Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

Contribuições do CNPD ao Guia Orientativo de Aferição Etária da ANPD

Este documento consolida as contribuições encaminhadas pelos membros do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD), em sua segunda composição, acerca do Guia Orientativo de Aferição Etária da ANPD, conforme solicitado pela Agência Nacional de Proteção de Dados (ANPD) por meio do Ofício nº 16/2026/SE/ANPD.

O Guia Orientativo tem como objetivo garantir segurança jurídica e efetividade à aplicação do ECA Digital (Lei nº 15.211/2025), bem como do Decreto nº 12.880/2026. As contribuições apresentadas no Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD) tem como objetivo garantir que tal norma esteja adequada aos direitos previstos.

Os Conselheiros encaminharam duas contribuições acerca do Guia Orientativo de Aferição Etária. A Conselheira Ana Paula Bialer sugere o reconhecimento de que o sinal etário íntegro, produzido por fonte confiável nos elos anteriores da cadeia, seja suficiente para o cumprimento do dever de aferição pelo fornecedor receptor em contextos de risco moderado, sem necessidade de nova coleta de dados. A Conselheira também entende serem necessários estímulos as lojas de aplicações e aos sistemas operacionais a transmitir, sempre que tecnicamente viável e compatível com os princípios de minimização de dados e privacidade por padrão, sinais de idade que indiquem a faixa etária apurada em granularidade suficiente para o cumprimento das obrigações legais diferenciadas por idade. Em relação à matriz de risco, a contribuição sugere a revisão da tabela 3 para incorporar as salvaguardas já implementadas pelos fornecedores como elemento relevante da avaliação contextual de risco. A contribuição também solicita esclarecimento quanto ao uso do CPF para autodeclaração de idade, visto que tal dado também pode ser utilizado em mecanismos de aferição de nível superior.

Já a Conselheira Myreilla Canto propõe delimitar mais claramente o escopo do Guia para evitar interpretação extensiva a setores já fortemente regulados, como o financeiro, de forma que a incidência do ECA Digital esteja condicionada a hipóteses em que o produto ou serviço seja efetivamente direcionado ao público infantojuvenil e acessado diretamente pelo menor. Além disso, a Conselheira também faz contribuições quanto as interpretações adequadas ao princípio da proporcionalidade, que deve considerar, a (i) ausência de conteúdo impróprio ou proibido; (ii) inexistência de interação social relevante entre usuários; (iii) utilização de dados previamente validados por terceiros confiáveis. Por fim, a contribuição recomenda que o Guia explicite sua natureza orientativa e não vinculante, de modo a evidenciar que seu

conteúdo não deve ser interpretado como engessamento, sobretudo em um contexto em que o próprio escopo do ECA Digital ainda se encontra em evolução e em construção normativa.

As contribuições reproduzidas neste documento são de autoria individual de cada Conselheiro e refletem posições pessoais e setoriais de quem as subscreve. Elas não resultam de deliberação ou votação majoritária do Conselho, tratando-se apenas de uma consolidação das contribuições recebidas.

O Conselho permanece à disposição da ANPD para aprofundar qualquer das propostas, participar de grupos de trabalho, consultas públicas e tomadas de subsídios, e contribuir para a regulamentação dos temas de competência desta Agência.

Victor Oliveira Fernandes

Presidente do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD)

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

Anexo - Contribuições das Conselheiras

Contribuição de aprimoramento do Guia Orientativo “Mecanismos de Aferição de Idade”

Conselheira Ana Paula Bialer

A elaboração de Guia Orientativo pela ANPD é um passo fundamental para conferir segurança jurídica à aplicação do ECA Digital (Lei nº 15.211/2025) e do Decreto nº 12.880/2026. Esta contribuição, apresentada no âmbito do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD), tem o propósito estritamente colaborativo de assegurar que o Guia reflita com fidelidade as diretrizes de proporcionalidade e as isenções consagradas pela legislação, evitando que suas orientações gerem distorções ou insegurança jurídica para os agentes regulados.

I. Comentários Gerais

a) Impacto da Cadeia Digital Multicamadas na Sistemática de Aferição de Idade

O Guia Orientativo descreve com precisão a cadeia digital de responsabilidades (Seção II), identificando dois níveis de aferição: o primeiro realizado por lojas de aplicações e sistemas operacionais, e o segundo pelos demais fornecedores. Nesse segundo nível, o modelo legal prevê regimes distintos conforme a natureza do conteúdo ofertado: fornecedores de conteúdos, produtos ou serviços proibidos devem adotar mecanismos próprios de verificação de idade, independentemente do sinal recebido (art. 15 do ECA Digital c/c art. 25, §4º do Decreto); já os fornecedores de conteúdos impróprios ou inadequados devem adotar medidas proporcionais ao risco identificado, as quais podem ou não incluir aferição de idade (art. 14 do Decreto). O que se inaugura, portanto, é um novo status quo regulatório no qual a aferição de idade passa a ser exigida, ou fortemente recomendada, em múltiplos pontos da jornada digital do usuário, operados por agentes distintos e, em grande medida, de forma desarticulada entre si.

Esse cenário, embora coerente com a lógica de proteção em camadas adotada pelo legislador, pode gerar efeitos colaterais relevantes: fricção excessiva na jornada do usuário; coleta desnecessária e multiplicada de dados pessoais, em tensão direta com o princípio da necessidade (art. 6º, III, da LGPD) e com as vedações ao compartilhamento contínuo previstas no art. 24 do Decreto; risco de inconsistência sistêmica entre sinais etários produzidos independentemente por diferentes agentes; e, no limite, uma forma de vigilância estrutural por acumulação incompatível com a vedação à implantação de mecanismos de vigilância massiva ou indiscriminada prevista no art. 37, parágrafo único, do ECA Digital.

A ANPD, ao emitir recomendações para a implementação de mecanismos confiáveis de aferição de idade, deve considerar explicitamente essa mudança de sistemática. Recomenda-se, nesse sentido, que o Guia Orientativo: (i) reconheça que o sinal etário íntegro, produzido por fonte confiável nos

elos anteriores da cadeia, pode ser suficiente para o cumprimento do dever de aferição pelo fornecedor receptor em contextos de risco moderado, sem necessidade de nova coleta de dados; (ii) calibre as orientações dirigidas a cada agente em função do que já foi verificado pelos elos anteriores, em consonância com o princípio da proporcionalidade (art. 24, I, do Decreto); e (iii) conecte explicitamente o requisito de interoperabilidade à problemática da aferição reiterada

b) O sinal de idade e as oportunidades de aprimoramento do modelo em camadas

O ECA Digital e o Decreto atribuem às lojas de aplicações e aos sistemas operacionais o papel de porta de entrada do ecossistema digital, conferindo a esses agentes o dever de fornecer o sinal de idade aos demais fornecedores (art. 12, §1º, do ECA Digital) e de realizar a aferição preferencialmente por meio de credenciais verificáveis (art. 25, §2º, II, do Decreto). A intenção do legislador é que uma aferição robusta na origem beneficie toda a cadeia subsequente, reduzindo o ônus dos demais fornecedores e conferindo maior coerência protetiva ao ecossistema como um todo.

Para que essa lógica se concretize na prática, seria importante que o Guia estimulasse os agentes a enriquecer o conteúdo do sinal de idade transmitido, para além do exemplo de confirmação binária maior/menor de 18 anos mencionado no documento. Isso por duas razões.

A primeira é que um sinal restrito à distinção maior/menor de 18 anos não permite que os demais fornecedores adaptem a experiência do usuário a faixas etárias intermediárias. O ECA Digital estrutura obrigações diferenciadas para diferentes grupos etários, como a vinculação de contas de menores de 16 anos a responsáveis legais (art. 24 do ECA Digital). Um fornecedor de rede social que recebe apenas a informação de que o usuário é menor de 18 anos não dispõe dos elementos necessários para cumprir adequadamente todas as suas obrigações legais sem realizar nova aferição, o que reconduz ao problema da coleta reiterada e desnecessária de dados pessoais tratado no tópico anterior.

A segunda razão é que o sinal de idade, na forma como atualmente descrito, não carrega informação de proveniência, isto é, não indica qual foi o método de aferição utilizado para produzi-lo. Sem esse elemento, o fornecedor receptor encontra dificuldades para avaliar o nível de confiabilidade do sinal recebido, determinar se é necessário acionar camada adicional de aferição proporcional ao risco do seu serviço e, sobretudo, cumprir a obrigação estabelecida no art. 25, §4º, do Decreto, que determina a adoção da alternativa mais protetiva em caso de divergência entre sinais. Um sinal produzido por autodeclaração e um sinal produzido por credencial verificável com respaldo documental têm pesos distintos para fins de tomada de decisão pelo fornecedor receptor, e o Guia poderia oferecer orientação mais clara sobre como distingui-los.

Nesse sentido, sugere-se que o Guia estimule as lojas de aplicações e os sistemas operacionais a transmitir, sempre que tecnicamente viável e compatível com os princípios de minimização de dados e privacidade por padrão, sinais de idade que indiquem a faixa etária apurada em

granularidade suficiente para o cumprimento das obrigações legais diferenciadas por idade, bem como metadado indicando o método de aferição utilizado. Essas informações adicionais permitiriam que os fornecedores receptores calibrassem suas próprias obrigações de forma proporcional ao que já foi verificado na origem, reduzindo a necessidade de aferições redundantes e tornando o ecossistema de dois níveis desenhado pelo ECA Digital mais coerente e eficiente na prática.

c) A divergência entre sinais de idade e a necessidade de maior clareza

O Guia menciona que, em caso de divergência entre o sinal de idade recebido e a aferição realizada pelo próprio fornecedor, devem ser adotadas as medidas correspondentes à alternativa mais protetiva a crianças e adolescentes (art. 25, §4º, do Decreto). Trata-se, contudo, de conceito que comporta ao menos duas leituras distintas, e cuja ambiguidade gera insegurança jurídica relevante para os fornecedores.

A expressão "alternativa mais protetiva" comporta ao menos duas leituras distintas. A primeira é que prevalece o sinal que indica a menor idade. A segunda é que prevalece o sinal produzido pelo mecanismo de aferição mais robusto e confiável, independentemente do resultado que ele produziu. As duas leituras levam a consequências práticas muito distintas, e a ausência de orientação sobre qual delas adotar gera insegurança jurídica relevante para os fornecedores que se deparam com essa situação na prática.

Além da ambiguidade conceitual, nem o ECA Digital nem o Decreto respondem ao que ocorre durante o período em que a divergência ainda não foi resolvida. O art. 27 do Decreto garante ao usuário o direito de contestar a idade aferida e exige decisão fundamentada em prazo razoável, e o art. 25, §2º, III, prevê a contestação e retificação da classificação etária mediante apresentação de evidência adicional, mas ambos os dispositivos tratam da contestação pelo usuário, não da hipótese específica de divergência entre sinais produzidos por agentes distintos da cadeia. Essa lacuna gera dúvidas operacionais relevantes para o fornecedor, que não dispõe de parâmetros claros sobre como agir enquanto a divergência persiste. Sugere-se que o Guia ofereça orientação mínima sobre esse ponto, de modo a permitir que os fornecedores adotem condutas proporcionais e juridicamente seguras diante de uma situação que, dado o modelo multicamadas adotado pelo ECA Digital, tende a ocorrer com alguma frequência na prática.

d) A matriz de risco e a necessidade de incorporar salvaguardas existentes

A Tabela 3 é apresentada como matriz exemplificativa e não exaustiva, com a ressalva de que não deve ser interpretada de maneira absoluta e estanque. Contudo, sua estrutura classifica categorias inteiras de serviços, como redes sociais, plataformas de vídeo com conteúdo misto e serviços de IA generativa, como risco moderado ou alto, sem considerar as salvaguardas que cada fornecedor já implementa. Essa abordagem produz um efeito problemático do ponto de vista da proporcionalidade: um fornecedor que implementa controles parentais robustos, defaults

protetivos avançados e sistemas sofisticados de detecção de idade é classificado na mesma categoria de risco que um fornecedor sem nenhuma dessas medidas.

O modelo regulatório deveria reconhecer que o risco efetivo de um serviço não deriva apenas de suas características e funcionalidades, mas da combinação dessas características com as medidas de proteção já implementadas. Essa lógica é, aliás, coerente com a abordagem baseada em risco que o próprio Guia consagra e com o requisito de proporcionalidade previsto no art. 24, I, do Decreto, que exige equilíbrio entre a solução adotada e o nível de risco associado ao serviço. Uma avaliação de risco que ignora as salvaguardas existentes não é uma avaliação de risco real: é uma avaliação de risco potencial, que pode superestimar significativamente o risco efetivo de serviços que já adotam medidas protetivas robustas. Além disso, essa abordagem desincentiva o investimento em salvaguardas adicionais, na medida em que o esforço protetivo do fornecedor não se reflete na sua classificação de risco.

Além disso, chama atenção que a Tabela 3 inclua mecanismos de verificação de idade entre os exemplos aplicáveis ao nível de risco moderado. O Decreto reserva a verificação de idade, espécie de alto grau de confiabilidade, para contextos de conteúdos, produtos e serviços proibidos, distinguindo-a das demais formas de aferição admissíveis em contextos de risco moderado. A presença da verificação como mecanismo de risco moderado na tabela cria risco de que fornecedores interpretem estar obrigados a adotar mecanismo que o Decreto reserva para situações de maior gravidade, o que contraria a própria lógica de proporcionalidade que estrutura o documento. Sugere-se que o Guia revise a tabela para refletir com maior precisão essa distinção e incorpore as salvaguardas já implementadas pelos fornecedores como elemento relevante da avaliação contextual de risco.

e) Aferição de idade no nível da funcionalidade para conteúdos impróprios ou inadequados

O Decreto já reconhece, para conteúdos, produtos e serviços proibidos, que a aferição de idade não precisa necessariamente ocorrer na entrada do serviço, podendo ser realizada no momento de acesso à funcionalidade específica que representa o risco. É o que se verifica, por exemplo, no art. 18, que autoriza a verificação no ato do cadastro ou no momento da aquisição do produto; e no art. 23, que admite a verificação no momento de acesso à funcionalidade de loot box, dispensando-a quando essa funcionalidade é restrita por padrão. Nesses casos, reconheceu-se que a proteção eficaz pode ser estruturada em torno da funcionalidade de risco, e não necessariamente da porta de entrada do serviço.

Sugere-se que o Guia estenda essa mesma lógica de flexibilidade aos fornecedores de conteúdos impróprios ou inadequados, orientando expressamente que a aferição de idade, quando adotada como medida protetiva nesse contexto, possa ser implementada tanto no acesso inicial ao serviço quanto no momento de contato do usuário com a funcionalidade específica que representa o risco identificado. Essa abordagem permitiria que o fornecedor, com base em sua própria avaliação de risco, escolha o ponto de aferição mais proporcional às características do seu serviço.

Essa orientação atenderia, ademais, de forma mais precisa aos requisitos que o próprio Guia consagra. Do ponto de vista da proporcionalidade, concentra a intervenção sobre o usuário no ponto de risco concreto, evitando que a totalidade dos usuários seja submetida a procedimentos de aferição em razão de uma funcionalidade específica. Do ponto de vista da minimização de dados, reduz o volume de dados pessoais coletados, já que apenas os usuários que efetivamente tentam acessar a funcionalidade de maior risco são submetidos ao procedimento. E do ponto de vista da abordagem multicamadas, representa sua expressão mais refinada, combinando diferentes níveis de proteção acionados progressivamente conforme o risco da funcionalidade acessada, em consonância com os princípios de proporcionalidade e necessidade que o próprio Guia consagra.

f) Tensão sistêmica entre proteção de dados e eficácia da aferição

O Guia estabelece, de forma coerente com o ECA Digital e com a LGPD, um conjunto de obrigações voltadas à proteção de dados pessoais no contexto da aferição de idade, entre as quais se destacam a eliminação imediata e irreversível dos dados brutos utilizados no processo, a vedação ao uso dos dados de aferição para qualquer finalidade diversa, e a exigência de controles técnicos robustos contra burla e fraude. Cada uma dessas obrigações, considerada isoladamente, é plenamente justificável. Quando consideradas em conjunto, contudo, surgem situações em que seu cumprimento simultâneo pode gerar dificuldades operacionais que merecem orientação adicional.

Um exemplo concreto diz respeito à eliminação imediata dos dados utilizados para realizar a aferição. Essa regra, prevista no art. 24, §3º, do Decreto e reforçada pelo Guia, pode criar dificuldades em situações igualmente previstas pelo próprio marco regulatório, como a revisão de contestações de usuários, e a demonstração de conformidade em eventuais processos administrativos e judiciais.

Situação semelhante ocorre em relação à vedação ao uso secundário. Em sua leitura mais literal, essa vedação poderia alcançar usos que são instrumentalmente necessários para a eficácia das próprias medidas de proteção que o ECA Digital exige, como a aplicação de restrições de conteúdo por faixa etária, a configuração de privacidade adequada ao perfil do usuário e a vinculação da conta ao responsável legal. Além disso, o aprimoramento contínuo dos modelos de aferição, indispensável para mitigar vieses e garantir acurácia, exigência que o próprio Guia impõe na seção de inclusão e não discriminação, poderia ser lido como uso secundário vedado. Seria importante que o Guia esclarecesse que a vedação ao uso secundário se dirige às finalidades incompatíveis com o sistema de proteção do ECA Digital e não a usos instrumentalmente necessários para a eficácia das próprias medidas protetivas.

Tensão de natureza similar se apresenta no campo da interoperabilidade. O Guia propõe, na Seção III, que a interoperabilidade entre sistemas evite a repetição de procedimentos de verificação e reduza a coleta e compartilhamento desnecessário de dados pessoais. Ao mesmo tempo, o art. 12, §1º, do ECA Digital veda o compartilhamento contínuo, automatizado e irrestrito de dados pessoais. A fronteira entre a interoperabilidade legítima, que o Guia incentiva, e o compartilhamento vedado, que a lei proíbe, não está juridicamente demarcada. O documento oferece soluções técnicas como arquiteturas double-blind e tokens criptográficos como exemplos de arranjos que respeitam essa

fronteira, mas não estabelece os critérios normativos que permitiriam ao fornecedor avaliar se uma arquitetura específica está dentro ou fora do que a lei permite.

Sugere-se, portanto, que o Guia reconheça essas tensões e ofereça orientação sobre hipóteses em que a retenção temporária de dados estritamente necessários seja compatível com o sistema de proteção do ECA Digital, estabelecendo parâmetros claros de finalidade, prazo e salvaguardas aplicáveis a cada situação, e indique os elementos que caracterizam o compartilhamento como contínuo, automatizado e irrestrito para fins da vedação legal, distinguindo-os dos elementos que qualificam a interoperabilidade como proporcional e finalística.

g) Os contornos da autodeclaração

O Guia afirma, na página 8, que o simples fornecimento do número de CPF pelo usuário equipara-se à autodeclaração. Essa afirmação é correta quando o CPF é utilizado como mero campo de formulário preenchido pelo usuário, sem qualquer validação posterior. Nesse caso, trata-se efetivamente de dado pessoal apresentado pela própria pessoa sem evidências adicionais para confirmar a veracidade ou a titularidade da informação, nos exatos termos do art. 2º, VI, do Decreto.

Contudo, o CPF é identificador vinculado a cadastros governamentais que contêm data de nascimento verificável. Quando utilizado como insumo para consulta a essas bases, como a base da Receita Federal, o CPF deixa de ser mera autodeclaração e passa a funcionar como ponto de partida para verificação indireta de atributo etário a partir de fonte íntegra e independente, que é exatamente o critério que o próprio Guia utiliza para definir confiabilidade na seção de acurácia, robustez e confiabilidade.

Sugere-se que o Guia esclareça que a equiparação entre CPF e autodeclaração se aplica ao fornecimento do número sem validação posterior, e não às hipóteses em que o CPF é utilizado como insumo para consulta a cadastros governamentais, caso em que pode constituir mecanismo de aferição de nível superior, a depender da robustez da integração adotada.

h) Sistemas operacionais: a necessidade de abordagem diferenciada

O Guia trata os sistemas operacionais de forma uniforme, sem distinguir entre ecossistemas com perfis de risco, contextos de uso e capacidades técnicas substancialmente distintas. Essa abordagem pode resultar em obrigações desproporcionais para sistemas operacionais cujas características intrínsecas já mitigam parcela significativa dos riscos que o ECA Digital visa endereçar, e em exigências tecnicamente inviáveis para dispositivos cujo contexto de uso é incompatível com a lógica de aferição individualizada que o Guia pressupõe. Sugere-se que o Guia reconheça essa heterogeneidade e adote abordagem diferenciada, orientada pelo princípio da proporcionalidade e pelo perfil efetivo de risco de cada categoria de sistema operacional.

Uma primeira distinção relevante é entre sistemas operacionais de uso geral e ecossistemas fechados ou funcionalmente limitados. Dispositivos como leitores digitais, por exemplo, operam sob lógica distinta da associada a sistemas operacionais de ampla finalidade: possuem

funcionalidades restritas, interfaces simplificadas, reduzida capacidade de instalação independente de aplicações e experiências centradas em conteúdo selecionado ou curado. Nesses casos, a arquitetura fechada do ecossistema já opera como salvaguarda estrutural, mitigando os principais riscos de exposição de crianças e adolescentes a conteúdos impróprios ou inadequados. Sugere-se que o Guia esclareça que o enquadramento regulatório de um sistema operacional deve considerar elementos como a finalidade principal do ambiente digital, o grau de abertura do ecossistema para instalação de aplicações de terceiros, a natureza das interações possibilitadas ao usuário e o nível efetivo de exposição aos riscos visados pelo ECA Digital, e não apenas a existência de funcionalidades digitais ou algum nível de conectividade.

Uma segunda distinção igualmente relevante diz respeito a dispositivos compartilhados, especialmente no caso de dispositivos como TVs conectadas. Diferentemente de smartphones e outros dispositivos de uso individual, uma TV conectada na sala de estar é tipicamente acessada por todos os membros da família, frequentemente sem câmera, sem tela sensível ao toque e com navegação por controle remoto. Nesses ambientes, a lógica de aferição individualizada pressuposta pelo Guia enfrenta obstáculos técnicos e de privacidade concretos: a exigência de login individual a cada uso gera fricção excessiva e é tecnicamente inviável na prática, enquanto a aferição baseada no dispositivo aplica restrições indiscriminadas a todos os usuários, incluindo adultos, limitando indevidamente o acesso a conteúdos lícitos. Sugere-se que o Guia reconheça expressamente que, em dispositivos compartilhados, abordagens alternativas como a aferição única no momento do cadastro da conta, combinada com controles parentais integrados e perfis protegidos por PIN, são igualmente válidas para fins de conformidade com o ECA Digital, em linha com o princípio da proporcionalidade e com a lógica de minimização de dados que o próprio documento consagra.

II. Análise dos exemplos

Para ilustrar a aplicação de suas diretrizes, a proposta de Guia Orientativo apresenta cenários hipotéticos ao longo do texto. A partir da leitura do Guia nota-se um preocupante descompasso entre a mitigação de risco que o ECA Digital e o Decreto desenharam para o contexto de proteção de crianças e adolescentes no ambiente digital e as condutas técnicas validadas pela Agência nesses cenários.

Abaixo analisa-se quatro dos exemplos apresentados na minuta do Guia, com a sua respectiva descrição, a análise crítica fundamentada nos dispositivos legais pertinentes e, quando aplicável, o pedido de ajuste correspondente:

a) Exemplo de João e o portal esportivo (Guia, p. 19 - Proporcionalidade)

O exemplo descreve um portal de estatísticas esportivas acessado por uma criança de 10 anos. O Guia narra que o portal não exige cadastro ou documentos, mas que, "em segundo plano", realiza uma "inferência de sinal de idade" detectando atributos como o perfil do sistema operacional, fuso horário e idioma do navegador. Na análise oficial, a ANPD elogia a conduta, afirmando que a

plataforma observou o princípio da proporcionalidade ao optar por mecanismos de "baixa fricção", respaldando-se na isenção do art.22, parágrafo único do Decreto[1].

- **Análise:** Embora a intenção do Guia de ilustrar um cenário de "baixa fricção" seja positiva, a conduta descrita no exemplo gera um conflito interpretativo com a própria isenção concedida pelo Decreto e com a Lei Geral de Proteção de Dados (LGPD). O dispositivo citado isenta de forma expressa e integral os provedores de conteúdo jornalístico e esportivo de adotarem qualquer método de aferição de idade. Se um serviço está isento, sugerir que ele realize inferências etárias "em segundo plano" cria uma impressão equivocada de que a isenção não é absoluta. Esta isenção demonstra um cenário de simetria regulatória com a Política Nacional de Classificação Indicativa do Ministério da Justiça: Em regra, competições, eventos e programas esportivos, assim como reportagens e programas jornalísticos não são objeto de classificação indicativa, em nenhuma mídia ou plataforma (incluindo a internet) por força do art. 6º, incisos I e IV, da Portaria MJSP nº 1.048/2025, sendo tratados como "conteúdos não classificáveis" (§ 1º do mesmo dispositivo). A leitura conjunta dos dispositivos confirma que conteúdos de natureza informativa, esportiva ou jornalística não carregam a presunção de risco e estão excluídos da lógica de restrição de acesso por faixa etária.

b) Exemplo do "Desafio do Balão" (Guia, p. 19-20 - Proporcionalidade)

O exemplo descreve o acesso de um jovem de 12 anos a uma plataforma de vídeos curtos. Narra-se que o sistema operacional, por já estar configurado com um perfil de criança, "envia automaticamente um sinal de idade (token etário)" para a plataforma, informando a faixa etária do usuário e permitindo a vinculação da conta à do responsável. A ANPD avalia que o fornecedor agiu corretamente ao, após a identificação do dano, alterar a classificação da funcionalidade e implementar "um bloqueio automático via sinais de idade".

- **Análise:** O cenário é feliz ao ilustrar o uso de um "token etário", que pode ser uma boa medida de aferição de idade para evitar o compartilhamento da data de nascimento exata, mas mistura institutos legais distintos. O exemplo narra uma falha de gerenciamento de risco de algoritmos de recomendação (obrigação do art. 8º, I, da Lei) e não uma falha dos mecanismos de aferição de idade em si. A inclusão desse exemplo na seção de Proporcionalidade da Aferição de Idade é equivocada pois sugere, perigosamente, que os mecanismos de aferição etária deveriam, por si só, prevenir danos de natureza algorítmica, imputando de forma equivocada a responsabilidade por falha na aferição de idade quando a causa real do dano é distinta. Há ainda um segundo problema no exemplo: o conteúdo do "desafio viral" narrado não é classificado como "proibido" (art. 15 do Decreto), é, no máximo, "impróprio ou inadequado" (art. 14 do Decreto). Para esse tipo de conteúdo a legislação estabelece instrumentos adequados: a Classificação Indicativa e a supervisão

[1] Art. 22. "Parágrafo único. Os provedores de conteúdos jornalísticos e esportivos não sujeitos à classificação indicativa e submetidos a controle editorial ficam dispensados de aferição de idade."

parental, que preservem o poder de escolha das famílias. A sugestão de "bloqueio automático via sinais de idade" desconsidera essa dinâmica e a própria natureza das plataformas de vídeos curtos. O art. 49 da Portaria MJSP nº 1.048/2025 reforça esse ponto ao determinar que o conteúdo produzido por usuário (UGC), quando hospedado em aplicações de internet, "não é objeto de classificação individual ou rotulagem dinâmica", servindo apenas como elemento de referência para atribuir uma classificação geral ao aplicativo como um todo. Portanto, exigir bloqueios automáticos por conteúdo em ambientes UGC a nível de sinal de idade subverte a lógica vigente.

c) Exemplo da plataforma audiovisual com parceiros (Guia, p. 20-21 - Proporcionalidade)

O exemplo descreve uma “plataforma de conteúdos audiovisuais” que, por possuir um catálogo inicial de classificação “Livre”, optou por não adotar a aferição de idade em seu cadastro. Posteriormente, a mesma plataforma recebe inúmeras denúncias de pais relatando que por meio de links parceiros e aplicações integradas dentro da interface foi possível acessar conteúdos proibidos para menores de 18 anos. Na análise oficial, a ANPD classifica a ausência inicial de aferição como "subestimação do risco" e elogia a implementação da verificação robusta.

- **Análise:** A descrição é compatível com a hipótese de dispensa do art. 22, caput, do Decreto. Caso a essa plataforma hipotética de conteúdos audiovisuais opere com controle editorial (o que parece ser o caso, dado que o catálogo inicial era composto apenas de vídeos com classificação livre), a ausência de aferição de idade no cadastro inicial não configura, por si só falha ou "subestimação de risco", tendo em vista que o art. 22 do Decreto isenta expressamente esse modelo de negócios de "adotar aferição de idade", desde que disponibilize perfis infantis e mecanismos de supervisão parental. Percebe-se que o exemplo busca descrever a atuação do art. 9º, §1º, da Lei nº 15.211/2025 c/c com art. 15, caput, do Decreto, relativos a disponibilização de conteúdo proíbido por meio das integrações, no entanto, equivoca-se ao penalizar o exercício de uma isenção legal e ao validar uma medida desproporcional. A exigência de verificação de idade com elevado grau de robustez é reservada pelo Decreto exclusivamente para o acesso a conteúdos proibidos (art. 15). Neste contexto, recomenda-se a exclusão do exemplo ou a alteração do serviço, com objetivo de preservar o objetivo pedagógico do Guia de alertar sobre os riscos de integrações não monitoradas, sem gerar insegurança jurídica e sem violar a isenção legal de aferição garantida ao setor de audiovisual com controle editorial pelo art. 22 do Decreto.

d) Exemplo de Maria e a “plataforma de filmes” (Guia, p. 25 - Acurácia, robustez e confiabilidade)

O exemplo descreve uma "plataforma de filmes" que utiliza inteligência artificial e biometria facial no cadastro para estimar a idade de uma usuária de 17 anos. Devido uma falha denominada como “zona cinzenta” de estimativa facial por 70 dias, período em que atinge a maioridade civil sem que

o sistema atualize seu status. O exemplo é usado para ilustrar falhas de acurácia e de governança no processo de aferição.

- **Análise:** Ao ambientar a lição sobre zonas de incerteza nesse setor específico, o Guia constrói premissa que sugere, tacitamente, que a adoção de biometria facial como um procedimento padrão para esse tipo de serviço (plataforma de filmes) - superando, na prática, o que a norma primária dispensa. O art. 24, I, do Decreto impõe que a aferição de idade observe a proporcionalidade ao nível de risco do serviço, o próprio Guia alerta que a estimativa biométrica facial "deve ser abordada com cautela devido aos significativos riscos à privacidade", exigindo o processamento de "dados biométricos sensíveis" e sendo suscetível a "vieses algorítmicos". Além de que a coexistência, em um mesmo documento, de uma tabela que reconhece a dispensa "Serviços com controle editorial" da aferição (Tabela 2, p. 15) e de exemplos práticos que tratam plataformas audiovisuais como sujeitas a procedimentos biométricos ou falhas por omissão, compromete a clareza interpretativa do Guia.

1. Considerando a proposta do Guia Orientativo, apresente suas contribuições sobre a seção "INTRODUÇÃO"

Inicialmente, destacamos como ponto de atenção os potenciais impactos decorrentes da amplitude atualmente conferida ao Guia Orientativo, especialmente no que se refere à possibilidade de sua extensão a setores regulados que não se encontram no foco principal da iniciativa. Não obstante, reforça-se a preocupação diante da ideia de que as orientações se destinam a guiar os agentes regulados até a edição de orientações definitivas, redação que pode ensejar interpretação extensiva e sem muita clareza a respeito do seu escopo de aplicação. Diante disso e pelo exposto no Guia, entende-se que o seu conteúdo possui um viés mais restritivo a alguns fornecedores portanto, sugere-se o aprimoramento do Guia, com a delimitação mais precisa do escopo subjetivo de aplicação, de modo a deixar claro que o Guia se destina prioritariamente a provedores de aplicações de internet e serviços digitais direcionados ou predominantemente acessados por crianças e adolescentes, evitando-se, assim, interpretações extensivas a setores já fortemente regulados por normativos próprios, e que não necessariamente possuem serviços direcionados para crianças e adolescentes.

No mais, é relevante observar que o Guia adota uma abordagem baseada em risco e que seu objetivo fundamental é proteger menores. No entanto, também é importante destacar que esse objetivo deve ser perseguido sem impor encargos excessivos aos usuários ou às empresas, em alinhamento com os princípios de privacidade desde a concepção, minimização de dados e experiência fluida do usuário. Isso proporcionaria maior clareza sobre a direção prática do Guia e reforçaria o princípio da proporcionalidade, considerando todas as partes envolvidas no tratamento de dados e na verificação de idade e identidade. Essa inclusão refletiria uma abordagem rigorosa, porém pragmática, do Brasil, consistente com as melhores práticas globais e apta a gerar confiança entre os stakeholders.

Na Introdução, sugerimos adicionar um parágrafo ou uma frase destacando que o Guia se baseia também no princípio de proporcionalidade e praticidade, por exemplo: "Esta Diretriz propõe soluções que combinam eficácia na proteção de menores com facilidade e viabilidade de implementação para agentes digitais, levando em conta a disponibilidade e viabilidade técnica das soluções existentes e sua implementação prática a depender do contexto e os diferentes níveis de maturidade tecnológica do mercado, seguindo uma abordagem que prioriza métodos proporcionalmente adequados ao risco." Isso definirá o tom do restante do documento, enfatizando a visão equilibrada que sustentará as orientações subsequentes[1].

[1] **Justificativa comparativa:** Na União Europeia, tanto o Regulamento Geral sobre a Proteção de Dados (GDPR) quanto a Declaração 1/2025 do EDPB ressaltam a necessidade de proteger menores no ambiente online por meio de medidas proporcionais, evitando excessos. No Reino Unido, o *Age Appropriate Design Code* (ICO) estabelece que, quando a idade dos usuários não puder ser verificada, os serviços devem aplicar, por padrão, o nível máximo de proteção de dados. No entanto, tal abordagem deve ser

Também é válido que o Guia contemple modelos B2B nos quais o fornecedor não realiza a coleta primária dos dados, mas recebe informações validadas por outros fornecedores. De forma exemplificativa, há empresas que operam majoritariamente em modelo B2B (como, por exemplo, no caso de empresas que viabilizam Benefício PAT ou Auxílio Alimentação), no qual empresas clientes realizam o cadastro dos beneficiários (empregados e dependentes), incluindo eventuais menores de idade, a partir de dados previamente validados no contexto da relação trabalhista. Nesse cenário as empresas que operacionalizam tais benefícios não possuem interação inicial com o usuário para coleta de dados; os dados são provenientes de fonte confiável (ex. empregador); e eventual aferição de idade já ocorre a montante da cadeia, não sendo necessário duplicar controles ou mecanismos de verificação de idade, quando aplicáveis.

Sugestão de correção: Alterar de "18 de outubro de 2026" para "18 de março de 2026" (p. 4).

2. Considerando a proposta do Guia Orientativo, apresente suas contribuições sobre a seção "ASPECTOS GERAIS"

No tocante aos Aspectos Gerais, entendemos necessário reforçar que a aferição de idade deve observar, quando aplicável, os princípios previstos na Lei Geral de Proteção de Dados Pessoais, em especial os princípios da necessidade e adequação, verificando no caso concreto, a informação mais apropriada para a identificação da idade do menor.

Ademais, é importante consolidar o entendimento de que nem toda interação digital exige verificação ativa de idade, devendo tal exigência estar diretamente vinculada ao risco concreto ao público infantojuvenil. Além disso, sugere-se explicitar que, em determinados contextos, como nos serviços financeiros, a identificação do cliente já é realizada em razão de exigências regulatórias, podendo a aferição de idade ser derivada desses processos, evitando duplicidade de controles.

Neste contexto, outro aspecto relevante a se considerar é que a aferição de idade não se confunde com a verificação de identidade exigida pela regulação setorial, ainda que sejam utilizados métodos que envolvam a análise documental ou outro mecanismo de verificação de identidade do usuário. Isso porque ambas as práticas possuem finalidades distintas. Porém, entendemos possível e recomendável o aproveitamento das informações e/ou de processos oriundos de verificação de identidade para os fins de aferição de idade, sendo recomendável que o Guia Orientativo explicite essa possibilidade.

interpretada à luz do princípio da proporcionalidade e considerando a natureza e o risco específico do serviço, de modo a evitar restrições desnecessárias ou impactos excessivos, Nos EUA, a FTC (COPPA) e novas leis estaduais (por exemplo, na Califórnia) também enfatizam a proteção de menores sem impedir a inovação, inclusive explorando novas tecnologias de verificação etária.

Deste modo, sugere-se incorporar ao Guia exemplos que evidenciem a distinção entre aferição e verificação de idade e de identidade, e a possibilidade de reaproveitamento das informações e processos de um fluxo para o outro.

No mais, em conexão com o mencionado, sugere-se esclarecer mais os conceitos trazidos pelo Guia, como a definição de "aferição de idade" já introduzida no Decreto 12.880/2026, art. 2º, IV (procedimentos para verificação, estimativa ou inferência da idade do usuário), diferenciando explicitamente entre verificação de idade (verificação formal com alto grau de certeza, por exemplo, por meio de documento oficial) e estimativa de idade (inferência de faixa etária sem identificação completa). Essa distinção conceitual ajuda as empresas a compreender que existem diferentes métodos, com distintos níveis de confiabilidade, todos englobados pela noção de "aferição de idade". Isso simplificaria a compreensão e anteciparia a lógica de aplicação gradual dos métodos, conforme necessário[2].

Outro tema importante que deve ser explorado neste tópico é explicar para o público em geral o que são “tokens etários”, tendo em vista a disponibilidade do guia orientativo em página aberta.

Sugestão de ajuste: “Decreto nº 12.880, de 18 de ~~outubro~~ de 2026” (incluir março de 2026 ao invés de outubro).

3. Considerando a proposta do Guia Orientativo, apresente suas contribuições sobre a seção "CADEIA DIGITAL DE RESPONSABILIDADES"

Com relação ao item, entendemos ser prudente esclarecer que a responsabilização dos agentes deve observar a posição efetivamente ocupada na cadeia de tratamento de dados pessoais, especialmente à luz das definições de controlador e operador constantes da LGPD, quando o tratamento envolver dados pessoais, bem como o grau de ingerência de cada agente sobre a interface e o serviço disponibilizado ao usuário.

[2] **Justificativa comparativa:** Estruturas já existentes ressaltam a importância de definir claramente o que se entende por verificação de idade:
• Na Europa, o EDPB define *"garantia de idade"* como um termo guarda-chuva que engloba qualquer método de estimativa ou verificação da idade, com diferentes graus de robustez. A Declaração Internacional Conjunta de 2024 (liderada pela ICO) reforça essa definição ampla, esclarecendo que a *garantia de idade* inclui métodos mais rígidos e mais flexíveis. Isso equivale à noção brasileira de "aferição de idade".
• Esses referenciais também especificam sub conceitos: fala-se em "verificação de idade" quando há checagem documental ou identidade robusta, e em "estimativa de idade" quando a idade é inferida sem, necessariamente, identificar integralmente o usuário. Essa dicotomia aparece nas diretrizes da Comissão Europeia (no contexto da Lei de Serviços Digitais) e é prática comum em fóruns do setor.
• Ao refletir essa distinção na seção de Aspectos Gerais, o Guia se alinhará à terminologia internacional, facilitando a interoperabilidade conceitual. Nos EUA, a FTC utiliza linguagem semelhante: em 2026, indicou que aceitaria "tecnologias de estimativa de idade" como alternativa em contextos apropriados, reconhecendo sua diferença em relação à verificação tradicional (atualizações do COPPA Safe Harbor).

Nesse sentido, deve-se evitar a imposição de responsabilização solidária indiscriminada, privilegiando-se critérios como a proporcionalidade (princípio já contemplado no próprio Guia), a governança sobre o risco e a capacidade concreta de prevenção e mitigação de danos, em alinhamento com o regime de responsabilização previsto nos arts. 42 e seguintes da LGPD.

No mais, sob a ótica do setor financeiro, a incidência do ECA Digital deve estar condicionada a hipóteses em que o produto ou serviço seja efetivamente direcionado ao público infantojuvenil e acessado diretamente pelo menor, circunstância em que poderiam se justificar eventuais salvaguardas específicas, caso necessário. Por essa razão, entende-se que se o Guia avançar quanto a este ponto, deve ser mais assertivo ao explicitar tal critério, sobretudo ao tratar de setores submetidos a regimes jurídicos próprios e fortemente regulados.

Nesse contexto, é relevante destacar que, caso o Guia inclua de forma ampla e não delimitada qualquer provedor de serviço digital, há risco de atribuição de obrigações e responsabilidades incompatíveis com sua atuação, especialmente em cenários nos quais operam exclusivamente como intermediárias de pagamento ou provedoras de infraestrutura financeira. Nesse sentido, é importante que o Guia delimite de forma mais precisa o seu escopo e reconheça que há diversas hipóteses de não incidência ou de incidência mitigada do ECA Digital, como, por exemplo no caso de ausência de conteúdo impróprio ou proibido, inexistência de interação social relevante entre usuários, serviços contratados exclusivamente por maiores de idade; situações em que não haja segmentação ou direcionamento específico ao público infantojuvenil; e casos em que inexista interação direta, autônoma e juridicamente relevante do menor.

No referido eixo, eventuais produtos voltados exclusivamente a crianças e adolescentes possuem, em geral, finalidade de educação financeira, estando estruturados sob controle parental, com mecanismos de gestão supervisionada e limites previamente definidos. Nesses casos, a contratação da conta é realizada pelo responsável legal, não havendo autonomia plena do menor sobre o instrumento. Ainda que existam funcionalidades direcionados ao público jovem, estas se inserem em ambiente regulado e contam com a atuação do responsável, o que afasta a caracterização de uso independente ou não supervisionado.

Diante disso, entendemos ser necessária a explicitação de que a responsabilização deve ser contextual, individualizada e baseada na atuação efetiva de cada agente, evitando-se interpretações que conduzam à responsabilização objetiva ampliada ou à solidariedade automática, especialmente em detrimento de setores já submetidos a regimes específicos de supervisão. Ademais, recomenda-se reconhecer que produtos destinados a crianças e adolescentes, mas estruturados sob responsabilidade e controle de adultos, estejam sujeitos a um regime interpretativo diferenciado.

Ainda sobre este tópico, estabelece-se a obrigação de que lojas de aplicativos e sistemas operacionais disponibilizem aos demais fornecedores “sinais de idade”, para viabilizar o cumprimento das finalidades previstas no ECA Digital. Contudo, não há

clareza quanto à **forma** e ao **momento** desse compartilhamento — se ocorreria antes do download do aplicativo ou apenas posteriormente.

Sugere-se maior detalhamento sobre os critérios, a forma e o momento de disponibilização do sinal de idade aos fornecedores. Nesta mesma linha, é válido destacar, de forma mais clara, as obrigações e a cooperação entre os diferentes elos da cadeia. Por exemplo, o Guia poderia detalhar como fornecedores de aplicações ou sistemas (lojas de aplicativos, navegadores) devem fornecer sinais etários confiáveis aos serviços, conforme sugerido na diretriz preliminar, e como os provedores de serviços online podem aproveitar esses sinais na medida em que sejam acessíveis, interoperáveis e tecnicamente integráveis a seus sistemas, em vez de duplicar controles de idade. Isso sem prejuízo do fato de que a implementação concreta dependerá da disponibilidade efetiva dessas soluções no mercado e de acordos com terceiros. Tal abordagem reduz a carga operacional de cada agente e proporciona uma experiência de usuário mais fluida, sem comprometer a proteção. Para os sinais de idade não verifica-se a necessidade de participação do pais e/ou responsáveis, porém, também é importante mencionar o papel dos pais ou responsáveis na cadeia, especialmente em relação a crianças e adolescentes mais jovens, e como as soluções devem permitir sua participação quando apropriado.

Proposta concreta: Incluir maior especificidade sobre a interação das responsabilidades. Por exemplo: "Colaboração entre agentes: “sempre que possível, mecanismos de aferição devem considerar a interoperabilidade e o aproveitamento de sinais etários provenientes de outros agentes da cadeia digital, sem prejuízo da responsabilidade do provedor pela adequação das medidas adotadas ao seu contexto específico.”

Por exemplo, sistemas operacionais, navegadores ou lojas de aplicativos podem, quando tais funcionalidades se tornarem disponíveis, fornecer aos serviços online indicadores etários confiáveis (como um sinal de 'usuário verificado como maior de 18 anos'), reduzindo a duplicação de procedimentos. Caso dependam de especialistas terceirizados em verificação, os provedores devem assegurar contratualmente a proteção dos dados e a qualidade do processo. Além disso, pode-se mencionar que cada elo possui uma responsabilidade definida e essa precisão ajudará cada ator a compreender seu papel específico na aplicação dos mecanismos, favorecendo a implementação bem-sucedida da regulamentação[3].

[3] **Justificativa comparativa:** A corresponsabilidade na proteção de crianças e adolescentes é um princípio reconhecido globalmente. A UE, por meio dos marcos do DSA e da identidade digital europeia, promove a ideia de identidades digitais verificáveis que facilitem um sinal etário reutilizável entre serviços. Isso reflete a necessidade de interoperabilidade, quando viável, permitindo que a verificação seja realizada uma vez e reconhecida por outras plataformas. No Reino Unido, embora não haja mandato expresso para lojas de aplicativos, as empresas são incentivadas a colaborar com terceiros (por exemplo, serviços externos de verificação) para cumprir o Código das Crianças sem reinventar soluções proprietárias. Já nos EUA, embora a regulamentação se concentre em fornecedores diretos, discute-se a conveniência de grandes sistemas (por exemplo, sistemas operacionais e provedores) assumirem um papel na facilitação de filtros etários. Alinhar a seção "Cadeia Digital de Responsabilidades" com essas ideias enfatizará que uma abordagem articulada pode ser, ao mesmo tempo, mais eficaz e mais eficiente.

4. Considerando a proposta do Guia Orientativo, apresente suas contribuições sobre a seção "REQUISITOS GERAIS"

No que se refere aos Requisitos Gerais, é recomendável reconhecer expressamente soluções já consolidadas em setores altamente regulados, como o financeiro, a exemplo de mecanismos robustos de autenticação multifator (a exemplo de utilização de senha com algum tipo de biometria, etc.), processos de validação cadastral (KYC) e rotinas de prevenção à fraude, os quais já se encontram alinhados a exigências regulatórias específicas (BACEN/CMN) e a padrões elevados de segurança da informação, privilegiando o reconhecimento da **equivalência funcional de mecanismos existentes**, desde que aptos a mitigar os riscos pretendidos.

Para serviços de natureza instrumental, como, por exemplo, aplicativos de gestão de benefícios trabalhistas, a aplicação do princípio da proporcionalidade deve considerar: (i) ausência de conteúdo impróprio ou proibido; (ii) inexistência de interação social relevante entre usuários; (iii) utilização de dados previamente validados por terceiros confiáveis.

No tópico de **"Proporcionalidade"**, o quadro-resumo de riscos apresenta: (i) as "características do serviço ou produto", (ii) a respectiva "aferição exigida" e (iii) "exemplos de mecanismos", organizados em três níveis de risco: baixo, médio e alto.

- Para **baixo risco**, considera-se que serviços digitais que **não oferecem conteúdo, produto ou serviço impróprio, inadequado ou proibido** para menores de 18 (dezoito) anos, **mas que ainda podem gerar impactos adversos**, ainda que indiretos, devem adotar **aferição com mínimo grau de impacto**, como o uso do sinal de idade fornecido por lojas de aplicativos e sistemas operacionais ou a adoção de credenciais verificáveis.
- Para **médio risco**, aplicável a serviços que permitam o compartilhamento ou a exposição a conteúdo, produto ou serviço impróprio ou inadequado para menores de 18 (dezoito) anos, exige-se **aferição proporcional**, como, por exemplo, por meio de mecanismos de estimação etária.
- Para **alto risco**, referente a serviços que oferecem conteúdo, produto ou serviço proibido, exige-se **aferição com alto grau de robustez**, como verificação etária baseada em documentos, inclusive com prova de vivacidade.

Por outro lado, no tópico **"Cadeia Digital de Responsabilidades"**, estabelece-se que: (i) a aferição de idade, independentemente da forma, é obrigatória para lojas de aplicativos e sistemas operacionais; (ii) é facultativa para fornecedores de conteúdo, produto ou serviço impróprio ou inadequado; e (iii) é obrigatória — mediante mecanismos eficazes de verificação de idade — para fornecedores de conteúdo, produto ou serviço proibido.

Verifica-se, portanto, um **desalinhamento entre os dois quadros-resumo**, na medida em que o critério de obrigatoriedade da aferição não coincide com a lógica de proporcionalidade por nível de risco. Recomenda-se, assim, a **uniformização dos**

entendimentos, a fim de evitar interpretações divergentes e inconsistências nas medidas de adequação.

No mais, a matriz de risco apresentada (p. 18) indica que serviços que façam uso de dados pessoais sensíveis estariam automaticamente no risco moderado. No entanto, é possível que o dado sensível seja cadastral, como a biometria facial, especificamente nos casos de setores regulados. Recomenda-se revisar as características e o contexto, para que o risco leve em consideração o uso do dado pessoal sensível e, sendo cadastral ou para autenticação transacional, considere o risco baixo. Além disso, como indicamos acima, o mesmo dado pessoal e/ou processo pode ser utilizado tanto para a verificação de identidade, como para a aferição de idade.

Os Requisitos Gerais do Guia consolidam as garantias mínimas que qualquer mecanismo de restrição etária deve cumprir. Reconhecemos que princípios robustos como proporcionalidade/risco, confiabilidade técnica, minimização e privacidade de dados, não discriminação, transparência e interoperabilidade já estejam contempladas. Nossas contribuições visam fortalecer e esclarecer esses requisitos para facilitar sua implementação prática:

• Proporcionalidade e abordagem baseada em risco é um fundamento importante. Cada solução deve ser tão rigorosa quanto o risco justificar. Também é relevante notar que a escolha do método mais adequado deve ser guiada não apenas pela precisão do mecanismo de aferição de idade e por sua compatibilidade com os direitos dos usuários e com os requisitos de proteção de dados pessoais, mas também pela necessidade de não impor encargos excessivos aos usuários ou às empresas, alinhando-se aos princípios de privacidade desde a concepção, minimização de dados e experiência fluida do usuário (veja o ponto 1 deste comentário), bem como o aproveitamento de processos já implementados e complementares, como no caso da verificação de identidade.

• Confiabilidade técnica e diferenciação dos métodos: para atender ao requisito de eficácia sem excessos, o Guia deve esclarecer que "confiável" nem sempre significa o método mais invasivo, mas sim um nível de certeza adequado ao contexto. Destacamos a importância da distinção entre verificação e estimativa (conforme discutido em Aspectos Gerais). Nossas submissões recomendam que métodos automatizados menos intrusivos (estimativa) sejam considerados suficientes quando puderem demonstrar precisão razoável em relação ao risco gerenciado. Isso facilitará a conformidade para os fornecedores, permitindo-lhes adotar soluções escaláveis de acordo com seu setor. (A UE e o Reino Unido promovem essa adaptabilidade: por exemplo, a Comissão Europeia sugere de forma mais enfática a verificação formal para produtos de alto risco, admitindo a estimativa de idade em serviços gerais.). De qualquer forma, deve ser preservado o aproveitamento de processos robustos já existentes.

• Minimização de dados e privacidade (privacidade por design e por padrão): sugerimos incentivar o uso de PETs (por exemplo, credenciais verificáveis e tokens etários anônimos), na medida em que tais soluções estejam disponíveis, maduras e

operacionalmente implementáveis no mercado, permitindo a confirmação da idade sem expor informações pessoais adicionais. Isso reduz riscos legais e de cibersegurança e também diminui custos de proteção de dados, já que haverá menos informações a proteger.

5. Considerando a proposta do Guia Orientativo, apresente suas contribuições sobre a seção "REQUISITOS ESPECÍFICOS"

Em alguns contextos, como no caso das instituições financeiras, os processos de *onboarding* já incorporam controles robustos, inclusive no contexto em que, em regra, não há autonomia plena do menor na utilização do serviço e há supervisão parental efetiva e a estrutura jurídica da contratação da conta se dá com adultos, especialmente no que se refere à responsabilização pelo uso.

Neste mesmo sentido, no tópico de "**Verificação Documental**", o capítulo reforça o princípio da necessidade (art.6º, III, LGPD) ao mencionar o art. 24, §3º, do Decreto, que 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.** Entretanto, é importante destacar, que para alguns setores, como o financeiro, a verificação documental não é somente uma opção operacional e está atrelada a obrigações legais e regulatórias, relacionadas a prevenção a fraude, identificação e autenticação do titular, observância de normas de PLD e regularidade cadastral, por exemplo.

Neste contexto, a conferência de documentos pessoais pode simultaneamente viabilizar a validação de identidade e a validação de idade do titular, inclusive em observância ao melhor interesse do menor. Assim, o armazenamento da realização da verificação da identidade e aferição da idade é necessário para comprovação da regularidade da documentoscopia do menor, rastreabilidade do processo, exercício regular de direitos e atendimento a auditorias, com fundamento nos princípios da LGPD, em especial, finalidade, adequação, necessidade e responsabilização, todos presentes no art. 6º, da referida norma. Desta forma, sugere-se que seja incluída exceção à vedação ao armazenamento, ou esclarecimento expresso de sua inaplicabilidade, de modo a evitar interpretações equivocadas e não prejudicar a guarda regular de evidências atreladas a obrigações regulatórias ou se mostrar necessária para a comprovação da regularidade e segurança do processo de identificação do titular em setores regulados. Nesse sentido, é importante ressaltar que não se trata de uso secundário de dados relacionados à aferição de idade, mas de uso de dados para finalidades distintas, como no caso, por exemplo, de identificação do usuário, cumprimento de obrigações legais e/ou regulatórias e cumprimento de contrato, e que para essas outras situações não são aplicáveis as restrições de uso e/ou de guarda de documentos e/ou evidências.

Na seção de Requisitos Específicos, consideramos importante que o Guia inclua orientações gerais sobre cenários ou casos de uso específicos. Vale a pena incluir

exemplos setoriais ou situações típicas para ilustrar como aplicar os princípios na prática. Por exemplo, para serviços financeiros, de pagamentos e programas de fidelidade (voltados principalmente para adultos), como já indicamos anteriormente, pode-se esclarecer que processos já implementados, como procedimentos de KYC e *onboarding*, podem ser considerados como parte da estratégia de aferição de idade, não implicando dispensa automática da avaliação de medidas complementares quando necessário. Assim, o Guia poderia dispensar a repetição desses controles quando a verificação existente puder ser reutilizada, desde que atenda aos padrões de confiabilidade. Em outro caso, em plataformas de conteúdo geral, o uso de estimativa de idade por IA pode ser adequado, enquanto em serviços de conteúdo adulto ou proibido, poderia ser aplicável outra medida mais robusta. Esse tipo de orientação específica facilita a compreensão do padrão e evita interpretações divergentes.

Proposta concreta: Enriquecer a seção de Requisitos Específicos com subseções ou tópicos por cenário (ou tipo de conteúdo/serviço).

• Serviços financeiros, de pagamentos e de fidelidade: reconhecer processos já implementados, como procedimentos de KYC e onboarding, podem ser considerados como parte da estratégia de aferição de idade.

Esses exemplos (ou outros que o regulador considere apropriados) ilustrarão como implementar os requisitos na prática, com o Guia atuando tanto como orientação técnica quanto como manual de boas práticas para diversos modelos de negócio. Com isso, as empresas terão mais clareza e confiança na adaptação dos mecanismos ao seu setor, minimizando o risco de excesso de conformidade ou de implementação ineficiente[4].

6. Considerando a proposta do Guia Orientativo, apresente suas contribuições sobre o "ANEXO I"

Em relação ao Anexo I, sugere-se a inclusão de casos práticos setoriais (ex:. do setor financeiro), bem como a definição de critérios objetivos para classificação de risco. Adicionalmente, é importante que o Anexo seja redigido de forma a evitar que seja

[4] **Justificativa comparativa:** Padrões maduros geralmente fornecem diretrizes ou códigos setoriais:
• Na UE, os Códigos de Conduta são promovidos por setores (por exemplo, indústria de jogos de azar online, redes sociais etc.) para detalhar como implementar a proteção de menores sob o GDPR. Embora no Brasil se trate de um Guia Geral, a inclusão de exemplos com lógica setorial pode cumprir essa função pedagógica.
• No Reino Unido, a ICO complementou o Código de Design Apropriado à Idade com FAQs setoriais e orientações práticas (por exemplo, sobre como um serviço de streaming pode aplicar controles parentais ou como um fórum pode limitar contatos).
• Nos EUA, a COPPA possui orientações específicas por setor (educação, aplicativos móveis etc.), e os estados com novas leis adotam prazos e abordagens diferentes conforme o setor (por exemplo, redes sociais versus varejistas online). Refletir essas distinções ajudará as empresas brasileiras a compreender o que se espera em seu contexto e a direcionar recursos para o que realmente importa.

interpretado como um checklist obrigatório, preservando o caráter orientativo do documento.

Sugestão de inclusão de nova categoria: “Serviços B2B corporativos, como no caso de dados fornecidos por empregadores”, com utilização de dados cadastrais fornecidos pelos empregadores como mecanismo válido de aferição de idade. Recomenda-se inclusão, no Guia, de referência a fornecedores que operacionalizam serviços com base em dados fornecidos por clientes corporativos, nos quais a responsabilidade pela coleta e validação inicial dos dados se dá fora do ambiente da aplicação. A exigência de nova aferição de idade não deve se aplicar quando o dado já estiver validado por fonte confiável, sob pena de gerar redundância e tratamento excessivo de dados pessoais.

No item **“Transparência e auditabilidade”,** consta a recomendação “evitem o armazenamento de dados pessoais biométricos, imagens ou dados extraídos de documentos de identidade para fins de auditabilidade”, no entanto, tal recomendação deve comportar esclarecimento expresso de que não é aplicável para outras hipóteses de tratamento de dados, inclusive biométricos, distintas da aferição de idade prevista no ECA Digital, como por exemplo, para identificação do usuário, cumprimento de obrigação legal ou regulatórias, execução de contrato e prevenção à fraudes, dado que qualquer recomendação no sentido de não armazenamento dessas evidências criaria um conflito normativo entre a orientação da ANPD e as obrigações impostas por outros reguladores, colocando os agentes de tratamento em situação de impossibilidade de cumprimento simultâneo.

O Anexo I do Guia, se corretamente compreendido, pode conter informações suplementares, como lista de métodos técnicos, definições detalhadas ou resultados de consultas anteriores. Para maximizar sua utilidade, sugerimos que o Anexo I inclua informações práticas e atualizadas sobre as tecnologias disponíveis e os padrões globais emergentes.

• Além disso, o Anexo poderia referenciar padrões internacionais ou esforços globais de interoperabilidade. Manter e reforçar um anexo com tais detalhes é valioso, pois complementa o Guia com uma perspectiva técnica e comparativa sem sobrecarregar o corpo principal do regulamento.

• Adicionar aviso: "A inclusão de tecnologias, metodologias ou exemplos neste Anexo é meramente ilustrativa e não implica sua disponibilidade, obrigatoriedade ou adoção generalizada no mercado brasileiro no momento da implementação."

Proposta concreta: Sugerimos que o Anexo I:

• Apresente uma tabela comparativa de métodos de aferição, com colunas como tipo de método, nível de intrusão, confiabilidade (por faixa etária), exemplos de uso, considerações legais (dados pessoais envolvidos) e custo de implementação. Isso ajudaria as empresas a tomar decisões informadas e a planejar seus desenvolvimentos.

• Inclua um glossário ou referências regulatórias relevantes (por exemplo, citações literais de definições constantes do Decreto 12.880, para evitar mal-entendidos terminológicos).

• Sugestão de Relatório de Impacto Regulatório ou outro material, estruturado de forma bastante prática (listas, diagramas, fluxos etc.), para servir como manual complementar a implementadores técnicos e jurídicos.

Em conclusão, o Anexo I poderia atuar como um repositório de informações concretas e acionáveis, integrando o melhor do debate internacional e das preocupações locais coletadas nesse processo participativo. Assim, ampliaria a utilidade do Guia para além da teoria, aproximando-o da realidade operacional das empresas[5].

7. Apresente suas contribuições adicionais

Por fim, como Contribuições Adicionais, recomenda-se explicitar que o Guia possui natureza orientativa e não vinculante, de modo a evidenciar que seu conteúdo não deve ser interpretado como engessamento, sobretudo em um contexto em que o próprio escopo do ECA Digital ainda se encontra em evolução e em construção normativa. Tal ressalva contribui para maior segurança jurídica, sobretudo dos agentes regulados e para a adequada margem de adaptação pelas diferentes realidades setoriais.

Por fim, sugere-se a inclusão de medidas complementares, como iniciativas de educação digital e o estímulo à corresponsabilidade de responsáveis legais, como estratégias adicionais para a proteção de crianças e adolescentes no ambiente digital.

Em todas as menções/citações ao “Decreto” especificar qual decreto faz referência, dada a possibilidade de coexistência de normas sobre o mesmo assunto, com alcances diferentes (ex. no início da p. 40, que menciona o “art. 15 do Decreto”, idem na fundamentação do anexo I).

De forma transversal, propomos uma recomendação adicional de que a versão final do Guia mantenha espaço de atualização, inclusive para a evolução tecnológica e para a cooperação internacional, quando aplicável.

[5] **Justificativa comparativa:** Reguladores de referência frequentemente fornecem material técnico adicional para apoiar a implementação. A Comissão Europeia produziu, em conjunto com seu Guia sobre DSA, um compêndio técnico sobre soluções de verificação de idade e seus níveis de maturidade. A ICO britânica, em sua página sobre o *Children’s Code*, oferece links para recursos destinados a desenvolvedores, incluindo avaliações de ferramentas de estimativa de idade. Se o Anexo I desempenhar esse papel, o Brasil estará alinhado a essa boa prática. Além disso, se reunir comentários da consulta pública (o que faz parte de seu propósito), seu conteúdo final refletirá um rico consenso multissetorial, conferindo-lhe maior legitimidade e utilidade prática.

Essa adição final reforça o compromisso com a melhoria contínua e a coerência internacional, deixando claro para as empresas que o regulador compreenderá seus desafios em um ambiente tecnológico dinâmico e as acompanhará com diretrizes atualizadas e factíveis à medida que o cenário evoluir.