CONTRIBUIÇÕES DA DATA PRIVACY BRASIL PARA A TOMADA DE SUBSÍDIOS SOBRE O GUIA ORIENTATIVO “MECANISMOS DE AFERIÇÃO DE IDADE”

2026

DataPrivacyBR

DataPrivacyBR Research

Sobre a Data

A Data Privacy Brasil é uma organização de ensino, pesquisa e incidência que produz conhecimento e forma pessoas para um ecossistema informacional justo. Fundada em 2018 como escola de formação, a Data deu origem a uma associação de pesquisa em 2020. Em 2026, as entidades foram integradas, operando com a mesma missão e visão. A Data já formou mais de 6 mil profissionais e realizou formações com Agência Nacional de Proteção de Dados Pessoais, governos e sistema de justiça. Além disso, organiza a conferência Data Privacy Global Conference e a Escola de Governança de Dados. Por meio da educação, da sensibilização e da mobilização da sociedade, almejamos uma sociedade democrática na qual as tecnologias estejam a serviço da autonomia, da dignidade das pessoas e da redução das assimetrias de poder.

Ficha técnica

A Data Privacy Brasil é uma organização de ensino, pesquisa e incidência que produz conhecimento e forma pessoas para um ecossistema informacional justo. Por meio da educação, da construção de saberes e da mobilização da sociedade, buscamos uma sociedade democrática na qual as tecnologias estejam a serviço da autonomia, da dignidade das pessoas e da redução das assimetrias de poder.

Direção

Bruno Bioni, Mariana Rielli e Rafael Zanatta

Coordenação

Carla Rodrigues, Jaqueline Pigatto, Pedro Martins, Pedro Saliba e Victor Barcellos

Equipe

Ana Luiza Serafini, Bárbara Yamasaki, Bianca Marques, Eduardo Mendonça, Gabriela Vergili, Gabriel Franco, Giovanna Amaral, Giovana Andrade, João Paulo Vicente, Larissa Pacheco, Louise Karczeski, Luize Ribeiro, Matheus Arcanjo, Natasha Nóvoa, Paula Uematsu, Pedro Henrique Santos, Rafael Guimarães, Rodolfo Rodrigues e Vanessa Nobre.

Imprensa

Para esclarecimentos sobre o documento e entrevistas, entrar em contato pelo e-mail imprensa@dataprivacy.br.org

Como citar esse documento

NÓVOA, Natasha; Mendonça, Eduardo; RODRIGUES, Carla; ZANATTA, Rafael. **Contribuições da Data Privacy Brasil para a tomada de subsídios sobre o guia orientativo "Mecanismos de Aferição de Idade"**. São Paulo: Data Privacy Brasil, 2026.

Sumário

Síntese executiva das recomendações

- A primeira recomendação é reforçar que a aferição de idade deve ser proporcional ao risco. O Guia deve orientar os fornecedores a avaliar o contexto concreto do serviço, da funcionalidade ou do conteúdo, adotando métodos mais robustos apenas quando houver risco relevante ou hipótese legal de restrição de acesso. Em ambientes de menor risco, soluções menos intrusivas, combinadas com configurações protetivas, classificação indicativa, supervisão parental e segurança por padrão, podem ser suficientes. A proporcionalidade deve funcionar em dupla direção: autoriza maior rigor quando necessário, mas também limita a coleta excessiva, a retenção indevida e a identificação desnecessária.

- A segunda recomendação é diferenciar, de forma expressa e transversal, aferição de idade, verificação de idade, sinal de idade, autodeclaração e verificação de identidade. Essa distinção é central para evitar que a proteção etária seja convertida em identificação civil obrigatória. A pergunta regulatória não deve ser "quem é exatamente esse usuário?", mas "qual informação mínima permite saber se aquela experiência, conteúdo, funcionalidade ou produto é adequado à sua idade?". Por isso, CPF, documento oficial, reconhecimento facial, identificadores persistentes e outros dados de identidade não devem ser tratados como padrão, mas como métodos excepcionais, sujeitos a justificativa reforçada, avaliação de impacto, retenção mínima, contestação e oferecimento de alternativas menos intrusivas.

- A terceira recomendação é afirmar a finalidade exclusiva de proteção. Dados, sinais, inferências ou resultados gerados para a aferição de idade não podem ser reutilizados para publicidade comportamental, recomendação personalizada, perfilamento comercial, treinamento de modelos de IA, enriquecimento cadastral, monetização, prevenção genérica à fraude ou compartilhamento com terceiros para finalidades incompatíveis. A aferição de idade deve reduzir riscos, e não ampliar a assimetria informacional entre fornecedores e usuários. Esse ponto é especialmente importante porque dados de crianças e adolescentes, quando associados à identidade, ao comportamento, à navegação ou às preferências, podem gerar riscos agravados de exploração comercial, vigilância e discriminação.

- A quarta recomendação é priorizar arquiteturas de preservação da privacidade. Sempre que tecnicamente possível, o Guia deve incentivar soluções baseadas em sinais de idade, credenciais verificáveis, APIs seguras, tokens, provas de conhecimento zero e outros mecanismos capazes de comprovar o atributo etário sem revelar a identidade civil, a idade exata, documentos, imagens faciais ou o histórico de navegação. A lógica do atributo mínimo deve orientar a implementação: o fornecedor deve receber apenas a informação necessária para adaptar ou restringir a experiência, sem acesso a dados pessoais adicionais.

- A quinta recomendação é tratar a biometria, a inferência comportamental e as soluções baseadas em IA com cautela reforçada. Esses métodos podem envolver dados

sensíveis, opacidade, margens de erro, vieses discriminatórios e exclusões indevidas. O Guia deve exigir documentação técnica, testes por subgrupos, avaliação periódica da acurácia, auditoria independente, canais de contestação e alternativas acessíveis. A confiabilidade de um mecanismo não deve ser confundida com infalibilidade nem com simples precisão estatística: ela depende também de governança, proporcionalidade, segurança, transparência, possibilidade de revisão e compatibilidade com direitos fundamentais.

- A sexta recomendação é estruturar a cadeia digital de responsabilidades a partir de uma lógica funcional. Responsabilidade compartilhada não significa responsabilidade equivalente. Cada agente deve responder de acordo com sua função técnica, seu grau de controle sobre a experiência digital, sua capacidade de mitigação de riscos e sua posição na cadeia de valor. Lojas de aplicativos e sistemas operacionais podem fornecer sinais de idade ou interfaces seguras, mas o provedor da aplicação permanece responsável por avaliar os riscos concretos de suas funcionalidades e adaptar a experiência. A família possui papel relevante de mediação, mas não pode ser tratada como substituta dos deveres empresariais de design seguro, transparência, minimização e governança.
- A sétima recomendação é considerar a realidade brasileira de desigualdade digital e de uso de dispositivos compartilhados. Soluções que dependam de smartphone recente, câmera de alta qualidade, conexão estável, documento formal, cartão de crédito ou biometria podem excluir crianças e adolescentes em situação de maior vulnerabilidade. O Guia deve prever alternativas equivalentes, acessíveis e contestáveis, inclusive para usuários sem documentação regular, pessoas com deficiência, famílias de baixa renda, usuários de dispositivos antigos e contextos de compartilhamento doméstico. Em serviços de maior risco, a aferição realizada apenas no cadastro, na instalação ou na configuração inicial pode ser insuficiente, exigindo revalidações contextuais proporcionais, sem monitoramento contínuo.
- A oitava recomendação é afirmar que a aferição de idade não substitui outras obrigações de proteção. Aferir a idade sem alterar o design, a recomendação, a publicidade, a interação, a moderação, os padrões de privacidade e as configurações padrão pode produzir apenas conformidade formal. O mecanismo deve funcionar como gatilho para experiências mais seguras: limitação da publicidade comportamental, restrição do contato com desconhecidos, redução de funcionalidades de maior risco, classificação indicativa efetiva, supervisão parental, transparência adequada e canais de contestação.
- A nona recomendação é fortalecer a governança regulatória. A escolha do método deve ser documentada por meio de avaliação de risco, finalidade, dados tratados, base legal, retenção, medidas de segurança, testes, margens de erro, riscos de viés, alternativas menos intrusivas e medidas contra usos secundários. Relatórios de impacto não devem ser tratados como formalidade, mas como instrumentos de identificação, mitigação e monitoramento contínuo dos riscos associados ao serviço digital e ao próprio mecanismo de aferição. A ANPD também deve incentivar auditorias independentes, relatórios de transparência e a revisão periódica dos métodos adotados.

Introdução

Em junho de 2026, a Autoridade Nacional de Proteção de Dados abriu Tomada de Subsídios sobre o Guia Orientativo "Mecanismos de Aferição de Idade", com o objetivo de colher contribuições para o aprimoramento das orientações aplicáveis à implementação de mecanismos confiáveis, proporcionais e compatíveis com a proteção de dados pessoais no contexto do ECA Digital.

A Data Privacy Brasil apresenta, por meio deste documento, suas contribuições à ANPD, partindo da premissa de que a aferição de idade deve ser compreendida como instrumento de proteção integral de crianças e adolescentes no ambiente digital, e não como finalidade autônoma, etapa cadastral obrigatória ou mecanismo generalizado de identificação civil. A idade, nesse contexto, deve funcionar como atributo operacional mínimo para adequar experiências digitais, orientar medidas de segurança, limitar funcionalidades incompatíveis, viabilizar a classificação indicativa, ativar salvaguardas e impedir o acesso a conteúdos, produtos ou serviços proibidos ou inadequados.

A contribuição se insere em uma trajetória institucional de atuação da Data Privacy Brasil nas agendas de proteção de dados pessoais, direitos digitais e infância. Em diálogo contínuo com a ANPD, a organização já apresentou contribuições sobre o tratamento de dados pessoais de crianças e adolescentes, defendeu a procedimentalização concreta do melhor interesse e a adoção de avaliações de impacto voltadas aos direitos desse público. Essa atuação também se projeta em debates públicos relevantes, incluindo a participação como amicus curiae em processos judiciais e administrativos, nos quais ressaltamos a importância de interpretar rigorosamente os princípios da finalidade, da necessidade e da proporcionalidade em conjunto com o melhor interesse da criança e do adolescente.

No tema específico da aferição de idade, esta contribuição também dialoga com a nossa publicação recente "Descomplicando o ECA Digital: Aferição de Idade e Proteção Integral no Ambiente Digital", de maio de 2026. O documento parte da insuficiência da autodeclaração simples e sustenta que a idade deve ser tratada como critério operacional de adequação da experiência digital, capaz de orientar bloqueios, restrições, classificação indicativa, supervisão parental, desenho de funcionalidades, medidas de segurança e canais de contestação.

As recomendações aqui apresentadas buscam contribuir para que o Guia da ANPD evite dois caminhos igualmente inadequados: de um lado, a manutenção de mecanismos frágeis, meramente formais e incapazes de produzir proteção efetiva; de outro, a adoção indiscriminada de soluções intrusivas baseadas em identificação civil, biometria, retenção documental, rastreamento comportamental ou coleta massiva de dados. O objetivo regulatório deve ser construir um modelo proporcional ao risco, tecnicamente confiável, auditável, contestável, inclusivo e compatível com os princípios da LGPD.

Nesse sentido, a Data Privacy Brasil defende que a aferição de idade seja integrada a uma arquitetura mais ampla de proteção desde a concepção e por padrão. A aferição

não substitui deveres de desenho seguro, limitação de publicidade comportamental, governança de conteúdo, restrição de interações de risco, transparência qualificada, supervisão parental, documentação, auditoria e responsabilização dos agentes da cadeia digital. Sua função é habilitar respostas protetivas proporcionais, e não deslocar para crianças, adolescentes ou famílias o ônus de lidar com ambientes digitais desenhados, monetizados e controlados por agentes econômicos especializados.

Por fim, esta contribuição também parte da compreensão de que a efetividade do Guia dependerá de sua capacidade de reduzir assimetrias informacionais e orientar práticas concretas por parte de fornecedores, lojas de aplicativos, sistemas operacionais, terceiros especializados e autoridades reguladoras. Assim como defendido pela Data Privacy Brasil em sua contribuição ao Guia do Usuário Brasileiro de Inteligência Artificial, instrumentos orientativos devem ir além da enunciação de direitos e oferecer caminhos operacionais, inteligíveis e acionáveis para sua efetivação em contextos reais de desigualdade, assimetria de poder e baixa transparência tecnológica.

Contribuições da Data Privacy Brasil na Tomada de Subsídios

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

A seção "Introdução" situa a aferição de idade no regime de prevenção de riscos, proteção integral e melhor interesse de crianças e adolescentes no ambiente digital. O texto pode ganhar precisão ao afirmar que a aferição de idade não é finalidade autônoma nem etapa cadastral obrigatória. Trata-se de medida instrumental para adaptar a experiência digital ao perfil etário do usuário, de modo proporcional ao risco e compatível com privacidade e proteção de dados.

A doutrina da proteção integral reforça essa interpretação. Lopes e Cardin registram que a proteção integral abrange "todas as necessidades de um ser humano para o pleno desenvolvimento de sua personalidade" (Elias, 2010, p. 2, apud Lopes e Cardin, 2023, p. 91). No ambiente digital, essa formulação exige que a aferição seja tratada como instrumento de adequação da experiência e prevenção de riscos, sem autorizar identificação ampla de usuários.

Essa leitura se aproxima da privacidade desde a concepção. Hoepman afirma que estratégias de desenho em privacidade "traduzem normas jurídicas vagas em requisitos concretos de desenho" (Hoepman, 2014, p. 446, tradução livre). A estratégia de minimização exige "limitar tanto quanto possível o tratamento de dados pessoais" (Hoepman, 2014, p. 449, tradução livre). O Guia deve incorporar essa premissa ao orientar fornecedores a definir o atributo etário necessário, o método proporcional ao risco e os dados que podem ser dispensados.

A idade deve ser tratada como atributo operacional mínimo. O dossiê Descomplicando o ECA Digital afirma que "a idade é tratada como critério operacional de adequação da

experiência no digital" (Data Privacy Brasil, 2026, p. 4). O mesmo documento afirma que "a pergunta correta não é 'quem é exatamente esse usuário?'. A pergunta é qual informação mínima permite saber se aquela experiência, conteúdo, funcionalidade ou produto é adequado à sua idade" (Data Privacy Brasil, 2026, p. 11). Essa formulação deve orientar a introdução e afastar leituras que convertam proteção etária em identificação civil generalizada.

A Introdução deve afirmar que a aferição de idade não substitui outras obrigações de proteção. Aferir idade sem modificar o desenho do serviço, os padrões de recomendação, os fluxos de coleta de dados e os mecanismos de proteção podem produzir conformidade formal, sem proteção material equivalente. Hoepman recomenda que o desenho de sistemas não se concentre em "apenas uma estratégia", pois "elas são todas potencialmente úteis" quando aplicadas de forma combinada (Hoepman, 2014, tradução livre).

O modelo regulatório deve ser compreendido como baseado em risco e direitos. A proporcionalidade pode justificar métodos mais rigorosos em contextos de alto risco, mas também deve limitar coleta excessiva, retenção indevida e identificação desnecessária. O dossiê resume essa lógica ao afirmar que "o fornecedor não deve perguntar apenas 'qual método existe?', mas qual método é proporcional ao risco daquele conteúdo, serviço ou funcionalidade" (Data Privacy Brasil, 2026, p. 28).

A Introdução deve reconhecer a diversidade das infâncias brasileiras. Métodos que dependem de documento formal, conexão estável, câmera de qualidade, reconhecimento facial ou determinados padrões corporais podem excluir usuários ou produzir taxas de erro desiguais. Freitas e Dias lembram que, no debate sobre internet, "aos mesmos sujeitos que são devidos direitos de proteção, também são devidos direitos de liberdade" (Dias, 2015, p. 12, apud Freitas e Dias, 2020, p. 267). A aferição de idade deve proteger sem bloquear experiências compatíveis com a autonomia progressiva.

A confiabilidade dos mecanismos exige formulação mais precisa. A confiabilidade não se confunde com precisão técnica isolada nem com infalibilidade. Nenhum método elimina completamente erro, burla ou incerteza. Mecanismos confiáveis devem prever zonas de incerteza, camadas sucessivas quando necessário, canais de contestação e documentação sobre escolha do método, riscos mitigados, dados tratados, retenção, segurança e alternativas menos intrusivas.

A Introdução pode antecipar a cadeia digital de responsabilidades. Lojas de aplicações, sistemas operacionais, fornecedores finais, terceiros especializados, famílias, poder público e autoridades reguladoras exercem funções distintas e conectadas. Como registra Rossato, a proteção infantojuvenil envolve "uma responsabilidade que, para ser realizada, necessita de uma integração, de um conjunto devidamente articulado de políticas públicas" (Rossato, 2010, p. 97, apud Freitas, 2024, p. 2148). Essa integração deve impedir que um agente transfira a outro o dever de adaptar a experiência e proteger direitos.

A seção pode ser reforçada com três ajustes. O primeiro é explicitar que a aferição de idade adequa a experiência digital. O segundo é interpretar o modelo baseado em risco à luz do melhor interesse e dos direitos fundamentais. O terceiro é vincular confiabilidade a método, governança e evidências.

Justificativa

A seção “Introdução” está conceitualmente bem orientada ao apresentar a aferição de idade no contexto de um marco regulatório voltado à prevenção de riscos, à proteção integral e ao melhor interesse de crianças e adolescentes no ambiente digital. Para que essa abertura fique mais precisa e metodologicamente robusta, convém explicitar desde o início que a aferição de idade não é um fim em si, nem uma mera formalidade cadastral, mas uma medida instrumental destinada a adaptar a experiência digital ao perfil etário do usuário, de modo proporcional ao risco e compatível com os princípios de privacidade e proteção de dados.

Essa leitura também se apoia na doutrina da proteção integral. Lopes e Cardin registram que a proteção integral deve ser compreendida como aquela que abrange “todas as necessidades de um ser humano para o pleno desenvolvimento de sua personalidade” (Elias, 2010, p. 2, apud Lopes e Cardin, 2023, p. 91)[1]. No ambiente digital, essa formulação exige que a aferição de idade seja tratada como instrumento de adequação da experiência e de prevenção de riscos, e não como autorização ampla para identificar usuários.

Essa leitura aproxima o Guia de uma abordagem de privacidade desde a concepção. Hoepman afirma que as estratégias de desenho em privacidade “traduzem normas jurídicas vagas em requisitos concretos de desenho” e orientam escolhas fundamentais desde as primeiras fases de concepção do sistema (Hoepman, 2014, p. 446, tradução livre)[2]. A mesma lógica se aplica à aferição de idade. O fornecedor deve definir qual atributo etário é necessário, qual método é proporcional ao risco e quais dados podem ser dispensados.

Como sintetiza Hoepman, a estratégia de minimização exige “limitar tanto quanto possível o tratamento de dados pessoais” (Hoepman, 2014, p. 449, tradução livre)[3]. O Guia deve incorporar essa premissa e deixar claro que a aferição de idade deve adaptar a experiência digital sem converter proteção etária em identificação generalizada, coleta excessiva ou retenção indevida de dados. O dossiê “Descomplicando o ECA Digital: Aferição de Idade e Proteção de Integral no Ambiente Digital” segue a mesma direção ao afirmar que “a idade é tratada como critério operacional de adequação da experiência no digital, capaz de orientar bloqueios, restrições, classificação indicativa, supervisão parental, desenho de funcionalidades, medidas de segurança e canais de contestação” (Data Privacy Brasil, 2026, p. 4)[4].

Nessa formulação, a idade deve ser tratada como atributo operacional mínimo, suficiente para modular salvaguardas, restringir funcionalidades, adaptar conteúdos, re-

1 LOPES, Claudia Aparecida Costa; CARDIN, Valéria Silva Galdino. **A responsabilidade civil pelo consentimento parental contrário ao melhor interesse e aos direitos personalíssimos da criança na Lei Geral de Proteção de Dados.** Revista IBERC, Belo Horizonte, v. 6, n. 1, p. 83-97, jan./abr. 2023. DOI: https://doi.org/10.37963/iberc.v6i1.244. Disponível em: https://revista.iberc.org.br/iberc/article/view/244. Acesso em: 22 mar. 2026.

2 HOEPMAN, Jaap-Henk. **Privacy design strategies.** In: ICT Systems Security and Privacy Protection. 2014. p. 446–459.

3 *Idem.*

4 MENDONÇA, Eduardo; NOVOA, Natasha; RODRIGUES, Carla. **Descomplicando o ECA Digital: aferição de idade e proteção integral no ambiente digital.** São Paulo: Data Privacy Brasil, maio 2026. E-book. Disponível em: https://www.dataprivacybr.org/documentos/ descomplicando-o-eca-digital-afericao-de-idade/. Acesso em: 26 jun 2026.

duzir exposições indevidas e calibrar medidas de segurança quando a faixa etária for relevante para a proteção do usuário. Essa perspectiva ajuda a evitar que a aferição de idade seja confundida com identificação civil generalizada. Hoepman sintetiza a estratégia de minimização como a exigência de "limitar tanto quanto possível o tratamento de dados pessoais" e afirma que a estratégia de abstração consiste em "limitar tanto quanto possível o nível de detalhe em que dados pessoais são tratados" (Hoepman, 2014, p. 449 e 452, tradução livre). O exemplo dado pelo autor é diretamente aplicável à aferição de idade, pois "em muitos casos, apenas a idade importa, e não a data específica de nascimento", bastando registrar atributos como "maior de dezoito anos" quando essa informação for suficiente para a finalidade pretendida (Hoepman, 2014, p. 453, tradução livre)[5]. Assim, o desenho regulatório e técnico deve partir da pergunta sobre qual informação mínima é necessária para adequar a experiência à idade, e não da identificação de quem é o usuário.

O dossiê Descomplicando o ECA Digital formula essa distinção de modo direto ao afirmar que "a pergunta correta não é 'quem é exatamente esse usuário?'. A pergunta é qual informação mínima permite saber se aquela experiência, conteúdo, funcionalidade ou produto é adequado à sua idade" (Data Privacy Brasil, 2026, p. 11)[6]. O Guia deve adotar essa lógica como eixo interpretativo. O desenho regulatório e técnico deve partir da informação mínima necessária para adequar a experiência à idade, e não da identificação de quem é o usuário.

Também é recomendável afirmar, já na abertura, que a aferição de idade não substitui outras obrigações de proteção. A literatura de engenharia de privacidade mostra que controles isolados perdem efetividade quando não integram uma arquitetura mais ampla de minimização, limitação de finalidade, transparência, governança, prestação de contas e demonstração de conformidade. Hoepman recomenda que o desenho de sistemas não se concentre em "apenas uma estratégia", pois "elas são todas potencialmente úteis" e devem ser aplicadas de forma combinada para tornar o sistema mais favorável à privacidade (Hoepman, 2014, tradução livre). O autor também associa a estratégia de demonstração ao dever de "documentar todos os passos importantes", "registrar decisões" e "motivá-las" (Hoepman, 2014, tradução livre)[7]. Essa lógica se aplica à aferição de idade. Aferir idade sem modificar o desenho do serviço, os padrões de recomendação, os fluxos de coleta de dados e os mecanismos de proteção podem produzir conformidade formal, sem proteção material equivalente.

Convém reforçar que o modelo regulatório deve ser lido como baseado em risco e direitos. A proporcionalidade opera em duas direções. Ela pode justificar métodos mais rigorosos em contextos de alto risco, mas também deve limitar a coleta excessiva, retenção indevida e identificação desnecessária. Essa leitura é coerente com abordagens de privacidade desde a concepção. Hoepman sintetiza a estratégia de minimização como a exigência de "limitar tanto quanto possível o tratamento de dados pessoais" e afirma que a separação busca "separar o tratamento de dados pessoais tanto quanto possível" para dificultar combinação e correlação entre contextos (Hoepman, 2014, tradução livre). O autor também define a estratégia de ocultação como a proteção dos dados pessoais

5 HOEPMAN, Jaap-Henk. **Privacy design strategies.** In: ICT Systems Security and Privacy Protection. 2014. p. 446–459.

6 *Idem.*

7 *Idem.*

ou sua transformação em dados "não vinculáveis ou não observáveis" e associa a demonstração de conformidade ao dever de "documentar todos os passos importantes", registrar decisões e justificá-las (Hoepman, 2014, tradução livre)[8]. Aplicada à aferição de idade, essa abordagem impede que o risco seja usado como justificativa genérica para identificar usuários, ampliar bases de dados ou reter informações além do necessário. O Guia deve orientar os fornecedores a escolher métodos proporcionais ao risco, separados de finalidades incompatíveis, protegidos contra rastreabilidade e acompanhados de evidências que demonstrem a necessidade da escolha adotada.

Aplicada à aferição de idade, essa abordagem impede que o risco seja usado como justificativa genérica para identificar usuários, ampliar bases de dados ou reter informações além do necessário. O dossiê Descomplicando o ECA Digital resume essa lógica ao afirmar que "o fornecedor não deve perguntar apenas 'qual método existe?', mas qual método é proporcional ao risco daquele conteúdo, serviço ou funcionalidade" (Data Privacy Brasil, 2026, p. 28)[9]. O Guia deve orientar os fornecedores a escolher métodos proporcionais ao risco, separados de finalidades incompatíveis, protegidos contra rastreabilidade e acompanhados de evidências que demonstrem a necessidade da escolha adotada.

A proporcionalidade prevista no art. 24 do Decreto nº 12.880/2026 funciona em duas direções. Ela permite exigir métodos mais confiáveis em contextos de maior risco e impede que serviços de baixo ou médio risco adotem métodos baseados em documento oficial, biometria ou identificação civil por conveniência operacional. Proporcionalidade é critério de intensificação quando o risco exige maior proteção e limite contra coleta excessiva, retenção indevida, restrição injustificada de acesso legítimo e transferência do ônus de proteção para o usuário.

A Introdução também deve reconhecer a diversidade das infâncias brasileiras. A implementação de mecanismos de aferição de idade ocorre em um país marcado por desigualdades de documentação, conectividade, letramento digital, acesso a dispositivos, deficiência, raça, território e renda. Métodos que dependem de documento formal, conexão estável, câmera de qualidade, reconhecimento facial ou determinados padrões corporais e comportamentais podem excluir usuários ou produzir taxas de erro desiguais. Por isso, a confiabilidade do mecanismo deve ser avaliada também por sua compatibilidade com inclusão e não discriminação.

Essa preocupação é coerente com a literatura sobre direitos de crianças e adolescentes no ambiente digital. Freitas e Dias lembram que, no debate sobre internet, "aos mesmos sujeitos que são devidos direitos de proteção, também são devidos direitos de liberdade" (Dias, 2015, p. 12, apud Freitas e Dias, 2020, p. 267)[10]. A aferição de idade deve operar nessa tensão. Ela deve proteger contra riscos relevantes sem bloquear, de forma uniforme e injustificada, o acesso a experiências compatíveis com a autonomia progressiva de crianças e adolescentes.

8 HOEPMAN, Jaap-Henk. **Privacy design strategies.** In: ICT Systems Security and Privacy Protection. 2014. p. 446–459.

9 *Idem.*

10 FREITAS, Nivaldo Alexandre de; DIAS, Lívia Ferreira. **Apontamentos sobre proteção e liberdade de crianças e adolescentes quanto ao uso da internet.** Reflexão e Ação, Santa Cruz do Sul, v. 28, n. 2, p. 263-275, maio/ago. 2020. DOI: https://doi.org/10.17058/rea.v28i2.12303. Disponível em: https://online.unisc.br/seer/index.php/reflex/article/view/12303. Acesso em: 22 mar. 2026.

A confiabilidade dos mecanismos de aferição merece uma formulação mais precisa. A Introdução menciona corretamente que os mecanismos devem ser confiáveis e eficazes, mas deve evitar que a confiabilidade seja confundida com precisão técnica isolada. A confiabilidade depende do método, da governança e da capacidade de demonstrar conformidade. Um mecanismo tecnicamente preciso pode ser inadequado se cria barreiras desproporcionais de acesso, retém dados além do necessário, permite rastreamento do histórico de verificações ou não oferece revisão em caso de erro.

Também se recomenda esclarecer que confiabilidade não significa infalibilidade. Nenhum método de aferição elimina completamente erros, burla ou incerteza. A estimativa facial pode apresentar margem de erro, especialmente em faixas etárias próximas. A verificação documental depende da autenticidade e da validade do documento. A inferência pode produzir falsos positivos ou se apoiar em sinais inadequados. Por isso, mecanismos confiáveis exigem salvaguardas de correção, zonas de incerteza, camadas sucessivas quando necessário e canais de contestação. A confiabilidade exige método proporcional ao risco, tecnicamente adequado e acompanhado de medidas para lidar com erros.

A eficácia prevista no ECA Digital não se resume ao bloqueio de conteúdos, produtos ou serviços proibidos. Ela também envolve a adaptação da experiência digital de forma compatível com autonomia progressiva, informação adequada e diversidade de contextos socioeconômicos. A aferição de idade não deve funcionar como barreira uniforme e indiscriminada. Ela deve servir à modulação da experiência conforme a faixa etária, as características do público e os riscos do serviço. O dossiê Descomplicando o ECA Digital expressa esse ponto ao afirmar que a aferição deve "sustentar tecnicamente a adequação da experiência oferecida" (Data Privacy Brasil, 2026, p. 7)[11].

O Guia também deve deixar claro que não impõe tecnologia única nem autoriza de forma geral métodos invasivos. A menção a estimativa facial, verificação documental e credenciais verificáveis deve ser compreendida como apresentação de abordagens possíveis, sujeitas aos requisitos gerais e aos limites legais aplicáveis. A escolha do mecanismo deve depender do caso concreto, do risco do serviço, da finalidade específica e do tratamento de dados envolvido.

Essa cautela é importante diante da expansão de um mercado de fornecedores de soluções de aferição de idade. A implementação do ECA Digital pode gerar incentivos para retenção excessiva de dados, concentração de informações biométricas e identitárias em poucos provedores privados e reutilização de dados para finalidades alheias à proteção etária. A Introdução não precisa desenvolver esse tema em profundidade, mas deve indicar que a confiabilidade dos mecanismos será avaliada também por sua compatibilidade com direitos fundamentais, proteção de dados e limites contra uso secundário.

O risco é individual, sistêmico e subsequente. Dados coletados ou gerados para aferição de idade, especialmente imagens faciais, documentos e dados biométricos, podem se tornar fonte de novos danos quando retidos, vazados ou reutilizados indevidamente. Esse ponto recomenda associar a aferição de idade à prevenção de danos subsequentes, e não apenas ao bloqueio imediato de acesso indevido, pois "quanto mais se sabe sobre uma pessoa, sem dúvida mais vulnerável ela se torna" (Fernández, 2013, p. 264, apud Falcão e Mill, 2018, p. 137)[12].

11 *Idem.*

12 FALCÃO, Patricia Mirella de Paulo; MILL, Daniel. **A criança e seu fascínio pelo mundo digital: o que o dis-**

Experiências comparadas reforçam esse cuidado. O Age Assurance Technology Trial, conduzido na Austrália em 2025, avaliou diferentes métodos de verificação, estimativa, inferência, validação sucessiva, controle parental e consentimento parental, sem apontar uma solução única para todos os contextos. O relatório evidencia a necessidade de combinar efetividade, privacidade, proporcionalidade e salvaguardas contra coleta excessiva. A referência comparada deve servir como alerta metodológico, não como prescrição de solução específica para o contexto brasileiro.

A distinção entre aferição de idade e verificação de identidade também pode ser antecipada como eixo de leitura do documento, sem prejuízo de seu desenvolvimento na seção de Aspectos Gerais. A pergunta correta para a implementação do ECA Digital não é quem é o usuário, mas qual informação mínima é necessária para adequar a experiência à idade. Essa formulação orienta a escolha do método, a avaliação de risco e a documentação das decisões.

A Introdução também deve apresentar a cadeia digital de responsabilidades como elemento estruturante do Guia. A proteção de crianças e adolescentes no ambiente digital não pode ser atribuída a um único agente. Lojas de aplicações, sistemas operacionais, fornecedores finais, terceiros especializados, famílias, poder público e autoridades reguladoras exercem funções distintas e conectadas. O cumprimento de deveres por um agente não elimina a responsabilidade dos demais pela proteção integral e pela adequação da experiência oferecida. Como registra Rossato, a proteção infantojuvenil envolve "uma responsabilidade que, para ser realizada, necessita de uma integração, de um conjunto devidamente articulado de políticas públicas" (Rossato, 2010, p. 97, apud Freitas, 2024, p. 2148)[13].

Essa cadeia deve ser apresentada de modo a evitar transferência indevida de responsabilidade. O fornecimento de sinal de idade por loja de aplicações ou sistema operacional pode reduzir a coleta repetida e apoiar a interoperabilidade, mas não transforma o sinal em formalidade nem isenta o fornecedor final de adaptar o serviço. Da mesma forma, a contratação de terceiro especializado pode apoiar a execução técnica, mas não afasta o dever de diligência, documentação e governança do fornecedor que oferece a experiência digital.

A Introdução deve indicar que a ANPD espera evidências de conformidade, e não apenas declarações gerais. A implementação do ECA Digital depende de registros que demonstrem avaliação de risco, escolha proporcional do método, limitação dos dados tratados, medidas contra uso secundário, testes de efetividade, canais de contestação e revisão periódica. Sem documentação mínima, a aferição de idade pode se tornar exigência formal sem capacidade de demonstrar proteção real.

Esse ponto é relevante porque parte da conformidade em proteção de dados ainda se apoia em políticas genéricas, avisos extensos e declarações de intenção. O ECA Digital exige outra postura. Produtos e serviços de tecnologia da informação direcionados a crianças e adolescentes, ou de acesso provável por esse público, devem demonstrar que

---

curso nos revela. Revista Tecnologia e Sociedade, Curitiba, v. 14, n. 30, p. 136-153, jan./abr. 2018. DOI: 10.3895/rts.v14n30.4615. Disponível em: https://periodicos.utfpr.edu.br/rts/article/view/4615. Acesso em: 20 mar. 2026.

13 FREITAS, Maria Luiza de Moura de Mello. **O princípio constitucional da proteção integral da criança e do adolescente e o papel do juiz no âmbito jurídico social.** Revista Ibero-Americana de Humanidades, Ciências e Educação, São Paulo, v. 10, n. 5, p. 2144-2163, maio 2024. DOI: https://doi.org/10.51891/rease.v10i5.14000. Disponível em: https://periodicorease.pro.br/rease/article/view/14000. Acesso em: 22 mar. 2026.

suas escolhas de desenho foram orientadas pelo melhor interesse, pela proteção integral, pela privacidade e pela prevenção de riscos. Registros técnicos, trilhas de decisão e evidências sobre a eficácia dos controles serão relevantes para avaliar a conformidade.

A Introdução também pode reconhecer soluções orientadas à privacidade desde a concepção e desde o padrão, inclusive por meio de credenciais verificáveis, provas de conhecimento zero, padrões abertos e arquiteturas que permitam comprovar o atributo etário sem revelar identidade civil ou dados pessoais adicionais. Essas soluções não devem ser tratadas como obrigatórias em todos os contextos, mas devem ser reconhecidas como compatíveis com minimização, interoperabilidade, não rastreabilidade e limitação de finalidade.

A divisão do Guia em Aspectos Gerais, Cadeia Digital de Responsabilidades, Requisitos Gerais e Requisitos Específicos é adequada. A estrutura ajuda os agentes regulados a compreenderem a progressão entre conceitos, responsabilidades, critérios gerais e parâmetros aplicáveis a tecnologias específicas. O anexo com quadro sintético de recomendações também pode ser útil, desde que seja tratado como instrumento de consulta rápida, e não como substituto da leitura das seções ou da análise contextual dos requisitos.

Em síntese, a Data Privacy Brasil considera que a seção "Introdução" está adequada em sua estrutura e propósito, mas pode ser reforçada com três ajustes. O primeiro é explicitar que a aferição de idade é medida instrumental voltada à adequação da experiência digital. O segundo é afirmar que o modelo baseado em risco deve ser filtrado pelo melhor interesse e que a proporcionalidade também funciona como limite contra coleta excessiva. O terceiro é esclarecer que a confiabilidade depende do método, da governança e da capacidade de demonstrar conformidade por evidências. Com esses ajustes, a Introdução orientará melhor a leitura das seções seguintes e reduzirá a margem para interpretações que transformem a proteção de crianças e adolescentes em justificativa para vigilância, identificação compulsória ou coleta desnecessária de dados.

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

A Data Privacy Brasil considera adequada a opção de iniciar o Guia com conceitos gerais da aferição de idade. Essa escolha ajuda a aplicar o Estatuto Digital da Criança e do Adolescente sem manter barreiras frágeis de autodeclaração e sem adotar soluções excessivas baseadas em identificação civil, biometria ou rastreamento. A aferição deve ser implementada por mecanismos "proporcionais, confiáveis, auditáveis e contestáveis", capazes de proteger sem ampliar indevidamente coleta de dados, identificação civil, vigilância ou rastreamento (Data Privacy Brasil, 2026, p. 4).

A interpretação do Guia deve observar a LGPD, em especial finalidade, necessidade, segurança, prevenção, responsabilização e melhor interesse. Essa leitura é compatível com a proteção integral, que abrange "todas as necessidades de um ser humano para o pleno desenvolvimento de sua personalidade" (Elias, 2010, p. 2, apud Lopes e Cardin, 2023, p. 91). Também deve considerar a tensão entre proteção e liberdade, pois "aos mesmos sujeitos que são devidos direitos de proteção, também são devidos direitos de liberdade" (Dias, 2015, p. 12, apud Freitas e Dias, 2020, p. 267).

A minuta acerta ao tratar a aferição de idade como categoria geral e distinta da verifica-

ção de identidade. O Decreto nº 12.880/2026 distingue aferição, verificação, sinal de idade e autodeclaração (Brasil, 2026). A pergunta central deve ser qual atributo etário é necessário para adequar a experiência digital, e não quem é o usuário. O dossiê afirma que "a pergunta correta não é 'quem é exatamente esse usuário?'. A pergunta é qual informação mínima permite saber se aquela experiência, conteúdo, funcionalidade ou produto é adequado à sua idade" (Data Privacy Brasil, 2026, p. 20).

Documento oficial, biometria, CPF e identificadores persistentes não devem ser tratados como solução padrão. Em Gender Shades, Buolamwini e Gebru demonstraram que "mulheres de pele mais escura foram o grupo mais erroneamente classificado" em sistemas comerciais de classificação facial (Buolamwini e Gebru, 2018, p. 1). Métodos biométricos exigem justificativa reforçada, avaliação de impacto, testes por subgrupos, limites de retenção e alternativa acessível. O CPF só deve ser admitido de forma excepcional, proporcional, documentada e vinculada à finalidade etária.

O Guia deve diferenciar material impróprio ou inadequado de material proibido por lei. Para conteúdos impróprios ou inadequados, a resposta envolve classificação indicativa, segurança por padrão e supervisão parental. Para produtos, serviços e conteúdos proibidos, exige verificação eficaz de idade e impedimento de acesso (Brasil, 2026). O dossiê sintetiza essa resposta como "implementar verificação eficaz de idade e impedir acesso, fruição, compra ou consumo" (Data Privacy Brasil, 2026, p. 29).

A proporcionalidade deve ser apresentada em termos práticos. A estimativa etária produz probabilidade, não confirmação absoluta. Punyani, Gupta e Kumar afirmam que "a estimativa facial de idade não pode ser abordada apenas como um problema clássico de classificação" (Punyani, Gupta e Kumar, 2020, p. 3301, tradução livre). Como há margem de erro, o fornecedor deve iniciar pelo método menos intrusivo compatível com o risco e avançar para camada mais exigente apenas quando o resultado for inconclusivo, contestado ou insuficiente.

A abordagem em camadas é adequada quando funciona como escalonamento, não como autorização para acumular dados. O dossiê afirma que "a aferição de idade, sozinha, não resolve todos os riscos" (Data Privacy Brasil, 2026, p. 13). Supervisão parental, classificação, segurança, governança e contestação devem funcionar como camadas complementares.

Dados tratados para aferição de idade não podem ser reutilizados para publicidade comportamental, perfilamento, recomendação, monetização, enriquecimento cadastral ou finalidade incompatível. O dossiê afirma que "aferição de idade não pode servir como pretexto para ampliar coleta, rastreamento ou exploração comercial de crianças e adolescentes" (Data Privacy Brasil, 2026, p. 27). Os sinais de idade devem conter apenas o atributo necessário, em resposta binária ou faixa etária ampla.

O Guia deve tratar de contestação, inclusão e documentação como requisitos do mecanismo. Usuários não podem ficar sujeitos a bloqueios opacos, sem explicação e sem revisão. Toda solução deve prever procedimento claro para erro de classificação, ausência de documento, falha técnica ou divergência entre sinais, além de alternativas acessíveis. A escolha do método deve ser documentada por avaliação de risco, finalidade, dados tratados, retenção, testes e medidas contra uso secundário.

A seção "Aspectos Gerais" deve afirmar que a aferição de idade existe para adequar experiências digitais ao melhor interesse de crianças e adolescentes, com o menor tratamento de dados possível, de forma proporcional, contestável, auditável e inclusiva.

Justificativa

A Data Privacy Brasil considera adequada a opção de iniciar o Guia Orientativo com uma seção dedicada aos conceitos gerais da aferição de idade. Essa escolha ajuda a aplicar o Estatuto Digital da Criança e do Adolescente sem manter barreiras frágeis baseadas apenas em autodeclaração e sem adotar soluções excessivas baseadas em identificação civil generalizada, coleta desnecessária de biometria ou rastreamento do usuário. A leitura do tema deve partir da proteção de dados pessoais como direito fundamental, inclusive nos meios digitais, e da proteção da criança e do adolescente com absoluta prioridade. O dossiê Descomplicando o ECA Digital resume esse ponto ao afirmar que a aferição de idade deve ser implementada por meio de mecanismos "proporcionais, confiáveis, auditáveis e contestáveis, capazes de proteger crianças e adolescentes sem ampliar indevidamente coleta de dados, identificação civil, vigilância ou rastreamento" (Data Privacy Brasil, 2026, p. 4)[1].

Falcão e Mill registram que crianças estão expostas às tecnologias digitais com aparente domínio, mas sem compreender plenamente o sentido da vigilância a que podem estar submetidas (Falcão e Mill, 2018)[2]. Na mesma direção, a literatura sobre proteção de dados de crianças e adolescentes lembra que "um terço dos usuários da internet é menor de idade" (UNICEF, 2018, apud Souza, 2020)[3], o que torna a aferição de idade uma questão de desenho de proteção, e não uma autorização para vigilância.

Essa interpretação também precisa observar a Lei Geral de Proteção de Dados (LGPD). O art. 6º exige que o tratamento de dados tenha finalidade definida, use apenas o necessário e adote medidas de segurança, prevenção e responsabilização. O art. 14 determina que dados pessoais de crianças e adolescentes sejam tratados em seu melhor interesse. Na prática, a aferição de idade deve proteger crianças e adolescentes sem transformar essa finalidade em base para vigilância ampla, identificação compulsória ou coleta excessiva de dados. A própria LGPD define necessidade como limitação do tratamento ao mínimo necessário (Brasil, 2018). Essa leitura é compatível com a doutrina da proteção integral, que compreende a proteção como aquela que alcança "todas as necessidades de um ser humano para o pleno desenvolvimento de sua personalidade" (Elias, 2010, p. 2, apud Lopes e Cardin, 2023, p. 91)[4]. Também se conecta ao melhor interesse, tratado como "vetor axiológico" quando estão em causa interesses de crianças e adolescentes (Padilha, 2017, p. 88, apud Lopes e Cardin, 2023, p. 91).

1 MENDONÇA, Eduardo; NOVOA, Natasha; RODRIGUES, Carla. **Descomplicando o ECA Digital: aferição de idade e proteção integral no ambiente digital.** São Paulo: Data Privacy Brasil, maio 2026. E-book. Disponível em: https://www.dataprivacybr.org/documentos/ descomplicando-o-eca-digital-afericao-de-idade/. Acesso em: 26 jun 2026.

2 FALCÃO, Patricia Mirella de Paulo; MILL, Daniel. **A criança e seu fascínio pelo mundo digital: o que o discurso nos revela.** Revista Tecnologia e Sociedade, Curitiba, v. 14, n. 30, p. 136-153, jan./abr. 2018. DOI: 10.3895/rts.v14n30.4615. Disponível em: https://periodicos.utfpr.edu.br/rts/article/view/4615. Acesso em: 20 mar. 2026.

3 SOUZA, Ana Carolina dos Santos. **A Lei Geral de Proteção dos Dados Pessoais e seus Efeitos em Relação à Proteção Especial Destinada às Crianças e aos Adolescentes na Internet.** VirtuaJus, Belo Horizonte, v. 5, n. 8, p. 540-561, 1. sem. 2020. DOI: https://doi.org/10.5752/P.1678-3425.2020v5n8p540-561. Disponível em: https://periodicos.pucminas.br/virtuajus/article/view/24272. Acesso em: 23 mar. 2026.

4 LOPES, Claudia Aparecida Costa; CARDIN, Valéria Silva Galdino. **A responsabilidade civil pelo consentimento parental contrário ao melhor interesse e aos direitos personalíssimos da criança na Lei Geral de Proteção de Dados.** Revista IBERC, Belo Horizonte, v. 6, n. 1, p. 83-97, jan./abr. 2023. DOI: https://doi.org/10.37963/iberc.v6i1.244. Disponível em: https://revista.iberc.org.br/iberc/article/view/244. Acesso em: 22 mar. 2026.

A minuta acerta ao tratar a aferição de idade como categoria geral e ao afirmar que ela não se confunde com verificação de identidade. O Decreto nº 12.880/2026 distingue a aferição de idade, que abrange procedimentos para verificar, estimar ou inferir idade ou faixa etária, da verificação de idade, que exige maior confiabilidade (Brasil, 2026). Também define o sinal de idade como informação que atesta idade ou faixa etária sem revelar dados pessoais adicionais, e a autodeclaração como indicação feita pelo próprio usuário sem evidências adicionais (Brasil, 2026). Essa distinção deve ser preservada porque crianças e adolescentes são sujeitos de direitos no presente, e não apenas pessoas em preparação para a vida adulta, uma vez que "aos mesmos sujeitos que são devidos direitos de proteção, também são devidos direitos de liberdade" (Dias, 2015, p. 12, apud Freitas e Dias, 2020, p. 267)[5]. A aferição deve proteger sem transformar o acesso à vida digital em identificação permanente.

A aferição de idade deve partir da pergunta sobre qual atributo etário é necessário para adequar a experiência digital, e não da identificação do usuário. Quando a finalidade puder ser alcançada por sinal de idade, faixa etária ampla, token ou credencial equivalente, a identificação individual não deve ser exigida por padrão. Essa leitura decorre da Lei nº 15.211, de 17 de setembro de 2025, que prevê o fornecimento de sinal de idade por API segura e pautada pela privacidade desde o padrão (Brasil, 2025), e do Decreto nº 12.880, de 18 de março de 2026, que limita esse sinal ao dado estritamente necessário e veda o envio de data de nascimento exata, identidade civil e dados de perfilamento (Brasil, 2026). O dossiê formula essa distinção de modo direto ao afirmar que "a pergunta correta não é 'quem é exatamente esse usuário?'. A pergunta é qual informação mínima permite saber se aquela experiência, conteúdo, funcionalidade ou produto é adequado à sua idade" (Data Privacy Brasil, 2026, p. 20)[6].

Essa formulação também dialoga com a noção de que "a adequada e necessária proteção ao menor se realiza mediante o diálogo de todas as fontes" (Lima e Sá, 2019, p. 87, apud Souza, 2020)[7]. O Guia deve aproximar ECA Digital, LGPD, Constituição, ECA e Convenção sobre os Direitos da Criança em uma mesma lógica de proteção, minimização e adequação.

Documento oficial, biometria, CPF e outros identificadores persistentes não devem ser tratados como solução padrão. Essa orientação decorre da proporcionalidade e da cautela técnica exigida em métodos que podem afetar direitos de forma desigual. Em *Gender Shades*, Buolamwini e Gebru demonstraram que, em sistemas comerciais de classificação por análise facial, "mulheres de pele mais escura foram o grupo mais erroneamente classificado", com taxas de erro de até 34,7%, enquanto a taxa máxima de erro para homens de pele mais clara foi de 0,8% (Buolamwini; Gebru, 2018, p. 1). As autoras também afirmam que "conjuntos de dados inclusivos e relatórios de acurácia por subgrupos" são necessários para aumentar transparência e responsabilização em

5 FREITAS, Nivaldo Alexandre de; DIAS, Lívia Ferreira. **Apontamentos sobre proteção e liberdade de crianças e adolescentes quanto ao uso da internet.** Reflexão e Ação, Santa Cruz do Sul, v. 28, n. 2, p. 263-275, maio/ago. 2020. DOI: https://doi.org/10.17058/rea.v28i2.12303. Disponível em: https://online.unisc.br/seer/index.php/reflex/article/view/12303. Acesso em: 22 mar. 2026.

6 *Idem.*

7 SOUZA, Ana Carolina dos Santos. **A Lei Geral de Proteção dos Dados Pessoais e seus Efeitos em Relação à Proteção Especial Destinada às Crianças e aos Adolescentes na Internet.** VirtuaJus, Belo Horizonte, v. 5, n. 8, p. 540-561, 1. sem. 2020. DOI: https://doi.org/10.5752/P.1678-3425.2020v5n8p540-561. Disponível em: https://periodicos.pucminas.br/virtuajus/article/view/24272. Acesso em: 23 mar. 2026.

inteligência artificial (Buolamwini; Gebru, 2018, p. 12, tradução livre)[8]. O Guia deve dizer isso de forma direta. Métodos biométricos exigem justificativa reforçada, avaliação de impacto, testes por subgrupos, limites de retenção e alternativa acessível.

O mesmo raciocínio se aplica ao CPF. O simples preenchimento de um número, sem evidência adicional de veracidade ou titularidade, não satisfaz o padrão de confiabilidade exigido em contextos de maior risco e amplia a possibilidade de correlação entre bases. Essa leitura é compatível com a distinção entre autodeclaração e verificação de idade prevista no Decreto nº 12.880, de 18 de março de 2026 (Brasil, 2026). O Guia deve deixar claro que o uso do CPF somente pode ser admitido, quando necessário, de forma excepcional, proporcional, documentada e estritamente vinculada à finalidade etária, nunca como meio rotineiro de enriquecimento cadastral. Lopes e Cardin registram que a vulnerabilidade é o elemento que justifica um sistema especial de proteção para crianças e adolescentes (Lopes e Cardin, 2023)[9], enquanto Barboza sustenta que a busca de igualdade substancial deve considerar "a vulnerabilidade inerente às pessoas humanas e as diferenças existentes entre elas" (Barboza, 2009, p. 108, apud Lopes e Cardin, 2023, p. 93)[10].

O Guia deve dar maior destaque à diferença entre material impróprio ou inadequado e material proibido por lei. Segundo o Decreto nº 12.880, de 18 de março de 2026, a disponibilização de conteúdo impróprio ou inadequado depende de classificação indicativa, medidas técnicas e organizacionais de segurança por padrão proporcionais aos riscos e ferramentas de supervisão parental . Para produtos, serviços e conteúdos proibidos para crianças e adolescentes, o fornecedor deve adotar mecanismos eficazes de verificação de idade e impedir o acesso, a fruição ou o consumo (Brasil, 2026). Essa distinção evita a proteção simbólica e a exigência desnecessária de dados em serviços de menor risco. O dossiê Descomplicando o ECA Digital organiza a mesma distinção ao afirmar que, diante de conteúdo, produto ou serviço proibido, a resposta exigida é "implementar verificação eficaz de idade e impedir acesso, fruição, compra ou consumo" (Data Privacy Brasil, 2026, p. 29)[11].

A proporcionalidade deve ser apresentada em termos práticos. A estimativa etária produz uma probabilidade sobre idade ou faixa etária, não uma confirmação absoluta. Punyani, Gupta e Kumar afirmam que "a estimativa facial de idade não pode ser abordada apenas como um problema clássico de classificação" e registram que a tarefa também pode ser tratada como regressão ou por combinação entre classificação e regressão (Punyani, Gupta e Kumar, 2020, p. 3301, tradução livre). As autoras também observam que ainda não é possível estimar idade exata de forma plenamente acurada, pois "a estimativa por grupo etário é a única possível com acurácia até o momento"

8 Buolamwini, Joy; Gebru, Timnit. **Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification.** In: Proceedings of the 1st Conference on Fairness, Accountability and Transparency. Proceedings of Machine Learning Research, v. 81, p. 77–91, 2018.

9 LOPES, Claudia Aparecida Costa; CARDIN, Valéria Silva Galdino. **A responsabilidade civil pelo consentimento parental contrário ao melhor interesse e aos direitos personalíssimos da criança na Lei Geral de Proteção de Dados.** Revista IBERC, Belo Horizonte, v. 6, n. 1, p. 83-97, jan./abr. 2023. DOI: https://doi.org/10.37963/iberc.v6i1.244. Disponível em: https://revista.iberc.org.br/iberc/article/view/244. Acesso em: 22 mar. 2026.

10 *Idem.*

11 MENDONÇA, Eduardo; NOVOA, Natasha; RODRIGUES, Carla. **Descomplicando o ECA Digital: aferição de idade e proteção integral no ambiente digital.** São Paulo: Data Privacy Brasil, maio 2026. E-book. Disponível em: https://www.dataprivacybr.org/documentos/ descomplicando-o-eca-digital-afericao-de-idade/. Acesso em: 26 jun 2026.

e fatores como óculos, pose, iluminação, oclusão, expressão facial e etnia influenciam o resultado (Punyani, Gupta e Kumar, 2020, p. 3303, tradução livre)[12]. Não há solução única para todos os contextos e resultados próximos ao limiar etário exigem margem de incerteza, camada complementar e possibilidade de correção. O Guia deve traduzir esse ponto em regra prática. O fornecedor deve iniciar pelo método menos intrusivo compatível com o risco e avançar para camada mais exigente apenas quando o primeiro resultado for inconclusivo, contestado ou insuficiente para aquele contexto. Essa regra deve considerar a tensão entre proteção, liberdade e participação, já que a Convenção sobre os Direitos da Criança reconhece direitos de "provisão, proteção e participação" (Soares, 1997, p. 82, apud Freitas e Dias, 2020, p. 267)[13]. A proporcionalidade não deve proteger à custa de exclusão injustificada.

A abordagem em camadas mencionada na minuta é adequada quando funciona como escalonamento do método menos intrusivo para o mais exigente, e não como autorização para acumular dados. Mecanismos de aferição podem ser usados de forma isolada ou combinada, conforme o nível de risco, desde que a combinação não amplie a coleta além do necessário. O fornecedor deve iniciar pelo mecanismo menos intrusivo compatível com o risco e avançar para uma camada mais exigente apenas quando o resultado for inconclusivo, contestado ou insuficiente. A experiência do Age Assurance Technology Trial australiano[14] reforça que não há solução única para todos os contextos e que diferentes métodos podem ser combinados de forma proporcional. Nessa leitura, "a aferição de idade, sozinha, não resolve todos os riscos" e deve funcionar em conjunto com medidas de classificação, supervisão, segurança e governança (Data Privacy Brasil, 2026, p. 13)[15]. Schwartz e Pacheco observam que estratégias de monitoramento e supervisão podem funcionar como fatores de proteção, mas sua eficácia varia conforme idade, relação familiar e conhecimento digital dos responsáveis (Schwartz e Pacheco, 2021)[16]. O Guia deve tratar supervisão parental como camada complementar, e não como substituição dos deveres de desenho do fornecedor.

O Guia deve afirmar com clareza que dados tratados para aferição de idade não podem ser reutilizados para publicidade comportamental, perfilamento, recomendação, monetização, enriquecimento cadastral, treinamento de sistemas ou finalidade incompatível com a proteção etária. A Lei nº 15.211, de 17 de setembro de 2025, determina que os dados coletados para verificação de idade sejam usados apenas para essa finali-

12 Punyani, Prachi; Gupta, Rashmi; Kumar, Ashwani. **Neural networks for facial age estimation: a survey on recent advances.** Artificial Intelligence Review, v. 53, n. 5, p. 3299–3347, 2020. DOI: 10.1007/s10462-019-09765-w.

13 FREITAS, Nivaldo Alexandre de; DIAS, Lívia Ferreira. **Apontamentos sobre proteção e liberdade de crianças e adolescentes quanto ao uso da internet.** Reflexão e Ação, Santa Cruz do Sul, v. 28, n. 2, p. 263-275, maio/ago. 2020. DOI: https://doi.org/10.17058/rea.v28i2.12303. Disponível em: https://online.unisc.br/seer/index.php/reflex/article/view/12303. Acesso em: 22 mar. 2026.

14 AGE CHECK CERTIFICATION SCHEME. **Age Assurance Technology Trial: Part A: Main Report.** Austrália: Age Assurance Technology Trial, 2025. Disponível em: https://www.infrastructure.gov.au/sites/default/files/documents/aatt_part_a_digital.pdf. Acesso em: 26 jun. 2026.

15 MENDONÇA, Eduardo; NOVOA, Natasha; RODRIGUES, Carla. **Descomplicando o ECA Digital: aferição de idade e proteção integral no ambiente digital.** São Paulo: Data Privacy Brasil, maio 2026. E-book. Disponível em: https://www.dataprivacybr.org/documentos/ descomplicando-o-eca-digital-afericao-de-idade/. Acesso em: 26 jun 2026.

16 SCHWARTZ, Fernanda Tabasnik; PACHECO, Janaína Thais Barbosa. **Mediação parental na exposição às redes sociais e a internet de crianças e adolescentes.** Estudos e Pesquisas em Psicologia, Rio de Janeiro, v. 21, n. 1, p. 217-235, jan./abr. 2021. DOI: https://doi.org/10.12957/epp.2021.59383. Disponível em: https://www.e-publicacoes.uerj.br/revispsi/article/view/59383. Acesso em: 24 mar. 2026.

dade (Brasil, 2025), e o Decreto nº 12.880, de 18 de março de 2026, inclui nessa vedação a criação de perfis comportamentais (Brasil, 2026). A proteção da criança e do adolescente não pode servir de pretexto para ampliar a exploração econômica de seus dados. Como afirma o dossiê Descomplicando o ECA Digital, "aferição de idade não pode servir como pretexto para ampliar coleta, rastreamento ou exploração comercial de crianças e adolescentes" (Data Privacy Brasil, 2026, p. 27)[17].

Essa vedação deve orientar a arquitetura do tratamento. Os sinais de idade devem conter apenas o atributo necessário à decisão de adequação, preferencialmente em resposta binária ou faixa etária ampla. O Decreto nº 12.880, de 18 de março de 2026, limita esse compartilhamento aos dados estritamente necessários à confirmação da idade mínima exigida e veda o envio de data de nascimento exata, identidade civil e dados de perfilamento (Brasil, 2026). O Guia deve desaconselhar qualquer desenho que permita rastrear o histórico de verificações, acessos ou interações do usuário. Essa realidade exige que sinais de idade sejam desenhados para reduzir a correlação e evitar inferências indevidas sobre crianças, adolescentes e seus responsáveis. Oliveira e Ishitani, ao discutirem desenho sensível a valores, também reforçam que valores como privacidade, autonomia, segurança e equidade precisam ser incorporados ao desenho de sistemas, e não apenas mencionados em políticas externas (Oliveira e Ishitani, 2022)[18].

O Guia deve tratar a contestação como parte do mecanismo de aferição de idade. Crianças, adolescentes, responsáveis legais e usuários em geral não podem ficar sujeitos a bloqueios opacos, sem explicação e sem revisão. O Decreto nº 12.880, de 18 de março de 2026, exige meio adequado para contestar idade ou faixa etária aferida ou verificada e determina que lojas de aplicativos e sistemas operacionais permitam contestação e retificação da classificação etária mediante evidência adicional, com decisão fundamentada em prazo razoável (Brasil, 2026). Essa exigência também encontra apoio na literatura sobre análise facial automatizada. Buolamwini e Gebru afirmam que "conjuntos de dados inclusivos e relatórios de acurácia por subgrupos serão necessários para aumentar a transparência e a responsabilização em inteligência artificial" e acrescentam que "a transparência e a responsabilização algorítmicas vão além de relatórios técnicos e devem incluir mecanismos de consentimento e reparação" (Buolamwini; Gebru, 2018, p. 12, tradução livre)[19]. Embora o estudo trate de classificação de gênero por análise facial, sua conclusão reforça a necessidade de revisão quando sistemas automatizados afetam o acesso de usuários a serviços digitais. Toda solução de aferição deve prever procedimento claro para erro de classificação, ausência de documento, falha técnica ou divergência entre sinais.

A inclusão deve ser tratada como requisito da aferição de idade. O art. 24 do Decreto nº 12.880, de 18 de março de 2026, inclui inclusão e não discriminação entre os critérios aplicáveis aos mecanismos de aferição (Brasil, 2026). Métodos que dependam de documento formal, conexão de alta qualidade, leitura facial ou determinado padrão corporal ou comportamental podem funcionar tecnicamente e ainda assim ser inadequados se

17 *Idem.*

18 OLIVEIRA, Jéssica Patrícia Dutra de; ISHITANI, Lucila. **Design Sensível a Valores na Computação: um Mapeamento Sistemático de Literatura.** Abakós, Belo Horizonte, v. 10, n. 2, p. 26-56, nov. 2022. DOI: https://doi.org/10.5752/P.2316-9451.2022v10n2p26-56. Disponível em: https://periodicos.pucminas.br/abakos/article/view/27836. Acesso em: 24 mar. 2026.

19 Buolamwini, Joy; Gebru, Timnit. **Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification.** In: Proceedings of the 1st Conference on Fairness, Accountability and Transparency. Proceedings of Machine Learning Research, v. 81, p. 77–91, 2018.

criarem barreiras desproporcionais para pessoas com deficiência, usuários sem documentação, populações vulneráveis ou grupos com maior taxa de erro em sistemas automatizados. O Guia deve orientar a adoção de alternativas acessíveis e equivalentes.

A mediação familiar também deve ser situada no lugar correto. Famílias e responsáveis exercem papel relevante, mas não substituem deveres de desenho, segurança e proteção por padrão. Schwartz e Pacheco registram que pais e filhos podem divergir sobre a percepção do controle parental exercido (Schwartz e Pacheco, 2021)[20]. Barbosa e Wagner mostram que regras familiares dependem de construção e reconhecimento pelos adolescentes, e não apenas de imposição unilateral (Barbosa e Wagner, 2014)[21]. Fortes de Sá Pianovski e Martins da Silveira, ao analisarem orientação on-line de pais para uso problemático de internet, identificam resultados positivos, mas também limites relacionados ao número de participantes, generalização e interferência do monitoramento (Fortes de Sá Pianovski e Martins da Silveira, 2022)[22]. O Guia deve evitar que ferramentas parentais sejam tratadas como solução suficiente para riscos estruturais do serviço.

A seção "Aspectos Gerais" deve deixar expresso que a escolha do mecanismo precisa ser documentada. A Lei nº 15.211, de 17 de setembro de 2025, já exige, em hipóteses relevantes, mapeamento de riscos e elaboração de relatórios de impacto, monitoramento e avaliação da proteção de dados pessoais, especialmente quando o tratamento de dados de crianças e adolescentes não for estritamente necessário à operação do serviço (Brasil, 2025). Esse dever, somado ao princípio da responsabilização e prestação de contas da LGPD, exige que o fornecedor demonstre o risco que pretende mitigar, o atributo etário necessário, o motivo da escolha do método, as alternativas menos intrusivas avaliadas, os dados tratados, os prazos de retenção, as medidas contra uso secundário e o canal de contestação disponível (Brasil, 2018).

Em síntese, a seção "Aspectos Gerais" deve afirmar de maneira direta que a aferição de idade existe para adequar experiências digitais ao melhor interesse de crianças e adolescentes, com o menor tratamento de dados possível, de forma proporcional, contestável, auditável e inclusiva. Esse é o ponto que melhor traduz a Constituição, a LGPD, a Lei nº 15.211/2025 e o Decreto nº 12.880/2026.

20 SCHWARTZ, Fernanda Tabasnik; PACHECO, Janaína Thais Barbosa. **Mediação parental na exposição às redes sociais e a internet de crianças e adolescentes.** Estudos e Pesquisas em Psicologia, Rio de Janeiro, v. 21, n. 1, p. 217-235, jan./abr. 2021. DOI: https://doi.org/10.12957/epp.2021.59383. Disponível em: https://www.e-publicacoes.uerj.br/revispsi/article/view/59383. Acesso em: 24 mar. 2026.

21 BARBOSA, Paola Vargas; WAGNER, Adriana. **A construção e o reconhecimento das regras familiares: a perspectiva dos adolescentes.** Psicologia em Estudo, Maringá, v. 19, n. 2, p. 235-245, abr./jun. 2014. DOI: 10.1590/1413-737222060007. Disponível em: https://www.scielo.br/j/pe/a/MjYdvsm4bQQDGzY37cPMWkm/?lang=pt. Acesso em: 24 mar. 2026.

22 FORTES DE SÁ PIANOVSKI, M.; MARTINS DA SILVEIRA, J. **Orientação de pais on-line no tratamento do uso problemático de internet pela criança.** Acta Comportamentalia, [S. l.], v. 30, n. 3, 2022. DOI: 10.32870/ac.v30i3.83280. Disponível em: https://actacomportamentalia.cucba.udg.mx/index.php/acom/article/view/83280. Acesso em: 20 mar. 2026.

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

Se mostra adequada a inclusão de uma seção específica sobre cadeia digital de responsabilidades, pois a aferição de idade não ocorre em um ponto isolado da experiência digital. Ela depende da atuação coordenada de diferentes agentes, incluindo fornecedores de aplicações, lojas de aplicativos, sistemas operacionais, fornecedores de tecnologia de aferição, responsáveis legais, poder público e autoridades reguladoras. Essa distribuição, contudo, não pode ser interpretada como autorização para diluir responsabilidades ou transferir integralmente às famílias o ônus de proteger crianças e adolescentes em ambientes projetados, monetizados e controlados por agentes econômicos especializados.

Nesse sentido, o Guia deve afirmar com maior clareza que responsabilidade compartilhada não significa responsabilidade equivalente. Ou seja, cada agente deve responder de acordo com sua função técnica, seu grau de controle sobre a experiência digital, sua capacidade de mitigação de riscos e sua posição na cadeia de valor. Provedores que definem arquitetura de recomendação, publicidade, coleta de dados, comunicação entre usuários, parâmetros de visibilidade e desenho de interação possuem deveres próprios de prevenção, segurança por padrão e adaptação da experiência. A família exerce papel relevante de mediação e orientação, mas não pode ser tratada como substituta de deveres empresariais de design seguro, transparência, minimização e governança.

Essa distinção se mostra fundamental diante da assimetria informacional entre usuários, responsáveis legais e plataformas. Em muitos casos, famílias não possuem condições técnicas para compreender sistemas de recomendação, práticas de perfilamento, fluxos de dados, riscos de contato com desconhecidos ou mecanismos de indução ao engajamento. Por isso, a cadeia digital de responsabilidades deve partir da premissa de que os agentes que criam, estruturam e se beneficiam economicamente do ambiente de risco devem adotar medidas proporcionais de mitigação, independentemente da atuação posterior dos responsáveis.

A seção também deve evitar a escolha binária entre centralização em lojas de aplicativos e responsabilização exclusiva do provedor final. Um modelo adequado poderia ser o de responsabilidade em camadas. Assim, lojas de aplicativos e sistemas operacionais podem fornecer sinais de idade ou interfaces seguras, quando tecnicamente apropriado, mas o provedor da aplicação continua responsável por avaliar o risco concreto de suas funcionalidades, bem como por ajustar a experiência de acordo com a faixa etária. O sinal de idade não substitui classificação de risco, governança de conteúdo, limitação de publicidade comportamental, restrição de interação com desconhecidos, moderação adequada e mecanismos de contestação.

Esse modelo em camadas também deve considerar a realidade brasileira de dispositivos compartilhados. A aferição realizada apenas no momento de instalação, cadastro ou configuração do dispositivo pode ser insuficiente quando celulares, tablets, computadores e televisões conectadas são utilizados por diferentes membros da família. Em serviços de maior risco, o Guia deve recomendar revalidação contextual ou sinais adicionais em momentos relevantes de uso, desde que sem acúmulo indevido de dados e sem conversão da aferição em monitoramento contínuo.

A participação de terceiros especializados em aferição de idade deve ser submetida a regras estritas de proteção de dados. O uso de provedores externos não pode criar uma nova camada opaca de tratamento, concentração ou monetização de dados pessoais. Esses agentes devem estar sujeitos a deveres de transparência, segurança, limitação de finalidade, retenção mínima, auditoria independente e vedação de reutilização dos dados ou sinais para publicidade, perfilamento, treinamento de sistemas de IA, enriquecimento cadastral ou outras finalidades incompatíveis.

A cadeia de responsabilidades deve, ainda, prever articulação institucional entre ANPD, MJSP, Senacon, Conanda e demais órgãos competentes. É importante que se reafirme, sempre que possível, que a proteção de crianças e adolescentes no ambiente digital envolve proteção de dados, defesa do consumidor, classificação indicativa, direitos da criança e segurança digital. Portanto, a coordenação regulatória é imprescindível para evitar lacunas, sobreposições e incentivos à conformidade meramente formal. A ANPD, apesar de possuir papel central na definição dos parâmetros de proteção de dados, não atua sozinha na proteção dessa responsabilidade.

Nesse sentido, é importante assegurar que nenhum agente utilize a complexidade técnica do ecossistema digital como fundamento para inércia ou deslocamento da responsabilidade para as famílias. Ao contrário, essa proteção deve orientar uma distribuição funcional de obrigações, na qual cada agente responde pelas decisões que controla e pelos riscos que tem capacidade de mitigar.

Justificativa

A inclusão de uma seção específica sobre cadeia digital de responsabilidades é necessária porque a aferição de idade não se realiza de forma isolada nem depende de um único agente. A experiência digital de crianças e adolescentes é estruturada por diferentes camadas técnicas, econômicas e regulatórias, que envolvem provedores de aplicação, lojas de aplicativos, sistemas operacionais, fornecedores de tecnologia de aferição, intermediários, responsáveis legais, poder público e autoridades reguladoras. Cada um desses atores possui diferentes níveis de controle sobre o ambiente digital e, portanto, diferentes capacidades de prevenir, mitigar ou agravar riscos.

Essa seção, portanto, deve evitar que a responsabilidade compartilhada seja interpretada como diluição de responsabilidade, uma vez que a proteção de crianças e adolescentes no ambiente digital não pode ser transferida integralmente às famílias, sobretudo em ambientes projetados, monetizados e controlados por agentes econômicos especializados. Embora os responsáveis legais exerçam papel relevante de orientação e mediação, eles não possuem, em regra, capacidade técnica para compreender ou controlar sistemas de recomendação, fluxos de dados, arquitetura de publicidade, mecanismos de engajamento, padrões de interação entre usuários ou riscos de contato com desconhecidos. Por isso, a cadeia de responsabilidades deve partir da premissa de que quem desenha, opera e se beneficia economicamente do ambiente de risco deve assumir deveres proporcionais à sua capacidade de intervenção.

Também se justifica a adoção de um modelo em camadas porque a aferição de idade pode ocorrer em diferentes pontos da experiência digital. Lojas de aplicativos e sistemas operacionais podem fornecer sinais de idade ou interfaces seguras, mas isso não elimina a responsabilidade do provedor da aplicação de avaliar o risco concreto de suas funcionalidades e adaptar a experiência à faixa etária do usuário. O sinal de idade, por si só, não substitui governança de conteúdo, limitação de publicidade comportamental, moderação adequada, restrição de funcionalidades de maior risco, mecanismos de contestação e transparência qualificada.

A seção também é importante para lidar com a realidade brasileira de dispositivos compartilhados. Em muitos contextos familiares, celulares, tablets, computadores e televisões conectadas são utilizados por diferentes pessoas, o que torna insuficiente uma aferição realizada apenas no momento de instalação, cadastro ou configuração inicial do dispositivo. Em serviços de maior risco, pode ser necessário prever revalidações contextuais ou sinais adicionais em momentos relevantes de uso, desde que isso não resulte em monitoramento contínuo, coleta excessiva ou criação de bases centralizadas desnecessárias.

Por fim, a cadeia digital de responsabilidades deve prever deveres específicos para terceiros especializados em aferição de idade. A contratação desses fornecedores não pode criar uma camada opaca de tratamento de dados, nem permitir a reutilização dos sinais etários para publicidade, perfilamento, treinamento de sistemas de IA, enriquecimento cadastral ou outras finalidades incompatíveis. A responsabilização em cadeia é, portanto, condição para que a aferição de idade funcione como mecanismo efetivo de proteção, e não como nova infraestrutura de vigilância ou de deslocamento de deveres.

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

Os requisitos gerais devem ser formulados de modo a impedir respostas inadequadas, como, por exemplo, a manutenção de mecanismos frágeis de autodeclaração em contextos de risco relevante, assim como a adoção indiscriminada de soluções intrusivas baseadas em identificação civil, biometria, rastreamento comportamental ou coleta massiva de dados. É importante que a aferição de idade seja proporcional, confiável, auditável, contestável, segura e inclusiva, sempre orientada pelo melhor interesse da criança e do adolescente e pelos princípios da LGPD.

A finalidade exclusiva de proteção pode ser tratada como um requisito geral. Dados, sinais, inferências ou resultados gerados para aferição de idade não podem ser reutilizados para publicidade comportamental, recomendação personalizada, perfilamento comercial, monetização, treinamento de modelos de IA, enriquecimento cadastral, mensuração de engajamento ou compartilhamento com terceiros para finalidades incompatíveis. Nesse sentido, a aferição deve responder apenas à pergunta mínima necessária para adequar uma experiência digital à faixa etária do usuário. Sempre que possível, a resposta deve ocorrer por sinal binário ou por faixa etária ampla, e não por identificação nominal, idade exata ou documento civil.

Essa orientação dialoga com a literatura de privacy by design. Hoepman afirma que estratégias de desenho em privacidade permitem traduzir normas jurídicas abstratas

em requisitos concretos de arquitetura técnica, destacando a minimização como uma das estratégias centrais para limitar, tanto quanto possível, o tratamento de dados pessoais (Hoepman, 2014, p. 446 e 449). Aplicada à aferição de idade, essa premissa exige que o fornecedor não parta da pergunta sobre como identificar o usuário, mas sobre qual atributo etário mínimo é necessário para adequar a experiência digital ao risco identificado.

Outro requisito importante é a minimização. O Guia deve recomendar que fornecedores adotem o método menos intrusivo capaz de mitigar o risco identificado. Em ambientes de baixo risco, métodos leves podem ser suficientes quando combinados com configurações protetivas. Em contextos de alto risco, como acesso a produtos, serviços ou conteúdos proibidos para determinadas faixas etárias, métodos mais robustos podem ser exigidos, desde que acompanhados de garantias de segurança, retenção mínima, contestação e alternativas acessíveis. Proporcionalidade não deve funcionar apenas como justificativa para intensificar a verificação, mas também como limite contra coleta excessiva.

A separação funcional entre aferição de idade e identificação de identidade também se mostra um requisito necessário. A Data Privacy Brasil tem sustentado que a aferição de idade não se confunde com verificação de identidade. Essa distinção é central para evitar que uma obrigação legítima de proteção infantojuvenil seja convertida em mecanismo generalizado de identificação, rastreamento e vigilância dos usuários. O Guia deve desencorajar a exigência de CPF, documento oficial, reconhecimento facial ou identificadores persistentes como único padrão. Quando tais métodos forem utilizados, deve haver justificativa reforçada, avaliação de impacto, documentação da necessidade, limites de retenção e alternativa menos intrusiva. Ainda que determinado dado possa ser tecnicamente coletado, isso não significa que sua circulação seja apropriada para a finalidade de proteção etária. É importante que a aferição preserve o contexto específico em que se justifica: adaptar ou restringir determinada experiência em razão da idade, sem produzir identificação generalizada, rastreamento transversal ou ampliação de perfis comportamentais (Nissenbaum, 2010).

A auditabilidade também deve ser um requisito. Confiabilidade não se confunde com promessa de infalibilidade. Todo método de aferição possui margem de erro, possibilidade de burla e risco de impacto desigual. Por isso, os fornecedores devem documentar o método escolhido, o risco que pretendem mitigar, os dados tratados, a base legal, o prazo de retenção, as medidas de segurança, os testes realizados, os critérios de acurácia, as margens de erro, os procedimentos de revisão e as alternativas disponíveis. Em métodos baseados em biometria, inferência comportamental ou IA, devem ser exigidos testes por subgrupos, avaliação de vieses e auditoria independente.

Não menos importante, também tem-se a contestabilidade. Usuários não podem ser bloqueados, classificados ou submetidos a experiências restritivas sem explicação adequada e sem possibilidade de revisão. O Guia deve prever canais claros para contestação de erro, reclassificação, falha técnica, ausência de documento, divergência entre sinais ou impossibilidade de uso de determinado método. Esses mecanismos devem ser acessíveis a crianças, adolescentes e responsáveis legais, em linguagem simples, clara e adequada à idade.

O sexto requisito deve ser a inclusão. Soluções de aferição que dependam de câmera

de alta qualidade, conexão estável, documento formal, smartphone recente, cartão de crédito, reconhecimento facial ou padrões biométricos específicos podem produzir exclusão digital ou discriminação indireta. O Guia deve exigir alternativas equivalentes para usuários em contextos de vulnerabilidade, inclusive crianças e adolescentes sem documentação regular, pessoas com deficiência, usuários de dispositivos antigos, famílias de baixa renda e pessoas que compartilham dispositivos.

O sétimo requisito deve ser a segurança da informação. Bases de dados criadas para aferição de idade podem se tornar alvos de ataques e gerar riscos especialmente graves quando envolvem dados de crianças e adolescentes, documentos, biometria ou padrões de comportamento. O Guia deve recomendar retenção mínima ou inexistente sempre que possível, criptografia, segregação de bases, controle de acesso, registro de operações, descarte seguro e vedação à criação de bases centralizadas desnecessárias.

Ressalta-se, por fim, que os requisitos gerais devem afirmar que a aferição de idade não substitui outras obrigações de proteção. Aferir idade sem alterar design, recomendação, publicidade, interação, moderação, padrões de privacidade e configurações padrão pode gerar apenas conformidade formal. O mecanismo deve funcionar como gatilho para experiências mais seguras, e não como etapa isolada de coleta ou bloqueio. Nesse sentido, a aferição deve integrar uma arquitetura mais ampla de proteção desde a concepção e por padrão, compatível com o melhor interesse da criança e do adolescente.

Justificativa

Aqui, busca-se qualificar os requisitos mínimos que devem orientar a implementação dos mecanismos de aferição de idade. O objetivo é evitar duas respostas igualmente inadequadas: de um lado, a manutenção de mecanismos frágeis de autodeclaração em contextos de risco relevante; de outro, a adoção indiscriminada de soluções intrusivas baseadas em identificação civil, biometria, rastreamento comportamental ou coleta massiva de dados.

Essa preocupação dialoga com a literatura de privacy by design. Hoepman (:p. 446 e p. 449) sustenta que estratégias de desenho em privacidade permitem traduzir normas jurídicas abstratas em requisitos concretos de arquitetura técnica, destacando a minimização como uma estratégia central para limitar, tanto quanto possível, o tratamento de dados pessoais. Aplicada à aferição de idade, essa premissa exige que o fornecedor não parta da pergunta sobre como identificar o usuário, mas sobre qual atributo etário mínimo é necessário para adequar a experiência digital ao risco identificado.

Desse modo, a aferição de idade só é legítima quando preserva o contexto específico que a justifica: adaptar ou restringir determinada experiência em razão da idade. Isso significa que dados, sinais ou inferências produzidos para proteção etária não devem circular para finalidades incompatíveis, como publicidade comportamental, perfilamento comercial, recomendação personalizada, monetização ou treinamento de sistemas de IA.

Por isso, recomenda-se que o Guia trate como requisitos gerais a finalidade exclusiva de proteção, a minimização de dados, a separação entre aferição de idade e verificação

de identidade, a auditabilidade, a contestabilidade, a inclusão e a segurança da informação. Esses elementos são fundamentais para que a aferição funcione como instrumento de adequação da experiência digital, e não como mecanismo de identificação generalizada, rastreamento transversal ou exploração informacional de crianças e adolescentes.

A contribuição também reforça que a aferição de idade não substitui outras obrigações de proteção. Se o mecanismo não vier acompanhado de mudanças no desenho do serviço, nos padrões de recomendação, na publicidade, nas interações, na moderação, nas configurações de privacidade e nos canais de contestação, há risco de produção de conformidade meramente formal. Por isso, os requisitos gerais devem orientar uma arquitetura mais ampla de proteção desde a concepção e por padrão, compatível com a LGPD, com o melhor interesse e com a proteção integral de crianças e adolescentes.

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

Entendemos que a seção de Requisitos Específicos representa parâmetros previstos no ECA Digital e na LGPD para orientar a escolha e implementação de mecanismos confiáveis de aferição de idade. A proposta apresentada pela ANPD está alinhada com uma abordagem baseada em risco e corretamente evita estabelecer uma hierarquia fixa entre tecnologias, privilegiando a avaliação contextual da proporcionalidade, necessidade e efetividade das soluções. Esse enfoque dialoga diretamente com o princípio do melhor interesse de crianças e adolescentes e com a ideia de que não existe uma solução única capaz de atender todos os cenários.

Como contribuição, entendemos que o Guia poderia reforçar alguns elementos. Em primeiro lugar, recomenda-se explicitar que a escolha do mecanismo de aferição de idade deve observar, além dos princípios da LGPD, os princípios previstos no ECA Digital, especialmente o dever de proteção integral, o desenvolvimento seguro e saudável e o desenho apropriado para crianças e adolescentes (child-centred design). Isso reforça que a aferição de idade não constitui um fim em si mesmo, mas um instrumento para reduzir riscos decorrentes do ambiente digital. Em segundo lugar, seria importante fortalecer a exigência de uma avaliação prévia de proporcionalidade entre o risco apresentado pelo serviço digital e o grau de intrusão do mecanismo utilizado.

O próprio Guia reconhece que soluções biométricas exigem justificativa mais robusta e somente devem ser empregadas quando inexistirem alternativas menos invasivas capazes de produzir resultado equivalente. Nesse sentido, seria pertinente recomendar expressamente que controladores documentem essa análise comparativa como parte de sua governança, demonstrando por que determinado mecanismo foi escolhido em detrimento de opções menos invasivas. Essa abordagem encontra respaldo tanto na lógica da minimização prevista na LGPD quanto nas recomendações constantes do próprio Guia sobre avaliação de riscos.

Também sugerimos que o Guia aprofunde as orientações relativas aos Relatórios de Impacto. Embora mencione a importância do Relatório de Impacto à Proteção de Dados Pessoais (RIPD) e da avaliação de impacto prevista no ECA Digital, seria recomendável indicar que esses instrumentos não devem ser tratados como mera formalidade documental. Eles devem servir como ferramentas efetivas de identificação, mitigação e monitoramento contínuo dos riscos associados tanto ao serviço digital quanto ao

próprio mecanismo de aferição de idade, especialmente diante da rápida evolução tecnológica.

Outro aspecto que merece maior desenvolvimento diz respeito à governança dos fornecedores de soluções de aferição de idade. O Guia poderia incentivar mecanismos de auditoria independente, documentação técnica das métricas de desempenho, transparência sobre limitações dos modelos empregados e revisão periódica da acurácia, robustez e confiabilidade das soluções. Essa recomendação fortalece o princípio da responsabilização e prestação de contas previsto na LGPD e contribui para aumentar a confiança no ecossistema.

É preciso enfatizar a necessidade de monitoramento de possíveis vieses discriminatórios, sobretudo em mecanismos baseados em inteligência artificial e biometria facial. A aferição de idade automatizada pode apresentar taxas de erro distintas conforme características como idade, gênero, raça ou deficiência, produzindo exclusões injustificadas ou restrições indevidas de acesso. Dessa forma, recomenda-se que o Guia incentive avaliações periódicas de desempenho segmentadas por grupos populacionais e a adoção de medidas corretivas sempre que identificadas disparidades relevantes.

Por fim, sugerimos que o Guia estimule expressamente a adoção de tecnologias de preservação da privacidade (Privacy Enhancing Technologies - PETs), como credenciais verificáveis e provas de conhecimento zero (Zero-Knowledge Proofs), mencionadas ao longo do documento (Mendonça; Novoa; Rodrigues, 2026). Embora corretamente apresentadas como exemplos, o Guia poderia destacar que tais soluções representam boas práticas por permitirem a comprovação da faixa etária sem necessidade de compartilhamento ou armazenamento de dados pessoais adicionais, concretizando os princípios da minimização de dados, privacidade por padrão e proteção desde a concepção previstos na LGPD.

Justificativa

A seção de requisitos específicos é importante porque traduz, para a escolha concreta dos mecanismos de aferição de idade, os parâmetros gerais de proporcionalidade, confiabilidade, segurança e proteção de dados. Enquanto os requisitos gerais indicam os princípios que devem orientar qualquer solução, os requisitos específicos ajudam a definir como esses princípios devem ser aplicados conforme o risco do serviço, a finalidade da aferição e o grau de intrusão do método adotado.

A Data Privacy Brasil considera adequada a opção do Guia de não estabelecer uma hierarquia fixa entre tecnologias. A aferição de idade não comporta uma solução única, aplicável indistintamente a todos os contextos. Serviços de baixo risco podem admitir métodos menos intrusivos, combinados com configurações protetivas, supervisão parental e canais de contestação. Já ambientes de maior risco, como aqueles que envolvem produtos, conteúdos ou funcionalidades legalmente restritos, podem exigir mecanismos mais robustos, desde que acompanhados de justificativa proporcional, documentação e salvaguardas adequadas.

Nesta seção deve haver uma preocupação para que a escolha tecnológica seja feita de forma automática. Métodos como biometria, reconhecimento facial, documentos oficiais ou inferências automatizadas podem parecer mais confiáveis em abstrato, mas en-

volvem riscos relevantes de erro, discriminação, coleta excessiva, tratamento de dados sensíveis e normalização de práticas de identificação. Por isso, a contribuição recomenda que o Guia reforce a necessidade de avaliação prévia de proporcionalidade entre o risco identificado e o grau de intrusão do mecanismo adotado.

A seção também deve orientar a documentação dessa escolha. Relatórios de Impacto e avaliações de risco não devem ser tratados como formalidade, mas como instrumentos para demonstrar por que determinado método foi escolhido, quais alternativas menos intrusivas foram consideradas, quais dados serão tratados, quais riscos se pretende mitigar e quais medidas serão adotadas para reduzir erros, vieses e usos incompatíveis.

Dialogando com a contribuição acima, uma seção destinada a requisitos específicos também é relevante para incentivar soluções que protejam sem identificar excessivamente. Tecnologias de preservação da privacidade, como sinais de idade, credenciais verificáveis, APIs seguras, tokens e provas de conhecimento zero, devem ser tratadas como boas práticas quando permitirem comprovar o atributo etário sem revelar identidade civil, documento, idade exata ou outros dados pessoais desnecessários. Assim, a seção pode orientar escolhas técnicas mais seguras, proporcionais e alinhadas à lógica de minimização da LGPD.

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

O Anexo I desempenha importante função ao apresentar exemplos de mecanismos de aferição de idade e suas respectivas características. Trata-se de um instrumento relevante para facilitar a compreensão técnica dos diferentes modelos disponíveis e apoiar decisões regulatórias e empresariais.

Como contribuição, entendemos que o Anexo poderia evoluir de um quadro predominantemente descritivo para uma ferramenta mais orientativa de avaliação de riscos. Nesse sentido, sugerimos que, além da descrição técnica de cada mecanismo, sejam incluídos critérios comparativos relacionados, por exemplo, ao grau de intrusão na privacidade, ao volume de dados pessoais tratados, à utilização de dados sensíveis, ao potencial de reutilização indevida das informações, ao risco de discriminação algorítmica, à suscetibilidade a fraudes, ao nível de acurácia esperado e à maturidade tecnológica da solução.

Essa abordagem auxiliaria controladores na realização das avaliações de proporcionalidade exigidas pelo Guia. Também seria interessante incorporar exemplos práticos de aplicação conforme diferentes níveis de risco do serviço digital. Em vez de sugerir implicitamente que determinados mecanismos seriam universalmente adequados, o Anexo poderia demonstrar como soluções distintas podem ser proporcionais conforme o contexto de risco, ilustrando cenários de baixo, médio e alto risco previstos no ECA Digital.

Outro aprimoramento relevante seria incluir uma seção específica sobre tecnologias emergentes. O próprio Guia faz referência a credenciais verificáveis, provas de conhecimento zero e outras tecnologias de preservação da privacidade, mas essas soluções poderiam aparecer de forma mais estruturada no Anexo, indicando seu potencial para reduzir a coleta de dados pessoais e fortalecer a conformidade com os princípios da

LGPD. Isso contribuiria para incentivar inovação regulatória sem impor determinada tecnologia.

Recomenda-se que o Anexo apresente de forma mais explícita as limitações conhecidas de cada mecanismo. Em vez de apenas indicar suas vantagens, seria útil informar situações em que determinada tecnologia pode produzir resultados inadequados, apresentar vieses conhecidos, depender de infraestrutura específica ou exigir salvaguardas adicionais.

Esse tipo de transparência favorece escolhas mais responsáveis pelos agentes de tratamento. Por fim, sugerimos que o Anexo seja concebido como um documento vivo, sujeito à atualização periódica pela ANPD. Considerando a rápida evolução dos mecanismos de aferição de idade e das tecnologias de inteligência artificial, um processo contínuo de revisão permitirá incorporar novas evidências técnicas, boas práticas internacionais e soluções inovadoras, mantendo o Guia atualizado e alinhado ao estado da arte tecnológica sem comprometer a segurança jurídica.

Justificativa

O Anexo I é uma das partes mais operacionais do Guia. Por isso, sua utilidade depende de ele não funcionar apenas como um catálogo de métodos disponíveis, mas como um instrumento que ajude os agentes a comparar riscos, limites e salvaguardas antes de escolher uma solução de aferição de idade. Isso porque mecanismos diferentes produzem riscos muito distintos. Uma solução baseada em autodeclaração, por exemplo, pode ser insuficiente em ambientes de maior risco; já métodos baseados em documento oficial, biometria ou reconhecimento facial podem gerar coleta excessiva, tratamento de dados sensíveis, exclusão de usuários e impactos discriminatórios. Sem critérios comparativos, há o risco de que fornecedores escolham mecanismos pela facilidade de implementação, pelo custo ou pela promessa de precisão, e não pela compatibilidade entre risco, finalidade e proteção de dados.

Por isso, sugerimos que o Anexo incorpore parâmetros capazes de orientar essa decisão: grau de intrusão na privacidade, volume de dados tratados, uso de dados sensíveis, risco de reutilização indevida, possibilidade de discriminação algorítmica, dependência de infraestrutura, suscetibilidade a fraude, acurácia esperada e maturidade tecnológica. Esses critérios tornam mais concreta a avaliação de proporcionalidade exigida ao longo do Guia e ajudam a evitar que determinadas tecnologias sejam tratadas como soluções universalmente adequadas.

A inclusão de exemplos por nível de risco também contribuiria para tornar o Anexo mais útil. Em vez de apenas descrever os mecanismos, o Guia poderia indicar em quais contextos uma solução tende a ser insuficiente, excessiva ou proporcional. Essa distinção é importante porque a aferição de idade não deve ser calibrada apenas pela tecnologia disponível, mas pelo tipo de conteúdo, serviço, produto ou funcionalidade acessado, bem como pelos danos que se pretende evitar.

Também seria importante dar maior visibilidade às tecnologias de preservação da privacidade, como sinais de idade, credenciais verificáveis, APIs seguras, tokens e provas de conhecimento zero. Essas soluções dialogam com a lógica do atributo mínimo defendida pela Data Privacy Brasil, pois permitem comprovar uma faixa etária ou condição de acesso sem revelar identidade civil, documento, idade exata ou outros dados pessoais desnecessários. Como apontamos em nossa última publicação, Descomplicando o ECA Digital, sinais de idade, credenciais verificáveis e APIs seguras podem permitir que a plataforma receba apenas o atributo etário necessário, sem coletar cópia de documento, nome completo, CPF ou imagem facial quando isso não for proporcional ao risco (Data Privacy Brasil, 2026, p. 12).

Assim, recomenda-se que o Anexo seja mantido sempre atualizado e aberto a novas contribuições, pois tecnologias de aferição de idade evoluem rapidamente, e novas evidências sobre falhas, vieses, acurácia e boas práticas tendem a surgir com a implementação concreta desses mecanismos. Nesse sentido, um Anexo periodicamente atualizado permitiria à ANPD incorporar esses aprendizados sem reabrir todo o Guia, preservando segurança jurídica e mantendo o instrumento alinhado ao estado da técnica.

Apresente suas **CONTRIBUIÇÕES ADICIONAIS**

A Data Privacy Brasil recomenda que o Guia destaque, de forma transversal, que a aferição de idade deve ser compreendida como parte de uma política mais ampla de proteção de crianças e adolescentes no ambiente digital. Conforme desenvolvido no documento Descomplicando o ECA Digital: Aferição de Idade e Proteção Integral no Ambiente Digital, a idade deve ser tratada como "critério operacional de adequação da experiência no digital", capaz de orientar bloqueios, restrições, classificação indicativa, supervisão parental, desenho de funcionalidades, medidas de segurança e canais de contestação (Data Privacy Brasil, 2026, p. 5). Essa formulação é importante porque afasta tanto a autodeclaração meramente formal quanto a identificação civil generalizada como respostas padrão.

Nesse sentido, a aferição de idade não deve ser tratada como solução autônoma para todos os riscos. O próprio documento da Data Privacy Brasil ressalta que a aferição de idade, sozinha, não resolve todos os riscos e deve ser compreendida como parte de um sistema mais amplo de governança digital, articulado a avaliações de risco, relatórios de transparência e salvaguardas de direitos fundamentais (Data Privacy Brasil, 2026, p. 14). O Guia poderia explicitar essa premissa para evitar que fornecedores tratem a aferição como etapa isolada de conformidade, sem alterar efetivamente o desenho do serviço, os fluxos de recomendação, os padrões de privacidade, os mecanismos de publicidade, as funcionalidades de interação e os canais de contestação.

Reforça-se a importância de se distinguir aferição de idade, verificação de idade, sinal de idade, autodeclaração e verificação de identidade. O documento da Data Privacy Brasil enfatiza que o ECA Digital exige adequação etária, e não vigilância generalizada, de modo que a pergunta correta não é "quem é essa pessoa?", mas "qual é a informação mínima necessária para saber se esta experiência é adequada à sua idade?" (Data

Privacy Brasil, 2026, p. 21). Essa distinção deve atravessar todo o Guia, especialmente para impedir que soluções de aferição sejam convertidas em mecanismos de identificação civil obrigatória, retenção documental, cruzamento de dados ou rastreamento transversal.

Reitera-se também a vedação a usos secundários. Dados e sinais gerados em processos de aferição de idade não podem ser reaproveitados para publicidade comportamental, recomendação personalizada, perfilamento comercial, treinamento de sistemas de IA, enriquecimento cadastral, prevenção genérica à fraude, monetização ou compartilhamento com terceiros para finalidades incompatíveis. Como aponta o documento da Data Privacy Brasil, a aferição de idade não pode servir como pretexto para ampliar coleta, rastreamento ou exploração comercial de crianças e adolescentes (Data Privacy Brasil, 2026, p. 28). Seu valor regulatório está em reduzir riscos, não em ampliar a assimetria informacional entre fornecedor e usuário.

Por fim, é importante que. sempre que tecnicamente possível, o Guia priorize soluções baseadas em sinais de idade, credenciais verificáveis, APIs seguras, tokens ou mecanismos criptográficos capazes de comprovar o atributo etário sem revelar identidade civil, idade exata, histórico de navegação ou outros dados pessoais adicionais. O documento da Data Privacy Brasil registra que sinais de idade, credenciais verificáveis e APIs seguras podem permitir que a plataforma receba apenas o atributo etário necessário, sem coletar cópia de documento, nome completo, CPF, imagem facial ou outros dados excessivos quando isso não for proporcional ao risco (Data Privacy Brasil, 2026, p. 12). Essa lógica de atributo mínimo deve orientar a interpretação do Guia.

Referências

AGE CHECK CERTIFICATION SCHEME. **Age Assurance Technology Trial: Part A: Main Report.** Austrália: Age Assurance Technology Trial, 2025. Disponível em: https://www.infrastructure.gov.au/sites/default/files/documents/aatt_part_a_digital.pdf. Acesso em: 26 jun. 2026.

BARBOSA, Paola Vargas; WAGNER, Adriana. **A construção e o reconhecimento das regras familiares: a perspectiva dos adolescentes.** Psicologia em Estudo, Maringá, v. 19, n. 2, p. 235-245, abr./jun. 2014. DOI: 10.1590/1413-737222060007. Disponível em: https://www.scielo.br/j/pe/a/MjYdvsm4bQQDGzY37cPMWkm/?lang=pt. Acesso em: 24 mar. 2026.

BARBOZA, Heloisa Helena. **Vulnerabilidade e cuidado.** In: PEREIRA, Tânia da Silva; OLIVEIRA, Guilherme de (coord.). Cuidado e vulnerabilidades. São Paulo: Atlas, 2009.

BUOLAMWINI, Joy; GEBRU, Timnit. **Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification.** In: Proceedings of the 1st Conference on Fairness, Accountability and Transparency. Proceedings of Machine Learning Research, v. 81, p. 77-91, 2018.

DIAS, Lívia Ferreira. **Os direitos da criança e do adolescente em artigos acadêmicos de educação.** 2015. 142 p. Dissertação (Mestrado em Educação) – Instituto de Ciências Humanas e Sociais, Universidade Federal de Mato Grosso, Rondonópolis, 2015.

ELIAS, Roberto João. **Comentários ao estatuto da criança e do adolescente.** 4. ed. São Paulo: Saraiva, 2010.

FALCÃO, Patricia Mirella de Paulo; MILL, Daniel. **A criança e seu fascínio pelo mundo digital: o que o discurso nos revela.** Revista Tecnologia e Sociedade, Curitiba, v. 14, n. 30, p. 136-153, jan./abr. 2018. DOI: 10.3895/rts.v14n30.4615. Disponível em: https://periodicos.utfpr.edu.br/rts/article/view/4615. Acesso em: 20 mar. 2026.

FERNÁNDEZ, Jorge Flores. **Sexting, Sextorsão e Grooming.** In: ABREU, Cristiano Nabuco; EISENSTEIN, Evelyn; ESTEFENON, Susana Graciela Bruno. **Vivendo esse mundo digital: Impactos na Saúde, na Educação e nos Comportamentos Sociais.** São Paulo: Artmed, 2013. p. 72-92.

FORTES DE SÁ PIANOVSKI, M.; MARTINS DA SILVEIRA, J. **Orientação de pais on-line no tratamento do uso problemático de internet pela criança.** Acta Comportamentalia, [S. l.], v. 30, n. 3, 2022. DOI: 10.32870/ac.v30i3.83280. Disponível em: https://actacomportamentalia.cucba.udg.mx/index.php/acom/article/view/83280. Acesso em: 20 mar. 2026.

FREITAS, Maria Luiza de Moura de Mello. **O princípio constitucional da proteção integral da criança e do adolescente e o papel do juiz no âmbito jurídico social.** Revista Ibero-Americana de Humanidades, Ciências e Educação, São Paulo, v. 10, n. 5, p. 2144-2163, maio 2024. DOI: https://doi.org/10.51891/rease.v10i5.14000. Disponível em: https://periodicorease.pro.br/rease/article/view/14000. Acesso em: 22 mar. 2026.

FREITAS, Nivaldo Alexandre de; DIAS, Lívia Ferreira. **Apontamentos sobre proteção e liberdade de crianças e adolescentes quanto ao uso da internet.** Reflexão e Ação, Santa Cruz do Sul, v. 28, n. 2, p. 263-275, maio/ago. 2020. DOI: https://doi.org/10.17058/rea.v28i2.12303. Disponível em: https://online.unisc.br/seer/index.php/reflex/article/view/12303. Acesso em: 22 mar. 2026.

HOEPMAN, Jaap-Henk. **Privacy design strategies.** In: ICT Systems Security and Privacy Protection. 2014. p. 446-459.

LIMA, Taísa Maria Macena de; SÁ, Maria de Fátima Freire de. **Ensaio sobre a infância e a adolescência.** 2. ed. Belo Horizonte: Arraes Editores, 2019.

LOPES, Claudia Aparecida Costa; CARDIN, Valéria Silva Galdino. **A responsabilidade civil pelo consentimento parental contrário ao melhor interesse e aos direitos personalíssimos da criança na Lei Geral de Proteção de Dados.** Revista IBERC, Belo Horizonte, v. 6, n. 1, p. 83-97, jan./abr. 2023. DOI: https://doi.org/10.37963/iberc.v6i1.244. Disponível em: https://revista.iberc.org.br/iberc/article/view/244. Acesso em: 22 mar. 2026.

MENDONÇA, Eduardo; NOVOA, Natasha; RODRIGUES, Carla. **Descomplicando o ECA Digital: aferição de idade e proteção integral no ambiente digital.** São Paulo: Data Privacy Brasil, maio 2026. E-book. Disponível em: https://www.dataprivacybr.org/documentos/descomplicando-o-eca-digital-afericao-de-idade/. Acesso em: 26 jun. 2026.

NÓVOA, Natasha; MENDONÇA, Eduardo; RODRIGUES, Carla; ZANATTA, Rafael. **Contribuições da Data Privacy Brasil para a tomada de subsídios sobre o guia orientativo "Mecanismos de Aferição de Idade".** São Paulo: Data Privacy Brasil, 2026.

OLIVEIRA, Jéssica Patrícia Dutra de; ISHITANI, Lucila. **Design Sensível a Valores na Computação: um Mapeamento Sistemático de Literatura.** Abakós, Belo Horizonte, v. 10, n. 2, p. 26-56, nov. 2022. DOI: https://doi.org/10.5752/P.2316-9451.2022v-10n2p26-56. Disponível em: https://periodicos.pucminas.br/abakos/article/view/27836. Acesso em: 24 mar. 2026.

PADILHA, Elisangela. **Novas estruturas familiares: por uma intervenção mínima do estado.** Rio de Janeiro: Lumen Juris, 2017.

PUNYANI, Prachi; GUPTA, Rashmi; KUMAR, Ashwani. **Neural networks for facial age estimation: a survey on recent advances.** Artificial Intelligence Review, v. 53, n. 5, p. 3299-3347, 2020. DOI: 10.1007/s10462-019-09765-w.

ROSSATO, Luciano Alves; LÉPORE, Paulo Eduardo; SANCHES, Rogério Cunha. **Estatuto da Criança e do Adolescente comentado.** São Paulo: Revista dos Tribunais, 2010.

SCHWARTZ, Fernanda Tabasnik; PACHECO, Janaína Thais Barbosa. **Mediação parental na exposição às redes sociais e a internet de crianças e adolescentes.** Estudos e Pesquisas em Psicologia, Rio de Janeiro, v. 21, n. 1, p. 217-235, jan./abr. 2021. DOI: https://doi.org/10.12957/epp.2021.59383. Disponível em: https://www.e-publicacoes.uerj.br/revispsi/article/view/59383. Acesso em: 24 mar. 2026.

SOUZA, Ana Carolina dos Santos. **A Lei Geral de Proteção dos Dados Pessoais e seus Efeitos em Relação à Proteção Especial Destinada às Crianças e aos Adolescentes na Internet.** VirtuaJus, Belo Horizonte, v. 5, n. 8, p. 540-561, 1. sem. 2020. DOI: https://doi.org/10.5752/P.1678-3425.2020v5n8p540-561. Disponível em: https://periodicos.pucminas.br/virtuajus/article/view/24272. Acesso em: 23 mar. 2026.