

Tomada de Subsídios

Guia de orientações preliminares para implementação de mecanismos confiáveis de aferição de idade

Complemento - Contribuição do Alana

Julho/ 2026

**Participa + Brasil - Tomada de Subsídios: ORIENTAÇÕES PRELIMINARES PARA
A IMPLEMENTAÇÃO DE MECANISMOS CONFIÁVEIS DE AFERIÇÃO DE IDADE**

SUMÁRIO

TÓPICO - REQUISITOS GERAIS.....	4
1. Capítulo de análise: Proporcionalidade	4
2. Capítulo de análise: Acurácia, robustez e confiabilidade	5
3. Capítulo de análise: Privacidade e proteção de dados pessoais.....	6
4. Capítulo de análise: Inclusão e não discriminação	8
5. Capítulo de análise: Transparência e auditabilidade	9
6. Capítulo de análise: Interoperabilidade	11
TÓPICO - REQUISITOS ESPECÍFICOS	12
1. Capítulo de análise: Estimativa Facial.....	12
a) A necessidade de diferenciação técnica expressa entre as espécies de tratamento biométrico facial	12
b) A qualificação do tratamento como biométrico não esgota a análise dos riscos nem das salvaguardas aplicáveis	16
c) A estimativa facial como medida de exceção, e não como mecanismo ordinário ..	18
d) A limitação estrutural da estimativa facial sobre o público que a norma pretende proteger	20
2. Capítulo de análise: Verificação Documental.....	22
3. Capítulo de análise: Credenciais Verificáveis.....	24

TÓPICO - REQUISITOS GERAIS

1. Capítulo de análise: Proporcionalidade

SÍNTESE DA CONTRIBUIÇÃO

- Recomenda-se explicitar que a avaliação de proporcionalidade deve ser orientada sempre pelo melhor interesse da criança e do adolescente e constitui critério bidirecional: quanto maior o risco do produto ou serviço, maior deve ser a robustez e a confiabilidade do mecanismo de aferição, sem prejuízo da adoção de soluções menos intrusivas sempre que igualmente eficazes.
- Recomenda-se exigir que a análise de proporcionalidade, incluindo a avaliação dos riscos do serviço e do mecanismo de aferição, seja devidamente documentada, de modo a assegurar a auditabilidade, a responsabilização e a fiscalização pela ANPD.

De início, ressaltamos que a avaliação de proporcionalidade deve ser orientada pelo melhor interesse da criança e do adolescente, de modo que, diante de diferentes alternativas regulatórias ou tecnológicas aptas a atingir a finalidade protetiva, deva prevalecer aquela que assegure maior proteção e garantia dos direitos de crianças e adolescentes. Nesse sentido, vale ressaltar que os mecanismos de aferição de idade não possuem apenas função restritiva, mas também habilitadora, permitindo que provedores identifiquem a presença de crianças e adolescentes e implementem as medidas de proteção, adaptações e salvaguardas previstas na LGPD e no ECA Digital.

De maneira similar, recomenda-se tornar explícito que a proporcionalidade constitui critério bidirecional, e não apenas limite à intrusividade das soluções adotadas. O texto corretamente enfatiza que os mecanismos de aferição não devem gerar efeitos adversos desproporcionais à privacidade e à proteção de dados pessoais. Essa dimensão de contenção, contudo, convive com uma dimensão positiva de proteção: quanto maior o risco apresentado pelo produto ou serviço à segurança, à saúde e ao desenvolvimento de crianças e adolescentes, maior deve ser a robustez e a confiabilidade do mecanismo empregado. Sem essa explicitação, abre-se margem para que fornecedores de serviços comprovadamente de alto risco invoquem a proporcionalidade como fundamento para adoção de mecanismos facilmente contornáveis, esvaziando a finalidade protetiva da norma.

Em coerência com o que o próprio documento afirma, a adoção de mecanismos mais invasivos, especialmente aqueles que envolvam tratamento de dados biométricos, somente deve ocorrer quando demonstrada sua necessidade diante dos riscos concretos do serviço, e inexistirem alternativas menos intrusivas igualmente eficazes.

Por fim, recomenda-se explicitar que a avaliação de proporcionalidade, inclusive a identificação e avaliação dos riscos inerentes ao serviço e ao mecanismo de aferição, deve ser documentada, de modo a possibilitar sua posterior verificação pela ANPD no exercício de suas competências fiscalizatórias. Embora o texto mencione o RIPD (art. 38 da LGPD e art. 16, parágrafo único, do ECA Digital) e a avaliação prevista no art. 47 do Decreto 12.880/26, seria recomendável deixar expresso que a ausência dessa documentação compromete a auditabilidade da solução e a demonstração da responsabilização e prestação de contas pelo fornecedor. Além disso, sempre que aplicável, recomenda-se que a análise de proporcionalidade seja subsidiada por uma Avaliação de Impacto sobre os Direitos da Criança ([Child Rights Impact Assessment – CRIA](#)) ou instrumento equivalente, de modo a considerar não apenas os riscos à privacidade e à proteção de dados pessoais, mas também os impactos sobre o conjunto de direitos assegurados a crianças e adolescentes pelo ECA, pela LGPD e pelo ECA Digital, reforçando a centralidade do princípio do melhor interesse da criança na escolha e implementação dos mecanismos de aferição de idade.

2. Capítulo de análise: Acurácia, robustez e confiabilidade

SÍNTESE DA CONTRIBUIÇÃO

- Recomenda-se exigir que a mensuração da acurácia, da robustez e da confiabilidade seja realizada de forma desagregada por grupos relevantes (como faixa etária, gênero e raça/etnia), em articulação com o requisito de inclusão e não discriminação, evitando que métricas agregadas ocultem desempenho insuficiente sobre grupos específicos.
- Sugere-se explicitar, no corpo do texto, que a robustez deve ser avaliada considerando as formas de contorno efetivamente acessíveis a crianças e adolescentes e que o parâmetro dos "meios técnicos razoavelmente disponíveis" possui natureza dinâmica, exigindo reavaliações periódicas dos mecanismos.
- Recomenda-se que a documentação das avaliações registre não apenas as métricas obtidas, mas também as condições em que os testes foram realizados e a representatividade das bases utilizadas em relação ao público

brasileiro, fortalecendo a auditabilidade e a confiabilidade dos resultados.

Recomenda-se explicitar que a mensuração da acurácia, da robustez e da confiabilidade seja realizada de forma desagregada entre diferentes grupos populacionais, e não apenas por métricas agregadas. Um mecanismo pode apresentar desempenho global satisfatório e, ainda assim, revelar desempenho significativamente inferior para determinados grupos, como adolescentes em faixas etárias próximas ao limiar dos dezoito anos ou pessoas pertencentes a diferentes grupos raciais, étnicos ou de gênero. Essa recomendação reforçaria a coerência com a seção dedicada à inclusão e à não discriminação, evitando que indicadores agregados ocultem vieses ou falhas concentradas justamente nos públicos que demandam maior proteção.

Quanto à robustez, recomenda-se reforçar que a avaliação da resistência a fraudes e tentativas de burla considere, de forma prioritária, os mecanismos de contorno efetivamente acessíveis a crianças e adolescentes. Também seria oportuno explicitar que o parâmetro dos "meios técnicos razoavelmente disponíveis" possui natureza dinâmica, exigindo reavaliações periódicas da robustez dos mecanismos à medida que evoluem as técnicas de fraude e as formas de contorno.

Por fim, recomenda-se que a documentação exigida a título de auditabilidade registre não apenas as métricas obtidas, mas também as condições em que os testes foram realizados - em especial a representatividade das bases populacionais em relação ao público brasileiro. Métricas de acurácia elevada obtidas em condições não representativas tendem a produzir resultados insatisfatórios em contexto real, hipótese que o documento já considera ao tratar de baixo desempenho em implementação. Explicitar a exigência de representatividade das condições de validação fortaleceria o requisito.

3. Capítulo de análise: Privacidade e proteção de dados pessoais

SÍNTESE DA CONTRIBUIÇÃO

- Recomenda-se explicitar a incidência do art. 14, § 6º, da LGPD e do regime de dados sensíveis quando a própria aferição tratar dados de pessoas com menos de 18 anos - hipótese em que o mecanismo protetivo pode, ele próprio, tornar-se fonte de risco.
- Sugere-se registrar que a vedação ao uso secundário e à rastreabilidade deve

alcançar também usos aparentemente benignos ("melhoria do serviço", "segurança", "prevenção à fraude"), interpretando-se restritivamente à exceção do art. 13 do ECA Digital / art. 24, III, do Decreto.

- Recomenda-se reforçar a minimização na dimensão da retenção: preferência por arquiteturas de verificação que dispensem o armazenamento dos dados de insumo após a produção do resultado étário.

Recomenda-se explicitar a articulação com o art. 14 da LGPD sempre que o mecanismo de aferição implicar tratamento de dados pessoais de crianças e adolescentes. Embora concebidos como salvaguardas destinadas à proteção desse público, mecanismos de aferição de idade podem eles próprios introduzir novos riscos aos direitos dos titulares, especialmente quando envolverem o tratamento de dados biométricos ou outros dados pessoais sensíveis. Nessa hipótese, a própria arquitetura da solução deve observar o regime reforçado de proteção previsto no art. 14 da LGPD, orientando-se pelo melhor interesse da criança e do adolescente e pela adoção de alternativas menos intrusivas sempre que capazes de atingir nível equivalente de proteção.

De maneira semelhante, recomenda-se explicitar que os mecanismos de aferição de idade sejam concebidos segundo os princípios de proteção de dados desde a concepção e por padrão, incorporando salvaguardas técnicas e organizacionais desde as etapas iniciais de desenvolvimento das soluções.

Quanto à vedação ao uso secundário e à rastreabilidade, sugere-se reforçar que essas vedações devem alcançar não apenas usos manifestamente ilícitos (publicidade comportamental, perfilamento, enriquecimento cadastral, por exemplo), mas também usos aparentemente legítimos ou apresentados genericamente como "melhoria do serviço", "segurança" ou "prevenção à fraude", que frequentemente operam como porta de entrada para o reaproveitamento de dados coletados para aferição. Considerando que o art. 13 do ECA Digital e o art. 24, III, do Decreto vedam o tratamento "para qualquer outro propósito", recomenda-se registrar que a exceção deve ser interpretada restritivamente, não comportando finalidades acessórias ainda que apresentadas como benéficas ao usuário.

Por fim, recomenda-se explicitar que o princípio da minimização de dados também se projeta sobre a dimensão temporal do tratamento, alcançando não apenas a coleta e o compartilhamento, mas igualmente a retenção dos dados pessoais. Nesse sentido, o Guia poderia registrar que os fornecedores devem optar por arquiteturas de aferição de idade que dispensem a conservação dos dados utilizados como insumo após a produção do resultado ou atributo étário estritamente necessário para a

finalidade pretendida. Essa orientação reforça a lógica da proteção de dados desde a concepção e dialoga com a recomendação, já presente na seção de transparência e auditabilidade, de evitar o armazenamento de dados biométricos, imagens e informações extraídas de documentos de identidade, inclusive para fins de auditoria, conferindo maior coerência sistêmica às orientações do documento.

4. Capítulo de análise: Inclusão e não discriminação

SÍNTESE DA CONTRIBUIÇÃO

- Recomenda-se articular este capítulo com o requisito de acurácia, robustez e confiabilidade, prevendo que a avaliação do desempenho dos mecanismos seja realizada de forma desagregada por grupos relevantes, de modo a identificar e mitigar impactos discriminatórios.
- Sugere-se explicitar que a prevenção e mitigação de vieses discriminatórios constituem obrigação dos fornecedores, e não mera recomendação, em conformidade com a Constituição Federal, a LGPD, o ECA e o ECA Digital.
- Recomenda-se reconhecer a importância do desenvolvimento de mecanismos de aferição apoiados em infraestrutura digital pública e interoperável, reduzindo barreiras de implementação e ampliando o acesso a soluções confiáveis.
- Sugere-se explicitar que a não discriminação também possui dimensão territorial, devendo os fornecedores assegurar que os mecanismos disponibilizados no Brasil observem padrões de qualidade, segurança e proteção equivalentes aos adotados em outras jurisdições.

A seção de inclusão e não discriminação complementa os requisitos de acurácia, robustez e confiabilidade, razão pela qual recomenda-se explicitar a articulação entre esses capítulos. Conforme sugerido anteriormente, a avaliação do desempenho dos mecanismos deve ser realizada de forma desagregada por grupos relevantes, como faixa etária, raça, etnia, gênero e deficiência, evitando que métricas agregadas ocultem desempenhos inferiores sobre populações específicas e comprometam a efetividade da proteção.

Também se recomenda fortalecer a redação relativa aos vieses discriminatórios. A prevenção da discriminação não deve ser apresentada como mera recomendação, mas como obrigação decorrente da Constituição Federal, da LGPD, do ECA e do ECA Digital. Assim, sugere-se explicitar o dever dos fornecedores de identificar, avaliar, mitigar e monitorar continuamente impactos discriminatórios associados aos mecanismos de aferição de idade.

Quanto ao requisito de inclusão, recomenda-se reconhecer a importância do desenvolvimento de mecanismos de aferição apoiados em infraestrutura digital pública e interoperável. Soluções dessa natureza podem reduzir barreiras econômicas e técnicas para provedores de menor porte, ampliando a adoção de mecanismos confiáveis e evitando que a proteção de crianças e adolescentes dependa exclusivamente de soluções privadas.

Por fim, recomenda-se explicitar que a não discriminação também possui dimensão territorial. Fornecedores que atuam globalmente devem assegurar que os mecanismos disponibilizados no Brasil ofereçam padrões de qualidade, precisão, segurança e proteção equivalentes aos adotados em outras jurisdições, vedada a oferta de soluções inferiores aos usuários brasileiros.

5. Capítulo de análise: Transparência e auditabilidade

SÍNTESE DA CONTRIBUIÇÃO

- Recomenda-se explicitar que as informações sobre os mecanismos de aferição de idade sejam fornecidas de maneira simples, clara e acessível, em conformidade com o art. 14, § 6º, da LGPD, harmonizando essa diretriz com o art. 10º do ECA Digital, de modo a reconhecer que uma experiência adequada à idade também compreende a apresentação de informações compatíveis com a autonomia progressiva e a capacidade de compreensão de crianças e adolescentes.
- Sugere-se ampliar o escopo da auditabilidade para que permita verificar não apenas a acurácia, robustez e confiabilidade dos mecanismos, mas também sua conformidade com os requisitos de proporcionalidade, não discriminação, privacidade, proteção de dados pessoais e demais princípios previstos no Guia, fortalecendo a responsabilização dos fornecedores e a fiscalização pela ANPD.
- Recomenda-se reconhecer e reforçar expressamente a possibilidade de utilização de auditorias independentes como instrumento de verificação da conformidade dos mecanismos de aferição de idade em procedimentos de fiscalização, em linha com as competências da ANPD previstas na LGPD e no ECA Digital.

A seção de transparência e auditabilidade estabelece diretrizes importantes para assegurar a compreensão e o controle sobre os mecanismos de aferição de idade. Nesse sentido, recomenda-se harmonizar a redação do Guia com o disposto no art. 14, § 6º, da Lei Geral de Proteção de Dados, explicitando que as informações sobre

o funcionamento dos mecanismos devem ser disponibilizadas de maneira simples, clara e acessível, especialmente quando dirigidas a crianças e adolescentes. Essa orientação deve ser interpretada em conjunto com o art. 10º do ECA Digital, que determina a adoção de mecanismos capazes de proporcionar experiências adequadas à idade, respeitada a autonomia progressiva.

Assim, recomenda-se explicitar que uma experiência adequada à idade não se limita ao desenho das funcionalidades ou das restrições de acesso, mas também compreende a forma como são apresentadas as informações relativas ao mecanismo de aferição de idade, permitindo que crianças e adolescentes compreendam, de maneira compatível com seu estágio de desenvolvimento, seu funcionamento, suas consequências e os direitos que lhes assistem

No que se refere à auditabilidade, recomenda-se ampliar sua finalidade para além da verificação da acurácia, robustez e confiabilidade dos mecanismos. A documentação e os registros produzidos devem permitir também a avaliação da conformidade do mecanismo com os demais requisitos previstos no Guia, especialmente aqueles relacionados à não discriminação, à privacidade, à proteção de dados pessoais, à proporcionalidade e à inclusão. A auditabilidade deve constituir instrumento apto a demonstrar que o mecanismo de aferição permanece aderente aos princípios e salvaguardas previstos na LGPD, no ECA Digital e nas orientações da ANPD ao longo de todo o seu ciclo de vida, fortalecendo a responsabilização dos fornecedores e conferindo maior efetividade às atividades de monitoramento e fiscalização da Agência. Para tanto, recomenda-se que os fornecedores disponibilizem, regularmente, informações agregadas, relatórios e evidências de conformidade capazes de permitir o escrutínio público e a avaliação independente de seu desempenho.

Nesse contexto, recomenda-se que o Guia reconheça expressamente a possibilidade de utilização de auditorias independentes como mecanismo de verificação da conformidade das soluções de aferição de idade, especialmente em procedimentos de fiscalização conduzidos pela ANPD. Trata-se de instrumento compatível com as competências fiscalizatórias conferidas à Agência pela LGPD e pelo ECA Digital, além de representar boa prática regulatória já adotada pela própria ANPD, como demonstrado na determinação de auditoria externa independente imposta ao WhatsApp¹ para verificar a efetiva implementação das medidas técnicas e

¹ G1. WhatsApp no Brasil terá que passar por auditoria para confirmar se Meta controla ou não dados de usuários do app. Disponível em: <https://g1.globo.com/tecnologia/noticia/2025/11/14/whatsapp-no-brasil-tera-que-passar-por-auditoria-para-confirmar-se-meta-control-a-ou-nao-dados-de-usuarios-do-app.ghtml>. Acesso em: 21 maio 2026.

organizacionais destinadas a limitar o compartilhamento de dados pessoais com a Meta.

Recomenda-se, ainda, incentivar a adoção de padrões técnicos abertos para a documentação, registro e intercâmbio das informações necessárias à auditoria, favorecendo a interoperabilidade entre diferentes soluções, a verificabilidade dos mecanismos e a realização de auditorias independentes, sem prejuízo da neutralidade tecnológica e da adoção de novas soluções que ofereçam níveis equivalentes ou superiores de proteção.

6. Capítulo de análise: Interoperabilidade

SÍNTESE DA CONTRIBUIÇÃO

- Recomenda-se fortalecer a disciplina de governança das soluções interoperáveis, explicitando as responsabilidades dos agentes envolvidos quanto à proteção de dados pessoais, à segurança da informação, à gestão de incidentes e ao atendimento dos direitos dos titulares, de modo a evitar a diluição de responsabilidades e assegurar a efetividade da fiscalização pela ANPD.
- Sugere-se reconhecer a importância da promoção de soluções interoperáveis baseadas em infraestrutura digital pública ou em padrões abertos, reduzindo a dependência de soluções proprietárias, ampliando o acesso a mecanismos confiáveis por fornecedores de diferentes portes e favorecendo a implementação efetiva do ECA Digital.

Também se recomenda ampliar a disciplina sobre governança das soluções interoperáveis. Embora o texto faça referência aos fluxos de dados e às salvaguardas de segurança, seria importante explicitar que os agentes envolvidos na arquitetura interoperável devem possuir responsabilidades claramente definidas quanto à proteção de dados pessoais, à segurança da informação, à gestão de incidentes e ao atendimento dos direitos dos titulares. A interoperabilidade não deve resultar em diluição das responsabilidades entre os diferentes participantes do ecossistema nem dificultar a atuação fiscalizatória da ANPD.

Além disso, recomenda-se reconhecer a importância da promoção de soluções interoperáveis apoiadas em infraestrutura digital pública ou em padrões abertos, reduzindo a dependência de soluções proprietárias e contribuindo para ampliar a

adoção de mecanismos confiáveis por fornecedores de diferentes portes. Essa abordagem favorece a inclusão, reduz barreiras econômicas de implementação e evita que a efetividade do ECA Digital fique condicionada à contratação de poucos provedores privados de aferição de idade.

TÓPICO - REQUISITOS ESPECÍFICOS

1. Capítulo de análise: Estimativa Facial

a) A necessidade de diferenciação técnica expressa entre as espécies de tratamento biométrico facial

O Guia registra, com acerto, que "sistemas de estimativa facial são diferentes de reconhecimento facial biométrico", esclarecendo que, nestes últimos, "a imagem é convertida em *template* e comparado com outro gerado a partir da imagem de documento oficial para fins de identificação ou autenticação", enquanto os sistemas de estimativa facial "classificam o rosto em uma faixa etária, produzindo como resultado exclusivo uma estimativa de idade".

A distinção técnica entre estimativa facial, verificação e identificação biométrica é fundamental, uma vez que essas diferentes modalidades de tratamento apresentam riscos distintos para os direitos fundamentais e, consequentemente, demandam salvaguardas proporcionais. O Guia já reconhece essa necessidade ao estabelecer que cabe ao agente de tratamento demonstrar, por meio de documentação técnica, incluindo Relatório de Impacto à Proteção de Dados Pessoais, que a solução adotada não gera nem utiliza *templates* de identificação biométrica e que sua finalidade não é a identificação ou autenticação de indivíduos determinados. Trata-se de previsão importante, que reforça a necessidade de comprovação da natureza do tratamento realizado.

Recomenda-se, contudo, aprofundar essa exigência mediante a definição de requisitos mínimos para essa demonstração, **considerando que não basta exigir documentação técnica; é importante explicitar quais elementos devem ser apresentados para permitir que a classificação da solução como mecanismo de estimativa facial seja efetivamente verificável.** Para esse fim, a documentação produzida pelo fornecedor deve conter **evidências técnicas e registros auditáveis capazes de demonstrar que a solução não realiza operações de identificação ou verificação biométrica, não cria ou retém templates biométricos persistentes e não permite o reaproveitamento das imagens ou dos dados derivados para finalidades diversas da aferição etária.**

Esse detalhamento mostra-se especialmente relevante porque diferentes soluções comercialmente disponíveis podem compartilhar etapas semelhantes de processamento da imagem facial, distinguindo-se principalmente pelas operações realizadas após a captura e pela forma como os dados são tratados, armazenados ou reutilizados. Na ausência de parâmetros objetivos para avaliação dessas operações, torna-se mais difícil verificar se uma determinada solução permanece limitada à estimação de idade ou se incorpora funcionalidades típicas de identificação ou verificação biométrica.

Por essa razão, recomenda-se que o Guia **complemente a exigência já prevista com critérios objetivos de verificabilidade e com a definição de um conteúdo mínimo para a documentação técnica exigida dos fornecedores, fortalecendo a atuação fiscalizatória e orientadora da ANPD e conferindo maior segurança jurídica à classificação das diferentes modalidades de tratamento biométrico.**

Para essa diferenciação, um caminho teórico inicial pode ser o Regulamento (UE) 2024/1689 (*Artificial Intelligence Act- AI act*)², o qual estabelece uma taxonomia para diferentes modalidades de tratamento biométrico, distinguindo, entre outras categorias, identificação biométrica, verificação biométrica e categorização biométrica. Essa sistematização oferece um referencial conceitual que pode ser utilizado para explicitar o alcance das soluções de aferição de idade baseadas em características faciais e diferenciar as operações efetivamente realizadas por cada tecnologia.

O AI Act parte de um conceito-base e dele deriva espécies distintas, com regimes jurídicos próprios:

- 1) **Dados biométricos (art. 3º, § 34).** São os dados pessoais resultantes de processamento técnico específico de características físicas, fisiológicas ou comportamentais, como imagens faciais ou dados dactiloscópicos. Trata-se do conceito-mãe, do qual derivam todas as demais categorias. No contexto nacional, os dados biométricos são classificados como uma espécie de dado pessoal sensível, nos termos do art. 5º, II, da LGPD.
- 2) **Identificação biométrica (art. 3º, § 35).** Responde à pergunta "*quem é esta pessoa?*". Consiste no reconhecimento automatizado de características humanas para estabelecer a identidade de uma pessoa mediante comparação de seus dados biométricos com os contidos em base de dados de referência. A lógica é de comparação **1:N** -um rosto contra muitos cadastros. No contexto brasileiro, esse modelo é empregado, por exemplo, em sistemas de reconhecimento facial utilizados para localizar pessoas em bancos de dados de órgãos de segurança pública³.

² Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que cria regras harmonizadas em matéria de inteligência artificial e que altera os Regulamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento da Inteligência Artificial) . Disponível em: <http://data.europa.eu/eli/reg/2024/1689/oj>.

³ O Smart Sampa é o maior sistema de monitoramento de segurança pública da América Latina, criado

- 3) **Verificação biométrica (art. 3º, § 36).** Responde à pergunta "você é quem diz ser?". Consiste em verificação automatizada individual, incluindo autenticação, comparando dados biométricos de uma pessoa com dados previamente fornecidos por ela mesma. A lógica é de comparação **1:1** -a pessoa se apresenta voluntariamente e o sistema confirma a correspondência com seu próprio cadastro. Corresponde, no Brasil, ao desbloqueio facial em aplicativos bancários ou ao embarque com reconhecimento facial em aeroportos⁴.
- 4) **Categorização biométrica (art. 3º, § 40).** Consiste em sistemas de IA destinados a atribuir pessoas singulares a categorias específicas com base em seus dados biométricos. As categorias podem ser relativamente inócuas - como **idade** ou cor dos olhos - ou mais sensíveis, como sexo, etnia, traços de personalidade e filiações pessoais.

Sob essa sistemática, a estimação facial de idade configura uma modalidade de categorização biométrica. Seu objetivo não é identificar quem é a pessoa nem verificar uma identidade previamente declarada, mas inferir uma característica, nesse caso, a faixa etária provável, a partir de atributos faciais. Essa distinção possui relevantes consequências regulatórias, pois delimita tanto as funcionalidades que podem ser legitimamente desempenhadas por essas soluções quanto os limites de seu tratamento de dados. Em outras palavras, **um sistema concebido para estimar idade não deve incorporar funcionalidades típicas de identificação ou verificação biométrica sem que isso implique sua reclassificação tecnológica e a incidência das salvaguardas correspondentes.**

Essa classificação produz, ao menos, três consequências regulatórias para o Guia:

- I. Em primeiro lugar, **a categorização biométrica somente permanece caracterizada como tal enquanto sua finalidade e sua arquitetura técnica estiverem restritas à inferência de um atributo, sem a realização de operações próprias de identificação ou verificação biométrica.** Um sistema que converte imagens faciais em representações biométricas persistentes (*templates*, *embeddings*, vetores de características ou equivalentes) e as conserva para utilização posterior pode ultrapassar os limites da mera categorização, passando a incorporar funcionalidades compatíveis com sistemas de verificação ou de identificação biométrica, a depender da forma como esses dados são posteriormente utilizados. Essa alteração pode ocorrer sem mudanças perceptíveis para o usuário, razão pela qual não pode ser aferida exclusivamente a partir da finalidade declarada pelo fornecedor.
- II. Em segundo lugar, a classificação evidencia a importância de prevenir a expansão funcional (*function creep*) dos sistemas de aferição etária. **Soluções inicialmente desenvolvidas para estimar idade podem, mediante alterações em sua arquitetura ou no tratamento dos dados coletados,**

pela Prefeitura de São Paulo. Disponível em: <https://smartsampa.prefeitura.sp.gov.br/>.

⁴ Aeroporto de Salvador (BA) dá início a embarques por reconhecimento facial. Disponível em: <https://www.mercadoeventos.com.br/noticias/aviacao/aeroporto-de-salvador-ba-da-inicio-a-embarques-por-reconhecimento-facial/>.

passar a desempenhar funcionalidades distintas daquelas originalmente declaradas, especialmente quando há retenção de representações biométricas, integração com outras bases de dados ou reutilização das informações para finalidades diversas da aferição etária. A delimitação clara dessas categorias contribui para evitar que tecnologias submetidas a um regime jurídico menos intrusivo passem, na prática, a desempenhar funções típicas de identificação ou verificação biométrica.

- III. O Guia já contempla importante salvaguarda ao estabelecer que cabe ao agente de tratamento demonstrar, por meio de documentação técnica, **incluindo Relatório de Impacto à Proteção de Dados Pessoais, que a solução adotada não gera nem utiliza templates de identificação biométrica e que sua finalidade não é a identificação ou autenticação de indivíduos determinados.** Recomenda-se, contudo, aprofundar essa previsão mediante a definição de requisitos mínimos para tal demonstração. Mais do que exigir documentação técnica, o Guia pode explicitar quais evidências devem ser apresentadas para permitir que a classificação da solução como mecanismo de estimação facial seja objetivamente verificável, fortalecendo a atuação fiscalizatória da ANPD e conferindo maior segurança jurídica à distinção entre categorização, verificação e identificação biométrica.

Recomendação: que o Guia estabeleça que o fornecedor que adote estimativa facial deve demonstrar, em documentação técnica auditável, no mínimo:

- que a arquitetura não gera representação biométrica persistente (*template*, *embedding*, vetor de características ou equivalente) aptas à identificação ou reidentificação de indivíduos e, caso tais representações sejam produzidas transitoriamente durante o processamento, que sejam eliminadas de forma imediata e irreversível ao término da inferência;
- que não há comparação dos dados capturados contra qualquer base de referência interna ou externa, própria ou de terceiros, destinada à identificação ou autenticação de indivíduos;
- que o resultado retornado ao serviço digital é exclusivamente o atributo etário binário derivado ("*é ou não maior de 18 anos*"), sem compartilhamento da imagem facial, da idade estimada ou de quaisquer outros atributos biométricos ou dados derivados;
- que os sistemas de aferição etária operam funcionalmente segregados das demais infraestruturas de tratamento de dados da plataforma - em especial daquelas destinadas a publicidade direcionada, análise comportamental, personalização de conteúdo e treinamento de modelos de IA, vedada a reutilização das imagens ou dos dados biométricos coletados para finalidades diversas da aferição etária, conforme já recomendado na seção de privacidade e proteção de dados deste Guia.

A definição desses requisitos mínimos fortalece a verificabilidade da classificação adotada pelo Guia e permite que a distinção entre categorização, verificação e identificação biométrica seja aferida com base em elementos objetivos e auditáveis, e não apenas na finalidade declarada pelo fornecedor. Dessa forma,

reforça-se a efetividade das salvaguardas previstas para cada modalidade de tratamento biométrico e amplia-se a capacidade de fiscalização da ANPD.

SÍNTESE DA CONTRIBUIÇÃO

Recomenda-se que o Guia, na seção de Estimativa Facial:

- utilize, como referencial interpretativo para a distinção entre as diferentes modalidades de tratamento biométrico, a diferenciação entre identificação biométrica, verificação biométrica e categorização biométrica, de modo a conferir maior precisão conceitual às soluções de aferição etária baseadas em características faciais;
- explicita que a classificação de uma solução como mecanismo de estimativa facial depende não apenas da finalidade declarada pelo fornecedor, mas também das operações efetivamente realizadas pela arquitetura técnica e do tratamento conferido aos dados coletados, prevenindo a expansão funcional (*function creep*) para atividades de identificação ou verificação biométrica;
- estabeleça que o fornecedor que adote mecanismos de estimativa facial demonstre, por meio de documentação técnica auditável, no mínimo:
 - que a arquitetura não gera representações biométricas persistentes (templates, embeddings, vetores de características ou equivalentes) aptas à identificação ou reidentificação de indivíduos e, caso tais representações sejam produzidas transitoriamente durante o processamento, que sejam eliminadas de forma imediata e irreversível ao término da inferência;
 - que não há comparação dos dados capturados com qualquer base de referência, interna ou externa, própria ou de terceiros, destinada à identificação ou autenticação de indivíduos;
 - que o resultado disponibilizado ao serviço digital restringe-se exclusivamente ao atributo etário necessário para a decisão de acesso, sem compartilhamento da imagem facial, da idade estimada ou de quaisquer outros atributos biométricos ou dados derivados;
 - que os sistemas de aferição etária operam de forma funcionalmente segregada das demais infraestruturas de tratamento de dados da plataforma, especialmente aquelas destinadas à publicidade direcionada, análise comportamental, personalização de conteúdo e treinamento de modelos de inteligência artificial, vedada a reutilização das imagens ou dos dados biométricos coletados para finalidades diversas da aferição etária, conforme já recomendado na seção de Privacidade e Proteção de Dados do Guia.

b) A estimativa facial como medida de exceção, e não como mecanismo ordinário

A Tabela 3 do Guia (Matriz de risco de produtos e serviços) arrola o “uso de mecanismos de estimação etária, incluindo análise biométrica” entre os exemplos de mecanismos adequados tanto para risco moderado quanto para alto risco, ao lado do recebimento de sinal de idade e da adoção de credenciais verificáveis. Embora a tabela reconheça diferentes soluções tecnológicas para aferição etária, a forma como essas alternativas são apresentadas pode transmitir a impressão de que constituem opções equivalentes sob a perspectiva da proteção de direitos fundamentais, quando, na realidade, envolvem níveis significativamente distintos de intrusão e tratamento de dados pessoais.

Essa compreensão, contudo, não encontra respaldo nas demais seções do próprio Guia. Ao longo do documento, reconhece-se que diferentes mecanismos de aferição de idade apresentam impactos distintos sobre a privacidade e a proteção de dados pessoais, devendo ser privilegiadas soluções capazes de atingir a finalidade pretendida mediante o menor tratamento possível de dados. Nesse sentido, o próprio Guia registra que o relatório do Ministério da Justiça e Segurança Pública⁵ identificou convergência multissetorial em favor de mecanismos que minimizem a exposição de dados pessoais e apontou cautela quanto à utilização de soluções baseadas em biometria facial, em razão dos riscos de vigilância, vieses algorítmicos e coleta excessiva de dados. O mesmo caminho é apresentado pelo Relatório consolidado do Grupo de Trabalho (GT) nº 2, sobre proteção de dados de crianças e adolescentes, do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPd)⁶, o qual aponta que “soluções biométricas faciais não devem ser adotadas como padrão” e que “a regra deve ser a busca por métodos menos invasivos, capazes de comprovar apenas o atributo etário necessário, sem coleta excessiva de dados sensíveis e sem ampliação da capacidade de rastreamento das plataformas”.

Vale destacar que a defesa de uma utilização excepcional da estimativa facial não implica, em nenhuma hipótese, a adoção da autodeclaração como mecanismo suficiente de aferição etária. Conforme também destacado no mesmo relatório do GT 02 do CNPD, e, “a política pública deve evitar a falsa alternativa entre ineficácia e biometrização”⁷. Entre a autodeclaração frágil e a coleta facial massiva existe um espectro de soluções - credenciais verificáveis, tokens criptográficos, provas de conhecimento zero, verificação por intermediário confiável em arquitetura duplo-cego - que o próprio Guia já reconhece e recomenda em outras seções.

Essa compreensão, inclusive, encontra respaldo no próprio Guia. O documento dedica seção específica às credenciais verificáveis, reconhecendo que elas “se

⁵ Minuta De Guia Orientativo - Mecanismos de Aferição (0284584) SEI 00261.003182/2026-47/ pg. 17.

⁶ Relatório consolidado do Grupo de Trabalho (GT) nº 2, sobre proteção de dados de crianças e adolescentes, do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPd). Disponível em: <https://www.gov.br/anpd/pt-br/cnpd/grupos-de-trabalho/gt2-relatorio-final-cnpd.pdf/@@display-file/file>.

⁷ Relatório consolidado do Grupo de Trabalho (GT) nº 2, sobre proteção de dados de crianças e adolescentes, do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPd). Disponível em: <https://www.gov.br/anpd/pt-br/cnpd/grupos-de-trabalho/gt2-relatorio-final-cnpd.pdf/@@display-file/file>.

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”. Na seção dedicada à privacidade e proteção de dados, recomenda que os fornecedores “privilegiem a implementação de arquitetura baseada em atributos etários tokenizados e o uso de credenciais verificáveis”. Da mesma forma, a Tabela 3 indica, para serviços de alto risco, a priorização de soluções que conciliem elevada acurácia, robustez e confiabilidade com mecanismos avançados de proteção da privacidade, como atributos etários tokenizados e provas criptográficas capazes de confirmar apenas o atributo etário necessário, sem revelar dados pessoais adicionais.

Dessa forma, recomenda-se que a sistemática do Guia reflita de maneira ainda mais explícita a lógica de proporcionalidade e minimização que orienta suas demais seções. Se o próprio documento reconhece que mecanismos de preservação da privacidade são capazes de oferecer elevado grau de confiabilidade com menor impacto aos direitos fundamentais, a estimativa facial não deve ser apresentada como alternativa equivalente, mas como medida subsidiária, a ser considerada apenas quando soluções menos intrusivas não forem aptas a atingir, no caso concreto, o nível de proteção necessário.

SÍNTESE DA CONTRIBUIÇÃO

Recomenda-se que o Guia, na subseção "Estimativa Facial":

- explicita que a estimativa facial constitui mecanismo de caráter subsidiário, cuja utilização deve observar os princípios da proporcionalidade, da necessidade e da minimização do tratamento de dados pessoais, sendo recomendada apenas quando mecanismos menos intrusivos de aferição etária, especialmente aqueles baseados em preservação da privacidade, não forem aptos a assegurar o nível de proteção exigido para o contexto de risco concreto;
- estabeleça que a opção pela estimativa facial seja acompanhada de fundamentação técnica documentada, registrada no Relatório de Impacto à Proteção de Dados Pessoais e, quando aplicável, na Avaliação de Impacto sobre os Direitos da Criança (*Child Rights Impact Assessment – CRIA*), demonstrando as razões pelas quais soluções menos intrusivas não se mostraram adequadas ou suficientes;
- revise a Tabela 3 para refletir essa lógica de subsidiariedade, deixando claro que mecanismos de preservação da privacidade — como credenciais verificáveis, atributos etários tokenizados, provas de conhecimento zero (*Zero-Knowledge Proofs – ZKP*) e outras soluções equivalentes — constituem a referência preferencial sempre que capazes de atingir o nível de proteção necessário, figurando a estimativa facial como medida excepcional e não como alternativa equivalente às demais tecnologias de aferição etária.

c) A limitação estrutural da estimativa facial sobre o público que a norma pretende proteger

A utilização da estimativa facial para aferição etária apresenta uma limitação estrutural que merece ser explicitada pelo Guia: a tecnologia tende a apresentar menor desempenho justamente em relação ao grupo que a disciplina pretende proteger, isto é, crianças e adolescentes.

O Guia reconhece a existência de uma "zona cinzenta" (*buffer zone*) e recomenda a adoção de margens de segurança etária para mitigar erros de classificação. Trata-se de recomendação relevante, mas é importante ponderar que a redação atual pode possibilitar a interpretação que essas margens como solução para uma dificuldade operacional, quando parte da literatura técnica aponta que a menor acurácia em relação a crianças e adolescentes decorre de características inerentes ao próprio objeto de análise.

O relatório *Face Recognition Vendor Test (FRVT) – Part 3: Demographic Effects*, do *National Institute of Standards and Technology* (NIST)⁸, demonstram que sistemas baseados em características faciais apresentam desempenho inferior quando aplicados a crianças e adolescentes, conclusões corroboradas pelo *Government Accountability Office* (GAO, 2020)⁹. A causa é morfológica: as faces de crianças e adolescentes passam por crescimento craniofacial não linear, envolvendo mudanças significativas na estrutura óssea, o que os torna, na expressão da literatura técnica, "maus candidatos" para a tecnologia. As alterações anatômicas deslocam os escores de similaridade, aumentando a probabilidade de erros de classificação.

Essa limitação também é reconhecida pelo relatório *But how do they know it's a child?*, da 5Rights Foundation, que destaca que mecanismos de estimativa facial apresentam menor precisão para crianças mais novas e que as margens de erro tornam especialmente sensível a classificação de usuários situados próximos aos limiares etários utilizados para decisões regulatórias. O relatório também chama atenção para variações de desempenho relacionadas a características demográficas, como tom de pele e gênero, e observa que ainda há incertezas quanto à eficácia desses mecanismos para crianças com deficiências ou diferenças craniofaciais, recomendando que esses riscos sejam considerados na avaliação das soluções de

⁸ O NIST é o National Institute of Standards and Technology, ou, em português, Instituto Nacional de Padrões e Tecnologia. Trata-se de uma agência do governo dos Estados Unidos, vinculada ao Departamento de Comércio, cuja função principal é criar padrões técnicos, promover inovações e garantir a precisão de medidas e tecnologias utilizadas tanto no setor público quanto no privado.

⁹ O GAO é o "Government Accountability Office", que em português pode ser traduzido como Escritório de Responsabilidade Governamental dos Estados Unidos. O trecho que faz menção à questão levantada é: "Although the accuracy of facial recognition technology has increased dramatically in recent years, differences in performance exist for certain demographic groups. National Institute of Standards and Technology tests found that facial recognition technology generally performs better on lighter-skin men and worse on darker-skin women, and does not perform as well on children and elderly adults". UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE. *Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses*. GAO-20-522. Washington, D.C., 13 jul. 2020. Disponível em: <<https://www.gao.gov/assets/gao-20-522.pdf#:~:text=For%20verification%20vendor%20tests%2C%20NIST,found%20that%20false%20negative%20rates%E2%80%9494>>.

aferição etária¹⁰.

O próprio Guia reconhece parte desse problema ao indicar, na Tabela 4, a limitação da disponibilidade de bases de treinamento e teste representativas de crianças e adolescentes como um risco específico da estimativa etária facial. Entretanto, o documento não aborda uma tensão regulatória relevante: o aprimoramento desses modelos depende, em grande medida, da ampliação e diversificação das bases de treinamento, o que não pode ocorrer mediante a reutilização dos dados coletados para fins de aferição etária.

Essa limitação decorre diretamente do art. 13 do ECA Digital e do art. 24, III, do Decreto nº 12.880/2026, que vedam a utilização dos dados coletados para aferição etária para finalidades secundárias incompatíveis com sua finalidade original. Assim, embora o aperfeiçoamento dos modelos possa constituir objetivo legítimo sob a perspectiva técnica, ele não autoriza a reutilização dos dados coletados no contexto da aferição de idade para treinamento, retreinamento ou validação de sistemas de inteligência artificial.

Por essa razão, recomenda-se que o Guia explicita que a busca por maior acurácia dos mecanismos de estimativa facial deve ocorrer por meios compatíveis com o regime jurídico aplicável à proteção de crianças e adolescentes, não sendo admissível utilizar, para treinamento ou aprimoramento dos modelos, os dados coletados durante a própria operação de aferição etária.

SÍNTESE DA CONTRIBUIÇÃO

Recomenda-se que o Guia, na subseção "Estimativa Facial":

- explicita que mecanismos de estimativa facial apresentam limitações estruturais de desempenho quando aplicados a crianças e adolescentes, especialmente em faixas etárias próximas aos limiares regulatórios, bem como potenciais variações de desempenho relacionadas a características demográficas e diferenças craniofaciais, devendo tais limitações ser consideradas na avaliação da adequação desses mecanismos;
- esclareça que a melhoria da acurácia desses sistemas deve ocorrer por meios compatíveis com o regime jurídico de proteção de crianças e adolescentes, não sendo admissível utilizar, para treinamento, retreinamento, validação ou aperfeiçoamento de modelos de inteligência artificial, os dados pessoais coletados durante a operação de aferição etária, em observância ao art. 13 do ECA Digital e ao art. 24, III, do Decreto nº 12.880/2026.

¹⁰ 5Rights Foundation. But How Do They Know It Is a Child? Age Assurance in the Digital World (Updated). 2021. Disponível em: <https://5rightsfoundation.com/resource/but-how-do-they-know-its-a-child/>. Acesso em: 31 jul. 2025

2. Capítulo de análise: Verificação Documental

O Guia qualifica a verificação documental como método determinístico, que “baseia-se em atributo declarado por autoridade emissora competente”, e registra que essa característica lhe confere “em regra, maior nível de robustez do que métodos estimativos, tornando-a particularmente adequada para serviços de maior risco”. A caracterização técnica é adequada e a seção apresenta requisitos operacionais consistentes quanto à autenticidade documental, à proteção contra falsificação e ao compartilhamento de dados. Recomenda-se, como complemento, que o Guia explicita também que essa robustez decorre da exposição de um conjunto mais amplo de dados pessoais, o que exige a adoção de salvaguardas proporcionais voltadas à minimização do tratamento.

Um documento de identidade não contém apenas a data de nascimento. Contém nome civil completo, filiação, número de registro geral, número de inscrição no Cadastro de Pessoas Físicas, naturalidade, fotografia e, conforme o tipo, impressão digital. A elevada confiabilidade da verificação documental decorre justamente da apresentação desse conjunto ampliado de informações ao fornecedor ou ao intermediário responsável pela validação, embora a finalidade do tratamento se restrinja à confirmação do atributo etário.

O Guia reconhece esse ponto em sua dimensão temporal, ao registrar, com apoio no art. 24, § 3º, do referido Decreto, que o tratamento “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”. Essa diretriz é coerente com a lógica geral adotada pelo próprio Guia, que privilegia, sempre que possível, o compartilhamento do atributo etário em substituição ao compartilhamento dos dados que lhe dão origem. Essa orientação manifesta-se em diferentes passagens do documento, especialmente na disciplina do sinal de idade, das credenciais verificáveis e das arquiteturas baseadas em atributos etários, todas voltadas a permitir que apenas a informação estritamente necessária circule entre os agentes da cadeia digital. Recomenda-se que a subseção dedicada à verificação documental seja interpretada à luz dessa mesma lógica, de modo que a apresentação do documento constitua apenas meio para extração do atributo etário necessário, e não fundamento para o tratamento ou circulação dos demais dados pessoais nele constantes.

A orientação é acertada e merece ser preservada. Recomenda-se, contudo, complementá-la com parâmetros aplicáveis à própria fase de captura. Entre a apresentação do documento e a extração do atributo etário, o conjunto integral de dados nele constante é necessariamente processado pela arquitetura da solução, permanecendo sujeito aos riscos de acesso indevido, incidentes de segurança e utilização incompatível com a finalidade originalmente declarada. Como sustentado

pelo Instituto Alana no capítulo dedicado à privacidade e proteção de dados desta contribuição, o princípio da minimização não se projeta apenas sobre a retenção das informações, mas também sobre a própria coleta e o processamento dos dados.

Recomenda-se, ademais, uma precisão quanto à formulação segundo a qual a verificação documental seria "particularmente adequada para serviços de maior risco" (p. 41 do Guia) . Nos termos do art. 24, I, do Decreto nº 12.880/2026, a adequação do mecanismo não decorre exclusivamente de seu grau de confiabilidade, mas do equilíbrio entre efetividade, necessidade, proporcionalidade e impacto sobre os direitos fundamentais dos titulares. Essa compreensão é reiterada pelo próprio Guia ao afirmar que a escolha do mecanismo "não deve ser orientada apenas pela precisão da aferição de idade, mas também pela sua compatibilidade com os direitos dos usuários e com as exigências de proteção de dados pessoais". Nesse contexto, recomenda-se que o Guia explicita ainda mais a relação entre a verificação documental e os mecanismos de preservação da privacidade já contemplados em outras seções, especialmente aqueles baseados em atributos etários, credenciais verificáveis e mecanismos criptográficos de comprovação de idade, como o ZKP. Sempre que tais soluções estiverem disponíveis e forem aptas a atingir o nível de proteção necessário, sua adoção mostra-se mais compatível com os princípios da minimização e da proporcionalidade.

Por fim, recomenda-se desenvolver nesta seção a ressalva que o Guia já registra no capítulo de inclusão e não discriminação, onde reconhece que “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”. A observação é particularmente relevante quando o público-alvo do mecanismo são crianças e adolescentes, parcela significativa dos quais não dispõe de documento oficial com fotografia em posse própria, situação mais frequente entre famílias em contexto de vulnerabilidade socioeconômica, populações indígenas, ribeirinhas e quilombolas, marcada por desigualdades regionais, dimensão que o art. 10 do ECA Digital determina considerar ao referir-se expressamente à “diversidade de contextos socioeconômicos brasileiros”.

SÍNTESE DA CONTRIBUIÇÃO

Diante do exposto, recomenda-se que o Guia, na seção de Verificação Documental:

- explicita que a maior robustez da verificação documental decorre do tratamento de um conjunto mais amplo de dados pessoais, razão pela qual sua utilização deve ser acompanhada de salvaguardas proporcionais voltadas à minimização do tratamento, observando-se os princípios da necessidade, da proporcionalidade e da proteção de dados pessoais;
- esclareça que a apresentação do documento constitui apenas meio para extração do atributo etário necessário à decisão de acesso, não justificando

o tratamento, a circulação ou o compartilhamento dos demais dados pessoais constantes do documento além do estritamente necessário para a aferição etária;

- estabeleça parâmetros aplicáveis também à fase de captura do documento, privilegiando mecanismos de extração seletiva de dados e outras medidas de minimização do tratamento, sempre que tecnicamente viáveis, bem como restringindo a circulação da imagem integral do documento e dos dados nele constantes ao estritamente necessário para a finalidade da operação;
- determine que as razões técnicas que eventualmente impeçam a adoção de mecanismos de extração seletiva ou de outras medidas de minimização sejam justificadas e documentadas no Relatório de Impacto à Proteção de Dados Pessoais;
- explicita que a utilização exclusiva da verificação documental pode comprometer o requisito de inclusão, recomendando a disponibilização de mecanismos alternativos de comprovação etária para pessoas que não disponham de documentação adequada ou enfrentem barreiras de acesso, especialmente crianças e adolescentes em contextos de vulnerabilidade social.

3. Capítulo de análise: Credenciais Verificáveis

O capítulo de Requisitos Específicos organiza-se em três seções, sendo que as de estimativa facial e verificação documental apresentam subseções com requisitos operacionais dirigidos aos fornecedores. A de credenciais verificáveis tem caráter predominantemente descritivo, explicando o funcionamento do modelo emissor-portador-verificador e concluindo com o reconhecimento de que essas soluções "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" (p.44 do Guia). O Instituto Alana subscreve esse reconhecimento e, justamente por isso, recomenda que a seção receba desenvolvimento equivalente ao das demais.

A observação tem fundamento prático: na tomada de decisão sobre implementação, fornecedores tendem a orientar-se pelo grau de segurança jurídica que cada caminho oferece, de modo que seções com requisitos claros reduzem custo de conformidade e incerteza. O desenvolvimento desta seção contribuiria, assim, para que mecanismos capazes de conciliar elevada confiabilidade com menor exposição de dados pessoais sejam efetivamente incorporados às arquiteturas de aferição de idade, fortalecendo a proteção integral de crianças e adolescentes no ambiente digital.

Essa recomendação também é coerente com posição anteriormente defendida

pelo Instituto Alana na Consulta Pública sobre Aferição de Idade do MJSP, segundo a qual a regulamentação deve privilegiar parâmetros de desempenho (como minimização de dados, interoperabilidade, auditabilidade, verificabilidade e proteção da privacidade) em vez da imposição de tecnologias específicas. Nesse contexto, o detalhamento da seção de credenciais verificáveis não significa privilegiar determinado modelo tecnológico, mas fornecer parâmetros regulatórios capazes de orientar a adoção das arquiteturas que melhor concretizam esses objetivos.

Quanto às provas de conhecimento zero, o Guia registra que, "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" (p.43 do Guia). A orientação é adequada e reforça o compromisso do Guia com arquiteturas que conciliam elevada confiabilidade e minimização do tratamento de dados pessoais. Recomenda-se, contudo, que a ressalva referente à viabilidade técnica seja acompanhada de parâmetros mínimos que permitam sua aferição e documentação. Sem tais critérios, a exceção tende a permanecer excessivamente aberta, dificultando o controle regulatório sobre as hipóteses em que mecanismos mais protetivos deixam de ser adotados.

Na mesma contribuição para a Consulta do MJSP, o Instituto Alana destacou que mecanismos como credenciais verificáveis, provas de conhecimento zero e tokens criptográficos materializam o princípio da proteção de dados desde a concepção (*privacy by design*), ao estruturarem a arquitetura da aferição etária para

compartilhar apenas o atributo necessário à verificação. Mais do que reduzir obrigações posteriores de retenção ou descarte, essas soluções diminuem, desde a origem, a quantidade de dados pessoais coletados, processados e compartilhados, concretizando os princípios da minimização e da limitação da finalidade previstos na LGPD.

O entendimento também encontra respaldo no Relatório Consolidado do Grupo de Trabalho nº 2 sobre Proteção de Dados de Crianças e Adolescentes, do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPd)¹¹ sobre o tema, recomenda "a utilização de soluções que comprovem apenas o atributo etário necessário, com modelos de prova de conhecimento zero, credenciais verificáveis e tokens criptográficos, não utilizando coleta de imagem facial, documento completo, data de nascimento e número de identidade civil", sustentando que tais arquiteturas permitem "responder à pergunta relevante (por exemplo, se o usuário está acima de determinado limite etário) sem transformar o rosto em senha universal de acesso". O Instituto Alana, na Contribuição à Tomada de Subsídios sobre Dados Biométricos, arrolou o uso de tecnologias do tipo *zero knowledge proof* entre as salvaguardas

¹¹ Relatório consolidado do Grupo de Trabalho (GT) nº 2, sobre proteção de dados de crianças e adolescentes, do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPd). Disponível em: <https://www.gov.br/anpd/pt-br/cnpd/grupos-de-trabalho/gt2-relatorio-final-cnpd.pdf/@@display-file/file>.

técnicas exigíveis, registrando a experiência da EU Age Verification Solution¹² como demonstração de que é possível desenvolver mecanismos de aferição etária que dispensam a coleta de dados biométricos.

No que se refere ao papel do poder público, o Guia menciona o Gov.br ao exemplificar entidades emissoras confiáveis, sem desenvolver o tema. Recomenda-se explicitar essa dimensão, **em articulação com o art. 11 do ECA Digital, que prevê o papel do poder público na promoção de soluções técnicas de aferição de idade, e com o art. 24, IX, do Decreto, que menciona expressamente a articulação entre sistemas e soluções públicas e privadas.**

Na contribuição do Instituto Alana à Consulta Pública sobre Aferição de Idade conduzida pelo MJSP, ressaltou-se que a efetividade de arquiteturas baseadas em credenciais verificáveis depende da adoção de padrões técnicos abertos, capazes de assegurar interoperabilidade, auditabilidade e ampla compatibilidade entre diferentes emissores, verificadores e carteiras digitais. Recomenda-se que o Guia incorpore essa orientação, explicitando que a implementação de credenciais verificáveis deve privilegiar especificações técnicas amplamente reconhecidas internacionalmente. A utilização de padrões abertos reduz barreiras de entrada para novos participantes, favorece a concorrência, amplia a auditabilidade das soluções e mitiga riscos de dependência tecnológica decorrentes de arquiteturas proprietárias

Como já sustentado nos capítulos de Inclusão e Não Discriminação e de Interoperabilidade desta contribuição, soluções apoiadas em infraestrutura digital pública reduzem barreiras econômicas e técnicas para fornecedores de menor porte, ampliam a adoção de mecanismos confiáveis e evitam que a efetividade do ECA Digital fique condicionada à contratação de poucos provedores privados. Preocupação semelhante é registrada no Relatório Consolidado do Grupo de Trabalho nº 2 sobre Proteção de Dados de Crianças e Adolescentes, do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPd)¹³, ao alertar que “a proteção de crianças e adolescentes no Brasil não pode depender da arquitetura técnica de grandes plataformas ou de fornecedores privados de biometria”, pois, “quando a aferição de idade passa a depender de sistemas fechados, bases externas, certificações privadas e modelos proprietários, o país transfere parte de sua capacidade regulatória para infraestruturas privadas, cujas possibilidades de controle democrático ficam bastante reduzidas se comparadas a uma solução pública construída com participação social”.

Cabe registrar que não se trata de horizonte hipotético. Debates técnicos promovidos no 2º Workshop de Credenciais Verificáveis, no âmbito do Ceweb.br/NIC.br¹⁴, reunindo representantes do Ministério da Gestão e da Inovação

¹² EUROPEAN COMMISSION. European Age Verification Solution. Bruxelas, 2025. Disponível em: <https://ageverification.dev>.

¹³ Relatório consolidado do Grupo de Trabalho (GT) nº 2, sobre proteção de dados de crianças e adolescentes, do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPd). Disponível em: <https://www.gov.br/anpd/pt-br/cnpd/grupos-de-trabalho/gt2-relatorio-final-cnpd.pdf/@@display-file/file>.

¹⁴ CEWEB. 2º Workshop de Credenciais Verificáveis. Disponível em: <https://credenciaisdigitais.ceweb.br/>

em Serviços Públicos, da Dataprev, do Ministério da Educação, da Rede Nacional de Ensino e Pesquisa, de instituições federais de ensino e do setor privado, evidenciam a existência de um ecossistema brasileiro de credenciais verificáveis em construção, com pilotos já em operação em áreas como crédito rural e certificação acadêmica.

Por meio das discussões promovidas pelo evento, é possível compreender que a aferição etária pode, assim, apoiar-se em infraestrutura que já vem sendo desenvolvida no país, em vez de partir do zero ou de depender exclusivamente de soluções importadas. Nesses mesmos debates foi identificada uma barreira estrutural que merece registro: o efeito de rede, pelo qual emissores tendem a aguardar a existência de verificadores e verificadores tendem a aguardar a existência de emissores, de modo que o ecossistema não alcança escala sem indução externa. Esse diagnóstico reforça a pertinência de um papel ativo do poder público, não apenas como emissor possível, mas como agente capaz de destravar a adoção. Foi igualmente apontado o risco de dependência tecnológica de fornecedores externos (*vendor lock-in*) caso o desenvolvimento nacional se atrase, preocupação que converge com o quanto levantado pelo já mencionado Relatório do CNPD¹⁵ quanto à transferência de capacidade regulatória a infraestruturas privadas.

Quanto às salvaguardas contra rastreabilidade, o Guia registra que “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”. Recomenda-se desenvolver essa orientação em parâmetros concretos. A verificação do *status* de validade da credencial a cada apresentação, que o próprio Guia estabelece, cria ponto de contato recorrente entre portador e emissor; caso essas consultas permitam ao emissor inferir quando e perante qual serviço a credencial foi apresentada, a arquitetura pode reproduzir, por outro meio, a rastreabilidade vedada no art. 24, VIII, do Decreto.

Contribui para esse debate a distinção, formulada em discussões técnicas recentes sobre o tema no Brasil, entre documentos permanentes e credenciais de trânsito: enquanto determinados registros precisam ser preservados para assegurar autenticidade, rastreabilidade ou memória institucional, credenciais utilizadas exclusivamente para autorizar o acesso a um serviço podem ser concebidas como instrumentos efêmeros, gerados sob demanda a partir da fonte confiável da informação e descartados após o cumprimento de sua finalidade. Aplicada aos mecanismos de aferição etária, essa lógica permite que a comprovação da idade ocorra sem a constituição de um identificador persistente ou de uma credencial destinada ao armazenamento e à reutilização. Em vez disso, a comprovação pode ser realizada por meio de uma prova gerada para cada interação específica, reduzindo simultaneamente a exposição de dados pessoais, o risco de reutilização indevida e a

¹⁵ Relatório consolidado do Grupo de Trabalho (GT) nº 2, sobre proteção de dados de crianças e adolescentes, do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD). Disponível em: <https://www.gov.br/anpd/pt-br/cnpg/grupos-de-trabalho/gt2-relatorio-final-cnpg.pdf/@@display-file/file>.

possibilidade de correlação entre diferentes acessos.

SÍNTESE DA CONTRIBUIÇÃO

Diante do exposto, recomenda-se que o Guia, na seção de Credenciais Verificáveis:

- incorpore recomendações operacionais dirigidas aos fornecedores, em estrutura equivalente à adotada nas demais seções do capítulo de Requisitos Específicos, estabelecendo parâmetros concretos para implementação, governança, interoperabilidade e auditabilidade dessas soluções;
- explicita que a implementação de credenciais verificáveis deve privilegiar arquiteturas orientadas pelos princípios da minimização, da limitação da finalidade, da proteção de dados desde a concepção (*privacy by design*) e da interoperabilidade, promovendo o compartilhamento exclusivo do atributo étário estritamente necessário para cada operação;
- estabeleça que a adoção de provas de conhecimento zero (*Zero-Knowledge Proof – ZKP*) ou de mecanismos criptográficos equivalentes constitui o padrão esperado nas soluções baseadas em credenciais verificáveis, cabendo ao fornecedor que adote solução diversa registrar, no Relatório de Impacto à Proteção de Dados Pessoais, as razões técnicas que justifiquem essa opção;
- recomende a adoção de padrões técnicos abertos e amplamente reconhecidos para implementação de credenciais verificáveis, bem como registre a relevância do desenvolvimento de credenciais étárias emitidas, reconhecidas ou credenciadas pelo poder público, em articulação com soluções privadas interoperáveis, de modo a ampliar a interoperabilidade, reduzir barreiras à entrada de novos participantes, mitigar riscos de dependência tecnológica associados a arquiteturas proprietárias e favorecer a adoção de mecanismos confiáveis por fornecedores de diferentes portes;
- determine que as soluções baseadas em credenciais verificáveis adotem arquitetura capaz de impedir que o emissor conheça a identidade da parte verificadora ou estabeleça correlação entre diferentes apresentações da credencial, em coerência com o modelo duplo-cego (*double-blind*) e com a vedação à rastreabilidade prevista no Decreto;
- explicita que credenciais destinadas exclusivamente à comprovação étária podem ser estruturadas como credenciais efêmeras ou provas geradas para cada interação específica, evitando a constituição de identificadores persistentes e reduzindo os riscos de rastreabilidade, reutilização indevida e correlação entre diferentes acessos.

EXPEDIENTE

Júlia Mendonça

João Coelho

Luíse Menezes