Novembro de 2025

Internet Society - Capítulo Brasil

Contribuição da ISOC-Br à Consulta Pública do Ministério da Justiça e Segurança Pública: Aferição de Idade na Internet Brasileira

Internet Society
Capítulo Brasil

Contribuição da ISOC-BR à Consulta Pública do Ministério da Justiça e Segurança Pública: Aferição de Idade na Internet Brasileira

Autores

Gabriela Amâncio Vieira da Paz

Danielle Novaes de Siqueira Valverde

Thobias Prado Moura

Nathan Paschoalini

Milena Cramar Lôndero

Laura Pereira

Revisores

Flávio Rech Wagner

Pedro de Perdigão Lana

Diretoria Executiva

Flavio Rech Wagner

Pedro de Perdigão Lana

André Lucas Fernandes

Thobias Prado Moura

Laura Gabrieli Pereira da Silva

1. INTRODUÇÃO

A ISOC Brasil parabeniza o Ministério da Justiça e Segurança Pública (MJSP) e a Secretaria Nacional de Direitos Digitais (SEDIGI) pela abertura da Consulta Pública sobre Aferição de Idade na Internet, etapa essencial para a construção participativa de regulação do Estatuto Digital da Criança e do Adolescente (Lei nº 15.211/2025)

Reconhecendo a relevância e a urgência do tema, a ISOC Brasil apresenta esta contribuição com base em sua missão institucional de promoção de uma Internet aberta, segura, confiável, interoperável e globalmente conectada. O objetivo é oferecer subsídios técnicos e normativos que apoiem o desenvolvimento de políticas públicas eficazes, proporcionais e compatíveis com os princípios da governança multissetorial da Internet.

A aferição de idade constitui um dos temas mais desafiadores no campo das políticas digitais contemporâneas, por exigir o equilíbrio entre proteção e inclusão, privacidade e segurança, autonomia e responsabilidade. As reflexões reunidas nesta contribuição estão ancoradas em evidências empíricas, boas práticas internacionais e princípios técnicos e normativos que orientam a governança da Internet, reafirmando o compromisso da ISOC com a construção de um ambiente digital que una segurança, confiança e liberdade de acesso.

2. APRESENTAÇÃO INSTITUCIONAL

A **ISOC (Internet Society)** é uma associação sem fins lucrativos, criada em 1992, com atuação internacional, que tem por objetivo promover liderança no desenvolvimento dos padrões da Internet, bem como fomentar iniciativas educacionais e políticas públicas ligadas à rede mundial de computadores. Para tanto, propicia a interação com governos, empresas e entidades em geral para adoção de políticas em relação à Internet que estejam de acordo com seus princípios: uma rede aberta, segura, confiável, interoperável e universalmente acessível, dando apoio à inovação, à criatividade e às oportunidades comerciais. A ISOC, por exemplo, oferece amparo financeiro e institucional para o IETF (*Internet Engineering Task Force*), responsável pelo desenvolvimento e discussão das diretrizes de funcionamento e padrões da Internet. A instituição possui mais de 120 escritórios locais (capítulos), e mais de 100 mil membros individuais e organizacionais espalhados pelo mundo.

A **ISOC Brasil** é o capítulo brasileiro da Internet Society, contando com 1200 membros ativos, espalhados por todo o país. Os membros da ISOC Brasil provêm de diversas comunidades: comunidade técnica envolvida no desenvolvimento tecnológico da Internet e na sua operação; comunidade empresarial envolvida na infraestrutura e na operação da Internet (como provedores de acesso) e no desenvolvimento de conteúdos (como empresas de mídia e de aplicações); comunidades acadêmicas de diferentes áreas que desenvolvem pesquisas sobre o desenvolvimento e uso da Internet e seus impactos sociais e econômicos; e organizações da sociedade civil que se preocupam com os impactos sociais e econômicos do desenvolvimento e uso da Internet e tecnologias associadas. A ISOC Brasil é o veículo que traz para a sociedade brasileira a promoção e a discussão dos princípios defendidos pela Internet Society, assim como de suas ações e seus posicionamentos.

Esta contribuição à Consulta Pública é resultado de um trabalho coletivo, conduzido por três dos Grupos de Trabalho da ISOC Brasil. Nesse sentido, participaram da elaboração deste documento o **Grupo de Trabalho de Responsabilidade de Intermediários (GT-RI)**, cujo enfoque está relacionado aos modelos de responsabilidade de provedores, incluindo regulação de plataformas digitais; o **Grupo de Trabalho de Conectividade Significativa e Redes Comunitárias**, que atua no grande campo da inclusão digital, com enfoque na noção de conectividade significativa; e o **Grupo de Trabalho de Criptografia**.

3. QUESTIONÁRIO

5. Por que adotar a aferição de idade?

A aferição de idade pode desempenhar um papel relevante para viabilizar proteções legais e técnicas voltadas a crianças e adolescentes no ambiente digital, garantindo que produtos e serviços de tecnologia ajustem suas funcionalidades, interfaces e práticas de coleta de dados conforme a faixa etária do usuário. Sem algum nível de aferição, instrumentos como *safety by design*, classificação indicativa e mediação parental não têm exequibilidade prática, pois dependem de uma referência técnica que permita aplicar as salvaguardas previstas em lei.

A adoção, contudo, deve ter finalidade de proteção, e não de controle. O *European Data Protection Board (EDPB)* orienta que os mecanismos de aferição limitem-se à comprovação do atributo etário estritamente necessário, sem recorrer à identificação civil do usuário, enquanto o *Office of the Privacy Commissioner* do Canadá recomenda que tais mecanismos sejam precedidos de avaliação de impacto e privilegiem métodos que minimizem a exposição de dados pessoais. Essas diretrizes convergem na defesa de um modelo de aferição efetivo, proporcional e respeitoso à privacidade, capaz de proteger crianças e adolescentes sem introduzir riscos adicionais à liberdade e privacidade dos demais usuários.

Sob essa ótica, a aferição de idade é fundamental porque viabiliza a aplicação prática das normas de proteção e estimula maior transparência e responsabilização, em conformidade ao que recomenda o princípio 8 do Decálogo de Recomendações sobre o Modelo Brasileiro de Responsabilidade de Intermediários da ISOC Brasil, doravante referido como **Decálogo da ISOC Brasil**. Ao permitir que provedores ajustem design, publicidade e funcionalidades de acordo com a faixa etária e ao exigir mecanismos

auditáveis de conformidade, a aferição fortalece a governança e torna operacionais as salvaguardas legais destinadas à proteção infantojuvenil.

Entretanto, nem toda situação justifica a adoção de mecanismos formais de aferição etária. Em serviços de baixo risco ou em níveis técnicos que apenas transportam ou armazenam dados — como provedores de rede e serviços de DNS — a exigência perde relação com o risco que se pretende mitigar. Nesses contextos, a verificação deixa de cumprir função protetiva e se converte em uma medida desproporcional, que amplia o tratamento de dados e impõe encargos a agentes sem vínculo direto com o conteúdo ou com a interação do usuário. A ISOC Brasil adverte que, deslocar a aferição para a infraestrutura, violaria a separação das camadas da Internet e comprometeria princípios essenciais como neutralidade, interoperabilidade e descentralização, ao misturar funções de transporte e aplicação e criar pontos únicos de controle e vulnerabilidade, contrariando também o **princípio 2 do Decálogo da ISOC Brasil** .

A missão da **Internet Society** é promover o desenvolvimento de uma Internet aberta, globalmente conectada, segura e confiável, sustentada por princípios técnicos e sociais que garantam sua integridade e resiliência. Nesse contexto, compreendemos que qualquer **política de aferição de idade deve preservar as propriedades fundamentais da rede, como a separação das camadas, a interoperabilidade e a ausência de pontos únicos de controle, evitando a introdução de mecanismos que imponham identificação compulsória, rastreamento ou coleta excessiva de dados**. A ISOC Brasil entende ainda que a proteção de crianças e adolescentes no ambiente digital é um objetivo legítimo e necessário, mas que deve ser alcançado por meios que não comprometam a privacidade, a liberdade de expressão e o caráter aberto da Internet.

No mesmo sentido, o caso Free Speech Coalition v. Ken Paxton (US Supreme Court) demonstra que as exigências legais de verificação obrigatória podem gerar

falsos sentimentos de segurança, criar barreiras de acesso, produzir exclusão digital e impor riscos significativos a usuários de todas as idades. Tecnologias hoje ofertadas (documentos governamentais, cartões de crédito, biometria, bases de dados, inferência comportamental) são falhas, suscetíveis a contorno por menores e discriminatórias contra quem não possui documentação ou meios tecnológicos, introduzindo novas vulnerabilidades à infraestrutura e à experiência cotidiana na Internet.

Por essa razão, a aferição de idade deve ser adotada apenas onde o risco concreto a justifique, como parte de uma estratégia de mitigação e não como um mecanismo universal de controle. A **Organização para a Cooperação e o Desenvolvimento Econômico** (OCDE) reforça esse entendimento ao recomendar que políticas de aferição sejam proporcionais ao risco, adequadas ao contexto e compatíveis com a proteção da privacidade, evitando abordagens generalizadas ou excessivamente intrusivas. No relatório *Towards Digital Safety by Design for Children*, a OCDE enfatiza que a eficácia dessas medidas depende de um equilíbrio entre precisão, usabilidade e minimização de dados, ajustado ao nível de risco e ao propósito do serviço. Além disso, também entendemos que ela deve ser **tecnicamente neutra**, **proporcional ao risco** e **implementada de forma a não comprometer a arquitetura aberta e a natureza interoperável da Internet**. Nesse sentido, acreditamos que iniciativas como esta consulta pública e a participação multissetorial são decisivas para o enfrentamento desse desafio.

Em resumo, a aferição de idade deve:

- ser adotada para tornar efetivas as proteções, especialmente de crianças e adolescentes no ambiente virtual;
- operacionalizar a aplicação de salvaguardas e não restringir o acesso por *default*;

- limitar sua finalidade à proteção legítima, não incorrendo em vigilância excessiva;
- ser aplicada de forma proporcional ao risco;
- ser precedida de avaliações de impacto e risco ao titular de dados pessoais;
- ser compatível com os princípios que sustentam uma Internet segura, plural e confiável.

6. Quais os princípios da aferição de idade?

A aferição de idade deve ser guiada por um conjunto de princípios que assegurem a proteção integral de crianças e adolescentes sem comprometer a proporcionalidade, a privacidade e o funcionamento estável da Internet. Esses princípios articulam fundamentos constitucionais, da Lei 15.211/2025 (ECA Digital), da Lei 13.709/2018 (Lei Geral de Proteção de Dados - LGPD) e dos marcos brasileiros de governança digital, além de refletirem boas práticas internacionais.

O **melhor interesse da criança e do adolescente** é o princípio estruturante da aferição de idade. Ele exige que políticas e sistemas digitais reconheçam as múltiplas infâncias com diferentes níveis de maturidade, letramento digital e contextos familiares e sociais — evitando soluções padronizadas (*one size fits all*) que possam gerar exclusão. Inspirada na abordagem de design centrado na criança (*child-centred design*) defendida pela OCDE, essa perspectiva orienta a criação de experiências digitais seguras, acessíveis e inclusivas, garantindo que a aferição etária sirva à promoção de direitos, e não à exclusão digital.

O segundo é o **princípio da proporcionalidade** ao risco, que deve orientar tanto a implementação atual quanto a regulação futura da aferição de idade. Ele impõe que a robustez técnica e as obrigações legais variem conforme o tipo de serviço e o potencial de dano, estabelecendo uma lógica de regulação baseada em risco. Essa proporcionalidade garante equilíbrio entre proteção e inovação e deve

evitar abordagens excessivas que comprometam a privacidade ou criem barreiras de acesso. Esse princípio, ao mesmo tempo, também é consistente com **a ideia de assimetria regulatória**, na qual políticas eficazes devem reconhecer as diferenças de porte, papel e capacidade técnica entre agentes, calibrando as obrigações de modo proporcional ao risco e à função exercida. Ignorar essas diferenças gera desproporcionalidade e incentiva a concentração, o que reduz a diversidade e a inovação no ecossistema digital.

O terceiro grupo de princípios decorre da **LGPD**, que orienta o tratamento de dados pela **finalidade, adequação e necessidade** (art. 6º, I–III). Isso significa que a coleta deve se limitar à comprovação do atributo etário, devendo cessar e resultar na eliminação dos dados após o cumprimento da finalidade. A Lei nº 15.211/2025 reforça essa regra ao proibir o uso secundário das informações — como publicidade, perfilamento ou aprendizado de máquina — e o compartilhamento automatizado com terceiros. Esses princípios se completam pelos de **segurança, prevenção e responsabilização** (art. 6º, VII–X), que exigem sistemas auditáveis, compreensíveis e supervisionáveis, garantindo transparência, prestação de contas e confiança pública. Nesse sentido, as tecnologias de aferição de idade devem ser avaliadas de forma independente, proporcionando a compreensão de como as informações são coletadas e como são processadas as interações e/ou compartilhamentos com os sistemas aplicativos, atestando também a ausência de vínculos entre essas instâncias.

Portanto, a **minimização da coleta de dados** é decorrência direta da necessidade, de forma que a aferição de idade deve restringir o tratamento ao atributo etário necessário, sem coletar ou reter elementos que permitam identificar o usuário, exigindo soluções tecnicamente capazes de reduzir a exposição de dados, inclusive por meio de técnicas criptográficas como provas de conhecimento zero, que permitem comprovar a idade sem revelar identidade, preservando a privacidade,

prevenindo usos secundários e evitando que mecanismos de proteção se convertam em vetores de vigilância ou exclusão.

Para além disso, a aferição de idade deve respeitar o **princípio da funcionalidade, segurança e estabilidade da Internet**, previsto nos **Princípios para a Governança e Uso da Internet no Brasil** (CGI.br), bem como no **princípio 2 do Decálogo da ISOC Brasil**. Isso implica preservar o funcionamento global, seguro e interoperável da rede, adotando medidas compatíveis com padrões técnicos internacionais e com as boas práticas de segurança. Qualquer tentativa de deslocar funções de controle para camadas técnicas — como provedores de rede, DNS ou sistemas operacionais — comprometeria essa estabilidade, criando pontos únicos de verificação e vulnerabilidade e contrariando a arquitetura aberta que sustenta a Internet.

Por fim, **garantir a acessibilidade a todos os usuários** também deve ser um princípio a ser observado. Idade, cor, raça, habilidades digitais e outras características não podem ser fatores que limitem a capacidade do usuário para concluir a etapa de verificação de idade e acessar o conteúdo desejado. As tecnologias de garantia de idade devem ser pensadas quanto ao seu impacto no acesso universal, fornecendo, inclusive, alternativas para que todos consigam ter possibilidade de uso dos serviços ou aplicativos. **Quando tecnologias obrigatórias são inacessíveis, a Internet se torna menos aberta, afetando, particularmente, populações mais idosas e vulneráveis**. Somado a isso, destaca-se que a noção de acessibilidade está ancorada não somente na possibilidade de acesso às tecnologias da informação e comunicação, mas também na capacidade do usuário saber manuseá-las; significa dizer que o princípio da acessibilidade deve servir ao propósito de garantir ao usuário as ferramentas necessárias para que seu acesso aconteça de forma plena.

7. Em que momento deve-se realizar a aferição de idade?

O momento da aferição de idade deve ser definido de forma **proporcional ao risco e adequado ao contexto de uso**, acompanhando o ciclo de interação do usuário com o serviço digital. O objetivo é garantir que a proteção ocorra no ponto em que o risco se manifesta, e não de forma generalizada ou redundante.

Em serviços cujo desenho envolve risco evidente ou restrições etárias claras, a aferição pode anteceder o acesso, desde que implementada na camada de aplicação e de forma minimamente intrusiva, sem criar identificação persistente ou dependência de dados sensíveis. Essa camada inicial responde ao princípio da precaução e reduz a exposição a riscos previsíveis, devendo ser considerada em serviços com potencial significativo de interação pública, coleta de dados pessoais ou exposição a conteúdo impróprio.

Em contextos dinâmicos, em que o risco se manifesta apenas em determinadas funcionalidades ou interações, **a aferição pode ocorrer durante o uso**, sempre de maneira pontual e limitada à finalidade, evitando mecanismos contínuos de monitoramento. Nesses casos, a aferição periódica tem o papel de reforçar o controle sobre a exposição a conteúdos e interações específicos, permitindo respostas proporcionais a riscos concretos, como o contato com desconhecidos ou a exploração comercial de dados de menores.

Por fim, para o acesso a conteúdo legalmente restrito a maiores de 18 anos, a lei determina que a aferição ocorra a cada acesso, de modo a garantir a aplicação da barreira protetiva no ponto de maior risco. Essa exigência se justifica pelo cenário nacional, onde é recorrente o **uso compartilhado de dispositivos**, no qual uma autenticação única seria insuficiente para proteger crianças e adolescentes de conteúdos de alto risco. Ainda assim, essa solução deve ser implementada com

atenção aos impactos sobre a privacidade e segurança dos adultos, pois a verificação reiterada amplia o volume de dados tratados e cria vetores de rastreamento.

Além disso, é importante tomar nota que, em qualquer cenário, a aferição deve ser temporária, não gerar vinculação entre serviços e preservar a privacidade e a arquitetura aberta da Internet, para que não haja riscos de reidentificação ou mesmo expansão indevida de finalidade na coleta destes dados.

O desafio, portanto, não é só definir o momento da aferição, mas garantir que a aplicação da regra legal seja acompanhada de salvaguardas proporcionais, com limitação da coleta, auditoria técnica e avaliações de impacto à proteção de dados.

8. Quais as formas de realizar aferição de idade?

As formas de aferição de idade **variam conforme o tipo de serviço, o contexto de uso e o nível de risco envolvido**. De acordo com o padrão ISO/IEC 27566, essas abordagens se dividem, em linhas gerais, entre verificação, estimativa e inferência, que diferem pelo grau de precisão e pela quantidade de dados exigida. Nenhum desses métodos é universalmente aplicável: a escolha deve resultar de uma avaliação técnica e regulatória contextualizada, capaz de equilibrar eficácia, privacidade e proporcionalidade.

A declaração conjunta de autoridades de proteção de dados sobre aferição de idade e segurança online (Joint Statement on Age Assurance and Online Safety, 2024) reforça que esses mecanismos devem ser implementados em conformidade com as normas de proteção de dados, de forma baseada em risco e proporcional, reduzindo o potencial de dano aos usuários e, particularmente, às crianças. O documento também estabelece que qualquer mecanismo adotado deve servir ao melhor interesse da criança, sem comprometer o direito fundamental de todos os usuários de acessar informações na Internet (Princípio #3). Essa dupla exigência — proteção sem exclusão — traduz a essência da proporcionalidade regulatória.

Além da multiplicidade de métodos existentes e de suas diferentes combinações possíveis, é válido ressaltar que aqueles que dependem da coleta ou retenção de documentos, biometria ou bases centralizadas de identidade ampliam a superfície de ataque e são particularmente arriscados em contextos marcados por recorrentes incidentes de vazamento de dados. Nesses casos, tecnologias baseadas em credenciais verificáveis e provas de conhecimento zero surgem como alternativas compatíveis com a proteção integral prevista na LGPD, pois permitem comprovar atributos etários sem revelar identidade ou gerar rastreamento. Tais soluções reduzem riscos sistêmicos, dificultam a reidentificação e impedem usos secundários incompatíveis com a finalidade original, como treinamento de modelos de IA ou enriquecimento de perfis comerciais.

Nesse sentido, as formas de aferição devem também operar de modo não discriminatório, garantindo que pessoas sem documentos brasileiros, migrantes, refugiados, usuários com baixo letramento digital ou com dispositivos limitados possam cumprir as exigências legais sem sofrer barreiras indevidas. Esse cuidado reforça a necessidade de múltiplas vias de verificação equivalentes, evitando dependência de tecnologias de alto custo, dispositivos específicos ou procedimentos que pressuponham conectividade estável e equipamentos de maior desempenho. Métodos baseados exclusivamente em biometria ou análise facial, além de apresentarem vieses e maior propensão a erros, podem excluir usuários com características físicas diversas ou com equipamentos sem capacidade técnica adequada.

A aferição de idade, portanto, não é uma solução única nem universal. A regulação deve incentivar avaliações de risco prévias que definam o método mais adequado a cada contexto, levando em conta a natureza do serviço, a interação com o usuário e o potencial de dano. Esse enfoque evita que se imponham obrigações uniformes sobre agentes desiguais, reconhecendo as assimetrias estruturais do

ecossistema digital e permitindo respostas proporcionais à escala e à função de cada ator, em conformidade com o **princípio 4 do Decálogo da ISOC Brasil**. Além disso, a declaração conjunta das autoridades de proteção de dados sublinha que a aferição de idade deve ser entendida como uma ferramenta técnica potencial, mas não a única (Princípio 11). Medidas complementares — como educação digital, campanhas de conscientização, filtros parentais e adoção de princípios de proteção de dados desde a concepção e por padrão (*privacy by design*) — podem atuar conjuntamente para fortalecer a segurança online sem ampliar a vigilância ou a coleta de dados.

Nesse sentido, políticas prescritivas e tecnicamente rígidas, que impõem um modelo único de verificação de idade, tendem a concentrar poder técnico, fragilizar a arquitetura aberta da Internet e gerar riscos de vigilância sistêmica. A aferição deve, portanto, limitar-se à verificação de atributos necessários e ocorrer de forma minimamente invasiva, interoperável e auditável, preservando a confiança pública e a neutralidade da rede.

9. O que o setor empresarial expressou sobre a aferição de idade?

XXX

10. Quais os principais desafios identificados no cenário brasileiro?

A construção de um sistema de aferição de idade no Brasil exige enfrentar desafios estruturais que ultrapassam o campo técnico. **O país combina alto grau de fragilidade na proteção de dados, baixo índice de letramento digital e forte desigualdade no acesso a dispositivos e conexões**, o que impõe limites concretos à adoção de soluções sofisticadas sem comprometer a inclusão.

O país ocupa a sétima posição global em vazamentos de dados (Valor Econômico, 2025), cenário que reforça a necessidade de cautela com modelos que centralizem informações sensíveis ou dependam de verificações biométricas e

documentais. Em contextos de infraestrutura precária, tais métodos ampliam a superfície de ataque e expõem cidadãos a riscos de *spoofing*, injeção de código e sequestro de identidade digital, agravando um quadro de confiança já frágil.

Também merece atenção o fato de que mecanismos de aferição de idade podem inadvertidamente ampliar riscos de vigilância e fragilidades de segurança cibernética caso se apoiem em modelos centralizados de identificação, em autenticações contínuas ou em bases unificadas de atributos sensíveis. Soluções desse tipo podem gerar efeitos sistêmicos, ao introduzir pontos únicos de falha e possibilitar usos secundários incompatíveis com a finalidade original. Esses riscos reforçam a necessidade de abordagens descentralizadas, baseadas em minimização e comprovação criptográfica de atributos, que reduzam a exposição de dados e impeçam que a aferição etária se transforme em peça de infraestrutura para vigilância ou controle indevidos.

O desafio da inclusão digital também é central. Soluções baseadas em autenticações biométricas, dispositivos de alto desempenho ou conectividade contínua tendem a acentuar desigualdades, especialmente em um país no qual apenas **30% da população possui habilidades digitais básicas**, segundo pesquisa encomendada pela Anatel (2024). O baixo índice de letramento digital aumenta o risco de exclusão e a má compreensão dos processos de autenticação, sobretudo entre famílias de baixa renda. Além disso, tecnologias de verificação que dependem de câmeras, conexão estável ou documentos digitais podem excluir grupos vulneráveis — como idosos, pessoas com deficiência, populações rurais e comunidades indígenas e quilombolas — tornando a Internet menos aberta e menos equitativa.

A confiança pública, como reconhece o próprio texto em consulta, é outro ponto decisivo. Mesmo mecanismos concebidos para proteger podem gerar resistência e perda de legitimidade social quando não são percebidos como seguros

ou transparentes. **A ISOC Brasil reforça que nenhuma verificação deve comprometer a acessibilidade universal**: os usuários devem dispor de múltiplas opções de aferição, proporcionais ao risco e compatíveis com diferentes níveis de letramento, dispositivos e recursos tecnológicos. A proteção não pode se transformar em barreira de acesso. Nesse sentido, políticas de aferição de idade devem ser acompanhadas de **estratégias amplas de educação digital e alfabetização midiática**, voltadas à formação crítica e autônoma de crianças, adolescentes e famílias no uso da Internet. Isso inclui compreender riscos, reconhecer práticas seguras, avaliar informações e exercer escolhas responsáveis em ambientes digitais.

Por isso, o desafio brasileiro não é apenas técnico, mas também de governança e confiança pública. Proteger jovens na Internet, e não da Internet, significa combinar mecanismos técnicos proporcionais com o desenvolvimento de competências sociais, educativas e digitais que promovam autonomia, cidadania e segurança.

11. Como garantir que os métodos de verificação de idade adotados por produtos e serviços de TI sejam proporcionais aos riscos à saúde, à integridade física e psicológica e aos direitos de crianças e adolescentes?

A proporcionalidade dos métodos de verificação de idade depende de avaliações prévias de risco que considerem a natureza do serviço, o tipo de interação oferecida, o potencial de dano e o impacto que a aferição pode gerar sobre os direitos de todos os usuários. Essa proporcionalidade não pode ser inferida apenas pela escolha de uma tecnologia específica, mas pela combinação entre desenho de produto, salvaguardas de proteção de dados e mecanismos complementares de segurança infantil. Assim, métodos mais robustos devem ser reservados a contextos de risco elevado, enquanto serviços de baixo risco devem adotar soluções menos intrusivas, evitando a coleta excessiva de dados ou práticas que produzam identificação persistente.

A aplicação desse critério exige, antes de tudo, avaliações de impacto e modelos de risco que identifiquem de maneira clara qual problema a verificação de idade pretende mitigar e quais potenciais efeitos adversos ela pode produzir, inclusive para adultos. Conforme previamente dito, verificações obrigatórias e desproporcionais tendem a gerar falsa sensação de proteção, ampliar riscos de vigilância, criar barreiras de acesso e fragilizar a arquitetura da Internet. Por isso, a proporcionalidade deve ser entendida como equilíbrio entre eficácia, privacidade e segurança, de modo que o método adotado nunca introduza riscos superiores aos que pretende mitigar.

Outro elemento essencial é a adoção de soluções que reduzam estruturalmente a exposição de dados, privilegiando mecanismos que comprovem atributos etários sem revelar identidade, biometria ou documentos. A proporcionalidade, nesse sentido, não se reduz à precisão técnica do método, mas à sua capacidade de proteger crianças sem ampliar riscos de reidentificação, exclusão ou coleta indevida de dados sensíveis. Métodos excessivamente invasivos - como biometria contínua ou vinculação a bases centralizadas de identidade - não atendem a esse critério, pois ampliam a superfície de ataque e elevam riscos de danos psicológicos, físicos e sociais decorrentes de vazamento ou mau uso dessas informações.

Por fim, **a proporcionalidade depende também da adoção de salvaguardas complementares que ultrapassam a verificação de idade, tais como**: (i) design seguro, (ii) moderação proporcional ao risco, (iii) controles parentais efetivos, (iv) políticas claras de privacidade, (v) mecanismos de denúncia, (vi) literacia digital e (vii) conectividade. A verificação, isoladamente, não garante proteção à saúde mental ou à integridade física; ela apenas permite ativar salvaguardas que precisam estar desenhadas, implementadas e continuamente avaliadas.

12. Quais métodos de verificação de idade apresentam melhor equilíbrio entre eficácia e proteção de dados pessoais, especialmente considerando o público infantojuvenil?

Este é um debate que vem sendo realizado no âmbito da Internet Society, que está em processo de elaboração de um documento orientativo sobre o tema, sob uma ótica internacional. O debate em curso reconhece que todos os métodos disponíveis apresentam *trade-offs* entre precisão, invasividade, privacidade e acessibilidade, devendo-se priorizar sempre os métodos menos invasivos e compatíveis com o nível de risco. Contudo, não há um método único que, em abstrato, apresente o "melhor" equilíbrio entre eficácia e proteção de dados; esse equilíbrio depende do contexto de uso, do nível de risco e das salvaguardas de privacidade que acompanham a solução. Nesse contexto, soluções baseadas em credenciais verificáveis e provas criptográficas de conhecimento zero (Zero-Knowledge Proofs) sugerem caminhos promissores, pois permitem comprovar apenas o atributo etário necessário, sem revelar a identidade do usuário nem vincular seu acesso a diferentes serviços.

Esse tipo de abordagem, quando combinado com os princípios de finalidade, necessidade e segurança previstos na LGPD, oferece um caminho mais compatível com a proteção do público infantojuvenil, pois viabiliza a aplicação de salvaguardas etárias sem transformar crianças e adolescentes em alvos permanentes de coleta de dados. Ao mesmo tempo, preserva a possibilidade de múltiplas implementações técnicas, permitindo que diferentes serviços adotem soluções interoperáveis, auditáveis e proporcionais ao risco, em vez de depender de um único repositório nacional de identidade ou de verificações biométricas contínuas.

Em contraste, métodos que exigem upload de documentos oficiais, autenticação por cartão de crédito, consulta a grandes bases de dados de terceiros ou reconhecimento facial sistemático tendem a oferecer pior equilíbrio entre eficácia

e proteção de dados, pois podem ser contornados por menores, discriminam quem não possui tais recursos e ampliam significativamente o risco de vazamentos, reidentificação e usos secundários indevidos, como treinamento de modelos de IA ou perfilamento comercial.

Outros princípios em debate na Internet Society incluem: a necessidade de avaliação independente e relatórios públicos sobre práticas de coleta e armazenamento de dados; a oferta de múltiplas opções de verificação, de modo a contemplar diferentes realidades de acesso, dispositivos e níveis de alfabetização digital; e a garantia de acessibilidade universal, para que nenhum grupo seja excluído por ausência de documentos, deficiência ou restrição tecnológica.

Por fim, nos parece fundamental evitar a aplicação de controles em nível de infraestrutura, preservando a separação das camadas técnicas e os princípios de interoperabilidade e neutralidade que sustentam a Internet, de forma a compreender assim que a aferição de idade deve ocorrer em camadas de aplicação, de forma descentralizada e sujeita a auditorias independentes.

Há consenso, ainda, sobre a importância de métodos interoperáveis, auditáveis e baseados em padrões abertos, que conciliem eficácia e proteção da privacidade. Tecnologias de credenciais verificáveis e provas criptográficas de conhecimento zero (*Zero-Knowledge Proofs*) são apontadas como instrumentos promissores, pois permitem comprovar atributos etários sem expor dados pessoais desnecessários.

Outra preocupação nesse sentido, embora para além da arquitetura técnica, envolve os riscos de uma **fragmentação regulatória**. Como reconhecem o *Joint Statement* e o relatório da OCDE – *Landscape on Age Assurance* (2025), a multiplicidade de abordagens nacionais ameaça a interoperabilidade global das soluções e, consequentemente, a experiência e a segurança dos usuários. Para enfrentar esse desafio, **a ISOC Brasil defende maior convergência regulatória e**

padronização técnica, com diretrizes claras que harmonizem os requisitos entre jurisdições e reduzam redundâncias, garantindo previsibilidade e coesão ao ecossistema digital.

Nesses termos, **a ISOC Brasil reforça a indicação de que o objetivo deve ser o de proteger crianças e adolescentes na Internet, e não da Internet**, ou seja, é necessário garantir segurança e bem-estar digital sem comprometer a privacidade, a confiabilidade, a segurança e a natureza global da rede.

13. A classificação indicativa é critério central para determinar se um produto ou serviço de TI exige verificação de idade, nos termos do art. 8º, inciso III do ECA Digital. É viável a aplicação de outros critérios para exigir a verificação de idade? Quais?

A classificação indicativa constitui, de fato, o critério primário e mais objetivo para determinar quando a verificação de idade é exigida, conforme previsto no art. 8º, III, do ECA Digital. A adoção de critérios adicionais só é viável quando diretamente vinculada ao risco concreto associado a determinadas funcionalidades ou dinâmicas de interação, evitando ampliar indevidamente o alcance da verificação e assegurando proporcionalidade ao impacto potencial sobre crianças e adolescentes.

Nesse sentido, critérios complementares podem considerar fatores como a existência de ambientes de interação aberta entre desconhecidos, a coleta intensiva de dados pessoais, mecanismos de recomendação voltados a públicos vulneráveis, práticas de publicidade direcionada ou funcionalidades que envolvam transações financeiras ou geolocalização. Esses elementos não substituem a classificação indicativa, mas ajudam a identificar situações em que o desenho do serviço cria risco significativo, justificando a ativação de salvaguardas etárias.

Por outro lado, a aplicação de critérios que não guardem relação direta com esses riscos - como o simples fato de um serviço ter grande base de usuários, tratar

dados genéricos ou envolver conteúdos amplamente acessíveis - seria desproporcional e poderia resultar em verificações generalizadas.

Reforçamos, ainda, ser especialmente importante evitar critérios que levem à imposição de verificações em níveis de infraestrutura ou em serviços cujas funcionalidades não envolvem mediação de conteúdo ou interação social, sob pena de comprometer a arquitetura aberta da Internet, criar barreiras de acesso e gerar riscos adicionais de vigilância ou exclusão.

Assim, além da classificação indicativa, somente critérios diretamente associados ao risco real e contextual, devidamente justificados por avaliações de impacto, são compatíveis com um modelo de aferição de idade que preserve proporcionalidade, minimização e segurança. Esses critérios devem ser aplicados de forma restrita, transparente e fundamentada, evitando que a verificação de idade se converta em medida universal ou desnecessariamente intrusiva.

14. ***Considerando que diferentes produtos e serviços de TI oferecem riscos distintos para crianças e adolescentes, quais critérios deveriam ser usados para definir quando um serviço deve ser classificado como de maior risco?***

15. ***Quais salvaguardas devem ser exigidas para a coleta e processamento de dados pessoais utilizados na verificação de idade, conforme os princípios da LGPD? Quais são os maiores riscos para a privacidade dos cidadãos nos processos de verificação de idade e que mecanismos técnicos e arranjos institucionais devem ser adotados para impedir a possível reidentificação dos usuários sem dificultar o acesso a conteúdos?***

Os dados utilizados em processos de verificação de idade devem observar estritamente os **princípios de finalidade, adequação e necessidade da LGPD**, limitando o tratamento ao atributo etário indispensável e vedando a coleta ou retenção de informações que permitam identificar o usuário. O tratamento deve ser sempre temporário, com eliminação imediata dos dados utilizados no cálculo, além de prevenção ativa contra reidentificação, conforme os princípios de segurança e prevenção previstos no art. 6º, VII e VIII da LGPD.

Conforme já descrito anteriormente, os riscos mais significativos à privacidade decorrem, justamente, de práticas que ampliam a superfície de ataque: sistemas que concentram documentos oficiais, bancos biométricos ou identificadores persistentes expõem os usuários a vazamentos, correlação indevida de dados e vigilância sistemática, podendo comprometer de maneira duradoura direitos fundamentais.

Para mitigar esses riscos, mecanismos técnicos como provas criptográficas de conhecimento zero, credenciais verificáveis e protocolos de minimização estrutural devem ser priorizados, pois permitem comprovar faixas etárias sem identificar indivíduos. Sob a perspectiva institucional, é necessário assegurar que atores responsáveis pela aferição sejam auditáveis, operem na camada de aplicação e estejam sujeitos a avaliações independentes de impacto, com governança que impeça a expansão de finalidade e o reuso comercial ou governamental dos dados. Em conjunto, essas medidas reduzem a possibilidade de reidentificação e reforçam o caráter de proteção - e não de vigilância - da verificação etária.

16. Considerando que credenciais anônimas são vistas como uma solução promissora, quais seriam os caminhos viáveis para implementá-las no Brasil, via soluções privadas ou públicas, de forma prática e confiável?

A adoção de credenciais anônimas no Brasil pode avançar por meio de modelos que combinem padrões técnicos internacionais, arranjos institucionais

descentralizados e mecanismos criptográficos que assegurem verificabilidade sem identificação. Uma via possível envolve provedores públicos ou privados aptos a realizar verificação inicial de documentos, gerando a partir desse processo credenciais verificáveis que contenham apenas atributos etários, sem qualquer dado pessoal que permita a identificação posterior. Esse modelo, ao operar com dados minimizados e com descarte imediato das informações utilizadas na verificação, reduz riscos e se mantém compatível com a LGPD.

Outra alternativa é o uso de infraestruturas federadas, em que diferentes entidades - públicas, privadas ou comunitárias - possam atuar como emissoras de credenciais, desde que observem padrões abertos de interoperabilidade definidos por organismos como W3C, IETF e ISO. Essa abordagem evita centralização indevida e amplia a resiliência do sistema, ao mesmo tempo em que permite que aplicativos e serviços utilizem essas credenciais para verificar faixas etárias sem acessar identidades. No caso de eventual integração com plataformas governamentais como o gov.br, é essencial que o desenho institucional preserve a autonomia dos serviços, elimine qualquer registro persistente da transação e evite transformar a plataforma em ponto único de controle ou vigilância. Independentemente do modelo, o caminho viável passa por credenciais criptograficamente protegidas, minimização estrutural, arranjos descentralizados e auditorias independentes, assegurando equilíbrio entre proteção de crianças, privacidade e preservação da arquitetura aberta da Internet.

17. De que forma é possível assegurar que métodos de verificação de idade não criem barreiras de acesso a produtos e serviços de TI para cidadãos e cidadãs?

Qualquer método de verificação de idade, exigido como pré-requisito ao acesso a determinados serviços e produtos, por si só, já constitui uma barreira contra o uso da tecnologia. Minimizar a dimensão desse obstáculo vem com a promoção de

políticas públicas de inclusão digital, desenvolvimento de tecnologias de verificação em observância aos princípios apresentados ao longo desta Consulta (em especial os constantes na Questão 6), e investimento e valorização de ferramentas de controle parental, atribuindo aos pais ou responsáveis a tarefa de controle de acesso e uso de produtos e serviços por seus dependentes, uma vez que a verificação de idade atinge a todos os usuários, crianças e adultos, tornando vulneráveis seus dados e a segurança online.

Ratificando ao que foi aludido alhures, as formas de aferição devem então operar de modo não discriminatório, garantindo que pessoas sem documentos brasileiros, migrantes, refugiados, usuários com baixo letramento digital ou com dispositivos limitados possam cumprir as exigências legais sem sofrer barreiras indevidas. Esse cuidado reforça a necessidade de múltiplas vias de verificação equivalentes, evitando dependência de tecnologias de alto custo, dispositivos específicos ou procedimentos que pressuponham conectividade estável e equipamentos de maior desempenho. **Métodos baseados exclusivamente em biometria ou análise facial, além de apresentarem vieses e maior propensão a erros, podem excluir usuários com características físicas diversas ou com equipamentos sem capacidade técnica adequada**.

18. Que mecanismos alternativos podem ser oferecidos a cidadãos que não possuem acesso às tecnologias de verificação digital, garantindo que não sejam excluídos?

A disponibilização de mecanismos alternativos é indispensável para garantir que a verificação de idade não exclua justamente parte do público em situação de maior vulnerabilidade, com acesso limitado a dispositivos, conectividade precária ou baixo letramento digital. Muitos métodos digitais exigem câmeras de boa qualidade, biometria, reconhecimento facial, conexão estável ou dispositivos recentes,

elementos que não estão igualmente distribuídos entre a população infantojuvenil e que podem transformar uma salvaguarda em barreira.

Para evitar esse problema, é fundamental oferecer alternativas equivalentes que possam ser utilizadas mesmo por quem não dispõe de recursos tecnológicos avançados, como o uso de credenciais previamente verificadas em serviços acessíveis, procedimentos presenciais ou offline em regiões com baixa conectividade e, de forma residual, a apresentação de documentos físicos tratada de forma minimamente invasiva e sem retenção de dados.

A oferta de múltiplas vias de verificação, associada a esforços de inclusão e letramento digital envolvendo famílias e comunidades, reduz o risco de exclusão e preserva o caráter aberto da Internet, assegurando que a aferição etária cumpra sua finalidade protetiva sem impor obstáculos adicionais a crianças e adolescentes que já enfrentam desigualdades no acesso às tecnologias.

19. Como impedir que a infraestrutura de aferição de idade seja usada para finalidades distintas da proteção infantojuvenil, como vigilância, treinamento não autorizado de aplicações de inteligência artificial, ou controle de acesso por outros atores?

A **prevenção ao uso indevido da infraestrutura de aferição de idade** depende do desenho combinado de salvaguardas técnicas, institucionais e regulatórias que impeçam sua conversão em instrumento de vigilância, discriminação, controle de acesso ou treinamento não autorizado de sistemas de inteligência artificial. Para que isso ocorra, a aferição deve operar exclusivamente na camada de aplicação, de forma descentralizada e temporária, sem geração de identificadores persistentes, sem retenção de dados sensíveis e sem possibilidade de correlação entre serviços, evitando a criação de pontos únicos de controle que fragilizem a arquitetura da Internet. A LGPD já estabelece limites claros ao uso

secundário dos dados, e a aplicação rigorosa dos princípios de finalidade, necessidade, segurança e prevenção exige que qualquer mecanismo de verificação seja projetado para não produzir registros permanentes, metadados rastreáveis ou bases que permitam treinamento algorítmico sem consentimento.

Além disso, é necessário que se estabeleça arranjo de governança capaz de impedir a expansão de finalidade e de limitar rigorosamente o papel de cada ator envolvido. Esse arranjo deve assegurar que entidades responsáveis pela emissão, verificação ou mediação de atributos etários operem sob parâmetros claros de minimização, retenção nula e impossibilidade técnica de reconstruir identidades, com mecanismos externos de supervisão que garantam transparência e controle social.

A estrutura de governança deve incluir **obrigações auditáveis de descarte imediato dos dados** utilizados no processo, documentação pública dos fluxos técnicos, relatórios periódicos de impacto e revisão independente por organismos com expertise técnica, jurídica e social. Também é necessário assegurar mecanismos que previnam o uso secundário das informações, como regras que impeçam a integração dessa infraestrutura com sistemas de identificação civil, bases biométricas, bancos comerciais ou aplicações de inteligência artificial, além de salvaguardas que dificultem a correlação de metadados ou o rastreamento longitudinal de usuários. Arranjos institucionais que garantam participação multissetorial, revisão contínua de riscos e interoperabilidade com padrões abertos fortalecem a confiança e reduzem a probabilidade de captura da infraestrutura por interesses alheios à proteção infantojuvenil. Esse conjunto de medidas impede que a aferição de idade se transforme, direta ou indiretamente, em vetor de vigilância, restrição excessiva de acesso ou fonte de dados para aplicações não autorizadas, preservando o propósito estrito para o qual foi concebida.

20. Em arquiteturas descentralizadas ou federadas, como a responsabilidade pela aferição de idade deve ser atribuída entre desenvolvedores de protocolo, operadores de servidor e criadores de aplicativos?

XXX

21. De que forma a verificação em dispositivos compartilhados pode ser feita sem comprometer a privacidade e a segurança de adultos, ao mesmo tempo que protege crianças e adolescentes dos riscos online, em ambientes familiares vulneráveis?

Segundo a edição de 2025 da **pesquisa TIC Domicílios**, conduzida pelo **Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação** (CETIC.br), 41% da população com 10 anos ou mais vivem em domicílios com mais de um dispositivo por morador. Este dado indica que cerca de **60% da população encontra-se em domicílios com um ou menos de um dispositivo por pessoa**, cenário que se torna mais grave quando se analisa as populações das classes DE, em que apenas 14% das pessoas vivem em domicílios com mais de um dispositivo *per capita*. Estes dados apontam para um cenário fático em que **há o uso compartilhado de dispositivos**, de modo que mecanismos de aferição de idade não devem pressupor que há um uso individualizado e contínuo destes por uma mesma pessoa.

Nesse sentido, soluções de verificação etária baseadas em autenticação biométrica ou no próprio dispositivo podem gerar barreiras de acesso e ampliar desigualdades, pois dependem de recursos e condições técnicas que não estão disponíveis para grande parte da população brasileira. Além de exigirem equipamentos com câmeras, sensores e conexão estável, essas abordagens pressupõem o uso individualizado dos aparelhos, o que não condiz com a realidade de milhões de famílias que compartilham dispositivos. Nesses contextos, o processo

de verificação pode se tornar inviável ou comprometer a privacidade dos usuários, resultando em situações concretas de exclusão digital. Desse modo, as abordagens mais adequadas a essa questão devem combinar letramento digital e configurações que considerem o uso compartilhado de dispositivos, garantindo que a proteção de crianças e adolescentes não se traduza em obstáculos adicionais ao acesso.

Ou seja, partindo da **noção de conectividade significativa** – que abrange não somente o acesso físico às TICs, mas também a capacidade de utilizá-las de forma autônoma e consciente e de se apropriar delas –, a implementação de soluções de aferição etária em contextos de uso compartilhado de dispositivos deve ser acompanhada por processos de formação e apoio às famílias. Tais processos devem fortalecer a compreensão sobre os riscos e responsabilidades associados ao uso da Internet e à verificação etária, visando capacitar os usuários para configurar e gerenciar ferramentas de proteção de modo adequado à sua realidade.

Paralelamente, é indispensável a promoção de políticas públicas de inclusão e letramento digital que visem ampliar o número de dispositivos por domicílio, garantir condições equitativas de conectividade e desenvolver competências digitais básicas e críticas entre crianças, adolescentes e adultos. Portanto, a efetividade de qualquer solução de verificação etária depende do enfrentamento de desigualdades estruturais, que condicionam como as pessoas se conectam, compartilham e se protegem no ambiente digital. Se não houver políticas integradas que articulem acesso, infraestrutura e letramento digital, as medidas técnicas permanecerão com alcance limitado e poderão reforçar exclusões preexistentes, ao invés de mitigá-las.

4. CONCLUSÃO

A **ISOC Brasil** reafirma seu compromisso com a promoção de uma Internet aberta, segura, confiável e interoperável, em que a proteção de crianças e adolescentes caminhe junto à preservação da privacidade, da inclusão e da inovação.

As contribuições apresentadas buscam **oferecer subsídios técnicos** para uma implementação do ECA Digital que seja proporcional, baseada em risco e compatível com os princípios da governança da Internet.

A **ISOC Brasil** coloca-se à disposição do Ministério da Justiça, da SEDIGI e da ANPD para aprofundar o debate e colaborar na definição de soluções técnicas e políticas públicas que reforcem a confiança e a segurança no ambiente digital brasileiro.

Internet Society
Capítulo Brasil