza dos dados pessoais tratados e com as vulnerabilidades do mecanismo de aferição de idade e do produto, serviço ou conteúdo ofertado.

Adicionalmente, os fornecedores, consoante o disposto no art. 16 do ECA Digital, deverão disponibilizar aos responsáveis legais, crianças e adolescentes, as informações sobre

os riscos e as medidas de segurança adotadas para esse público, incluídas as que se refiram à privacidade e à proteção de dados pessoais. [23]

Diante disso, a Tabela 4 exemplifica riscos identificados no contexto de produtos, serviços e conteúdos e os relacionados aos próprios mecanismos de aferição de idade. Ademais, são trazidas amostras de ações de mitigação aptas a serem empregadas. Importante mencionar, ainda, que a escolha das medidas de segurança aplicáveis dependerá de cada caso concreto, do estado da arte tecnológico e da gestão de riscos conduzida.

Exemplos de riscos[24]	Exemplos de medidas de mitigação
Riscos advindos do tratamento de dados pessoais e de proteção à privacidade	• Tratar apenas os dados pessoais que sejam estritamente necessários para o processo de aferição etária, em obediência ao princípio da necessidade; • Determinar de forma clara a finalidade do tratamento de dados pessoais para o processo de aferição de idade; • Observar o princípio da transparência; • Escolher a hipótese legal mais adequada quanto ao tratamento a ser realizado; • Elaborar Relatório de Impacto à Proteção de Dados – RIPD e Registro de Operação de Tratamento - ROT; • Não possibilitar que os dados pessoais tratados de determinado usuário fiquem visíveis para outros usuários do serviço ou produto; • Garantir privacidade por *design* e por padrão; • Excluir imediatamente os dados pessoais, ao final do processo de aferição de idade; • Coletar dados pessoais necessários para fornecer cada elemento do serviço ou produto apenas quando a criança ou adolescente estiver ativo e conscientemente envolvido no elemento em específico; • Manter conformidade com níveis adequados de acurácia, robustez e confiabilidade quanto à aferição de idade; • Implementar medidas que elevem os níveis de acurácia, robustez e confiabilidade quanto à aferição de idade; • Utilizar credenciais verificáveis e tecnologias como duplo-cego; e • Fornecer informações concisas, claras e acessíveis a crianças, adolescentes e responsáveis legais.

[23] Art. 16. Os fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável por eles deverão disponibilizar a pais, responsáveis legais, crianças e adolescentes, com acesso de forma independente da aquisição do produto, informações sobre os riscos e as medidas de segurança adotadas para esse público, incluídas a privacidade e a proteção de dados, em conformidade com o disposto no art. 14 da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais).

[24] Alguns dos riscos e exemplos de mitigação aqui delineados foram baseados na publicação "Age appropriate design: a code of practice for online services", do Information Commissioners's Office, disponível em: < https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/ >, e outros na pesquisa "*Age Assurance Data Access Study*", conduzida pelo Departamento de Ciência, Inovação e Tecnologia do Governo do Reino Unido, disponível em <https://www.gov.uk/government/publications/age-assurance-data-access-study>.

	• Estabelecer a configuração de privacidade do usuário no mais alto nível de proteção disponível; • Limitar, por padrão, o tratamento de dados pessoais de crianças e adolescentes ao uso essencial do produto ou serviço; • Dar ao usuário a possibilidade de alterar suas configurações de privacidade permanentemente ou de retornar às configurações padrão quando a sessão for encerrada; • Não incentivar o usuário a escolher uma opção de privacidade inferior; e • Manter todas as configurações de privacidade aplicadas pelo usuário quando da atualização do produto ou serviço. Caso não seja possível, definir a configuração de privacidade no nível mais alto.
Riscos advindos do uso de Inteligência Artificial	• Informar previamente aos usuários acerca da utilização de Inteligência Artificial para o processo de aferição de idade; • Tratar apenas dados pessoais estritamente necessários para a consecução da finalidade proposta; • Não utilizar para outras finalidades dados pessoais coletados para fins de aferição de idade; • Mitigar vieses e garantir a não discriminação ilícita ou abusiva; • Garantir que os métodos de aferição de idade atendam ao grau mínimo de acurácia, robustez e confiabilidade; e • Avaliar o risco algorítmico à segurança e à saúde de crianças e adolescentes.
Riscos advindos da verificação como serviço (VaaS)	• Diligenciar previamente quanto à robustez, acurácia e confiabilidade da idade confirmada e quanto à conformidade com as legislações aplicáveis, em especial a LGPD e o ECA Digital; • Fornecer aos usuários informações claras sobre o serviço de aferição de idade utilizado; e • Confirmar a idade do usuário por meio de um titular de conta que seja comprovadamente maior de idade.
Burla de mecanismos de aferição de idade	• Desencorajar *designs* de produto ou serviço no qual haja a pré-seleção, automática, de determinadas idades por padrão; e • Impedir que usuários enviem imediatamente uma nova idade caso tenham o seu acesso negado.
Riscos advindos da verificação etária	• Adotar mecanismos de aferição com menor grau de impacto à privacidade, desde que atendam aos graus mínimos de acurácia, robustez e confiabilidade e nas hipóteses permitidas.
Riscos advindos do compartilhamento de dispositivos	• Permitir, em caso de dispositivos compartilhados, que os usuários possam configurar perfis próprios com suas configurações de privacidade individuais. Os perfis podem ser acessados por meio de opções na tela ou usando tecnologia de reconhecimento de voz para serviços *online* ativados por voz; e • Incluir informações claras para a pessoa que configura ou registra o dispositivo, alertando-a sobre a possibilidade de os dados pessoais de vários usuários serem coletados.
Riscos advindos de estimativa biométrica	• Realizar o processamento no próprio dispositivo do usuário, com armazenamento centralizado; • Adotar medidas de segurança robustas, aptas a protegerem os dados sensíveis tratados;

	• Limitar o pré-processamento e a extração de características biométricas às informações estritamente necessárias para a estimativa de idade; • Utilizar sistemas de inteligência artificial adequados para somente estimar idade, com preferência por soluções que classifiquem a idade em faixas etárias; • Implementar a zona de incerteza ("buffer zone") para casos em que haja proximidade ao limiar legal aplicável; • Adotar ferramentas de controle de integridade e prova de vivacidade ("liveness detection"); e • Explorar o uso de métodos alternativos de estimativa etária.
Limitação da disponibilidade de conjuntos de dados de treinamento e de teste representativos e de alta qualidade, especialmente de crianças e adolescentes, para estimativa etária facial	• Aprimorar os conjuntos de dados utilizados, de forma a reduzir vieses e aumentar a acurácia; • Garantir a minimização do uso de dados pessoais; • Elaborar o Relatório de Impacto à Proteção de Dados Pessoais; e • Estruturar os testes, de forma a viabilizar a identificação de onde as ferramentas apresentam dificuldades, possibilitando melhorias em termos de imparcialidade e confiabilidade.

Tabela 4 – Exemplos de riscos e medidas de segurança aplicáveis.

Para além do que já foi disposto, cumpre enfatizar que 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 LGPD[25] e do art. 16, parágrafo único, do ECA Digital[26], 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 é a avaliação de impacto de riscos à segurança e à saúde de crianças, prevista no art. 47 do Decreto. O documento tem um escopo ligeiramente mais amplo do que o RIPD, na medida em que analisa o risco sob outras óticas, as quais são igualmente importantes para o sistema legal de tutela de crianças e adolescentes no ambiente digital. De toda forma, todos eles devem dialogar entre si, a fim de gerar coesão nas ações protetivas tomadas pelos fornecedores.

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:

[25] Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.

[26] Art. 16, Parágrafo único. Na hipótese de tratamento de dados de crianças e de adolescentes, sobretudo quando realizado para fins que não os estritamente necessários para a operação do produto ou serviço, o controlador a que se refere o inciso VI do art. 5º da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), deverá:
I – mapear os riscos e envidar esforços para mitigá-los; e
II – elaborar relatório de impacto, de monitoramento e de avaliação da proteção de dados pessoais, a ser compartilhado sob requisição da autoridade administrativa autônoma de proteção dos direitos de crianças e de adolescentes no ambiente digital, na forma de regulamento.

- Identifiquem e avaliem os riscos associados ao conteúdo, produto ou serviço digital, especialmente os potenciais efeitos adversos sobre a privacidade, a segurança e a saúde de crianças e adolescentes. Nesse sentido, recomendam-se que sejam avaliadas questões como o grau de interação social entre usuários e riscos de aliciamento ou contato com desconhecidos, por exemplo;

- 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;

- Avaliem a proporcionalidade entre os riscos do produto ou serviço e os riscos decorrentes do mecanismo de aferição de idade a ser implementado;

- Definam o nível de risco de seu produto, serviço ou conteúdo e adotem medidas, técnicas e administrativas, aptas a mitigar os riscos identificados; e

- Elaborem instrumentos de governança, como o Relatório de Impacto à Proteção de Dados Pessoais e a Avaliação de Impacto de riscos à segurança e à saúde de crianças.

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 sob condições controladas**. 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.

Quando o método de aferição etária gerar resultados binários — como a indicação de que um determinado usuário é maior ou menor que determinada idade — poderão ser empregadas métricas de medição como Taxa de Verdadeiros Positivos[27], Taxa de Falsos Positivos[28] e Taxa de Falsos Negativos[29]. Já nos casos em que o resultado do método seja a idade aproximada ou a indicação de uma faixa etária, poderão ser utilizadas métricas

[27] Segundo a ISO/IEC 27566-1:2025, a Taxa de Verdadeiros Positivos refere-se ao valor medido correto em resultados positivos, ou seja, o caso em que tanto o resultado medido quanto o resultado correto são positivos.
[28] Segundo a ISO/IEC 27566-1:2025, a Taxa de Falsos Positivos relaciona-se ao valor medido incorreto em resultados positivos, ou seja, o caso em que o valor medido é positivo, mas o valor correto é negativo.
[29] Segundo a ISO/IEC 27566-1:2025, a Taxa de Falsos Negativos é valor medido incorreto em resultados negativos, ou seja, o caso em que o valor medido é negativo, mas o valor correto é positivo.

estatísticas como Desvio Padrão[30], Erro Percentual Absoluto Médio[31] e Pontuação Cumulativa.[32]

Ademais, os métodos de aferição de idade devem ser reavaliados periodicamente, de forma a assegurar que a acurácia seja melhorada quando possível, seja através de novas tecnologias ou de modificações no processo de aferição de idade. Nos casos que envolverem estimativa de idade e os testes de acurácia indicarem risco de erro, recomenda-se a adoção de margens de segurança. Por exemplo, quando a margem de erro estimada for significativa em relação ao limiar legal, poderá ser necessário empregar mecanismo adicional de aferição para usuários cujas idades estimadas se encontrem próximas desses limites.

Exemplo: Maria tem 17 anos e 10 meses e tenta criar uma conta na plataforma de filmes. O serviço utiliza um sistema de inteligência artificial para estimar a idade através da biometria facial, alegando uma Taxa de Verdadeiros Positivos de 96%. No entanto, ao processar a imagem do rosto de Maria, o sistema situa o usuário na "zona cinzenta" (entre 17 e 20 anos), onde a precisão cai para 82%. Em vez de oferecer uma solução célere, a plataforma bloqueia o acesso e informa que realizará uma análise manual por especialistas, sem fornecer uma previsão de conclusão. Devido à ineficiência operacional, o processo de conferência se arrasta por 70 dias. Nesse intervalo, Maria completa 18 anos, atingindo a maioridade legal. Contudo, como o seu pedido original ainda consta como "em análise" no sistema, ele permanece impedido de acessar os conteúdos da plataforma, ficando totalmente excluído do serviço mesmo após possuir a idade adequada.

Análise: O exemplo aborda uma falha no requisito de acurácia e nos deveres de governança. Ao não prever um fluxo que leve em consideração os possíveis desdobramentos para idades na faixa de transição, o fornecedor permitiu que uma imprecisão técnica temporária se transformasse em uma restrição ilegítima de acesso à plataforma. Assim, a aferição tornou-se um obstáculo técnico desproporcional, que impediu o exercício da autonomia de um usuário que já havia atingido a plena capacidade civil.

A **robustez** corresponde à **capacidade do mecanismo de aferição de idade em 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.

Entre as medidas indicadas, cita-se a autenticação multifator[33], o envio de códigos temporários (*One Time Passcode* – OTP)[34] e a solicitação de captura de imagem por parte do

[30] Desvio Padrão: indica o grau de variação de um conjunto de elementos. Serve para dizer o quanto os valores dos quais se extraiu a média são próximos ou distantes da própria média.
[31] Erro Percentual Absoluto Médio: média de todos os erros absolutos percentuais. Fornece uma indicação do tamanho médio do erro, expresso como uma percentagem do valor observado, independentemente de o erro ser positivo ou negativo.
[32] Pontuação Cumulativa: pontuação agregada calculada pela soma das pontuações individuais ao longo de um período/categoria *etc*.
[33] Verificação da identidade de um determinado usuário através de dois ou mais fatores de autenticação, como senha, biometria, *tokens* e cartões inteligentes.
[34] Código gerado automaticamente e válido para uma única sessão.

usuário no momento do envio de documentos para fins de aferição de idade. A utilização de prova de vivacidade[35] poderá ser adotada como controle técnico adicional para dificultar ou impedir o uso de imagens estáticas ou sintéticas, assim como outros recursos destinados a contornar a eficácia do mecanismo de aferição etária. Adicionalmente, reitera-se a necessidade de reavaliação periódica dos mecanismos de aferição de idade, considerando a evolução tecnológica ou eventuais modificações no processo de aferição. A reavaliação contribui para assegurar a robustez do método empregado ao longo do tempo.

Exemplo: Samara, uma adolescente de 14 (catorze) anos, decide utilizar seus conhecimentos no mundo esportivo e tenta realizar o cadastro em uma plataforma de apostas esportivas de quota fixa, **atividade classificada "proibida"** para crianças e adolescentes, podendo ser considerada, por isso, como de Alto Risco. Ciente de que sua idade a impede de acessar o serviço, Samara utiliza o documento de identidade de sua mãe e, durante a etapa de validação facial exigida pelo aplicativo, tenta burlar o sistema posicionando uma fotografia impressa em alta resolução do rosto de sua mãe em frente à câmera do dispositivo. O *software* faz a coleta dos dados biométricos, mas não é capaz de identificar características para comprovar se as informações estão sendo captadas em tempo real. Com isso, acreditando se tratar de adulto, o sistema permite o acesso ao portal principal da plataforma e oferece crédito especial para a primeira aposta.

Análise: O cenário ilustra a aplicação prática da falta de robustez. Diferente da acurácia, que mede o desempenho em ambientes controlados, a robustez foca na resiliência do sistema diante de estratégias de contorno que estejam ao alcance do público infantojuvenil. Como o serviço de apostas é considerado como de Alto Risco, o fornecedor possui o dever legal de implementar mecanismos de verificação de idade eficazes que garantam o impedimento efetivo de acesso por crianças e adolescentes. Assim, a escolha da validação de informações por meio da biometria facial pode, *a priori*, ser justificada. No entanto, a sua implementação deve ser acompanhada de técnicas que garantam uma aplicação correta e eficaz, sob o risco de ofensa à robustez. No caso narrado, a ausência de detecção de vivacidade como parâmetro adicional gera vulnerabilidades nítidas para o sistema, pois permite a ocorrência de fraudes e falsos positivos. Portanto, o emprego desse método deve ser acompanhado de providências que garantam a sua eficácia.

A **confiabilidade** (em sentido estrito)[36], 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

[35] Segundo a ISO/IEC 27566-1:2025, a prova de vivacidade pode ser entendida como a medição e análise de características anatômicas ou reações involuntárias ou voluntárias, a fim de determinar se uma amostra biométrica está sendo capturada de um sujeito vivo presente no ponto de captura.

[36] 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 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.*

dependem de informações facilmente manipuláveis e carecem de fontes de dados íntegras e independentes.[37]

Nesses termos, os sistemas devem ser testados e monitorados de forma contínua, garantindo-se que os resultados possam ser reproduzíveis, isto é, assegurando que entradas iguais ou semelhantes produzam saídas iguais ou semelhantes, dentro de parâmetros aceitáveis de variação. Para tanto, recomenda-se a definição prévia de indicadores de desempenho que permitam avaliar a estabilidade, a reprodutibilidade e a previsibilidade dos resultados obtidos, tanto em ambientes de teste quando em ambientes de utilização real. Em situações em que sejam identificados resultados inesperados ou inconsistentes, deve ser conduzida análise de causa-raiz, com a adoção de medidas corretivas adequadas.

Com efeito, os fornecedores devem ser capazes de demonstrar, de forma documentada, que o mecanismo de aferição de idade foi implementado de maneira confiável e em conformidade com os requisitos legais e técnicos aplicáveis. Para tanto, deverão ser mantidos registros auditáveis das ações realizadas em cada processo de aferição de idade, garantindo-se, assim, rastreabilidade e transparência das operações.

Exemplo: João, um usuário adulto, tenta acessar um portal de serviço de anúncio de acompanhantes. Ao entrar no *site*, todas as imagens de conteúdo sexualmente explícito aparecem com um efeito de ocultação. Para visualizar o conteúdo completo e remover as restrições, o portal exige uma estimação de idade por biometria facial. João aceita os termos e autoriza a coleta de sua biometria. No entanto, antes mesmo de a câmera realizar a leitura facial, o *script* do mecanismo de aferição trava devido a uma instabilidade crônica no servidor da plataforma. João tenta atualizar a página, mas, em razão de um erro na programação do *site*, o conteúdo explícito é exibido integralmente, mesmo sem que a verificação de idade tenha sido concluída com sucesso. Devido a essa falha técnica, o portal expõe conteúdos proibidos sem qualquer controle.

Análise: O cenário ilustra uma violação ao requisito de confiabilidade, previsto no art. 24, II, do Decreto. Neste caso, o sistema demonstrou não ser tecnicamente qualificado, ao permitir que uma falha técnica resultasse na exposição de conteúdos sensíveis. Para serviços de Alto Risco, como os de acompanhantes, a legislação exige o impedimento efetivo de acesso por crianças e adolescentes, devendo-se ocultar o conteúdo pornográfico, por padrão (arts. 16, §1º; e, 17, I, do Decreto). Um sistema confiável deve ser projetado sob a égide da segurança por padrão, garantindo que, em caso de erro ou travamento, o acesso permaneça bloqueado até que a idade seja confirmada. Assim, a aferição falhou em sua instrumentalidade, pois em vez de viabilizar um ambiente seguro, a tecnologia instável tornou-se uma porta aberta para a violação de direitos do público infantojuvenil.

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:

[37] 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.

- 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;

- 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; e

- 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.

- Implementem medidas técnicas e organizacionais de segurança que abranjam todo o ciclo de vida do tratamento dos dados, de maneira a detectar tentativas de burla e fraudes. Nesse sentido, os sistemas utilizados devem permitir: a captura segura e a validação automática de documentos oficiais, quando for o caso; a realização de análise de consistência entre o documento utilizado para a aferição etária e o usuário; a detecção de documentos adulterados, falsificados, reutilizados ou quaisquer outras tentativas de fraudes; e a invalidação automática de tokens ou credenciais expiradas.

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, 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 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 Poder 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 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 confiram 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, 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 Proof* – 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 inferências sobre hábitos, preferências e padrões de navegação. A limitação do uso secundário, nesse contexto, deve aplicar-se tanto aos dados brutos coletados durante a aferição quanto aos dados derivados produzidos pelo sistema de aferição utilizado, incluindo sinais etários, classificações de faixa etária ou tokens de idade emitidos para autorizar o acesso ao serviço ou produto.

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.

Em relação ao tratamento de dados pessoais decorrente da coleta de documentos para fins de aferição etária, a necessidade de **eliminação imediata e irreversível** após o cumprimento da finalidade de aferir a idade ou faixa etária é prevista no art. 24, § 3º do Decreto.

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.

- Privilegiem a implementação de arquitetura baseada em atributos etários tokenizados e o uso de credenciais verificáveis.

- Utilizem mecanismo de aferição etária que adotem arquitetura em modelo *double-blind*. O fornecedor de serviços ou produtos digitais, sempre que possível e considerado o risco da plataforma, não deve ter acesso à identidade civil do usuário ou a qualquer dado que o identifique direta ou indiretamente.

- Façam a separação funcional entre sistemas de aferição etária e outros sistemas da plataforma ou serviço digital. Os sistemas responsáveis pela aferição etária devem operar de forma segregada das demais infraestruturas de tratamento de dados da plataforma, especialmente aquelas destinadas a publicidade direcionada; análise comportamental; personalização de conteúdo; e treinamento de modelos de inteligência artificial.

- Restrinjam o acesso aos dados pessoais coletados no procedimento de aferição etária. Os dados pessoais coletados durante o processo de aferição etária devem estar sujeitos a controles rigorosos de acesso, de modo que apenas sistemas e profissionais estritamente envolvidos na operação da aferição possam acessar tais informações.

- Limitem o armazenamento de dados pessoais brutos utilizados na aferição. Sempre que possível, os dados brutos utilizados durante o processo de aferição etária devem ser eliminados imediatamente após a conclusão da aferição. Os sistemas devem reter apenas o resultado da aferição etária, eliminando-se os dados brutos utilizados.

- Incluam cláusulas de limitação do uso secundário dos dados pessoais em políticas internas e contratos com colaboradores. É recomendável que esses instrumentos contenham cláusulas específicas que proíbam expressamente o uso secundário dos dados coletados no contexto da aferição de idade.

Exemplo: Uma aplicação de vídeos adota um sistema de inferência de idade de alta precisão que utiliza um "rastreamento de rotina". O mecanismo monitora constantemente a geolocalização do dispositivo e cruza esses dados com o Cadastro Nacional de Estabelecimentos de Ensino. Ao detectar que o usuário permanece em perímetros escolares ou creches em horários letivos, o sistema infere a condição de criança ou adolescente, bloqueando determinados conteúdos. Além disso, a empresa utiliza dados de parceiros comerciais para monitorar se o usuário consome produtos restritos a adultos em outros *sites* para validar a sua maioridade.

Análise: O cenário apresentado descreve um mecanismo que, apesar de eficaz do ponto de vista técnico, é juridicamente defeituoso por violar pilares fundamentais da LGPD, do ECA Digital e do Decreto. Primeiramente, a utilização de geolocalização e o monitoramento de hábitos externos configuram uma prática desproporcional e incompatível com o princípio do melhor interesse da criança e do adolescente. Ademais, conforme o art. 13 do ECA Digital e o art. 24, III, do Decreto, os dados coletados para aferição de idade não podem ser utilizados para qualquer outra finalidade, especialmente para a criação de perfis comportamentais ou rastreamento de rotina. Por fim, a estratégia viola a vedação à rastreabilidade da identidade e do histórico de acessos (art. 24, VIII, do Decreto), uma vez que a aferição se baseia na vinculação da identidade do usuário a padrões de vida privada.

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 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 de forma ilícita ou abusiva.

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 de forma ilícita ou abusiva 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;

- Avaliem, periodicamente, o desempenho dos sistemas de inteligência artificial, a fim de conferir a existência de vieses algorítmicos em mecanismos automatizados de aferição etária, que podem envolver fatores como idade, gênero, raça, etnia ou outras condições; e

- Garantam a acessibilidade tecnológica dos sistemas de aferição etária implementados para dispositivos com menor capacidade tecnológica ou com conexões de internet limitadas.

Exemplo: Uma aplicação de internet implementa um mecanismo de aferição de idade para acesso a salas de bate-papo moderadas. O sistema exige uma "prova de vivacidade" por meio de biometria facial, na qual o usuário deve seguir comandos rápidos de voz (como "pisque os olhos", "vire a cabeça para a direita" ou "sorria") e realizar um desafio de coordenação motora fina (capacidade de realizar movimentos preciso com as mãos e dedos) na tela. Maria, uma usuária com deficiência motora severa e deficiência auditiva, não consegue processar os comandos sonoros nem executar os movimentos físicos exigidos no tempo estipulado pelo *software*. Sem a oferta de um método alternativo acessível, Maria tem seu acesso negado sistematicamente, sendo impedida de participar da comunidade digital.

Análise: O cenário descreve uma violação direta ao requisito de inclusão e não discriminação previsto no art. 24, X, do Decreto. Ao ignorar a diversidade de capacidades dos usuários, a plataforma cria barreiras tecnológicas e nas comunicações, definidas pelo art. 3º, IV, "d" e "f", da Lei nº 13.146/2015[38], Estatuto da Pessoa com Deficiência (EPD), que dificultam ou impedem o acesso da pessoa com deficiência às tecnologias. Conforme estabelece o art. 4º, VII, do ECA Digital, a proteção de crianças e adolescentes no ambiente digital deve observar obrigatoriamente os princípios do EPD. Isso significa que a incapacidade de ajuste dos mecanismos adotados não pode impedir o acesso de pessoas com necessidades especiais às plataformas. A falha do fornecedor em oferecer adaptações razoáveis ou métodos alternativos resulta em uma exclusão indevida da vida digital. A implementação de tais soluções não deve resultar no impedimento desproporcional de acesso a serviços legítimos para grupos vulnerabilizados, sob pena de configurar discriminação algorítmica e produzir efeitos desvantajosos injustificados baseados na condição de saúde ou deficiência.

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,

[38] Art. 3º Para fins de aplicação desta Lei, consideram-se: [...] IV - barreiras: qualquer entrave, obstáculo, atitude ou comportamento que limite ou impeça a participação social da pessoa, bem como o gozo, a fruição e o exercício de seus direitos à acessibilidade, à liberdade de movimento e de expressão, à comunicação, ao acesso à informação, à compreensão, à circulação com segurança, entre outros, classificadas em: [...] d) barreiras nas comunicações e na informação: qualquer entrave, obstáculo, atitude ou comportamento que dificulte ou impossibilite a expressão ou o recebimento de mensagens e de informações por intermédio de sistemas de comunicação e de tecnologia da informação; [...] f) barreiras tecnológicas: as que dificultam ou impedem o acesso da pessoa com deficiência às tecnologias.

XI, do Decreto. Especificamente em relação às 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).

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 tipo de mecanismo de aferição de idade utilizado, o funcionamento e a finalidade desse mecanismo, 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 regulatórias, esse tipo de documento não cumpre o objetivo mais amplo de reduzir assimetrias informacionais e empoderar o usuário. Por isso, é deve-se disponibilizar as informações mais essenciais sobre o funcionamento do mecanismo de aferição de idade, em linguagem simples e em formatos acessíveis, incluindo recursos interativos e visualmente atrativos, antes do início do procedimento de aferição. 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, os fornecedores de produto ou serviço de tecnologia da informação devem documentar 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, deve-se, ainda, manter registros de auditoria (*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 os tipos de mecanismos de aferição de idade utilizados, as suas finalidades, quais dados são utilizados, quem são os

agentes envolvidos no tratamento, inclusive em caso de compartilhamento, bem como os seus papéis nos procedimentos, e as consequências da aferição de idade para o usuário;

- 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 auditabilidade; e
- Garantam integridade, rastreabilidade e possibilidade de auditoria independente de componentes, operações e registros associados aos mecanismos de aferição de idade.

Exemplo: Um fornecedor disponibiliza serviços de aferição de idade para aplicações de internet, processando a validação etária por meio da coleta de fotos de documentos de identidade e selfies, incluindo prova de vivacidade. Em seu site e em seus termos de uso, a empresa afirma: "não armazenamos seus documentos; as imagens são descartadas imediatamente após a validação". Contudo, após um incidente de segurança, uma auditoria técnica revela que as imagens originais permaneciam salvas em uma pasta temporária de cache do servidor e, além disso, eram utilizadas para o treinamento de sistemas Inteligência Artificial da própria empresa.

Análise: O cenário descreve violações aos requisitos de transparência e auditabilidade (Art. 24, XI, do Decreto) e ao dever de eliminação de dados. A disponibilização de informações que não correspondem à prática efetivamente realizada pela empresa, configura uma infração ao princípio da transparência. Ademais, conforme o art. 24, § 3º, do Decreto, o tratamento de dados decorrente da coleta de documentos deve limitar-se à confirmação da idade, sendo vedado o armazenamento ou retenção da imagem, que deve ser eliminada de modo imediato e irreversível após a captura da informação necessária. Por fim, a utilização desses dados para treinar algoritmos viola a vedação ao uso secundário, estabelecida pelo art. 13 do ECA Digital e reforçada pelo art. 24, III, do Decreto.

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.

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.

No âmbito do ECA Digital, a interoperabilidade está prevista no art. 12, III. De acordo com este dispositivo, as lojas de aplicações de internet e sistemas operacionais de terminais deverão possibilitar, por meio de Interface de Programação de Aplicações 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 salvaguardas 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 etário 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.[39]

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,

[39] 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.

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.

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.

A interoperabilidade também preserva *a liberdade de escolha do usuário*, nos termos do art. 49, caput do Decreto, em relação às soluções adotadas, ao evitar o aprisionamento do usuário a um único provedor ou tecnologia específica, favorecendo a autonomia da escolha e impulsionando o constante desenvolvimento de soluções de aferição de idade confiáveis e eficazes.

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 a finalidade do compartilhamento, os agentes autorizados, as salvaguardas de segurança e os mecanismos destinados a impedir o compartilhamento contínuo, automatizado e irrestrito de dados pessoais.

Exemplo: Com o objetivo de reduzir a fricção no acesso e evitar a coleta repetitiva de dados sensíveis, um consórcio de plataformas digitais adota o sistema "V-Idade". Ao realizar seu cadastro inicial no V-Idade, o usuário passa por uma verificação robusta de identidade uma única vez, gerando um *passkey* associado ao seu perfil. Posteriormente, ao tentar acessar uma rede social, em vez de submeter novos documentos, o usuário seleciona a opção "entrar com meu Selo de Idade". O V-Idade envia à rede social apenas um sinal criptográfico confirmando que o usuário possui "+18 anos". Por meio de uma arquitetura técnica específica, o V-Idade não recebe informações sobre qual perfil ou conteúdo o usuário está acessando na rede social e esta, por sua vez, recebe a confirmação etária sem ter acesso à identidade civil ou aos documentos originais do usuário.

Análise: O cenário ilustra a aplicação prática da interoperabilidade entre sistemas e soluções. Esta integração cumpre um duplo papel, reduzindo a fricção na experiência do usuário e atuando como uma salvaguarda de privacidade. Ao transmitir apenas o atributo necessário (ex.: "maior de 18"), o sistema respeita os princípios da necessidade e da finalidade, evitando que cada fornecedor da cadeia trate dados pessoais desnecessariamente. O modelo de duplo-cego garante que o verificador não monitore o histórico de navegação do usuário e que o provedor de conteúdo não vincule a identidade real ao comportamento de uso. Para assegurar que essa promessa tecnológica seja efetiva, é importante que o provedor de atributos mantenha *logs* técnicos que comprovem a integridade do sinal durante a transmissão entre sistemas, permitindo que auditorias examinem se a separação de papéis e o isolamento de dados estão sendo cumpridos.

IV. REQUISITOS ESPECÍFICOS

Demonstrados os requisitos gerais contidos no Decreto, passa-se à exposição de determinações específicas para certos tipos de métodos e tecnologias que vêm sendo recorrentemente incorporados pelos fornecedores ou sendo objeto de estudos por autoridades nacionais e internacionais.

É importante esclarecer que não se trata de uma validação, chancela ou autorização irrestrita de utilização por parte da ANPD, mas tão somente uma baliza de como alguns desses mecanismos podem ser adotados. Em acréscimo, os parâmetros abaixo não excluem os contidos nos tópicos acima. Pelo contrário, eles complementam e dão concretude àquilo que foi dito anteriormente.

Estimativa facial

A estimativa de idade por análise facial constitui técnica de aferição que utiliza modelos algorítmicos para inferir a idade de um indivíduo a partir de atributos biométricos captados por imagem ou vídeo, sem necessidade de apresentação de documento de identidade ou de identificação do usuário.

Cabe destacar que sistemas de estimação facial são diferentes de reconhecimento facial biométrico. Nestes, a imagem é convertida em *template* e comparado com outro gerado a partir da imagem de documento oficial para fins de identificação ou autenticação. Já os sistemas de estimação facial classificam o rosto em uma faixa etária, produzindo como resultado exclusivo uma estimativa de idade.

Não obstante essa distinção técnica, o tratamento de imagens faciais por meio de técnicas específicas pode configurar tratamento de dado biométrico, classificado como dado

pessoal sensível pelo art. 5º, II, da LGPD, a depender da arquitetura do sistema e da finalidade do tratamento.[40]

Nesse sentido, cabe ao agente de tratamento demonstrar, por meio de documentos técnicos, incluindo Relatório de Impacto à Proteção de Dados Pessoais, que a solução adotada não gera e nem utiliza *templates* de identificação biométrica, bem como que sua finalidade não é de identificação ou de autenticação de indivíduo determinado. Esse entendimento tem respaldo similar ao adotado pela Autoridade de Proteção de Dados do Reino Unido (*Information Commisioner's Office – ICO*) no *Age assurance for the Children's code*.[41]

Os sistemas de aferição etária devem ser projetados de modo a retornar ao serviço digital apenas o atributo etário necessário para autorizar ou restringir o acesso do usuário, evitando o compartilhamento de dados pessoais adicionais. Para esse fim, recomenda-se a adoção de arquiteturas baseadas em tokenização ou credenciais digitais, nas quais o resultado da aferição etária seja representado por um sinal de idade ou token criptográfico que indique apenas se o usuário atende ao requisito etário exigido pelo serviço ou produto. Nessa arquitetura, o sistema responsável pela aferição etária não deve transmitir ao serviço digital a imagem capturada, a idade exata do usuário ou outros dados pessoais utilizados durante o processo de aferição. Em vez disso, deve emitir apenas um atributo etário binário derivado, como se é ou não "maior de 16 anos" ou se é ou não "maior de 18 anos".

Em razão dos riscos específicos que essa tecnologia apresenta, incluindo a possibilidade de uso de imagens sintéticas ou *deepfakes*, com potencial de viés algorítmico e com impacto abusivo ou ilícito sobre grupos vulneráveis, os fornecedores de produtos ou serviços de tecnologia da informação que adotarem esse tipo de mecanismo de aferição de idade devem observar os requisitos específicos estabelecidos nesta Seção, bem como aos gerais previstos neste Guia Orientativo.

Medidas de controle a burla

Os sistemas de estimativa facial devem ser tecnicamente robustos contra tentativas reiteradas de burla no contexto da aferição de idade. É recomendável que a configuração não permita ao usuário obter resultado favorável de acesso mediante persistência, múltiplas submissões ou exploração de variações de entrada. Nesse sentido, o sistema deve ser parametrizado para proibir acesso após determinado número de tentativas malsucedidas.

Ademais, recomenda-se observar que:

- Resultados divergentes em submissões sucessivas de um mesmo usuário devem acionar mecanismo de escalonamento para aferição mais robusta; e
- As tentativas devem ser documentadas para fins de responsabilização e prestação de contas pelo prazo mínimo estabelecido na política de segurança da informação ou documento similar dos fornecedores de produtos ou serviços de tecnologia da informação, que devem estar em conformidade com a LGPD.

[40] Art. 5º Para os fins desta Lei, considera-se: [...] II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

[41] ICO. 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/

Sistemas de alta confiabilidade

Conforme explorado acima, os sistemas de estimativa de idade devem estabelecer medidas eficazes para impedir o acesso de criança e adolescentes a serviços ou conteúdos proibidos, nos termos do art. 9º do ECA Digital e art. 15 do Decreto.

Nesse sentido, recomenda-se que:

- O fornecedor de produtos ou serviços de tecnologia da informação documente as métricas de desempenho, como taxas de falso positivo e de falso negativo e erro absoluto médio (*Mean Absolute Error*), considerando padrões técnicos e recomendações internacionais;
- Resultados limítrofes ou inconclusivos não sejam tratados como resultado favorável de acesso. Nessas situações, recomenda-se a criação de uma zona de incerteza ou "*buffer zone*", dentro da qual o sistema não deve emitir um veredito definitivo sobre a faixa etária do usuário. No modelo em camadas, tais resultados devem acionar, portanto, a camada subsequente de aferição; e
- O sistema adote margem de segurança etária, de modo a reduzir o risco de falsos negativos para usuários que se encontrem próximos ao limite de idade.

Progressividade e proporcionalidade

Outro ponto que merece ser mencionado é que a estimação facial deve integrar-se ao modelo de aferição em camadas, baseado no risco do conteúdo, serviço ou produto, sendo complementada por método de maior confiança para os casos em que o resultado seja limítrofe ou inconclusivo, atentando-se que:

- Resultados de baixa confiança obtidos pelo sistema de estimação facial devem acionar automaticamente métodos de verificação mais robustos, especialmente em contexto de Alto Risco; e
- A parametrização do sistema deve prever graus de exigência proporcionais ao nível de risco do conteúdo, produto ou serviço.

Aplicação antecipada e consistente

A aferição de idade por estimação facial deve ser implementada como requisito prévio de acesso ao conteúdo, produto ou serviço ou à funcionalidade restrita, considerando-se que:

- A aferição deve ocorrer no momento do cadastro ou imediatamente antes da primeira exposição ao conteúdo ou funcionalidade restritos, conforme o caso; e
- A aferição deve ser aplicada de forma uniforme a todos os usuários, sem distinções que possam caracterizar tratamento discriminatório ilícito ou abusivo.

Medidas de segurança técnicas fortes

Os sistemas de estimativa facial devem incorporar controles técnicos fortes destinados a garantir a integridade do processo de verificação e a proteção contra manipulação. Esses sistemas podem ser alvo de ataques que envolvam dados sintéticos e *deepfakes* gerados, por exemplo, por meio de inteligência artificial generativa. Assim, recomenda-se a adoção das seguintes medidas:

- Prova de vivacidade: verificação de que a imagem ou vídeo corresponde a uma pessoa real presente no momento da captura, com proteção contra apresentação de fotografias, vídeos, máscaras ou imagens sintéticas;

- Proteção contra *spoofing* e injeção de dados: o sistema deve implementar proteções contra possíveis ataques de injeção de imagens sintéticas no fluxo de captura, incluindo verificação de integridade do canal de captura; e
- Eliminação dos dados biométricos: os dados biométricos coletado (imagens faciais) devem ser descartados imediatamente após a conclusão do processo de aferição, sendo vedado o armazenamento permanente de biometria facial para fins de aferição de idade.

Adoção de padrões internacionalmente reconhecidos

Recomenda-se que os fornecedores de produtos ou serviços de tecnologia da informação que adotem sistemas de estimativa facial utilizem padrões internacionalmente reconhecidos para o processo de aferição.[42]

Vinculação do usuário

O resultado da estimativa facial deve ser vinculado de forma segura à conta ou sessão do usuário verificado, de modo a impedir a reutilização do resultado por terceiros, sendo que:

- O fornecedor de produtos ou serviços de tecnologia da informação deve implementar mecanismo técnico que garanta a correspondência entre o resultado da aferição e o usuário autenticado na plataforma; e
- O mecanismo de vinculação deve ser documentado no Relatório de Impacto à Proteção de Dados Pessoais elaborado pelo fornecedor.

Privacidade e Proteção de Dados

O fornecedor de produtos ou serviços de tecnologia da informação que utilizar o mecanismo de estimativa facial deve observar os requisitos de privacidade e proteção de dados abordados neste Guia Orientativo, principalmente em relação ao princípio da necessidade; ao tratamento dos dados para a finalidade de aferição de idade, vedado o tratamento para outra finalidade e assegurada a eliminação dos dados imediatamente após a conclusão do tratamento.

Em particular, recomenda-se a adoção de arquiteturas baseadas em tokenização ou credenciais digitais, nas quais o resultado da aferição etária seja representado por um sinal de idade ou token criptográfico que indique apenas se o usuário atende ao requisito etário exigido pelo serviço ou produto.

Verificação documental

A verificação documental consiste na utilização de documento de identidade emitido por autoridade competente — tais como cédula de identidade, carteira de motorista, passaporte ou documento digital equivalente — para confirmar que o usuário atende ao requisito etário exigido para acesso a determinado serviço ou conteúdo digital. O sistema verifica os dados constantes do documento e os compara com o critério de idade estabelecido pelo fornecedor de produtos ou serviços de tecnologia da informação em cumprimento ao ECA Digital, produzindo um resultado binário: apto ou inapto.

[42] Existem organismos internacionais de padronização que produzem recomendações internacionalmente reconhecidas, como ISO — International Organization for Standardization, IEEE — Institute of Electrical and Electronics Engineers, ETSI — European Telecommunications Standards Institute, W3C — World Wide Web Consortium e NIST — National Institute of Standards and Technology (EUA).

Diferentemente da estimativa de idade por análise facial — que infere probabilisticamente uma faixa etária a partir de características biométricas — a verificação documental é método determinístico, ou seja, baseia-se em atributo declarado por autoridade emissora competente.

Essa característica confere à verificação documental, em regra, maior nível de robustez do que métodos estimativos, tornando-a particularmente adequada para serviços de maior risco, podendo ser utilizada de forma isolada ou combinada por meio do modelo em camadas em contextos que exijam elevada confiança no resultado, especialmente em contextos de alto risco.

O art. 24, §3º, do Decreto, em aderência ao princípio da necessidade (art. 6º, III, LGPD), estabelece que 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 LGPD.

Os requisitos estabelecidos nesta Seção aplicam-se aos fornecedores de produtos ou serviços de tecnologia da informação que adotem a verificação documental como mecanismo de aferição de idade, isoladamente ou combinado como camada de verificação no modelo de aferição em camadas. São cumulativos com os requisitos gerais previstos neste Guia.

Autenticidade, integridade e validade do documento

O mecanismo de verificação deve confirmar que o documento apresentado é autêntico, não foi adulterado e se encontra dentro do prazo de validade. A verificação de autenticidade é condição prévia e inafastável para a aceitação do documento como evidência de idade, ou seja, um documento adulterado ou inválido não produz resultado de aferição confiável, independentemente da precisão dos demais componentes do mecanismo.

É recomendável observar:

- A verificação da validade temporal do documento — documentos vencidos não devem ser aceitos como evidência de idade;
- A análise automatizada dos elementos de segurança do documento, incluindo, conforme o seu tipo, zona de leitura óptica (*Machine Readable Zone* - MRZ), código de barras, chip RFID, hologramas, microimpressão e demais elementos de segurança previstos no padrão de emissão;
- Quando tecnicamente viável e proporcional ao nível de risco do serviço, a realização de consulta a fontes autorizadas para a validação documental, observada as disposições na LGPD.

Proteção contra burla e falsificação

O mecanismo deve ser tecnicamente robusto contra as principais tentativas de burla da verificação documental previsíveis no contexto de aferição de idade de crianças e adolescentes. Recomenda-se que as medidas utilizadas para a proteção de burlas ou falsificações estejam dispostas no Relatório de Impacto à Proteção de Dados.

Compartilhamento dos dados

No caso de compartilhamento de dados para validação dos documentos oficiais, deve-se transmitir somente os dados necessários para a finalidade de verificação da idade, vedado o envio de data de nascimento exata, da identidade civil ou de dados para perfilamento.

Privacidade e Proteção de Dados

Recomenda-se observar o disposto neste Guia Orientativo sobre o tema, em especial quanto à eliminação dos dados imediatamente após a conclusão do processo de verificação, sendo vedado o armazenamento permanente dos dados para fins de aferição de idade.

Adoção de padrões internacionalmente reconhecidos

Recomenda-se que os fornecedores que adotem mecanismos de verificação documental utilizem padrões internacionalmente reconhecidos para o processo de aferição.

Credenciais verificáveis

A aferição de idade por meio de credenciais verificáveis se baseia na apresentação, por parte do usuário, de atributo etário previamente emitido por uma entidade confiável (como uma autoridade governamental – por exemplo o Gov.Br, como uma entidade certificadora, entre outras). O termo "verificável" se refere à possibilidade de a autenticidade e a integridade de uma credencial, fornecida por um "emissor" e apresentada por um "portador", ser recebida e validada por uma "parte verificadora", por meio de suas próprias regras de negócio.[43] No campo etário, um atributo pode consistir em uma informação binária ou categórica a respeito de uma pessoa (por exemplo, "maior de 18 anos" ou "estar entre 13 e 17 anos").

Diferentemente de outros mecanismos, nos quais pode ocorrer o compartilhamento e a análise de documentos de identificação e de informações biométricas, as credenciais verificáveis **devem conter apenas os atributos estritamente necessários à finalidade de comprovação da idade ou faixa etária** de um usuário, sem revelar dados pessoais adicionais, como data de nascimento. Adicionalmente, sempre que tecnicamente possível, deve-se **privilegiar o uso de provas de conhecimento zero** (*Zero-Knowledge Proof - ZKP*) ou mecanismos equivalentes que permitam a verificação da idade sem revelação do dado pessoal relacionado.

Dessa forma, o uso de credenciais verificáveis contribui para a redução do tratamento de dados pessoais para fins de aferição de idade e dos riscos associados à coleta excessiva de dados, na medida em que permite a comprovação de determinado atributo sem a necessidade de compartilhamento de um conjunto completo de dados pessoais. Assim, corrobora com a consecução da privacidade e proteção dos dados pessoais dos usuários, especialmente de crianças e adolescentes.

As credenciais verificáveis operam por meio de declarações digitais assinadas criptograficamente, emitidas por uma entidade confiável – o emissor, governamental ou de natureza privada, a qual atesta as informações contidas na credencial. O **emissor** é responsável por validar a identidade e atributos de um usuário e por emitir uma credencial verificável correspondente. O emissor deve, ainda, garantir a veracidade das informações constantes em uma credencial verificável.

Cabe destacar ainda a necessidade de a credencial ter seu ***status* de validade checado a cada apresentação pelo usuário**. Para isso, o emissor deve: (i) verificar seu estado e manter controles que assegurem a revogação imediata de credenciais inválidas ou caso as afirmações sobre o portador deixem de ser verdadeiras; e (ii) atualizar informações sempre que

[43] Ao longo dessa seção, recorre-se a conceitos e critérios de governança do ecossistema de credenciais verificáveis da W3C. Fonte: W3C. W3C Recommendation: Verifiable Credentials Data Model v2.0. 2025. Disponível em: < https://www.w3.org/TR/vc-data-model-2.0/#what-is-a-verifiable-credential> Acesso em 22 abr. 2026.

necessário e indicar o estado atual de validade da credencial verificável (como, por exemplo, se válida ou revogada).

Uma vez emitida e assinada digitalmente pelo emissor, **a credencial verificável pode ser armazenada no próprio dispositivo do usuário** – o portador, como em carteiras digitais ou em *cookies* de navegadores *web*. O **portador** é o titular da credencial, responsável pelo seu armazenamento e apresentação quando necessário. Cabe a ele o controle sobre a credencial, decidindo quando e com quem compartilhá-la.

Em outras palavras, o usuário deve dar seu consentimento, de forma livre, informada e inequívoca, sobre o compartilhamento da credencial ou de apenas parte dela (isto é, de apenas alguns atributos escolhidos). Para tanto, o portador deve ser informado, de maneira clara e acessível, acerca de quais atributos da credencial serão compartilhados e para quais finalidades.

Por sua vez, a **parte verificadora** solicita ao usuário a apresentação de um ou mais atributos necessários para a tomada de decisão, limitando-se apenas aos dados estritamente indispensáveis para a finalidade de aferição de idade. Posteriormente, após verificar a assinatura criptográfica da credencial, a parte verificadora procede à validação das informações recebidas, por meio de suas próprias regras de negócio, para decidir se o acesso será concedido ou não.

Um repositório de credenciais verificáveis, como uma carteira digital, um sistema de arquivos ou um cofre de armazenamento, deve garantir o armazenamento seguro de uma credencial verificável, de forma a assegurar sua confidencialidade, ou seja, não permitir sua divulgação indevida para além do próprio portador, e a integridade das informações, evitando que venham a ser corrompidas ou perdidas enquanto estiver sob sua responsabilidade. Além disso, o emissor e a parte verificadora não devem ter acesso direto ao repositório de credenciais verificáveis do portador, fato que contribui para a sua privacidade e para a mitigação do risco de monitoramento indevido de suas atividades no ambiente digital.

O armazenamento de forma local em um dispositivo do usuário permite que uma credencial verificável possa ser reutilizada de forma segura, reduzindo a necessidade de repetidas coletas de documentos e de dados pessoais e uma menor fricção quanto à experiência do usuário. Uma vez emitida, ela pode ser apresentada a distintas partes verificadoras, desde que mantida válida.

Por sua natureza descentralizada e orientada ao controle pelo usuário, as credenciais verificáveis se apresentam como métodos para a aferição de idade no ambiente digital que permitem conciliar elevados níveis de segurança e confiabilidade com a proteção dos direitos fundamentais à privacidade e à proteção de dados pessoais de crianças e adolescentes.

ANEXO I

Mecanismos confiáveis de aferição de idade

Síntese – Requisitos Gerais

Requisitos Mínimos	Fundamentação	Recomendações
Proporcionalidade	Arts. 24, I; e 47 do Decreto. Arts. 6º; 8º, III; 16, parágrafo único, ECA Digital Art. 38, LGPD	• Identifiquem e avaliem os riscos associados ao conteúdo, produto ou serviço digital, especialmente os potenciais efeitos adversos sobre a privacidade, a segurança e a saúde de crianças e adolescentes. Nesse sentido, recomendam-se que sejam avaliadas questões como o grau de interação social entre usuários e riscos de aliciamento ou contato com desconhecidos, por exemplo; • 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; • Avaliem a proporcionalidade entre os riscos do produto ou serviço e os riscos decorrentes do mecanismo de aferição de idade a ser implementado; • Definam o nível de risco de seu produto, serviço ou conteúdo e adotem medidas, técnicas e administrativas, aptas a mitigar os riscos identificados; e • Elaborem instrumentos de governança, como o Relatório de Impacto à Proteção de Dados Pessoais e a Avaliação de Impacto de riscos à segurança e à saúde de crianças.
Acurácia, robustez e confiabilidade	Art. 9º, § 1º, do ECA Digital e art. 24, II, do Decreto.	• 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; • 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; e • 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. • Implementem medidas técnicas e organizacionais de segurança que abranjam todo o ciclo de vida do tratamento dos dados, de maneira a detectar tentativas de burla e fraudes. Nesse sentido, os sistemas utilizados devem permitir: a captura segura e a validação automática de documentos oficiais, quando for o caso; a realização de análise de consistência entre o documento utilizado para a aferição etária e o usuário; a detecção de documentos adulterados, falsificados, reutilizados ou quaisquer outras tentativas de fraudes; e a invalidação automática de tokens ou credenciais expiradas.
Proteção de dados pessoais	Arts. 12, I e III, § 1º; 13; e 37, parágrafo único, do ECA Digital. Art. 24, III, IV, V, VI, VII, VIII do Decreto. Art. 5º, X, da Constituição Federal Arts. 6º, I, III e VII, da LGPD Lei nº 12.965/2014 (Marco Civil da Internet)	• 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. • Privilegiem a implementação de arquitetura baseada em atributos etários

		tokenizados e o uso de credenciais verificáveis. • Utilizem mecanismo de aferição etária que adotem arquitetura em modelo *double-blind*. O fornecedor de serviços ou produtos digitais, sempre que possível e considerado o risco da plataforma, não deve ter acesso à identidade civil do usuário ou a qualquer dado que o identifique direta ou indiretamente. • Façam a separação funcional entre sistemas de aferição etária e outros sistemas da plataforma ou serviço digital. Os sistemas responsáveis pela aferição etária devem operar de forma segregada das demais infraestruturas de tratamento de dados da plataforma, especialmente aquelas destinadas a publicidade direcionada; análise comportamental; personalização de conteúdo; e treinamento de modelos de inteligência artificial. • Restrinjam o acesso aos dados pessoais coletados no procedimento de aferição etária. Os dados pessoais coletados durante o processo de aferição etária devem estar sujeitos a controles rigorosos de acesso, de modo que apenas sistemas e profissionais estritamente envolvidos na operação da aferição possam acessar tais informações. • Limitem o armazenamento de dados pessoais brutos utilizados na aferição. Sempre que possível, os dados brutos utilizados durante o processo de aferição etária devem ser eliminados imediatamente após a conclusão da aferição. Os sistemas devem reter apenas o resultado da aferição etária, eliminando-se os dados brutos utilizados. • Incluam cláusulas de limitação do uso secundário dos dados pessoais em políticas internas e contratos com colaboradores. É recomendável que esses instrumentos contenham cláusulas específicas que proíbam expressamente o uso secundário dos dados coletados no contexto da aferição de idade.

Inclusão e não discriminação	Arts. 5º, § 2º; e 10, caput, do ECA Digital Arts. 4º, IX; e 24, X, do Decreto. Art. 6º, IX, da LGPD	• Avaliem previamente se o método adotado pode gerar barreiras desproporcionais de acesso ou produzir efeitos discriminatórios de forma ilícita ou abusiva 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; • Avaliem, periodicamente, o desempenho dos sistemas de inteligência artificial, a fim de conferir a existência de vieses algorítmicos em mecanismos automatizados de aferição etária, que podem envolver fatores como idade, gênero, raça, etnia ou outras condições; e • Garantam a acessibilidade tecnológica dos sistemas de aferição etária implementados para dispositivos com menor capacidade tecnológica ou com conexões de internet limitadas.
Transparência e auditabilidade	Arts. 12, I; e 12, § 3º, do ECA Digital Arts. 24, XI; 25, § 2º, III; e 27, do Decreto. Arts. 6º, VI e X; 9º; 14, § 6º; e 37, da LGPD	• Informem de forma clara, precisa e acessível os tipos de mecanismos de aferição de idade utilizados, as suas finalidades, quais dados são utilizados, quem são os agentes envolvidos no tratamento, inclusive em caso de compartilhamento, bem como os seus papéis nos procedimentos, e as consequências da aferição de idade para o usuário; • 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 auditabilidade; e • Garantam integridade, rastreabilidade e possibilidade de auditoria independente de componentes, operações e registros associados aos mecanismos de aferição de idade.

Interoperabilidade	Arts. 11; 12, III e § 3º, do ECA Digital Arts. 24, IX, do Decreto.	• 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 a finalidade do compartilhamento, os agentes autorizados, as salvaguardas de segurança e os mecanismos destinados a impedir o compartilhamento contínuo, automatizado e irrestrito de dados pessoais.