

NOTA DE TEMA

Regulamentação da Aferição Etária

Diferentes abordagens para uma abordagem equilibrada, proporcional e baseada em risco

FEVEREIRO / 2026

Sobre o Conselho Digital

O Conselho Digital é uma entidade brasileira, sem fins lucrativos ou afiliações políticas, que coordena, estuda e representa o ecossistema dos aplicativos de internet e toda a diversidade dos seus modelos de negócios.

Nossa organização acredita que a tecnologia, quando bem construída e utilizada, é uma porta para o futuro. Ela nos mantém conectados, potencializa habilidades, desenvolve novas oportunidades e pode mudar a vida das pessoas para melhor.

Partindo dessa premissa, atuamos através de estudos, eventos e atividades de advocacy em favor de políticas públicas e setoriais que fortaleçam uma internet livre, segura e responsável no Brasil e no mundo.

Defendemos políticas que respeitem a neutralidade tecnológica, a inovação e a diversidade de modelos de negócios; e que tenham como consequência:

- Usuários conscientes e com poder de escolha;
- Uma sociedade plural e próspera;
- Ambientes de negócio juridicamente seguros;
- Mercados abertos e dinâmicos; e
- Empresas responsáveis e competitivas.

Por fim, assumimos o compromisso de construir um ambiente harmonioso e produtivo entre nossos associados, assim como uma relação transparente e colaborativa com a sociedade e governo.



Diretor-Executivo

www.conselhodigital.org.br

Takeaways – Posição do Conselho Digital

- **Não existe solução única** para aferição de idade: a regulação deve admitir **modelos escalonados**, proporcionais ao risco e ao contexto de uso.
- **Autodeclaração tem papel legítimo** em ambientes de baixo risco; descartá-la por princípio tende a gerar **fricção desnecessária** e empurrar soluções excessivamente intrusivas.
- **Níveis máximos de restrição não são sinônimo de experiência apropriada à idade**: impor controles fortes em todos os contextos banaliza exceções, normaliza intrusão e enfraquece princípios de proporcionalidade.
- **Proteger não pode significar vigiar**: Boa regulação não é a que escolhe a tecnologia mais forte, mas a que calibra proteção, inclusão e viabilidade sem criar dependência, exposição ou custo sistêmico desnecessário.
- **Centralizar a aferição em infraestruturas únicas** como validadores obrigatórios pode, entre os trade offs, criar **dependência estrutural** que precisa ser considerada como risco regulatório.
- **ID Techs são legítimas, mas não podem virar padrão compulsório**: terceirização deve ser opcional, adequada ao risco e compatível com a diversidade do ecossistema digital.
- **Padronização proprietária, exclusiva e excessiva favorece concentração de mercado** e cria barreiras de entrada, especialmente para PMEs, serviços gratuitos e modelos não transacionais.
- **Flexibilidade arquitetural é condição de efetividade**: a regulação deve definir objetivos e salvaguardas, não impor uma única solução técnica.
- **Custo sistêmico importa tanto quanto custo unitário**: modelos “eficientes” por transação podem ser inviáveis quando generalizados.
- **Educação e literacia digital são insubstituíveis**: nenhuma solução técnica resolve sozinha problemas estruturais de proteção de crianças e adolescentes.
- **Responsabilidade é compartilhada**, não transferida: plataformas, Estado, fornecedores e sociedade devem atuar conjuntamente, sem criar novos gatekeepers regulatórios.
- **Boa regulação equilibra proteção, inclusão e viabilidade**, evitando tanto permissividade quanto maximalismo técnico.

O que o Conselho Digital pensa sobre a regulamentação da aferição etária?

- **Abordagem proporcional e baseada em risco:** O Conselho Digital do Brasil entende que a regulação de mecanismos de aferição de idade deve partir de uma abordagem **proporcional, baseada em risco e orientada por direitos fundamentais**, reconhecendo tanto a necessidade de proteção integral de crianças e adolescentes quanto os limites técnicos, econômicos e sociais das soluções disponíveis. Não há solução única ou universalmente adequada: diferentes contextos de uso, níveis de risco e tipos de serviço demandam **modelos escalonados**, que combinem camadas distintas de proteção sem transformar o acesso à internet em um ambiente de vigilância generalizada **ou em um sistema excessivamente centralizado e dependente de intermediários obrigatórios**.
- **Autodeclaração em baixo risco:** Nesse sentido, o Conselho Digital reconhece que mecanismos menos intrusivos – soluções que observem o princípio da minimização de dados, reduzam a fricção operacional para o usuário e demandem menor custo de implementação – como a autodeclaração, podem ter papel legítimo em **contextos de baixo risco**, desde que integrados a estratégias mais amplas de proteção¹, e não apresentados como solução suficiente para ambientes impróprios ou inadequados ou proibido para menores, o que é vedado pelo ECA Digital. **A desqualificação automática dessas soluções tende a ignorar sua função prática na organização do acesso digital e a induzir a adoção de modelos únicos, mesmo quando o risco não os justifica.**
- **Riscos de soluções únicas:** O Conselho Digital defende que o oferecimento de experiências adequadas à idade **ocorra de maneira**

¹ integrados a uma abordagem multicamadas de proteção, baseada em gestão de risco, design seguro e mecanismos complementares de supervisão. Como limitações funcionais, configurações padrão mais restritivas e mecanismos de denúncia e moderação.

contextual e tecnologicamente neutra, evitando a **generalização de controles e padrões definidos abstratamente nos "níveis máximos possíveis"**. A aferição de idade, por sua vez, deve ser **desenvolvida em camadas, de maneira proporcional ao risco e evitando ficar cristalizada em torno de arquiteturas fechadas ou padronizadas como requisito regulatório**. A imposição de soluções únicas para aferição de idade — ainda que tecnicamente robustas — e em **desconsideração ao mosaico de soluções públicas e privadas disponíveis no mercado**, pode gerar dependência estrutural, reduzir a diversidade de modelos e bloquear o avanço tecnológico, o surgimento de novas soluções com o passar do tempo, e gerar efeitos relevantes sobre concorrência e custo sistêmico.

- **Riscos da terceirização automática:** O Conselho Digital manifesta preocupação com abordagens que tratem a **terceirização da verificação como solução automática**, desconsiderando que a intermediação obrigatória também redistribui poder, risco e custo dentro do ecossistema digital. **A existência de fornecedores especializados é legítima e desejável, mas sua adoção deve permanecer opcional, proporcional ao risco e compatível com a diversidade de serviços e modelos de negócio existentes.**
- **Riscos do maximalismo técnico:** Da mesma forma, o Conselho Digital alerta para os riscos de uma regulação excessivamente rígida, que imponha soluções de alta complexidade técnica ou custo recorrente como padrão transversal. **Mesmo quando eficientes do ponto de vista operacional, tais modelos podem se mostrar desproporcionais para serviços de baixo risco, inviáveis para pequenas e médias empresas e excludentes em contextos de uso não transacionais.**
- **Diretrizes para uma regulamentação proporcional e tecnicamente adequada:** O Conselho Digital acredita que qualquer determinação regulatória deva considerar as diferentes realidades técnicas dos serviços abarcados e não exclua alternativas já efetivas atualmente.
- **Educação digital:** Para o Conselho Digital, a discussão sobre aferição de idade não pode ser dissociada de uma **estratégia estrutural de educação e literacia digital**. Nenhum mecanismo técnico, por mais avançado que seja, substitui políticas públicas voltadas à formação de crianças, adolescentes, famílias e

responsáveis para o uso seguro, crítico e informado da internet. **A transferência excessiva da responsabilidade para infraestruturas técnicas ou intermediários especializados tende a produzir uma falsa sensação de segurança regulatória**, sem enfrentar os determinantes sociais do risco.

- **Vantagens da flexibilidade:** Por fim, o Conselho Digital defende que, em alinhamento com o artigo 227 da Constituição Federal, a responsabilidade pela proteção de crianças e adolescentes no ambiente digital deve ser **compartilhada**, envolvendo plataformas, Estado, fornecedores de tecnologia e sociedade e responsáveis, com regras claras, incentivos adequados e salvaguardas institucionais. **A regulação deve preservar flexibilidade arquitetural, evitar a criação de novos gatekeepers obrigatórios e garantir que a proteção seja efetiva sem gerar dependência, exclusão ou concentração indevida de poder.**

MODELOS DE AFERIÇÃO DE IDADE

MODELO	DESCRIÇÃO	DEFENDIDO POR	JUSTIFICATIVA CENTRAL	O QUE OS CRÍTICOS ALEGAM
Autodeclaração simples	Usuário informa a idade sem validação técnica adicional	Roku; PROTESTE (com ressalvas)	Alta usabilidade; baixo custo; adequada a contextos de baixo risco	Ineficaz em serviços de alto risco; facilmente contornável; governo a trata como insuficiente para conteúdos sensíveis, sendo seu uso isolado vedado pelo ECA Digital.
Autodeclaração assistida / validada	Autodeclaração combinada com verificação de sinais de inconsistência	Setores do comércio e serviços digitais	Preserva usabilidade; reduz dependência de documentos e biometria; modelo intermediário	Pode derivar em monitoramento indireto; baixo nível de garantia; não destacada pelo governo como solução adequada para alto risco
Controle parental no nível do dispositivo (SO)	Faixa etária configurada no sistema operacional, com envio de sinal genérico ao app	Fabricantes de sistemas operacionais	Empoderamento parental; redução da coleta de dados pelos apps	Pressupõe dispositivos individuais; alto letramento digital; insuficiente em alto risco; governo o trata como camada complementar
Estimativa facial de idade	IA estima idade a partir da imagem do rosto	Fornecedores de tecnologia	Automatização da verificação	Uso de dados sensíveis; viés; baixa precisão; governo não recomenda, salvo exceções restritas
Inferência de idade por IA (comportamento)	Estimativa da idade a partir de padrões de uso, linguagem e interações	Grandes plataformas digitais	“Sem atrito”; não exige documento ou foto; escalável	Vigilância contínua; alto risco de incompatibilidade com LGPD e ECA; governo descreve como método mais invasivo
Infraestrutura estatal (Gov.br / ICN)	Uso de bases públicas e login governamental para aferição de idade	Parte do setor privado; academia	Estado já validou identidades; evita duplicação de esforços	Dependência de infraestrutura única; ponto único de falha; rigidez excessiva
Provas criptográficas (ZKP / credenciais verificáveis)	Comprovação de idade sem revelar identidade, via criptografia	Sociedade civil; academia	Privacy by design; minimização de dados; separação identidade/atributo	Alta complexidade técnica; custo elevado; difícil implementação em larga escala

MODELO	DESCRIÇÃO	DEFENDIDO POR	JUSTIFICATIVA CENTRAL	O QUE OS CRÍTICOS ALEGAM
Terceiros validadores / ID Techs	Verificação por empresas especializadas que retornam apenas o atributo etário	Fornecedores de tecnologia de identidade	Especialização técnica; redução de risco jurídico; padronização	Concentração de mercado; dependência estrutural; custo sistêmico para PMEs; governo aponta risco de baixo nível de garantia
Teste de capacidade / maturidade cognitiva	Avaliação de habilidades cognitivas do usuário	Propostas acadêmicas pontuais	Busca avaliar maturidade, não idade cronológica	Eficácia limitada; facilmente burlável; governo considera insuficiente para fins regulatórios
Verificação documental direta	Envio de documentos oficiais (RG, CNH, passaporte)	Parte do setor privado; poder público	Documento é mais universal que tecnologias avançadas; segurança jurídica	Honeypots de dados; coleta excessiva; risco de vazamento; governo reconhece eficácia, com ressalvas quanto ao armazenamento
Verificação por cartão de crédito (inferência)	Inferência de idade pela posse de cartão	Plataformas transacionais	Baixa fricção para o usuário	Baixa garantia; excludente; facilmente contornável; governo aponta insuficiência e riscos sociais
Verificação por operadora (MNO)	Idade inferida a partir do titular da linha telefônica	Operadoras de telecom	Aproveita infraestrutura existente	Falha em aparelhos compartilhados; risco de vazamento; governo classifica como insuficiente
Abordagem regulatória flexível e baseada em risco	Combinação de múltiplos mecanismos conforme tipo de serviço, público e nível de risco, sem imposição de solução única	Conselho Digital	Proporcionalidade; viabilidade econômica; preservação da diversidade de modelos; redução de fricção desnecessária	Suposta permissividade por não garantir proteção máxima em todos os contextos