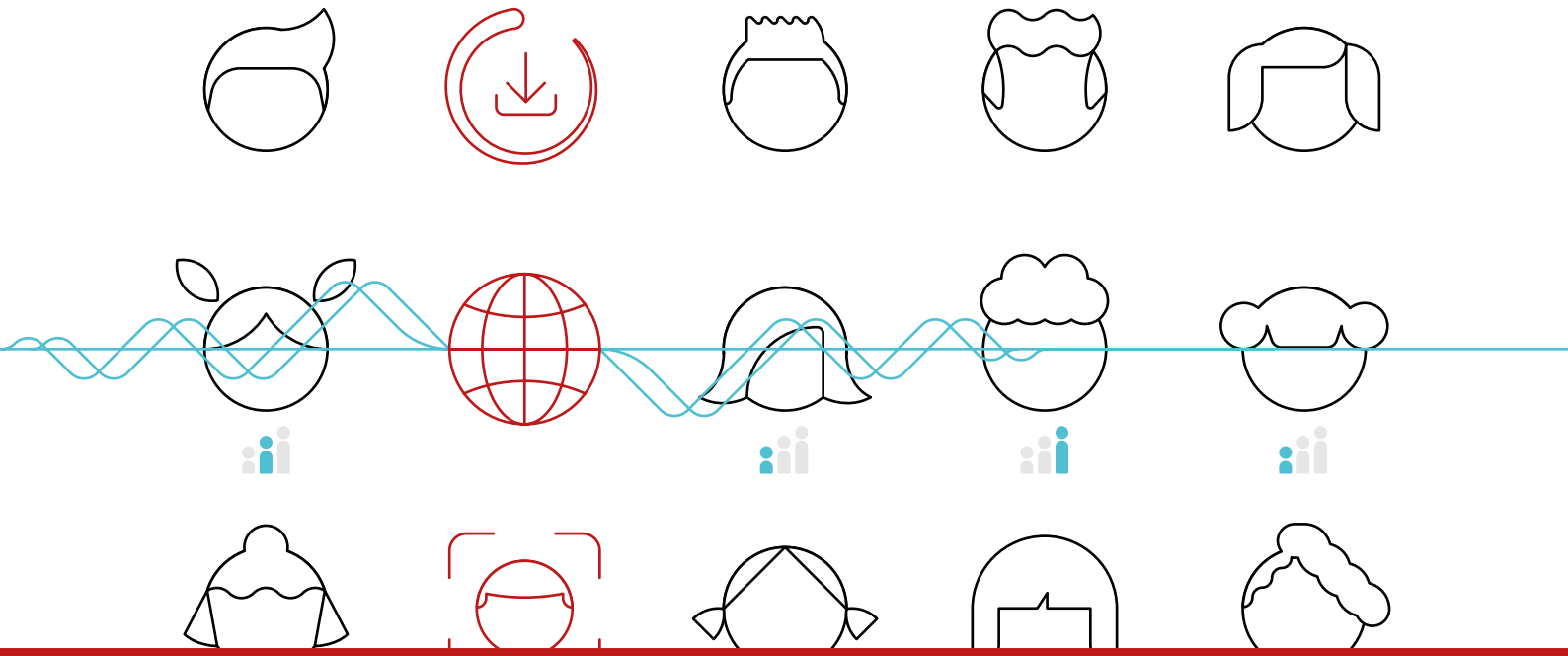
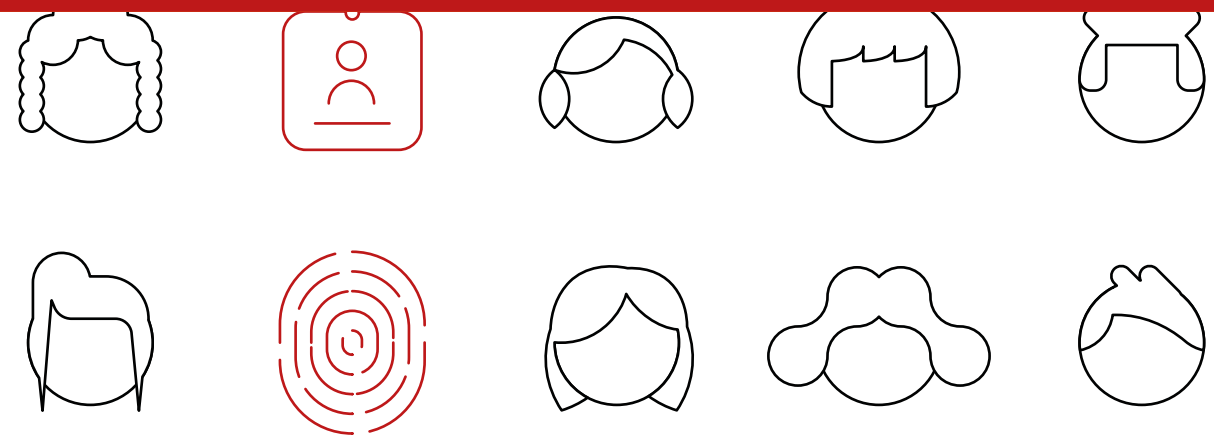


‹ radar tecnológico ›

mecanismos de aferição de idade



ANPD

Agência Nacional de Proteção de Dados

‹ radar tecnológico ›

n° 5

mecanismos de aferição de idade

Edgard Costa Oliveira
Roseane Salvio
Jayme Marrone Júnior

ANPD
Brasília, DF
2025

ANPD – Agência Nacional de Proteção de Dados

Diretor-Presidente
Waldemar Gonçalves Ortunho Junior

Diretores
Arthur Pereira Sabbat
Iagê Zendron Miola
Lorena Giuberti Coutinho
Miriam Wimmer

Equipe de elaboração
Coordenação-Geral de Tecnologia e Pesquisa (CGTP)
Edgard Costa Oliveira
Roseane Salvio
Jayme Marrone Júnior

Coordenação e revisão
Lucas Costa dos Anjos
Gustavo Andrade Bruzzeguez
Adi Balbinot Junior
Albert Franca Josua Costa
Angela Halen Claro Franco

Projeto gráfico / editoração eletrônica / capa
André Scofano Maia Porto

Infográficos
Ewerton Luiz Costadelle

1ª edição
Publicação digital – PDF
Radar Tecnológico, Número 5, OUT 2025

ANPD
SCN, Qd. 6, Conj. A, Ed. Venâncio 3000, Bl. A, 9º andar
Brasília, DF · Brasil · 70716-900
t. (61) 2025-8101 · www.gov.br/anpd

Como referenciar esta publicação:

ANPD. **Mecanismos de aferição de idade**. Brasília, DF: ANPD, 2025. (Radar Tecnológico, n. 5). Disponível em: incluir link do documento. Acesso em: incluir data de acesso ao documento.

‹ sobre a série ›

A série "Radar Tecnológico" é uma produção periódica da ANPD que objetiva realizar abordagens concisas de tecnologias emergentes que vão impactar ou já estejam impactando o cenário nacional e internacional da proteção de dados.

Sem a intenção de esgotar as temáticas ou firmar posicionamentos institucionais, o propósito da série é agregar informações relevantes ao debate da proteção de dados no País, com textos estruturados de forma didática e acessível ao público em geral.

Para cada tema, são abordados os conceitos principais, as potencialidades e as perspectivas de futuro, sempre com ênfase na proteção de dados no contexto brasileiro. ▪

‹ lista de abreviaturas e siglas ›

AATT – Age Assurance Technology Trial
ACCS – Age Check Certification Scheme
AEPD – Agencia Española de Protección de Datos
API – Application Programming Interface
ARCOM – Autorité de Régulation de la Communication Audiovisuelle et Numérique
AVPA – Age Verification Providers Association
BBFC – British Board of Film Classification
BSI – British Standards Institute
CHAMPS – Children Amplified Prevention Services
CIN – Carteira de Identidade Nacional
CNH – Carteira Nacional de Habilitação
CNIL – Commission Nationale de l'Informatique et des Libertés
CONANDA – Conselho Nacional dos Direitos da Criança e do Adolescente
CPF – Cadastro de Pessoa Física
DPIAs – Data Protection Impact Assessments
ECA – Estatuto da Criança e do Adolescente
EDCA – Estatuto Digital da Criança e do Adolescente
EDPB – European Data Protection Board
EDRI – European Digital Rights
EFA – Electronic Frontiers Australia
EPRS – European Parliamentary Research Service
FOSI – Family Online Safety Institute
GDPR – General Data Protection Regulation
HEAA – Highly Effective Age Assurance
IA – Inteligência Artificial
ICO – Information Commissioner's Office
IEC – International Electrotechnical Commission
IEEE – Institute of Electrical and Electronic Engineers
KU Leuven – Katholieke Universiteit Leuven
ISO – International Standards Organization
LGPD – Lei Geral de Proteção de Dados Pessoais
MDHC – Ministério dos Direitos Humanos e da Cidadania
MJSP – Ministério da Justiça e Segurança Pública
MNO – Mobile Network Operator

NLP – Natural Language Processing
OCDE – Organização para a Cooperação e Desenvolvimento Econômico
OCR – Optical Character Recognition
OFCOM – Office of Communications
ONU – Organização das Nações Unidas
PEReN – Pôle d'Expertise de la Régulation Numérique
PNPDCAAD – Política Nacional de Proteção dos Direitos da Criança e do Adolescente no Ambiente Digital
SEDIGI – Secretaria de Direitos Digitais
SVE – Sistemas de Verificacíon de Edad
UNODC – United Nations Office on Drugs and Crime
VaaS – Verification as a Service
ZKP – Zero Knowledge Proof

‹ sumário ›

‹ introdução ›

A Internet, seus serviços e produtos, as redes sociais, os sistemas de entretenimento, jogos, educação, saúde e transporte, ou seja, o ambiente digital como um todo tem proporcionado à sociedade oportunidades de exercício da cidadania, direitos fundamentais, vivências e experiências, obtenção de conhecimento, acesso a informações diversas que podem ser úteis aos indivíduos.

Crianças e adolescentes querem e precisam ter acesso ao ambiente digital, mas isso deve ser feito de maneira a melhor atender seu melhor interesse, de modo que estejam protegidos do mau uso da informação não destinada a suas faixas etárias. Existe o risco da exposição de crianças e adolescentes a conteúdos digitais impróprios e danosos a sua formação física, emocional, psicológica e cognitiva, como pornografia, indução ao suicídio e à automutilação. Além disso, pessoas desse público podem ser submetidas, no ambiente digital, a práticas nocivas como *cyberbullying*[1] , contatos indevidos com estranhos e chantagens via uso de dados pessoais por aliciadores com fins sexuais. Também podem estar expostos a publicidade enganosa ou abusiva sobre apostas, cigarros, armas, bebidas alcoólicas e outros itens impróprios para crianças e adolescentes.

Em 2025, foi promulgada no Brasil a Lei nº 15.211/2025, que dispõe sobre a proteção de crianças e adolescentes em ambientes digitais, também conhecida como o ECA Digital (Estatuto Digital da Criança e do Adolescente). A lei estabelece em seu Art. 10 que

> *os fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável por eles deverão adotar mecanismos para proporcionar experiências adequadas à idade, nos termos deste Capítulo, respeitadas a autonomia progressiva e a diversidade de contextos socioeconômicos brasileiros (Brasil, 2025c).*

1 *"O Cyberbullying é a modalidade virtual do bullying, que é identificado pelas intimidações repetitivas entre crianças e adolescentes, mas com características próprias, pois tem um efeito multiplicador e de grandes proporções quando acontece na web" (SaferNet, [2019?]).*

A aferição de idade é a atividade de identificar e confirmar a idade de uma pessoa, seja ela uma criança ou adolescente ou adulto, com o objetivo de verificar ou estimar se possuem determinada idade para adentrar nos ambientes digitais, redes sociais, jogos eletrônicos, ou para restringir ou autorizar a venda de produtos restritos. O resultado da aferição de idade é garantir que o acesso ao ambiente digital será dado em razão da idade mínima da criança para que ela apenas acesse conteúdos próprios para a sua idade, bem como para impedir que adultos se passem por crianças e interajam com elas de modo ilícito.

Para aferir a idade de usuários, há mecanismos específicos que são abordagens utilizadas para verificação e estimativa de idade de usuários da Internet por meio de diversas aplicações disponíveis. Eles possuem papel especial na proteção das crianças e adolescentes em ambientes digitais, em razão do crescente número de usuários dessa faixa etária que utilizam produtos e serviços na Internet.

De acordo com a 11ª edição da pesquisa TIC Kids Online Brasil, realizada pelo Cetic.br/NIC.br, 93% da população entre 9 e 17 anos é usuária da Internet no Brasil (NIC.BR, 2024, p.21). A pesquisa também trouxe um dado inédito sobre a frequência de uso de plataformas digitais por crianças e adolescentes: mais da metade da população investigada que está na faixa entre 9 e 12 anos acessa plataformas de mensagens e de compartilhamento de vídeos e fotos "várias vezes ao dia" ou "todos os dias ou quase todos os dias". Em média, 70% são usuárias frequentes de uma das plataformas de vídeos (NIC.BR, 2024, p.22 e 67).

O mesmo estudo, realizado em 2023, mostrou que um quarto dos entrevistados revelaram ter começado a acessar a Internet antes mesmo dos seis anos de idade, a maioria por meio do telefone celular, mas também pela televisão, e uma minoria pelo computador (NIC.BR, 2023, p.27). A pesquisa revelou ainda que, no Brasil, 68% daqueles entre 9 e 10 anos possuem perfil em ao menos uma das plataformas digitais investigadas, e esse número sobe para 82% entre jovens de 11 a 12 anos, e 99% entre jovens de 15 a 17 anos (NIC.BR, 2023, p.30).

do público entre 9 e 17 anos estão na internet

é o que revelou a pesquisa TIC Kids Online Brasil (NIC.BR, 2024, p.21) sobre a frequência e uso de plataformas digitais por crianças e adolescentes

entre 9 e 12 anos são usuários frequentes

e responderam que acessam uma plataforma de vídeos "várias vezes ao dia" ou "todos os dias ou quase todos os dias"

tiveram o primeiro acesso antes dos 6 anos de idade

a maioria por meio do telefone celular, mas também pela televisão e uma minoria pelo computador (NIC.BR, 2023, p.27)

Figura 1 *Percentuais de usuários infantis na Internet.*

Fonte: Elaboração própria com base em NIC.BR (2023)

A Lei Geral de Proteção de Dados Pessoais (LGPD) reflete a preocupação com a proteção de dados pessoais e a privacidade de crianças e adolescentes nesses ambientes. A Seção III do Capítulo II da lei é dedicada a esse grupo vulnerável (Brasil, 2018). Entre os temas da agenda regulatória da Agência Nacional Proteção de Dados (ANPD) para o biênio 2025-2026, destaca-se a iniciativa para o tratamento de dados pessoais de crianças e adolescentes, que integra os seguintes temas: (i) o princípio do melhor interesse; (ii) o consentimento fornecido por pais e responsáveis; (iii) a coleta de informações por jogos e aplicações de Internet; (iv) a transparência das operações realizadas com dados pessoais de crianças e adolescentes; (v) os mecanismos de aferição de idade de usuários de jogos e aplicações de Internet; e (vi) a definição de orientações e a identificação de boas práticas, que expressem um conjunto de princípios normativos, tecnologias e medidas de *design*, que promovam e assegurem a privacidade e a efetiva proteção de dados pessoais de crianças e adolescentes em jogos e aplicações de Internet (ANPD, 2024c).

Além disso, o Mapa de Temas Prioritários da ANPD para o biênio 2024-2025 também aborda o assunto: realizar ações de fiscalização para assegurar o melhor interesse da criança e do adolescente, por meio da verificação da compatibilidade entre a LGPD e o tratamento dado por plataformas digitais, assim como propor medidas de salvaguarda para assegurar a verificação de idade de usuários dessas plataformas (ANPD, 2023c).

Visando operacionalizar a implementação da aferição de idade no país, em 2025, o Ministério da Justiça e Segurança Pública (MJSP), por meio da Secretaria de Direitos Digitais, criou um Comitê Consultivo para formulação de proposta de metodologia e requisitos mínimos de verificação etária em serviços digitais que podem ser acessados por crianças e adolescentes. O comitê, formado por membros do MJSP, da ANPD e de organizações da sociedade civil, atua na "[...] formulação de proposta de metodologia e requisitos mínimos de verificação etária em serviços digitais que podem ser acessados por crianças e adolescentes" (Brasil, 2025e, p.86).

Outras jurisdições têm implementado iniciativas relacionadas a essa temática. Na Espanha, foi criado em 2024 o *Comité de Personas Expertas para el desarrollo de un entorno digital seguro para la juventud y la infancia*, incumbido de elaborar boas práticas em ambientes digitais, assim como avaliar os riscos envolvidos, e propor recomendações de curto, médio e longo prazos para a administração pública implementar de modo a garantir o desenvolvimento integral da infância e da juventude. O documento estabeleceu medidas como a regulação da indústria de criação de Sistemas de Verificação de Idade (SVE – *Sistemas de Verificacíon de Edad*), a proteção de dados e as medidas de não localização, não identificação e não perfilamento[2] do usuário, com a devida evolução dos requisitos de controle parental e de verificação de idade, de acordo com os modelos e padrões técnicos internacionais (Espanha, 2024, p. 65).

Além da necessidade de se adotarem mecanismos de aferição de idade que protejam crianças e adolescentes dos riscos nos ambientes digitais, há sobretudo o desafio de conciliar esses mecanismos com a proteção de dados pessoais e a preservação da privacidade. Em muitos casos, o acesso a serviços digitais pode ser negado caso o usuário não forneça informações pessoais para comprovar sua idade, incluindo dados sensíveis, como biometria facial (por exemplo, uma imagem do rosto capturada por sistemas de reconhecimento facial). Como orientam a proposta de norma ISO/IEC 27566 (FDIS em processo de aprovação final) e o *Age Appropriate Design Code* do Reino Unido, os sistemas de aferição de idade devem buscar um equilíbrio entre a proteção de crianças e o respeito aos direitos à privacidade e à minimização de dados pessoais, evitando especialmente a coleta desnecessária de dados sensíveis, como biometria facial (ICO, 2022; ISO; IEC/FDIS 2025).

2 *Segundo o art. 1º, V, da Lei 15.211 (ECA Digital): "V – perfilamento: qualquer forma de tratamento de dados pessoais, automatizada ou não, para avaliar certos aspectos de uma pessoa natural, com o objetivo de classificá-la em grupo ou perfil de modo a fazer inferências sobre seu comportamento, situação econômica, saúde, preferências pessoais, interesses, desejos de consumo, localização geográfica, deslocamentos, posições políticas ou outras características assemelhadas" (Brasil, 2025c).*

Em estudo realizado pela autoridade francesa Autorité de Régulation de la Communication Audiovisuelle et Numérique (ARCOM), identificou-se que telas são consumidas principalmente por crianças e adolescentes quando desacompanhados, e o monitoramento realizado pelos responsáveis está cada vez mais restrito, uma vez que o tamanho pequeno das telas de dispositivos celulares nem sempre permite a visualização do conteúdo consumido (ARCOM, 2024a, p. 8).

Outro estudo publicado pela ARCOM afirma que a exposição de crianças e adolescentes a conteúdos pornográficos na Internet está aumentando acentuadamente. A estimativa é de que a quantidade de crianças e adolescentes que visitam sítios eletrônicos de pornografia todos os meses passou de 19% em 2017 para 28% no final de 2022 (a publicação considerou maiores de dois e menores de dezoito anos). Em média, 12% da audiência de *sites* adultos é composta por crianças e adolescentes (ARCOM, 2024b, p. 5).

Diversas iniciativas têm sido empreendidas para dar embasamento a políticas e ações regulatórias sobre aferição de idade, no Brasil e no exterior. Para melhor compreensão das tecnologias envolvidas nessas iniciativas, apresentam-se neste documento alguns conceitos e termos utilizados para caracterizar a ação de se identificar a idade de usuários de serviços em ambientes digitais.

Este Radar Tecnológico visa analisar o cenário atual da aferição de idade de crianças e adolescentes em ambientes digitais. O estudo é fundamentado na perspectiva de entidades de proteção de dados, órgãos de defesa da criança e do adolescente, especialistas e na legislação nacional, com destaque para a Lei nº 15.211 (Brasil, 2025c). A seção 2 estabelece, a partir da literatura internacional, os principais conceitos relacionados, distinguindo os mecanismos de verificação e estimativa de idade, e definindo a aferição de idade como o resultado almejado. A seção 3 descreve e exemplifica os tipos de mecanismos utilizados. Na seção 4, são relacionadas as implicações de privacidade e proteção de dados no tratamento de informações pessoais inerentes a esses mecanismos. Por fim, a seção 5 oferece uma breve explanação sobre o tratamento do tema no Brasil, seguida, na seção 6, pelas perspectivas de futuro.

‹ conceitos principais ›

Nesta seção são apresentadas algumas definições de mecanismos utilizados para se identificar idade. A terminologia sobre este assunto tem sido adotada com algumas variações, como por exemplo o uso de termos aferição, verificação, estimativa e inferência de idade, muitas vezes usadas como sinônimos, e com o objetivo de se identificar a idade para assegurar, dar certeza ou garantir a idade de usuários em ambientes digitais, com a finalidade de se restringir ou permitir o acesso a determinados produtos ou serviços.

No Brasil, a Lei nº 15.211 (Brasil, 2025c) utiliza os termos aferição e verificação de idade, e representa um marco para a proteção de crianças e adolescentes em ambiente digital. Ela estabelece no art. 9º que os fornecedores de produtos ou serviços de tecnologia da informação que ofereçam conteúdo, produto ou serviço impróprio, inadequado ou proibido para menores de 18 anos deverão adotar mecanismos confiáveis de verificação de idade. A Lei também veda o uso da autodeclaração de idade, recurso muito utilizado por diversos provedores para atribuir ao usuário a responsabilidade por declarar a própria idade, sem nenhum tipo de comprovação ou garantia na resposta dada.

A Lei nº 15.211/2025 dedica o capítulo IV aos mecanismos de aferição de idade, facultando ao poder público a sua atuação "[...] como regulador, certificador ou promotor de soluções técnicas de verificação de idade, observados os limites da legalidade, da proteção à privacidade e dos direitos fundamentais previsto em lei" (Art. 11). No Art. 12, I, a lei determina ainda que os provedores de lojas de aplicações de Internet e de sistemas operacionais tomem "[...] medidas proporcionais, auditáveis e tecnicamente seguras para aferir a idade ou a faixa etária dos usuários, observados os princípios previstos no art. 6º da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais)".

Segundo a proposta de norma, a qual está em fase de aprovação final, ISO/IEC FDIS 27566-1 *Information security, cybersecurity and privacy protection – Age assurance systems: Part 1: Framework* (ISO; IEC 2025), garantia de idade é o processo de estabelecer, determinar ou confirmar um atributo

de garantia de idade. Um atributo de garantia de idade é a indicação de que uma pessoa possui uma determinada idade, o que pode ser identificado por meio das seguintes atividades: estimativa de idade (*age estimation*), verificação de idade (*age verification*) e inferência de idade (*age inference*).

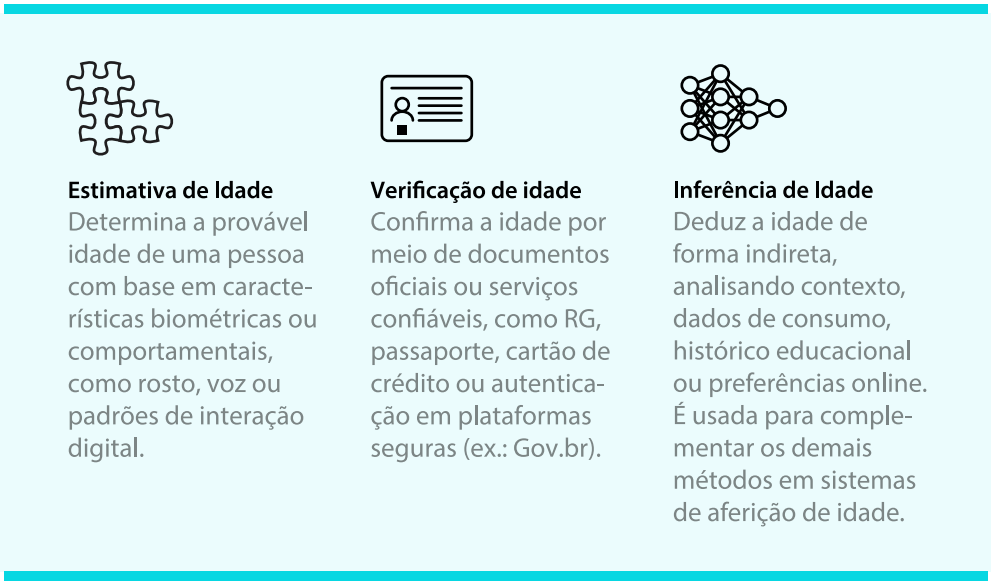


Figura 2 *Atividades que identificam a idade de uma pessoa em ambientes digitais.*

Fonte: Elaboração própria com base em ISO e IEC (2025).

O Office of Communications (Ofcom), autoridade reguladora do Reino Unido para as indústrias de radiodifusão, Internet, telecomunicações e correios, também adotou o termo *age assurance*, o qual refere-se tanto à verificação quanto à estimativa de idade. No entanto, a autodeclaração de idade, para este órgão, não é considerada uma forma de aferição de idade, uma vez que essa é informada pelo próprio usuário (Ofcom, 2023, p. 16).

Já o Information Commissioners Office (ICO), órgão executivo de transparência da informação e proteção de dados pessoais do Reino Unido, publicou o *Age appropriate design: a code of practice for online services* (ICO, 2022) em que foram definidas quatro abordagens principais para garantia de idade: i) verificação de idade; ii) estimativa de idade; iii) autodeclaração; e iv) técnicas em cascata e *buffers* de idade.

Foram também identificadas metodologias variadas para operacionalizar o conceito de verificação de idade, como apresentado primeiramente pela Commission Nationale de l'Informatique et des Libertés (CNIL), autoridade de proteção de dados francesa, que a dividiu em declaração, certificação e inteligência artificial (CNIL, 2021). Já na abordagem sugerida

pelo European Digital Rights (EDRI), o conceito de verificação de idade foi dividido em três subcategorias: declaração, verificação baseada em documentos e estimativa, como sinônimo de 'pontuação', 'avaliação' ou 'garantia' (EDRI, 2023, p. 10). Para o eSafety Commissioner, órgão regulador independente da Austrália para a segurança online, o termo garantia de idade é um termo guarda-chuva que se refere aos níveis de certeza para estimativa e verificação de idade (Austrália, 2023, p. 9).

Segundo a International Standards Organization (ISO), enquanto os mecanismos de verificação de idade determinam a idade de uma pessoa com alto nível de acurácia, geralmente por meio de documentos de identidade oficiais, os mecanismos de estimativa de idade oferecem uma idade aproximada para fins de restrição a conteúdo ou serviços disponíveis online, utilizando-se para tanto de dados comportamentais ou biométricos, com base em análises estatísticas (ISO; IEC, 2025, seção 3). O conceito adotado pela ISO evoluiu da definição do Bristish Standards Institute (BSI, 2018), que considera que "verificação de idade é o padrão ouro para garantia de idade", pela sua precisão na identificação real da idade do usuário. Por esse motivo, outros meios de checagem de idade, como a autodeclaração, não seriam considerados formas de se garantir a idade do usuário (AVPA, 2025).

Segundo o Family Online Safety Institute (FOSI), entidade estadunidense da sociedade civil, a garantia de idade é um termo mais amplo, que descreve vários métodos como verificação, estimativa e restrição de idade (*age gating*) (FOSI, 2023, p. 3). E, de acordo com o *Research Report: Mapping age assurance typologies and requirements*, a garantia de idade refere-se a métodos utilizados para determinar a idade de um indivíduo, com diferentes níveis de confiança e precisão, agrupados em três categorias: estimativa de idade, verificação de idade e autodeclaração de idade (Shaffique; Hof, 2024, p. 12). O relatório também define os provedores de serviços digitais como principais responsáveis por garantir ou assegurar a idade apropriada dos usuários que acessam os seus serviços (Shaffique; Hof, 2024, p. 21).

Em pesquisa realizada em 2024 pelo ICO e pela IFF Research, agência de pesquisa independente situada em Londres, de um total de 235 instituições do Reino Unido, 63% revelaram utilizar métodos de aferição de idade, sendo que 53% deles são métodos de autodeclaração, e 38% o uso

de cartões de crédito para verificação de idade. Mecanismos biométricos e identificação por fotografia são 28% e os demais métodos em torno de 10% cada, a exemplo de bases de dados de terceiros e de operadores de telefonia celular, pegada digital e open banking. Os demais métodos representam entre 1% e 2% (ICO; IFF Research, 2024, p.3).

O Ofcom estabeleceu um guia com critérios de avaliação da efetividade de métodos de garantia de idade ou *HEAA Guidance – Highly Effective Age Assurance* (Ofcom, 2025, p. 8), que visa identificar se os métodos são tecnicamente precisos, robustos, confiáveis e justos. A partir desse guia, o Ofcom pretende realizar uma análise para medir as tecnologias de aferição de idade junto a provedores de serviços e produtos pornográficos na Internet. O objetivo é avaliar o uso dos métodos e informações decorrentes de open banking, de identificação por foto, de estimativa biométrica da face, de prestador de telefonia móvel (*mobile network operator*, MNO), de cartões de crédito e de carteiras digitais (*digital wallets*) e autodeclaração, dentre outros, em sites com conteúdo pornográfico.

No Brasil, em 2024, o MJSP e o *United Nations Office on Drugs and Crime* (UNODC) firmaram acordo para a construção da Estratégia para Eliminar a Violência Contra Crianças e Adolescentes e para instituir a iniciativa *Children Amplified Prevention Services* (CHAMPS). Para subsidiar o acordo, a Secretaria Nacional de Direitos Digitais (SEDIGI) do MJSP elaborou a Nota Técnica no 4 (Brasil, 2025d), em que definiu a garantia etária como o conjunto de ferramentas e métodos utilizados para evitar o acesso por crianças e adolescentes a produtos e serviços inadequados à idade. A estratégia brasileira, fruto desse acordo, originou a publicação do *Plano Crescer em Paz: Estratégia de Justiça e Segurança Pública para Proteção de Crianças e Adolescentes*, que propõe quarenta e cinco medidas de prevenção a violências, o acolhimento e a recuperação das vítimas e a facilitação do acesso à justiça, e entre elas, o aperfeiçoamento das práticas da indústria, de serviços digitais e de sites de conteúdo adulto, para melhoria dos padrões de verificação etária, conforme as melhores práticas internacionais (Brasil, 2025b).

Na seção seguinte, estão listados exemplos e definições relacionadas ao tema, a partir das diversas abordagens e conceitos apresentados anteriormente. Portanto, visando a uma harmonização terminológica, este

documento adota o termo guarda-chuva *aferição de idade* para se referir às aplicações utilizadas para *a garantia de idade de uma pessoa, seja por meio de mecanismos de verificação, estimativa ou inferência de idade*.

‹ mecanismos de aferição de idade ›

Uma série de aplicações tem sido apresentadas, por diversas instituições, para se aferir a idade de usuários de produtos e serviços em ambientes digitais. As aplicações são, muitas vezes, apresentadas com diferentes nomes como mecanismos, métodos, abordagens ou tipologias de aferição de idade. A declaração ou autodeclaração de idade, por muitas instituições analisadas, não é considerada, por si só, um método de aferição de idade, pois depende que o próprio indivíduo forneça sua idade ou confirme sua faixa etária, sem que tenha de informar nenhuma evidência como prova da declaração. Por esse motivo, para fins deste estudo, o mecanismo de declaração ou autodeclaração de idade não será considerado um método de aferição de idade se utilizado isoladamente e, sim, uma característica ou requisito adotado em conjunto com outros métodos de aferição de idade.

A proposta de norma ISO/IEC FDIS 27566-1 (ISO; IEC, 2025), por exemplo, propõe que a garantia de idade no ambiente digital ocorra de três formas: pela verificação documental (diferença entre datas extraídas de registros oficiais), pela estimativa biométrica (características do rosto, da voz ou do corpo) e pela inferência indireta, baseada em dados contextuais ou padrões de uso.

Nas seções seguintes, apresentamos uma descrição geral de cada um dos tipos de mecanismos de aferição de idade, na seção 4, são levantadas questões relacionadas à privacidade e à proteção de dados decorrentes do uso desses mecanismos voltados para a aferição de idade.

Mecanismos de verificação de idade

A verificação de idade refere-se a qualquer método adotado para verificar a idade exata de uma pessoa de modo a confirmar que ela possui a idade permitida para ter acesso a determinados ambientes digitais. A verificação pode ser feita por meio do escaneamento de um documento de identidade digital, por um documento identificador oficial, ou por algum serviço de terceiros, como dados da Receita Federal (inscrição no Cadastro de Pessoas Físicas – CPF), dados bancários, eleitorais ou outros. Os mecanismos de verificação de idade estão subdivididos em três tipos principais: verificação baseada em documentos, verificação baseada em ato de terceiros e verificação como serviço.

Verificação de idade baseada em documentos

Esse tipo de mecanismo requer que o usuário forneça algum documento de identificação em que a idade possa ser verificada de forma manual ou automática. Essa é uma forma de aferição em que são exigidos documentos originais do usuário, a partir do envio da imagem, ou verificação de filmagem online, validada por um sistema de informação, ou por uma pessoa. A partir de bases de dados centralizadas, os dados são acessados pelos provedores de serviços para verificação automática de integridade do documento, por vezes utilizando-se de sistemas de inteligência artificial.

Foram identificados dois principais mecanismos de verificação de idade baseada em documentos: por documento oficial e por cartão de crédito. Na *verificação por documento oficial*, o provedor solicita cópia de documentos como carteira de identidade, motorista ou passaporte, extraindo a data de nascimento e verificando a autenticidade através de análise manual ou automática, além de comparar uma fotografia do usuário com a foto do documento.

A *verificação por cartão de crédito* consiste na validação do cartão pelo usuário, geralmente por meio de cobrança de pequeno valor. É um método voltado para garantir que o usuário é maior de 18 anos.

Verificação de idade baseada em dados de terceiros

A verificação de idade por terceiros utiliza informações fornecidas por outras pessoas para validar a idade do usuário, abrangendo três modalidades principais: verificação por consentimento parental, por reconhecimento social e verificação como serviço (*Verification as a Service* - VaaS).

Na *verificação de idade por consentimento parental*, os responsáveis legais realizam a confirmação utilizando meios oferecidos pela própria plataforma. A eficiência deste método depende da verificação prévia da idade do responsável e da confirmação do vínculo familiar, geralmente por meio de análise documental. Uma variação desse método é a conta familiar, na qual o titular principal vincula suas informações pessoais aos dados da criança ou adolescente, permitindo controle adequado dos serviços conforme a faixa etária (ICO; IFF Research, 2024, p. 15).

De acordo com a Lei nº 15.211/2025, no art. 24 do capítulo IX dedicado a redes sociais,

> *no âmbito de seus serviços, os provedores de produtos ou serviços direcionados a crianças e a adolescentes ou de acesso provável por eles deverão garantir que usuários ou contas de crianças e de adolescentes de até 16 (dezesseis) anos de idade estejam vinculados ao usuário ou à conta de um de seus responsáveis legais (Brasil, 2025c).*

Assim aplicativos ou serviços que são voltados para crianças e adolescentes (ou que eles provavelmente vão usar) precisam garantir que a conta de um usuário menor de 16 (dezesseis) anos esteja conectada à conta de um de seus pais ou responsáveis legais. Isso é uma forma de dar mais controle aos pais sobre o que os filhos fazem online, em particular nas redes sociais.

Na *verificação de idade por reconhecimento social*, permite-se que usuários já verificados confirmem a idade de novos usuários, funcionando como um sistema de fiança, segundo o qual a plataforma confia na garantia fornecida por titulares de contas já existentes.

Já a *verificação de idade como serviço* (VaaS) consiste na terceirização do processo de verificação para instituições públicas ou privadas confiáveis, que assumem a responsabilidade de identificar e garantir a idade do usuário. Esse mecanismo utiliza dados pessoais como nome e data de nascimento, comparando-os com informações obtidas em bases de dados oficiais de órgãos públicos, bancos ou serviços sociais. O método é utilizado em muitos países para a verificação de idade de adultos em sites com restrições etárias, para autorização de compras de produtos controlados como álcool e tabaco, realização de apostas online e prevenção do acesso de crianças e adolescentes a esses serviços. Nesse processo de verificação de idade, há a possibilidade de se recorrer a intermediários confiáveis que emitem *tokens* de idade (*age tokens*) para os usuários se autenticarem, conferindo maior segurança aos seus dados pessoais (Shaffique; Hof, 2024, p. 33). Isso ocorre porque o *token* é um tipo de prova de idade digital que criptografa a idade do usuário para uso no ambiente digital por um provedor de aplicação, sendo armazenado em seu navegador, como um *cookie*, ou em uma carteira digital do telefone celular. Conforme o usuário navega na Internet, o *token* permite ou não que ele entre em determinados sites ou serviços, conforme sua idade.

Há também os métodos de verificação por meio de operador de rede de telefonia celular MNO+18 – *Mobile Network Operator 18+ Content Restriction Filter* (ICO; IFF Research, 2024). De acordo com este método, disponível no Reino Unido, a operadora oferece um serviço de filtro de conteúdo que impõe restrição de conteúdo no chip do aparelho de celular, a fim de proteger clientes menores de 18 anos, tendo como referência as regras do Conselho Britânico de Classificação de Filmes (BBFC).

A verificação de idade como serviço também pode ocorrer por meio de autenticação multiplataforma (Shaffique; Hof, 2024, p. 28), uma das formas de garantia mais utilizadas pelas grandes empresas de tecnologia. Ela é feita por meio de métodos de autenticação a partir do cadastro em suas bases (de e-mail, rede social, serviços diversos de *streaming*), que são usadas para verificação de idade por terceiros. Esses terceiros atuam como autenticadores centrais do usuário para todos os serviços da plataforma.

Mecanismos de estimativa de idade

A estimativa de idade refere-se aos métodos para estimar a idade ou a faixa etária de um usuário, em vez de determinar sua idade exata, sem o uso de documentos comprobatórios ou confirmações de terceiros. Esses mecanismos utilizam dados comportamentais (histórico de navegação e preferências de compra, por exemplo), dados biométricos, testes de capacidade, entre outros, para calcular a idade provável, por meio de modelos de estimativa. Esse método pode ser usado para criação de contas ou para monitoramento do uso de serviços.

Os mecanismos de estimativa de idade podem ser divididos em três métodos principais: estimativa de idade via análise de comportamento online, por biometria e via teste de capacidade.

A *estimativa de idade via análise de comportamento online* é feita por meio da análise de dados históricos alimentados em um sistema de inferência, com apoio de inteligência artificial, que estima a idade aproximada do usuário. Pode-se rastrear as "pegadas" do usuário por meio do número do telefone celular, ou endereço de e-mail, análise das interações, ou de contas criadas com esses dados em diferentes sites (ICO, 2024b).

A *estimativa de idade por biometria* consiste no uso de dados biométricos (por exemplo, a imagem da face ou a voz do usuário) para que o modelo estime a idade, geralmente por meio de uma tecnologia de inteligência artificial. A imagem da face pode ser capturada em tempo real pela câmera do celular ou por uma câmera específica, com maior nível de acurácia e eficiência, embora esses resultados variem em relação ao tom da pele, ao sexo e à idade.

Finalmente, a *estimativa de idade via teste de capacidade* consiste na formulação de uma ou mais perguntas-desafio ao usuário, que identifica seu conhecimento sobre determinado assunto, sua capacidade, ou sua aptidão em resolver algum problema (de matemática, de conhecimentos gerais ou de ortografia, por exemplo) e assim agrupá-lo em uma faixa etária. É utilizada para estimar a idade aproximada de um usuário em razão do conhecimento prévio que ele tenha sobre um determinado conteúdo ensinado em uma série escolar e, portanto, dentro de uma faixa etária estimada.

Mecanismos de inferência de idade

De acordo com a proposta de norma ISO/IEC FDIS 27566-1 (ISO; IEC, 2025) a inferência de idade é um método de garantia de idade baseado em informações verificadas que indiretamente implicam que um indivíduo está acima ou abaixo de uma determinada idade ou dentro de uma faixa etária. É um termo muitas vezes utilizado como sinônimo de estimativa de idade, em especial quando se utilizam tecnologias de inteligência artificial para se inferir a idade do usuário a partir de dados comportamentais. Utilizando-se da análise de padrões contextuais, comportamentais e interações digitais, a inferência de idade busca determinar a idade provável de um usuário ou uma faixa etária com base em sinais indiretos e verificáveis coletados a partir de seu comportamento, contexto e dados digitais, sem a necessidade de exigir documentos de identidade ou dados biométricos. Ou seja, em vez de perguntar diretamente

Figura 3 *Tipos de mecanismos de verificação e estimativa de idade..*

Fonte: Elaboração própria.

a idade ou pedir um documento, o sistema busca pistas indiretas, com o objetivo de tirar uma conclusão razoável sobre a idade de um usuário ao analisar um conjunto de fatos digitais. Os mecanismos de inferência de idade baseiam-se em análise de padrões sobre a forma como o usuário interage na plataforma, como, por exemplo, a velocidade de navegação, o tipo de vocabulário utilizado ou o tempo de fala, o tipo de conteúdo consultado historicamente, que tipo de transações foram realizadas e quais produtos ou serviços foram utilizados.

Etapas de funcionamento dos mecanismos

A partir da abordagem da proposta de norma ISO/IEC FDIS 27566-1 (ISO; IEC, 2025), foi possível organizar o conjunto de soluções em quatro eixos: verificação documental, identificação vinculada à identidade civil, estimativas biométricas e inferências comportamentais. Do ponto de vista técnico, em geral essas abordagens seguem uma mesma lógica de funcionamento, que pode ser descrita como um *pipeline* de cinco etapas[3], descritas a seguir.

1. **Coleta dos dados**: o sistema recebe como entrada uma fotografia, vídeo, áudio, documento oficial ou até sinais indiretos, como padrões de navegação ou características do dispositivo.

2. **Pré-processamento**: os dados brutos são tratados para se tornarem utilizáveis: um documento é lido por *Optical Character Recognition* (OCR), uma imagem ou áudio são normalizados para corrigir iluminação, ruídos ou distorções, e apenas os traços mais relevantes (features) são extraídos, como o contorno do rosto ou a textura da pele. Esse filtro evita erros simples que poderiam comprometer a análise.

3. **Processamento principal**: é a fase decisiva. Dependendo da tecnologia, pode envolver a comparação entre um documento e uma base oficial, a estimativa algorítmica da idade com base em biometria, ou a simples classificação em faixas (“menor de 13 anos”, “maior de 18 anos”). Em aplicações mais avançadas, o resultado

3 *A opção por descrever os mecanismos de aferição de idade em formato de pipeline foi inspirada na ISO/IEC 27566-1:2025, que caracteriza tais sistemas como compostos por componentes interdependentes (credenciais, subsistemas de processamento, provedores de serviços) e recorre a diagramas de fluxo para ilustrar a tomada de decisão sobre elegibilidade etária. Essa abordagem sequencial também é adotada em relatórios acadêmicos, como o Trustworthy Age Assurance (Sas; Mühlberg, 2024), que organiza a análise em fases encadeadas (autodeclaração, verificação documental, estimativa biométrica ou comportamental, emissão de tokens e transmissão da prova). Sobre as etapas, embora parte da literatura simplifique o processo em três macrofases (coleta, processamento e emissão), as normas técnicas (ISO/IEC 27566-1:2025) e guias regulatórios (CNIL, 2022; Ofcom, 2025) apontam a relevância de detalhar cinco etapas: (i) coleta, (ii) pré-processamento, (iii) processamento principal, (iv) controles de integridade e (v) emissão da evidência. Essa fragmentação mais fina reflete exigências contemporâneas de segurança, privacidade e robustez, justificando a adoção de um modelo de cinco fases neste trabalho.*

não revela a identidade, mas gera uma credencial digital ou token que atesta apenas o atributo etário.

4. **Controles de integridade**: para reduzir fraudes, aplicam-se técnicas de prova de vivacidade, detecção de apresentações falsas (como *deepfakes* ou fotos estáticas), limitação de tentativas e, quando necessário, revisão humana. Esses mecanismos garantem que a verificação não seja enganada por manipulações.

5. **Emissão de evidência**: o sistema produz a prova final de que o critério etário foi cumprido. Diferentemente de métodos antigos que expunham nome ou data de nascimento, as aplicações atuais buscam emitir apenas o atributo essencial, muitas vezes em forma de token digital, com prazo de validade, restrições de uso e proteção criptográfica. Em alguns casos, aplicam-se protocolos avançados, como provas de conhecimento-zero, ou *zero-knowledge proofs* (ZKP)[4], que permitem confirmar a maioridade sem revelar quem é o usuário nem para qual serviço a informação foi apresentada.

Para além da teoria, alguns países têm avaliado essas tecnologias em ambientes controlados de teste, conhecidos como *testbeds*, em que diferentes métodos são analisados de forma comparável, considerando critérios como acurácia, viés, resiliência a fraudes e impacto no direito de proteção de dados. O exemplo mais notório é o *Age Assurance Technology Trial* (Austrália, 2025a) realizado na Austrália em 2025, que colocou lado a lado aplicações documentais, biométricas, inferenciais e modelos baseados em *tokens*. O estudo também mediu o desempenho dessas tecnologias em diferentes camadas do ecossistema digital como dispositivos, sistemas operacionais, navegadores e plataformas, destacando a importância da interoperabilidade (ACCS, 2025, p. 8)[5].

Uma visão geracional de mecanismos de aferição de idade

A partir de uma análise do panorama internacional sobre o assunto, organizamos a evolução das aplicações em cinco

4 *As provas de conhecimento zero (Zero-Knowledge Proofs – ZKP) são protocolos criptográficos que permitem a um usuário demonstrar a veracidade de uma informação, como ser maior de idade, sem revelar o dado subjacente, garantindo privacidade e minimização de atributos pessoais. Trata-se de técnica destacada em debates regulatórios internacionais sobre mecanismos de verificação de idade, como nos relatórios da CNIL (2022) e da Comissão Europeia (Comissão Europeia, 2025d), que apontam seu potencial para equilibrar robustez e proteção de dados.*

5 *O Age Assurance Technology Trial (Austrália, 2025a) foi conduzido pelo eSafety Commissioner da Austrália em 2025, em ambiente controlado de testes (testbed), comparando métodos documentais, biométricos, inferenciais e baseados em tokens, com foco em critérios como acurácia, viés, resiliência antifraude e impacto na proteção de dados. Já o Global Age Assurance Standards Summit (ACCS, 2025) não realizou diretamente o* testbed*, mas sistematizou e discutiu os resultados obtidos, destacando a importância da interoperabilidade e da padronização internacional.*

gerações[6], cada uma marcada por avanços técnicos, demandas regulatórias e exigências sociais. Essa cronologia não deve ser entendida como rígida, já que há sobreposições, mas ajuda a visualizar a trajetória que vai da autodeclaração rudimentar até os sistemas sofisticados de credenciais auditáveis e testadas em escala.

1ª Geração | Autodeclaração (anos 2000–2010)

O primeiro estágio da aferição de idade no ambiente digital foi marcado pela autodeclaração. Nesse modelo, o próprio usuário informa a sua idade, seja ao digitar uma data de nascimento, seja ao marcar caixas do tipo "Tenho mais de 18 anos". Em algumas plataformas, buscou-se reforçar esse procedimento com *proxies* como número de cartão de crédito, SMS, e-mail validado ou autenticação via conta de terceiros.

Apesar dessas variações, o método continua dependente da boa-fé do usuário e não estabelece vínculo com a identidade civil. Reguladores como a CNIL (2022) e o Ofcom (2024) classificam a autodeclaração como prática de baixa intrusão, mas de baixa confiabilidade, adequada apenas a serviços de risco reduzido (ICO, 2022). Como mencionado anteriormente, o mecanismo de declaração ou autodeclaração de idade não será considerado um método de aferição de idade se utilizado isoladamente. Nesse mesmo sentido, a ANPD também já se posicionou, em sua Nota Técnica nº 50/2024, ao avaliar práticas de plataformas digitais, destacando que a autodeclaração, quando utilizada de forma exclusiva, não configura mecanismo idôneo de aferição de idade (ANPD, 2024b).

Do ponto de vista técnico, a primeira geração de mecanismos de aferição de idade se baseia em formulários simples, geralmente em HTML ou incorporados em aplicativos. Alguns sistemas adotam validações básicas de formato, como impedir idades negativas ou acima de 120 anos, verificar a coerência de datas ou limitar tentativas sucessivas para reduzir fraudes e ataques de força bruta. Os dados declarados são então gravados no registro da conta ou do dispositivo e utilizados para liberar ou restringir funcionalidades, como acesso a determinados conteúdos ou habilitação de recursos de interação.

6 *Para justificar a opção metodológica de classificar as tecnologias de garantia da idade em "gerações", ressaltamos alguns pontos de nossa investigação: 1 - A literatura técnica e normativa trata as soluções como etapas ou categorias distintas, refletindo uma evolução histórica. 2 - Há marcos regulatórios (CNIL, ICO, Ofcom, EDPB, Comissão Europeia) que impulsionaram ondas de mudança em forma de evolução. 3 - A ISO/IEC 27566-1:2025 organiza os métodos em tipos/categorias (verificação, estimativa, inferência), com diferentes níveis de confiança e maturidade temporal. 4 - Estudos comparativos como Trustworthy Age Assurance? (Sas; Mühlberg, 2024) também agrupam os métodos em "famílias" tecnológicas, evidenciando um caráter progressivo de sofisticação. 5 - Órgãos reguladores (CNIL, 2022; Ofcom, 2025) e o EDPB (2025) ressaltam que métodos mais simples (autodeclaração) são ineficazes, e que tecnologias mais recentes (*tokens *criptográficos, provas de conhecimento-zero) representam um avanço em confiabilidade e proteção de dados, o que ocorre em uma escala evolucionária. Esses argumentos nos levaram a optar por uma classificação que envolvesse tempo, complexidade e recursos tecnológicos.*

Na prática, esse fluxo é tecnicamente pouco robusto. A previsibilidade e a facilidade de manipular datas de nascimento tornam esse tipo de informação pouco confiável para fins de verificação de idade. Como resultado, é muito mais fácil criar múltiplas contas usando dados falsos, pois a informação não é única o suficiente para impedir a fraude. Em outras palavras, por ser um dado facilmente dedutível e de simples falsificação, a data de nascimento favorece a criação de múltiplos cadastros com informações inverídicas. Além disso, a ausência de mecanismos de vinculação à identidade civil e de camadas adicionais de comprovação, como biometria ou verificação documental, limita a confiabilidade desse método.

Estudos de autoridades reguladoras, como os conduzidos pelo Ofcom (2024) e por autoridades australianas no *Age Assurance Technology Trial* (Australia, 2025a, p. 142), mostram taxas elevadas de falsificação etária (*lying up*) por crianças, confirmando que, mesmo com pequenos controles compensatórios, a autodeclaração permanece uma solução de baixa confiabilidade.

2ª Geração | Verificação documental e biometria (2010–2018)

A segunda geração de mecanismos de aferição de idade surgiu com a popularização de *smartphones* com câmera e a digitalização de serviços financeiros e públicos. O fluxo técnico, descrito em normas internacionais de padronização (ISO; IEC, 2025), em nota técnica da SEDIGI (Brasil, 2025d) e nos relatórios do Ofcom (2024), começa com a captura de um documento oficial como carteira de identidade, CNH ou passaporte, que é submetido a OCR (Reconhecimento Óptico de Caracteres).

Essa etapa converte a imagem em texto estruturado, permitindo a extração automática de informações como nome, número do documento e data de nascimento. Sistemas mais avançados não apenas leem o texto, mas também analisam padrões gráficos (hologramas, fontes, margens e microtexturas) para detectar indícios de falsificação.

Em seguida, aplica-se a correspondência facial (*face matching*), no qual o usuário fornece uma *selfie* ou um breve vídeo que é comparado à fotografia presente no documento. Essa etapa, baseada em algoritmos de reco-

nhecimento facial, cria um vínculo entre a identidade declarada e a pessoa que busca acesso, reduzindo o risco de uso de documentos de terceiros.

Para reforçar a eficiência, os sistemas incorporam a prova de vivacidade (liveness detection). No modelo passivo, algoritmos avaliam características sutis da captura, como reflexos de luz na pele ou profundidade da imagem sem exigir interação do usuário. Já no modelo ativo, há uma exigência de movimento em tempo real, como piscar, sorrir ou virar o rosto em diferentes ângulos. Ambos os métodos são recomendados por estudos recentes (Australia, 2025a) e nos relatórios do Ofcom (2025), como forma de impedir que fotos impressas, vídeos ou deepfakes enganem o sistema.

3ª Geração | Estimativas ou inferências biométricas e comportamentais (2018–2022)

A terceira geração de mecanismos de aferição de idade foi impulsionada pelo avanço da inteligência artificial e pelo uso crescente de modelos de aprendizado profundo em visão computacional e análise de padrões. Diferentemente da verificação documental, esse modelo não depende do envio de credenciais oficiais, pois a idade é estimada diretamente a partir de características biométricas ou comportamentais.

O fluxo técnico envolve, em primeiro lugar, a captura de dados como imagens faciais, amostras de voz, vídeos curtos ou até padrões de interação com dispositivos (por exemplo, digitação, velocidade de navegação, uso de aplicativos). Esses dados são tratados em redes neurais treinadas com grandes bases de exemplos rotulados, permitindo identificar *features* discriminativas (linhas de expressão, textura da pele, variações na voz, tempo de reação, entre outros).

Os algoritmos de regressão estimam uma idade numérica aproximada, enquanto os modelos de classificação estimam, para cada faixa etária definida no treinamento, a probabilidade de pertencimento e atribuem ao usuário a classe com maior probabilidade, como "menor de 13 anos", "13 a 17 anos" ou "18+". Esse modelo é descrito em normas internacionais de padronização (IEEE, 2024; ISO; IEC, 2025), em estudos de autoridades

reguladoras como o *Age Assurance Technology Trial* (Austrália, 2025a), em publicações de entidades como *Global Age Assurance Standards Summit* (ACCS, 2025) e em relatórios do Ofcom (2024). Tal abordagem é considerada mais prática no contexto regulatório, pois reduz a necessidade de coleta e armazenamento de documentos pessoais. Entretanto, essa geração apresenta limites técnicos e éticos relevantes. A precisão varia de acordo com a qualidade do dado de entrada e com a diversidade da base de treinamento.

Um método biométrico também utilizado nessa geração é a análise de voz, que parte da premissa de que características acústicas se modificam ao longo do desenvolvimento humano. A operação inicia com a coleta de amostra vocal em que o usuário repete uma frase ou lê um texto curto. A seguir ocorre a extração de parâmetros como o cálculo da frequência fundamental (*pitch*), distribuição de formantes (ressonâncias vocais), velocidade de articulação e variação prosódica. Por fim, ocorre a classificação algorítmica em que modelos de aprendizado de máquina, *Random Forest* ou redes neurais, associam o vetor acústico a uma faixa etária provável.

Embora menos preciso que a análise facial, o reconhecimento de voz pode ser útil em contextos em que a câmera não está disponível, como assistentes virtuais e jogos baseados em áudio. Outra forma de marcador etário é a análise de escrita e padrões linguísticos. O sistema coleta textos digitados ou falas transcritas do usuário e aplica técnicas de processamento de linguagem natural (NLP) para identificar, por exemplo, a frequência de gírias, emojis e abreviações; a estrutura sintática típica de adolescentes (frases curtas, erros ortográficos frequentes); e até mesmo a riqueza lexical em conjunto com escolhas estilísticas associadas a faixas etárias mais altas.

Modelos supervisionados de classificação textual conseguem estimar ou inferir a idade com acurácia crescente, mas ainda enfrentam problemas de adaptação cultural e de manipulação (crianças podem imitar vocabulário adulto).

Além de voz e linguagem, os padrões de interação com dispositivos fornecem sinais úteis como a velocidade e cadência de digitação (*keystroke dynamics*), o tempo de resposta em jogos e charadas (crianças costumam

ter tempos diferentes de adultos) e o uso de dispositivos (horários, duração, tipos de aplicações).

A coleta desses dados gera vetores comportamentais analisados por algoritmos de classificação probabilística. Essa modalidade, chamada de biometria passiva, aparece descrita em normas internacionais de padronização (IEEE, 2024; ISO; IEC, 2025), em estudos como o *Age Assurance Technology Trial* (Austrália, 2025a). Pesquisas aplicadas demonstram que padrões de digitação podem servir como indicadores etários. Pentel (2018), por exemplo, mostrou que a análise de *keystroke dynamics* em diferentes dispositivos permite distinguir grupos etários com elevado grau de acurácia, mesmo em cenários de entrada curta e não controlada. Esse tipo de tratamento de dados funciona em segundo plano, sem interação explícita com o usuário.

4ª Geração | Tokens e provas criptográficas (2022–2025)

Após 2022, observa-se uma intensificação na agenda regulatória global de proteção de dados. Nesse momento, ganha força a ideia de que não é necessário expor identidade completa para garantir apenas um atributo, como a maioridade. Soluções baseadas em provas de conhecimento-zero (ZKP) e protocolos *double-blind* surgem em paralelo ao avanço das credenciais digitais soberanas (*self-sovereign identity*) e às exigências de privacidade por *design*.

A quarta geração de tecnologias de aferição de idade baseia-se em abordagens criptográficas avançadas que permitem comprovar atributos etários (como ser maior de idade) sem revelar informações pessoais identificáveis. Nesse modelo, credenciais mínimas, muitas vezes organizadas como "*tokens* criptográficos", são emitidas e utilizadas de forma seletiva e segura.

Na União Europeia, o *EU Age Verification Solution*, lançado pela Comissão Europeia em julho de 2025, representa um marco nessa transição. A proposta permite que o usuário comprove que é maior de 18 anos sem compartilhar quaisquer outros dados pessoais. A emissão e a apresentação dessa prova são realizadas por entidades separadas, garantindo confidencialidade e evitando rastreamento entre serviços, modelo que

a Comissão associa ao princípio da privacidade por *design* (Comissão Europeia, 2025a). Além disso, o uso de provas de conhecimento-zero continua em desenvolvimento para garantir que tais autenticações sejam não vinculativas e não rastreáveis.

Esse movimento encontra respaldo em análises acadêmicas e governamentais que destacam o papel das ZKPs na promoção da minimização de dados, especialmente em sistemas como carteiras digitais compatíveis com o *General Data Protection Regulation* – GDPR (União Europeia, 2016) e o eIDAS (Comissão Europeia, 2025c). A tecnologia permite apresentar provas válidas sem expor metadados adicionais que poderiam comprometer a privacidade do usuário. A seguir, apresentam-se algumas dessas tecnologias com mais detalhes.

Tokens criptográficos (age tokens)

É uma espécie de credencial digital, emitida e assinada por uma entidade de confiança, que serve para comprovar um atributo específico de uma pessoa sem expor seus dados completos. Esse modelo é descrito em normas internacionais de padronização (ISO/IEC, 2025; W3C, 2025) e em estudos recentes na Austrália (Australia, 2025b) e na União Europeia (Comissão Europeia, 2025a). No contexto da aferição de idade, o *token* não carrega dados como nome, CPF ou data de nascimento. Em vez disso, ele contém apenas a informação necessária, por exemplo ser "maior de 13 anos" ou "entre 16 e 18 anos" ou ainda "maior de 18 anos". Essa credencial é protegida por criptografia, o que garante sua autenticidade e impede falsificações.

Observamos que a emissão e uso de *tokens* segue quatro etapas principais:

1. Validação inicial. O usuário comprova sua idade a um prestador de confiança (por documento oficial, biometria ou outro método robusto).

2. Geração do *token*. O prestador emite um *token* digital criptograficamente assinado (padrões como JWT ou credenciais verificáveis em *blockchain*). Esse *token* contém apenas o atributo necessário: "18+" ou "entre 16 e 18 anos".

3. Armazenamento seguro. O *token* é mantido pelo usuário, seja em *wallets* digitais, seja em armazenamento local no dispositivo (com prazo de validade definido).

4. Apresentação em serviços de terceiros. Quando requisitado, o usuário apresenta o *token*, que é validado pela chave pública do emissor.

De maneira geral, esse fluxo cria uma camada de desvinculação (*unlinkability*), em que o serviço acessado não sabe qual método de verificação foi usado originalmente, e o prestador de verificação não sabe em quais serviços o *token* será utilizado.

Modelo duplo-cego

Na arquitetura contemporânea de aferição de idade, é importante distinguir entre o que se entende por *token* criptográfico e o que se denomina modelo duplo-cego (*double-blind*). Como mencionado, o *token* é, em essência, uma credencial digital emitida por uma entidade confiável. Ele funciona como uma espécie de carimbo matemático que atesta apenas um atributo específico, por exemplo, que o usuário é maior de 18 anos, sem revelar a data de nascimento ou qualquer outro dado pessoal. Essa credencial pode ser temporária, sujeita a políticas de reuso e protegida por assinatura digital que impede sua falsificação.

O modelo duplo-cego, por sua vez, é o protocolo que rege o uso desses *tokens*. O termo "duplamente cego" expressa o arranjo em que as partes envolvidas têm acesso apenas a informações mínimas sobre o usuário. Assim, nem quem emite a credencial sabe em qual serviço ela será apresentada, nem o serviço que a recebe consegue identificar quem está por trás dela. Em outras palavras, o emissor não rastreia o comportamento do usuário, e o receptor não tem acesso à sua identidade, ficando restrito à informação binária de que o requisito etário foi atendido. A estrutura do duplo-cego aparece nos padrões do W3C (2025), no framework da proposta de norma ISO/IEC/FDIS 27566 (2025), no *European Age Verification Solution: Operational, Security, Product and Architecture Specifications* (Comissão Europeia, 2025d) e nos experimentos do *Age Assurance Technology Trial*, na Austrália (2025a).

Assim, enquanto o *token* criptográfico representa o instrumento de minimização de dados, a "chave digital" que contém apenas o atributo etário, o modelo duplo-cego define as regras de circulação desse *token* de modo a preservar a privacidade em todo o ciclo. Juntos, eles compõem uma estratégia que reduz drasticamente a possibilidade de rastreamento e fortalece a proteção contra abusos no tratamento de dados pessoais.

Provas de conhecimento zero

Entre as abordagens analisadas, uma das aplicações mais promissoras para reforçar o respeito às normas de proteção de dados nos sistemas de aferição de idade é o uso de provas de conhecimento zero (em inglês: *zero-knowledge proofs* – ZKP). Nesse modelo, não há necessidade de compartilhar dados pessoais como a data de nascimento, mas apenas de comprovar matematicamente o atendimento ao requisito de idade.

Em termos práticos, o dispositivo ou a carteira digital do usuário realiza um cálculo criptográfico sobre suas informações (data de nascimento, por exemplo), que permanecem armazenadas de forma segura e não são reveladas. O resultado dessa operação é um comprovante matemático enviado ao serviço. A plataforma, por sua vez, não tem acesso ao dado pessoal, mas recebe uma prova suficiente para confirmar se a condição foi atendida. O desfecho é simples e objetivo: a resposta chega em forma de "sim" ou "não", permitindo ou negando o acesso.

Esse modelo evita a criação de bases centralizadas com datas de nascimento, diminui a possibilidade de rastreamento entre diferentes serviços e reduz de forma significativa os riscos em caso de vazamento de dados.

Embora os conceitos do ZKP e do modelo duplo-cego possam ter alguma similaridade, são duas abordagens distintas que podem ser aplicadas em sistemas de aferição de idade, mas atuam em níveis diferentes. O ZKP é um método criptográfico, já o modelo duplo-cego é um arranjo de confiança entre diferentes atores. Para melhor visualizar a diferença, segue um quadro comparativo.

Quadro 1 *Comparação entre ZKP e duplo-cego*

Aspecto	ZKP (Prova de Conhecimento Zero)	Modelo duplo-cego
Definição	Protocolo criptográfico que permite provar um fato sem revelar o dado em si.	Arquitetura de confiança onde emissor e receptor não têm acesso completo aos dados.
Como funciona	Usuário autoriza que o dispositivo ou carteira digital realize uma prova matemática sobre seus dados (ex.: idade ≥ 18) e envia apenas o resultado verificável.	Uma autoridade confiável emite um *token*/credencial cega; a plataforma só vê o token, e a autoridade não sabe onde ele foi usado.
Privacidade	Muito alta: a plataforma só recebe 'sim' ou 'não', nunca a data de nascimento.	Muito alta: separação de poderes evita rastreamento cruzado entre emissor e plataforma.

Fonte: Sas e Mühlberg (2024), ISO e IEC (2025), CNIL (2022), EDPB (2025).

Embora diferentes, essas duas abordagens podem ser complementares, visto que tokens emitidos em modelo duplo-cego podem, por exemplo, ser baseados em provas ZKP, somando densidade criptográfica e proteção contra rastreamento.

5ª Geração | Ambientes de testes (*testbeds*) e integração no *ecossistema tecnológico* (2025 em diante)

A 5ª geração desloca o foco sobre "qual método usar" para "como comprovar, integrar e auditar" em ecossistemas reais, com evidências de desempenho e de proteção de dados, orientando decisões regulatórias e de políticas públicas. A ideia é que, enquanto as gerações anteriores eram centradas no serviço individual (cada site e aplicação rodando sua própria verificação), esta geração é centrada na infraestrutura digital como um todo, com protocolos auditáveis e integração nativa.

Países como Austrália e Reino Unido iniciaram ambientes de testes[7] (*testbeds*) voltados à comparação de diferentes tecnologias de verificação etária. Nesses ambientes, as aplicações são avaliadas segundo critérios padronizados de acurácia, viés, resiliência antifraude e proteção da privacidade. Essa etapa representa uma fase de integração mais robusta, em que os mecanismos de aferição de idade passam a ser testados em todo o ecossistema tecnológico, incluindo dispositivos, sistemas operacionais, navegadores e plataformas. A lógica é assegurar que funcionem de forma interoperável, com credenciais padronizadas e sujeitas a auditorias independentes. Destaque é dado ao estudo australiano *Age Assurance Technology Trial* (Australia, 2025a), o qual foi implementado por um organismo certificador independente, com apoio de instituições acadêmicas e do setor industrial, e representa um estágio prático de experimentação regulatória, cujo relatório final compara acurácia, viés, detecção de fraude e salvaguardas de privacidade, e documenta como as soluções se comportam em camadas do ecossistema tecnológico, dispositivo, sistema operacional, navegador e plataforma, condição necessária para uma implementação realmente interoperável e auditável.

Em paralelo, o Reino Unido vem alinhando a exigência de "garantia de idade altamente eficaz" (*Highly Effective Age Assurance* – HEAA) à sua execução regulatória (Ofcom, 2024), enquanto a Comissão Europeia publicou um plano de verificação etária que prioriza credenciais minimizadas e integração futura com a *European Digital Identity Wallet*, reforçando a tendência de testes controlados, métricas padronizadas e desenho que preserva a privacidade desde sua arquitetura (Comissão Europeia, 2025a).

Os principais elementos tecnológicos dessa geração incluem arquiteturas de interoperabilidade, credenciais derivadas no ecossistema, tokens criptográficos avançados e integração com carteiras digitais soberanas, acompanhados de camadas reforçadas de segurança. Além disso, experiências regulatórias como o *Overall Architecture – European Age Verification Solution* da Comissão Europeia (2025) e o *Age Assurance Technology Trial* da Austrália (2025a) apontam a importância de *testbeds* para avaliação de desempenho, viés e impacto em privacidade. Apresentamos uma descrição resumida desses elementos que caracterizam a 5ª geração de mecanismos de aferição de idade:

7 ***Testbeds*** *são ambientes controlados de experimentação criados para avaliar, de forma comparativa, diferentes tecnologias de aferição de idade antes de sua adoção em larga escala. Tais ambientes permitem analisar a eficácia técnica, a proporcionalidade, os impactos sobre a privacidade e a inclusão digital. A Comissão Europeia, por exemplo, tem conduzido projetos-piloto com a chamada "mini carteira de idade" como forma de comprovação etária preservando a privacidade (Comissão Europeia, 2025b). A CNIL, por sua vez, recomenda que modelos de verificação sejam testados em condições controladas para garantir robustez sem comprometer a minimização de dados (CNIL, 2022). No Reino Unido, a Ofcom passou a exigir que serviços de alto risco empreguem métodos considerados "altamente eficazes", avaliados previamente em ambientes de teste (Ofcom, 2025). De forma convergente, a ISO/IEC 27566-1 estabelece parâmetros de confiança e segurança que podem ser validados em testbeds antes da implementação em ecossistemas digitais (ISO; IEC, 2025).*

+ **Arquiteturas de interoperabilidade**: protocolos padronizados que permitem que diferentes métodos de verificação (documento, biometria, *tokens* criptográficos) funcionem em conjunto.

+ **Credenciais derivadas no *ecossistema tecnológico***: sistemas operacionais e navegadores passam a oferecer APIs nativas de aferição de idade, de forma que o aplicativo não manipula diretamente dados brutos, apenas recebe a evidência (ex.: "18+ válido até 2026").

+ ***Tokens* criptográficos avançados**: emissão de atributos de idade minimizados, vinculados ao domínio (*audience-bound*) e de curta duração, reduzindo risco de rastreamento. Esses tokens podem usar assinaturas criptográficas ou provas de conhecimento-zero para garantir privacidade.

+ **Integração com identidades digitais soberanas (eID, *wallets*)**: uso de carteiras como o *EU Digital Identity Wallet* ou o Gov.br no Brasil para atestar atributos etários sem expor dados pessoais.

+ **Camadas de segurança reforçadas**: mecanismos de *liveness* (Ofcom, 2025), proteção contra-ataques de conluio e validação contínua de credenciais, embutidos no dispositivo.

+ **Ambientes de teste (*testbeds*)**: plataformas que reúnem reguladores, indústria e academia para comparar soluções em cenários idênticos, avaliando desempenho, viés e impacto na privacidade (exemplo: *Age Assurance Technology Trial* da Australia, 2025a).

No Quadro 2 apresentamos um resumo que diferencia a 5ª geração das demais, mostrando seus aspectos, funcionamentos e limites.

Quadro 2 *Resumo da 5ª geração de mecanismos de aferição de idade*

Aspecto	O que é	Como funciona	Limites / Desafios
Conceito central	Integração da aferição de idade ao próprio ecossistema digital: dispositivo, sistema operacional, navegador e plataforma.	APIs nativas em navegadores e sistemas operacionais fornecem às plataformas apenas a evidência etária ("≥ 18"), sem expor dados brutos.	Complexidade de padronização global e dependência de cooperação entre grandes atores de tecnologia.
Arquiteturas interoperáveis	Protocolos comuns avaliados em *testbeds* regulatórios.	Diferentes métodos (documento, biometria, *tokens*) são comparados lado a lado quanto à acurácia, o viés, à fraude e privacidade.	Custos elevados de teste e necessidade de critérios de avaliação transparentes e auditáveis.
***Tokens* criptográficos avançados**	Credenciais digitais mínimas que atestam apenas o atributo etário.	Emissão por autoridade confiável, validade curta, vinculação ao domínio (*audience-bound*), uso de ZKP e assinaturas cegas para evitar rastreamento.	Requer infraestrutura de carteiras digitais e emissoras confiáveis amplamente distribuídas.
Integração com identidades digitais soberanas	Uso de *wallets* como o *EU Digital Identity Wallet* ou Gov.br.	Compartilhamento seletivo de atributos derivados (ex.: "≥ 18"), sem expor nome, CPF ou DOB.	Risco de exclusão de pessoas sem acesso à identidade digital robusta.
***Testbeds* regulatórios**	Ambientes de ensaio com academia, reguladores e setor privado.	Ex.: *Age Assurance Technology Trial* na Austrália – comparou documental, biométrico, inferencial e *tokens* em condições idênticas.	Ainda experimentais; resultados nem sempre transferíveis para outros contextos culturais e jurídicos.

Fonte: CNIL (2022), EDPB (2025), Ofcom (2024) e Australia (2025a).

‹ a aferição de idade e a proteção de dados pessoais[8] ›

Muitos riscos ao direito à proteção de dados pessoais das crianças surgem da coleta de dados por instituições públicas ou privadas, ou mesmo pelo compartilhamento de fotos por membros da própria família (*sharenting*[9]), que podem revelar a localização da criança, suas atividades e emoções, bem como aspectos de saúde e relacionamentos.

Nesse contexto, com relação à proteção da criança em ambientes digitais, o Comentário Geral 25 de 2021 (ONU, 2021), do Comitê de Direitos da Criança da Organização das Nações Unidas, em sua seção E, considera o direito das crianças à privacidade como uma questão vital para a autonomia, dignidade e segurança, assim como para o exercício de seus direitos. Também recomenda que países definam medidas para garantir a privacidade das crianças, com o uso de privacidade desde a concepção e segurança desde a concepção (*privacy and security by design*) nos produtos e serviços que afetem crianças.

Fernandes (2021, p. 243-252) propôs uma série de recomendações para a regulação da proteção de direitos de crianças, entre as quais a verificação de idade. Sobre isso, a autora afirma que "é imprescindível que os produtos ou serviços que tratem dados pessoais saibam quem costuma utilizá-los, a fim de estabelecer os padrões de proteção mais rigorosos quando crianças e adolescentes possam acessá-los" (Fernandes, 2021, p. 247).

Livingstone, Stoilova e Rahal (2023) e Livingstone e Pothong (2023) dissertaram sobre como a competência e o letramento digital apoiam os direitos das crianças, e indicam 11 princípios de direitos das crianças aplicáveis ao ambiente digital. No princípio 4 (adequação à idade), as autoras indicam que devem ser desenvolvidas políticas e produtos adequados à idade desde a concepção e que se considere a aferição de idade. Segundo a autora (2024, p. 8), as medidas de aferição de idade adotadas nos ambientes digitais atualmente não atendem aos requisitos do regula-

8 *Essa seção traz alguns aspectos encontrados na literatura sobre a proteção de dados pessoais em relação aos mecanismos de aferição de idade estudados. Porém, não possui caráter exaustivo e não tem o objetivo de apresentar sugestões específicas sobre o tema.*

9 ***Sharenting*** *é um termo que une as palavras "sharing" (compartilhamento) e "parenting" (paternidade/maternidade). Se refere à prática dos pais de compartilhar fotos, vídeos e detalhes da vida de seus filhos nas redes sociais de forma excessiva (Alana, 2025).*

mento geral sobre a proteção de dados da União Europeia, o GDPR, uma vez que são insuficientes e não protegem as crianças contra o acesso a conteúdo inapropriado e a produtos e serviços nocivos.

No Brasil, sob a ótica da proteção de dados, a LGPD estabelece que o tratamento dos dados pessoais de crianças e adolescentes deve ser realizado em seu melhor interesse (Brasil, 2018, art. 14). A ANPD, em 2022, aprovou o regulamento da aplicação da LGPD para agentes de tratamento de pequeno porte, onde em seu art. 4º considerou como de alto risco o tratamento de dados de crianças e adolescentes quando realizado em larga escala e/ou possa afetar significativamente interesses e direitos fundamentais dos titulares (ANPD, 2022, art. 4º). Em 2023, a ANPD emitiu um enunciado a respeito das possíveis interpretações do art. 14 da LGPD, concluindo que no tratamento de dados pessoais de crianças e adolescentes podem ser aplicadas também as hipóteses previstas nos arts. 7º ou 11, desde que observado o melhor interesse desse público (ANPD, 2023a).

O Guia Orientativo sobre as Hipóteses Legais de Tratamento de Dados Pessoais e o Legítimo Interesse tece considerações sobre o tratamento de dados de crianças e adolescentes. Ele cita o Comentário Geral n° 14, de 2013, do Comitê dos Direitos da Criança da ONU (2013), que enfatiza que a criança tem o direito de ter o seu melhor interesse apreciado e levado em consideração de forma primária e deve-se sempre avaliar os possíveis impactos positivos e negativos de decisões que afetem uma determinada criança, um grupo identificado de crianças ou crianças em geral. Assim, qualquer ação ou decisão que envolva esse público deve garantir a conformidade com o melhor interesse da criança, levando em consideração o seu desenvolvimento físico, emocional e educacional, bem como os princípios para o tratamento de dados pessoais previstos no art. 6º da LGPD, como finalidade, necessidade, transparência e medidas de segurança e mitigação de riscos (ANPD, 2024a, p. 9).

Os mecanismos de aferição de idade apresentados neste estudo, em particular os mecanismos de verificação de idade baseada em documentos e de estimativa de idade, necessitam coletar, tratar e, em alguns casos, armazenar dados pessoais de adultos e crianças, alguns deles sensíveis, como por exemplo os que fazem uso de biometria. Isso levanta preocupações acerca da proteção de dados pessoais.

No estudo de Sas e Mühlberg (2024, p. 7) os autores concluíram pela inexistência de um método de aferição de idade capaz de atestar a idade do usuário com infalibilidade e que proteja adequadamente os direitos fundamentais dos indivíduos, adultos e crianças. Alertaram, ainda, que a existência de aplicações de aferição sem a devida proteção aos direitos fundamentais pode normalizar a intrusão excessiva da privacidade e aumentar os riscos de vazamento e uso indevido de dados.

O EDPB corrobora que os mecanismos de aferição de idade disponíveis podem impactar nos direitos fundamentais dos usuários (EDPB, 2022, p. 26). Os princípios da proporcionalidade e da necessidade (Brasil, 2018, art. 6º) devem ser observados na análise da natureza do serviço, dos dados coletados, processados e tratados, e dos riscos do serviço ou conteúdo que serão associados às tecnologias de aferição de idade (CNIL, 2021). Além disso, o nível de confiabilidade dos métodos deve ser proporcional ao nível de gravidade dos riscos identificados relacionados ao serviço. Porém, a precisão e confiabilidade estão diretamente relacionadas a métodos considerados mais invasivos e arriscados (Sas; Mühlberg, 2024, p. 19).

Há que se levar em conta que a determinação do conteúdo considerado inapropriado e seus riscos associados podem variar, tendo usuários e reguladores visões distintas do que pode ser prejudicial (Caglar; Nair; 2021, p. 4), e que a adequação dos métodos disponíveis muda com os avanços tecnológicos e seus riscos associados, sendo necessária uma análise periódica (EDPB, 2023).

A implementação de tecnologias de verificação de idade que revelam a identidade dos usuários em serviços online pode permitir a associação de informações pessoais ao conteúdo acessado. Isso pode representar uma ameaça para usuários que dependem do anonimato para garantir sua segurança física e o adequado exercício de suas funções profissionais. Da mesma forma, afeta negativamente membros de comunidades marginalizadas e vítimas de violência, que necessitam de proteção contra exposição indevida. Além disso, pode comprometer o exercício de liberdades fundamentais tanto de crianças quanto de adultos, criando um efeito inibidor sobre atividades legítimas dos usuários (EDPB, 2022, p. 26; EDRI, 2023, p. 27). Por fim, existem ainda riscos cibernéticos e associados à

reutilização desses dados para fins de publicidade comportamental e perfilamento comercial, policial ou político (Sas; Mühlberg, 2024, p. 34-35).

Como já mencionado, embora não seja considerado por si só um mecanismo de aferição de idade, a autodeclaração reduz a exposição de dados pessoais, mas oferece pouca ou nenhuma garantia efetiva de idade e pode ser facilmente burlada pelo usuário.

O uso da verificação de idade por documento oficial é um dos métodos de verificação mais eficientes em termos de acurácia, e, no entanto, demanda uma infraestrutura tecnológica bastante segura para processar e armazenar grandes volumes de dados. Ademais, essa aplicação pode excluir crianças sem documentação oficial (Shaffique; Hof, 2024, p. 26).

Já o uso da verificação por cartão de crédito traz riscos de perfilamento e de segurança, pois realiza coleta de dados pessoais e financeiros (Sas; Mühlberg, 2024, p. 66). Possui baixa fidelidade, uma vez que crianças podem usar o cartão de adultos para ter acesso a serviços restritos a maiores de 18 anos (Shaffique; Hof, 2024, p. 27). Possui acessibilidade restrita, já que nem todos possuem cartão de crédito, e a idade mínima para obtenção varia entre países, limitando seu uso por crianças e adolescentes. Portanto, esses métodos podem revelar mais informações do que o necessário para estabelecer a idade do usuário, podendo violar o princípio da necessidade a depender do contexto em que é exigido.

Em alguns países, a verificação documental pode ser fortalecida pelo vínculo direto a sistemas nacionais de identificação digital, como o Gov.br no Brasil ou a identificação eletrônica (eID) na União Europeia. Nesse arranjo, em vez de submeter documentos a cada serviço, o usuário autoriza o compartilhamento de um atributo derivado, como a condição "maior de 18 anos". Essa estratégia reduz a exposição de dados pessoais (nome, CPF, endereço), em conformidade com a necessidade de minimização e desvinculação.

Apesar do ganho técnico em relação à autodeclaração, esse método apresenta limites significativos. Caso o serviço exija mais informações que viabilizem a identificação do usuário, ele pode possibilitar o rastreamento de atividades com alto grau de confiabilidade, aumentando os riscos de vigilância, uso inadequado por atores privados e riscos cibernéticos. Ade-

mais, a concentração de informações de identidade em servidores governamentais ou privados aumenta a superfície de risco em caso de vazamentos e exige altos padrões de segurança para evitar ataques cibernéticos ou incidentes potencialmente danosos (EDRI, 2023, p. 30; Sas; Mühlberg, 2024, p. 61). A repetição desse processo em diferentes plataformas multiplica os pontos de coleta de dados, em desacordo com princípios de proteção de dados pessoais, a exemplo do princípio da necessidade. Nesse contexto são percebidos desafios relacionados à inclusão digital e acessibilidade, especialmente para o público infanto-juvenil que constitui o principal alvo das verificações de idade online. O EDRI estimou que a eID *wallet* poderá excluir 20% de usuários (EDRI, 2023, p. 30).

Métodos de verificação de idade baseados em ato de terceiros, como a verificação por reconhecimento social, podem exigir que o usuário tenha conexões com amigos e parentes ativos no serviço ou plataforma que se pretende utilizar, além da possibilidade de um longo tempo de espera para se obter o consentimento (EDRI, 2023, p. 17). Esse mecanismo apresenta baixa eficácia devido à impossibilidade de garantir a veracidade das informações prestadas pelos acreditadores. Além disso, no caso de usuários crianças e adolescentes, o consentimento válido é somente aquele fornecido por um de seus pais ou responsável legal segundo a LGPD (Brasil, 2018, art. 14).

Em relação à verificação pelo consentimento parental, há que se levar em consideração as condições dos pais ou responsáveis em avaliar os riscos envolvidos no acesso e compartilhamento de determinadas informações em plataformas ou serviços e no tratamento dos dados pessoais coletados. Nascimento e Bernardes (2025) realizaram uma pesquisa sobre a criação de perfis de crianças em redes sociais pelos próprios pais, ainda que as recomendações legais e a política dessas redes não permitam o acesso desse público. Olszewski (2025, p. 17) fez uma pesquisa sobre a superexposição digital (oversharetting[10]), tão comum hoje em dia. Não só adultos participam dessa superexposição, já que cada vez mais crianças têm vídeos, fotos, rotinas e informações sensíveis publicados pelos próprios pais em redes sociais, infringindo direitos de personalidade, privacidade e imagem das crianças.

Ambos os métodos de verificação por terceiros enfrentam desafios relacionados à confiabilidade das informações fornecidas e à necessidade de

10 ***Overshareting*** *é o ato de compartilhar informações pessoais em excesso, muitas vezes sem pensar nas consequências. É a união das palavras em inglês "over" (excessivo) e "sharing" (compartilhamento). Isso pode acontecer com qualquer tipo de informação e com qualquer pessoa, seja em redes sociais, mensagens privadas ou até mesmo em conversas online (Olszewski, 2025).*

validação adicional dos próprios acreditadores e dos responsáveis legais, tornando essencial a implementação de controles complementares para assegurar a precisão do processo de verificação etária.

Por outro lado, o EDRI (2023) alerta sobre o risco da terceirização da verificação obrigatória da idade para empresas, como na VaaS. Essa terceirização de responsabilidade pode minar o envolvimento de pais e responsáveis, e gerar ambientes extremamente restritivos para crianças e adolescentes devido à possível exclusão de categorias amplas de conteúdo não nocivo, por simples precaução, enquanto não houver regulamentação legal, impactando o direito das crianças e adolescentes à informação. Reforçam-se também os riscos inerentes dos provedores terem excessivo controle sobre o que as crianças podem ver e fazer online (EDRI, 2023, p. 26 e 27). O nível de garantia desse método depende da forma como a idade foi verificada inicialmente, além de delegar a essas empresas a autoridade pelo controle da aplicação, aumentando o domínio sobre os dados de verificação de idade sob sua custódia.

Embora ofereça maior confiabilidade por meio da validação cruzada com bases oficiais, a VaaS demanda forte integração tecnológica entre o serviço e as bases de dados, além de requerer coleta e processamento de grandes volumes de dados pessoais. Essa característica confere à aplicação um alto risco tecnológico, exigindo protocolos de segurança e conformidade com regulamentações de proteção de dados para mitigar possíveis vulnerabilidades e garantir a privacidade dos usuários verificados.

Sas e Mühlberg (2024, p. 67) mencionam três riscos associados a esse método, do ponto de vista da proteção de dados pessoais: i) o conhecimento da identidade do usuário pelo site, ou aplicativo (provedor de serviços) acessado; ii) o conhecimento do provedor de serviços quanto ao relacionamento estabelecido entre o usuário e o verificador terceirizado; e iii) o conhecimento do verificador terceirizado sobre quem é o provedor e qual serviço que está sendo acessado. Caso essas três informações sejam combinadas, viabilizam-se a vigilância e o perfilamento.

Embora *tokens* de idade criptográficos possam evitar a identificação do usuário, a transmissão direta via API do verificador para o provedor de serviços introduz riscos de privacidade e segurança. Tal método revela a

identidade do provedor, expondo o propósito da verificação e permitindo o rastreamento das atividades do usuário (Sas; Mühlberg, 2024, p. 70).

Para resolver isso, métodos duplo-cego empregam mecanismos criptográficos para garantir que nem o provedor de serviços nem o verificador terceirizado conheçam um ao outro. Esses verificadores são geralmente certificados por uma autoridade que estabelece as especificações de implementação do sistema de verificação de idade (Gorin; Biéri; Brocas, 2022; PEReN, 2022, p. 10). A solução, no entanto, exige a escolha de um intermediário independente e confiável para realizar a transmissão do comprovante de idade.

A coleta de biometria em massa para fins de estimativa de idade levanta preocupações quanto à proporcionalidade da interferência nos direitos à privacidade e à proteção de dados pessoais, especialmente quando não há garantia de que os dados não serão reutilizados para outros propósitos, como vigilância, perfilamento, filtragem de informação e monitoramento em massa. Além disso, armazenamento desse dado sensível enseja riscos de vazamentos. Ademais, segundo a Lei n. 15.211/2025, "os dados coletados para a verificação de idade de crianças e de adolescentes poderão ser utilizados unicamente para essa finalidade, vedado seu tratamento para qualquer outro propósito" (Brasil, 2025c, art. 13).

Além das questões mencionadas, há limitações no método, pois o usuário poderia exibir para a coleta a fotografia de uma outra pessoa, um adulto por exemplo, para burlar a ferramenta tecnológica, o que tornaria a coleta ineficaz. Outro ponto relevante diz respeito à precisão da verificação do resultado, principalmente para os usuários com idade próxima a um determinado valor limite (por exemplo, 18 anos), o que coloca em dúvida a acurácia do mecanismo, especialmente quando se exige adoção em cenários de alto risco (ICO, 2024b).

Métodos de estimativa que avaliam o comportamento do usuário necessitam de muitos dados que extrapolam a idade, o que também pode vir a revelar outras informações sobre o titular de dados, levando a riscos de tratamento massivo de dados para perfilamento (Shaffique; Hof, 2024, p. 31). Caso esses dados sejam agregados, podem revelar a identidade do usuário. Perfis detalhados podem ser utilizados para fins de vigilância, ou

uso por atores maliciosos (Sas; Mühlberg, 2024, p. 51). Há que se contrabalancear então a acurácia desses métodos e a segurança, a proteção da privacidade e dos dados pessoais (EDRI, 2023, p. 24).

A estimativa de idade por meio de testes de capacidade elimina a coleta de dados pessoais, mas não é muito precisa e pode levar a vieses em razão da dificuldade em se identificar uma idade dependendo do resultado da resposta dada aos desafios. A capacidade cognitiva de cada criança é variável e há dificuldade de se estabelecer conhecimentos mínimos por idade em função de uma faixa etária ou série escolar (Shaffique; Hof, 2024, p. 32), além dos riscos de exclusão (Sas; Mühlberg, 2024, p. 58).

Embora estejam em desenvolvimento técnicas promissoras que preservam a privacidade, como identidades digitais, elas ainda enfrentam desafios de segurança e de inclusão. Para garantir um equilíbrio justo entre proteção e autonomia, Sas e Mühlberg (2024, p. 42) sugerem a realização de avaliações de risco obrigatórias e a criação de um arcabouço regulatório claro para garantir que essas tecnologias sejam implementadas de forma segura e responsável, além de estudos sobre soluções técnicas alternativas como sistemas de denúncia, filtragem e aviso de conteúdo prejudicial, incorporação de botões de pânico acessíveis e adoção de *designs* apropriados para a idade que priorizem a privacidade e a segurança. Do ponto de vista social, destacam a importância da educação e conscientização de adultos e crianças, e o debate aprofundado entre formuladores de políticas e a sociedade.

O ensaio *Age Assurance Technology Trial* (Australia, 2025a), encomendado pelo governo australiano para avaliar a eficácia, confiabilidade e os impactos na privacidade de diversas tecnologias de verificação de idade tem como objetivo principal proteger crianças de riscos online, como exposição à pornografia e a serviços ou redes sociais com restrição de idade. O relatório analisa exaustivamente as tecnologias de verificação de idade, avaliando 48 provedores e suas soluções (como verificação, estimativa e inferência de idade, controle parental e consentimento parental). A avaliação se baseia em critérios internacionais, incluindo precisão, interoperabilidade, confiabilidade, facilidade de uso, minimização de vieses, proteção de dados e privacidade, além da prontidão para implementação. O documento também investiga como essas tecnologias se integram ao ecossistema digital.

A conclusão do ensaio foi a de que a aferição de idade se mostra viável e eficaz na Austrália, sem grandes barreiras tecnológicas, com soluções já prontas para uso e validadas de forma independente. Entendeu-se que o setor é dinâmico e inovador o suficiente, impulsionado por investimentos privados, com uma grande variedade de opções que podem ser adaptadas para diferentes contextos, demonstrando que não existe uma solução única que sirva para todos os casos. No entanto, essas conclusões foram contestadas pela Electronic Frontiers Australia (EFA), organização de direitos digitais que participou do conselho consultivo do estudo. A EFA argumentou que as alegações de que a verificação de idade pode ser "privada, robusta e eficaz" são "difíceis de reconciliar com as evidências" e criticou a metodologia utilizada para chegar a essas conclusões (EFA, 2025). A organização destacou preocupações específicas sobre fornecedores de tecnologia que proativamente estabeleceram capacidades para reter dados pessoais e biométricos, antecipando possíveis solicitações de autoridades policiais ou reguladores, mesmo quando não existe exigência legal para tal retenção. A EFA também criticou que a avaliação de conformidade com privacidade baseou-se simplesmente na leitura de políticas de privacidade externas, caracterizando essa abordagem como "*Privacy Washing*".

A análise aponta desafios, como a necessidade de evitar a retenção excessiva de dados por parte dos provedores, que pode gerar riscos relevantes ao direito à privacidade. No entanto, os sistemas de verificação mostraram um desempenho consistente entre diversos grupos demográficos. O sucesso do modelo de avaliação do ensaio, baseado em normas internacionais, sugere que ele pode servir como base para a criação de um sistema de acreditação e certificação na Austrália, garantindo que os provedores de verificação de idade atendam aos padrões de segurança e privacidade exigidos no país, o que pode servir de inspiração a outros países no mundo.

A EFA (2025) também expressou preocupação de que o estudo possa ser usado como justificativa para a implementação mais ampla de sistemas de identificação digital, caracterizando a regulamentação de idade mínima para redes sociais como um "cavalo de Tróia" para a adoção generalizada de ID digital.

Convergência do tema entre marcos regulatórios

A crescente presença de crianças e adolescentes no ambiente digital tem desafiado as autoridades de proteção de dados a repensarem suas abordagens regulatórias. Nesse cenário, diversos marcos regulatórios recentes ganham relevância por propor caminhos técnicos e jurídicos para a construção de uma proteção mais estruturada e efetiva da infância online: a proposta de norma ISO/IEC/FDIS 27566-1:2025 (ISO; IEC, 2025) e o *Age Appropriate Design*, publicado pelo ICO do Reino Unido (ICO, 2022), a Lei Geral de Proteção de Dados (LGPD – Brasil, 2018), o Guia sobre o Uso de Dispositivos Digitais (Brasil, 2025a) e a Lei 15.211, o ECA Digital (Brasil, 2025c).

A proposta de norma ISO/IEC FDIS 27566-1 (ISO; IEC, 2025) surge como uma tentativa de organizar, de maneira padronizada, os diferentes métodos que podem ser usados para identificar a idade de um usuário em serviços digitais. Ela propõe uma matriz de cinco níveis de garantia, que variam de acordo com o grau de certeza e a solidez técnica. Essa classificação não se restringe à engenharia dos sistemas, mas também está diretamente vinculada ao grau de risco que o serviço pode representar para uma criança. Assim, serviços que ofereçam conteúdo sensível, como jogos com elementos violentos ou redes sociais abertas, devem operar com mecanismos mais rigorosos de verificação, enquanto outros, de menor risco, podem adotar abordagens mais leves. Ao estabelecer essa lógica de proporcionalidade, a proposta de norma FDIS 27566-1 (ISO; IEC, 2025) não perde de vista a privacidade como valor central, já que propõe que os mecanismos de verificação de idade sejam elaborados para proteger atributos sensíveis, evitar rastreamento desnecessário e minimizar a coleta de dados.

O *Age Appropriate Design Code*, em vigor no Reino Unido desde 2021, é um código de conduta que estabelece padrões a provedores de serviços ou produtos online (*providers of information society services*) acerca de práticas de proteção por padrão em serviços que sejam acessíveis a crianças, ainda que não sejam explicitamente destinados a elas. Um de seus pontos mais inovadores está no Padrão 3 (ICO, 2022), que determina que os serviços devem conhecer a idade do usuário com o grau de certeza adequado ao risco envolvido, ou, então, aplicar todas as regras de proteção infantil a todos os usuários indistintamente.

Além disso, o código britânico traz o conceito de "melhor interesse da criança" para o centro da concepção de produtos digitais. Isso significa que, por padrão, o serviço deve operar com a máxima privacidade possível, com funcionalidades como geolocalização, perfilamento e coleta de dados sensíveis desabilitadas. A LGPD, sobretudo no art. 14, exige consentimento específico em destaque por pelo menos um dos pais ou pelo responsável legal, quando esta for a hipótese legal utilizada, mas também remete à adoção de medidas proporcionais, transparentes e baseadas em boas práticas. Esses elementos estão presentes tanto na ISO/IEC FDIS 27566-1 (2025) quanto no *Age Appropriate Design Code* (ICO, 2022). Além disso, o Guia sobre o Uso de Dispositivos Digitais, publicado no Brasil em 2025, reforça esses entendimentos ao recomendar que políticas públicas busquem métodos técnicos de aferição de idade e protejam, por padrão, a navegação e o consumo de conteúdos digitais pelas crianças (Brasil, 2025a).

A Lei 15.211 de 2025 (ECA Digital) estabelece obrigações severas para garantir a segurança e a privacidade de crianças e adolescentes no ambiente digital. A lei exige que a verificação de idade seja feita por mecanismos eficazes, proporcionais e auditáveis, vedando a simples autodeclaração e permitindo que o Poder Público atue como regulador. Um dos pilares centrais é o princípio da privacidade desde a concepção (*privacy by design*): todos os produtos e serviços devem operar com o nível máximo de proteção ativado desde o início. Essa proteção se estende à privacidade, com a exigência da minimização de dados e a restrição de geolocalização por padrão. Além disso, a lei veda o uso de designs que manipulem os usuários, comprometendo sua autonomia ou induzindo à desativação das salvaguardas.

Em relação à exploração comercial e ao controle parental, o ECA Digital proíbe expressamente o perfilamento de crianças e adolescentes para fins de publicidade direcionada, exigindo que as redes sociais informem claramente as restrições etárias. Para os pais e responsáveis, a lei determina a oferta de ferramentas parentais acessíveis, que também devem operar com proteção máxima por padrão e fornecer métricas claras de uso.

O Quadro 3 ilustra similaridades de entendimento, comparando os principais mecanismos de aferição de idade em ambientes digitais, com base nas seguintes referências: proposta de norma ISO/IEC FDIS 27566-1 (ISO;

IEC, 2025), *Age Appropriate Design Code* (ICO, 2022), Lei Geral de Proteção de Dados (LGPD – Brasil, 2018), Guia sobre o Uso de Dispositivos Digitais (Brasil, 2025a) e a Lei 15.211, o ECA Digital (Brasil, 2025c).

Quadro 3 *Convergência normativa entre a LGPD e o Guia de Telas da SEDIGI/MJSP a ISO/IEC FDIS 27566-1, o ICO Age Appropriate Design Code e a Lei 15.211.*

Aspecto abordado	ISO/IEC 27566-1:2025 (ISO; IEC/FDIS, 2025)	Age Appropriate Design (ICO, 2022)	Lei 13.709 LGPD (Brasil, 2018)	Guia de Telas (Brasil, 2025a)	Lei 15.211 ECA digital (Brasil, 2025c)
Aferição de idade (*age assurance*)	Define três métodos: verificação, estimativa e inferência de idade (seção 4.3).	*Standard* 3: Aplicação apropriada por idade, com verificação proporcional ao risco.	Art. 14: tratamento de dados de crianças exige consentimento específico dos pais ou responsáveis e deve usar meios razoáveis para verificar a idade.	Cap. 10 e p. 135: recomenda mecanismos de verificação de idade apropriados para impedir acesso a conteúdo impróprio.	Arts. 9º e 10: mecanismos de aferição eficazes, vedada autodeclaração; Art. 11: poder público pode atuar como regulador/certificador.
Categorização por risco e proporcionalidade	Estabelece níveis de garantia (básico ao rigoroso) conforme o risco (seção 6).	*Standards* 2 e 3: DPIA e verificação devem considerar riscos à criança.	Art. 50, §1º: exige medidas adequadas conforme o tipo de dado e riscos envolvidos.	Cap. 10: indica uso proporcional de métodos e políticas conforme a faixa etária.	Art. 12: medidas proporcionais, auditáveis e seguras para aferir idade.
Minimização de dados	Prevê objetivos como 'minimização de atributos' (seção 7.1.5).	*Standard* 8: Coletar apenas o mínimo necessário para o serviço.	Art. 6º, III: princípio da necessidade – limitar tratamento ao mínimo necessário.	Cap. 8: destaca a necessidade de minimizar a coleta de dados e priorizar anonimato.	Art. 12, §1º: princípio da minimização; vedado compartilhamento irrestrito.
Privacidade por *design* e por padrão	Prevê privacidade como pilar do sistema (seção 7).	*Standard* 7: Configurações-padrão devem ser de alta privacidade.	Art. 6º, VII: princípios de segurança e de proteção à privacidade; art. 46: medidas de segurança.	Cap. 6 e 10: recomenda privacidade por padrão como princípio de *design* digital.	Art. 7º: produtos devem operar por padrão com nível máximo de proteção.

Aspecto abordado	ISO/IEC 27566-1:2025 (ISO; IEC/FDIS, 2025)	Age Appropriate Design (ICO, 2022)	Lei 13.709 LGPD (Brasil, 2018)	Guia de Telas (Brasil, 2025a)	Lei 15.211 ECA digital (Brasil, 2025c)
Transparência e controle informado	Inclui a conscientização do usuário e práticas transparentes (seções 7.1.6 e 4.4).	*Standards* 4, 10 e 15: Clareza nos termos e avisos adaptados à idade.	Art. 9º, 14, §6º e 18: direito à informação clara e adequada sobre o tratamento.	Cap. 4 e 10: orienta que crianças devem receber explicações claras e adequadas à idade.	Art. 7º, §1º: informações claras; Art. 24: redes sociais devem informar restrições etárias.
Geolocalização e rastreabilidade	Prevê não rastreabilidade como objetivo (seção 7.1.4).	*Standard* 9: Geolocalização desativada por padrão, com aviso ativo.	Art. 12 e 13: devem ser adotadas medidas para proteger privacidade, inclusive geolocalização sensível.	Cap. 5: geolocalização deve ser evitada ou controlada com transparência.	Art. 17, §4º, VI: restrição de geolocalização por padrão, aviso claro.
Perfilamento e inferência	Aborda inferência como método e exige indicadores de confiança (seções 4.3.3, 6.2.3).	*Standard* 12: Perfilamento desligado por padrão; evitar efeitos nocivos.	Art. 20: direito de revisão de decisões automatizadas; princípios de não discriminação.	Cap. 7: alerta sobre riscos do perfilamento e uso indevido de dados comportamentais.	Art. 22 e 26: vedado perfilamento para publicidade ou criação de perfis.
Técnicas de persuasão (*nudges*)	Contraindicada a coleta ou uso indevido de atributos sem base (Anexo A.3).	*Standard* 13: Proíbe *nudges* que incentivem fornecimento excessivo de dados.	Art. 6º, IV e V: prevenção e adequação; proíbe indução à entrega de dados sem necessidade.	Cap. 8: desaconselha uso de estratégias que manipulem comportamento da criança.	Art. 17, §2º: veda *design* que comprometa autonomia ou induza desativação de salvaguardas.
Inclusão e acessibilidade	Recomenda inclusão de diferentes públicos, inclusive os vulneráveis (Anexo A.4).	Preambular e transversal: reconhece diferentes capacidades e acessos.	Art. 6º, VIII: princípio da não discriminação; art. 50: boas práticas e governança.	Cap. 3: políticas inclusivas devem contemplar diversidade e acesso equitativo.	Art. 3º: respeito à autonomia progressiva; Art. 17: ferramentas acessíveis.
Direito à informação e ferramentas de controle	Prevê declarações de prática claras e controle pelo indivíduo (seção 4.4).	*Standard* 15: Ferramentas acessíveis para exercer direitos e reportar preocupações.	Art. 18: direito de acesso, retificação e portabilidade garantido ao titular e responsáveis legais.	Cap. 9: reforça o direito à informação, denúncia e acesso aos próprios dados.	Art. 16 e 18: ferramentas parentais com proteção máxima por padrão, métricas de uso.

Fonte: elaboração própria com base em ISO e IEC/FDIS (2025), ICO (2022), Brasil (2018, 2025a, 2025c).

Conforme pode-se observar no quadro 3, existe uma convergência entre marcos regulatórios comparados, assim como uma complementariedade, cuja aplicação vem a auxiliar na elaboração de políticas, regulamentações, soluções e na definição de requisitos para os mecanismos de aferição de idade.

Princípios de aferição de idade

Nesta seção, apresentamos o resultado de uma coleta de princípios de aferição de idade propostos por algumas autoridades de proteção de dados no mundo[11] que visam a regular ou orientar a adoção da aferição de idade em ambientes digitais. Identificamos que a definição de princípios é um dos primeiros passos na regulação da aferição de idade nesses países.

A CNIL defende a criação de sistemas de verificação de idade online que não comprometam a liberdade de navegação. A autoridade francesa estabeleceu um conjunto de princípios-chave para guiar o desenvolvimento desses sistemas, garantindo que eles sejam eficazes e respeitem a privacidade dos titulares (CNIL, 2021). A verificação de idade em ambientes digitais deve ser pautada por uma abordagem que equilibra segurança e privacidade. Os princípios de minimização, proporcionalidade, robustez e simplicidade são fundamentais para isso. A minimização garante que a coleta de dados seja limitada ao essencial, evitando usos indevidos, como marketing. A proporcionalidade assegura que o método de verificação seja adequado ao nível de risco do conteúdo, sem comprometer indevidamente a privacidade do usuário. A robustez exige que, em situações de alto risco, a verificação seja rigorosa, indo além da autodeclaração, enquanto a simplicidade promove soluções fáceis de usar que integram a verificação de idade e o consentimento parental. Juntos, esses princípios visam criar um ambiente online mais seguro para todos, sem sacrificar as liberdades individuais ou os direitos à privacidade e à proteção de dados pessoais.

A Comissão Europeia (CE) lançou um relatório que estabelece um conjunto abrangente de requisitos para a aferição de idade em ambientes digitais, com o objetivo de proteger os usuários, especialmente crianças e adolescentes (Shaffique; Hof, 2024). O documento se baseia em princípios como proporcionalidade, privacidade, segurança e precisão,

11 *Foram coletadas propostas de princípios ou requisitos para a verificação de idade junto às seguintes instituições: a Commission Nationale de l'Informatique et des Libertés da França (CNIL), a Comissão Europeia (Shaffique; Hof, 2024), o Conselho Europeu para a Proteção de Dados / European Data Protection Board (EDPB), a ARCOM, a Agência Espanhola de Proteção de Dados (AEPD) e o Comité de Personas Expertas da Espanha, a e-Safety Commissioner, o Global Age Assurance Standards Summit, a Ofcom e finalmente a 5RighstFoundation, organização não governamental inglesa precursora em definir princípios de verificação de idade, cujos princípios embasaram a noção de inovação digital adequada à idade contida no padrão IEEE 2089.1-2024 / IEEE Standard for Online Age Verification (IEEE, 2024).*

enfatizando que os sistemas de verificação de idade devem ser eficazes sem comprometer a liberdade ou a privacidade do usuário. A CE também destaca a importância da inclusão, da transparência e, notavelmente, da escuta às opiniões das crianças no desenvolvimento dessas aplicações. Complementando esse relatório, a Comissão está propondo o uso da carteira digital como uma arquitetura de verificação de idade, baseada em princípios de proteção de dados como a minimização de dados, a centralidade no usuário e a segurança. Essa abordagem busca criar um sistema robusto e seguro, garantindo que o titular mantenha o controle sobre seus dados pessoais.

Os princípios estabelecidos por instituições como a CNIL e a Comissão Europeia demonstram uma abordagem unificada e cuidadosa para a aferição de idade em ambientes digitais. Ambas as entidades reconhecem a necessidade de se equilibrar a proteção de crianças e adolescentes com a liberdade de navegação na Internet. Essas entidades defendem que os sistemas de verificação de idade devem ir além da simples auto-declaração, de forma similar ao previsto no ECA Digital. Eles precisam ser proporcionais ao risco, robustos o suficiente para serem eficazes e, ao mesmo tempo, simples de usar. O foco na minimização de dados e na proteção de dados pessoais é central, garantindo que os dados pessoais não sejam coletados em excesso ou usados para outros fins, a exemplo da publicidade comercial.

A Organização para a Cooperação e Desenvolvimento Econômico (OCDE) publicou, em 2024, o relatório "*Towards digital safety by design for children*", com o objetivo de guiar governos e provedores de serviços digitais na criação de um ambiente online mais seguro para crianças. O documento destaca que a segurança infantil deve ser uma prioridade, desde a concepção de plataformas e serviços. Para isso, a OCDE (2024) propõe a adoção de medidas essenciais, como a implementação de mecanismos de aferição de idade, design centrado na criança, detecção proativa de danos, rigorosa proteção de dados pessoais e privacidade, a garantia de informações adequadas, e a criação de canais eficazes para reclamações. Além disso, o relatório enfatiza a importância de se incentivar a participação das crianças nas decisões que as afetam, promovendo uma cultura de segurança e bem-estar digital.

O Comitê Europeu para a Proteção de Dados (EDPB) emitiu, em 2025, a Declaração 1/2025 sobre garantia de idade, com o objetivo de orientar o tratamento de dados pessoais nesse contexto, seguindo os princípios do GDPR. A declaração estabelece dez princípios fundamentais, com foco em garantir que as aplicações de verificação de idade sejam proporcionais e não violem direitos e liberdades. Entre os pontos principais estão a limitação da coleta e uso de dados ao mínimo necessário, a avaliação de riscos, a proteção de dados desde a concepção e a segurança de tais mecanismos. O documento ressalta a importância de assegurar a licitude e a transparência em todos os processos, além da responsabilidade dos provedores de serviços (EDPB, 2025).

A autoridade francesa de regulação de mídia, ARCOM, publicou um guia em 2024 para exigir que serviços de conteúdo pornográfico online implementem mecanismos confiáveis de verificação de idade. O guia não impõe uma tecnologia específica, mas estabelece requisitos mínimos que os sistemas devem atender para serem considerados aceitáveis (ARCOM, 2024b). Entre as exigências, destacam-se a independência dos fornecedores de verificação em relação às plataformas de conteúdo, a garantia de confidencialidade para os usuários e a proteção de dados pessoais e privacidade. O documento também exige que os mecanismos sejam amplamente acessíveis à população e que demonstrem de forma clara e explícita seu nível de proteção da vida privada. O objetivo é assegurar que esses serviços não possam operar na França sem um sistema robusto que proteja a privacidade dos usuários e evite o acesso de crianças e adolescentes a conteúdos impróprios.

Em dezembro de 2023, a Agência Espanhola de Proteção de Dados (AEPD) divulgou um Decálogo de Princípios para Verificação de Idade, visando proteger crianças e adolescentes de conteúdo impróprio online. A agência definiu um sistema de proteção que inclui não apenas um mecanismo de verificação, mas também políticas de classificação de conteúdo, aplicação de filtragem de acesso e a exibição de quais sites são restritos por idade. A AEPD enfatizou que esses sistemas devem evitar a identificação e o rastreamento de crianças e adolescentes, focando em comprovar o status de "pessoa autorizada ao acesso" de forma anônima e apenas para conteúdos considerados impróprios. O documento também reforçou a ideia de que a educação digital e a seleção de conteúdo

são uma responsabilidade compartilhada entre famílias, governos e a indústria, destacando a urgência de regulamentações e políticas públicas eficazes (AEPD, 2023).

A e-Safety, órgão regulador da segurança online na Austrália, em conjunto com o órgão de proteção de dados OAIC, tem atuado para fortalecer a proteção de crianças e jovens no ambiente digital. Com base no *Online Safety Act* de 2021, a entidade publicou em 2023 o *Roadmap for Age verification*, um guia que propõe um arcabouço regulatório que determina às plataformas digitais a adoção de mecanismos de aferição de idade para restringir o acesso a pornografia. O documento também sugere a criação de um sistema de acreditação para os provedores desses serviços, com o objetivo de assegurar princípios como privacidade, segurança, transparência e respeito aos direitos humanos. A iniciativa, que inclui consultas com a sociedade e ações educativas, busca uma abordagem ampla e holística para mitigar os riscos da exposição de crianças a conteúdos impróprios (Australia, 2023).

O Ofcom publicou em 2023 um guia para que provedores de conteúdo pornográfico cumpram a Parte 5 do *Online Safety Act*, com o objetivo de impedir que crianças acessem esses serviços. O documento orienta sobre a implementação de métodos de aferição de idade, listando exemplos de mecanismos de verificação e estimativa. As obrigações principais incluem a escolha e implementação de métodos listados no guia, a garantia de que o processo é eficaz em identificar se o usuário é uma criança e de que o conteúdo pornográfico não será encontrado por crianças e adolescentes. Além disso, o guia recomenda que os provedores documentem e publiquem informações detalhadas sobre o tipo de método usado, como ele funciona e como a privacidade e a proteção de dados são garantidas, promovendo a transparência e a responsabilidade no setor (Ofcom, 2023).

A 5Rights Foundation, uma organização inglesa, foi pioneira em estabelecer princípios para a verificação de idade na Internet, com foco na proteção de crianças e adolescentes. Esses princípios defendem a importância de reconhecer crianças e suas necessidades como usuários da Internet, garantir uma abordagem centrada nesse público para o uso de dados, bem como publicar termos de uso em linguagem apropriada para a idade. Com base nesses conceitos, o Instituto de Engenheiros Eletricistas

e Eletrônicos (IEEE) desenvolveu a norma técnica IEEE 2089.1-2024 (IEEE, 2024), que detalha um conjunto de 11 princípios. O documento enfatiza que a verificação de idade deve preservar a privacidade, ser proporcional ao risco, fácil de usar para as crianças, acessível e inclusiva. Também destaca a necessidade de os provedores de verificação oferecerem segurança, transparência, e canais para contestação, além de se responsabilizarem por seus métodos (5Rights, 2023).

O *Global Age Assurance Standards Summit*, organizado pela *Age Check Certification Scheme* (ACCS), resultou em um *Communiqué* que estabelece princípios para a aferição de idade, com foco em segurança para crianças no ambiente digital. O documento baseia-se em seis princípios: i) direitos humanos e melhores interesses do indivíduo, exigindo um equilíbrio entre proteção e empoderamento; ii) implementação proporcional e baseada em riscos, que demanda avaliações de impacto antes da adoção de sistemas; iii) preservação da privacidade desde a concepção, com a preferência por tecnologias como a prova de conhecimento zero (ZKP) e a minimização de dados; iv) interoperabilidade baseada em padrões, incentivando o uso de normas internacionais de padronização como a ISO/IEC e a IEEE; v) inclusão digital e acessibilidade, garantindo que as aplicações sejam acessíveis a todos; e vi) transparência, responsabilidade e inovação, que pede a certificação independente dos sistemas e a colaboração entre reguladores e a indústria para incentivar a conformidade e o desenvolvimento ético de novas tecnologias (ACCS, 2025).

Em resumo, a partir de uma análise comparativa das diretrizes internacionais apresentadas acima, percebe-se uma significativa convergência dos princípios que devem nortear os sistemas de aferição de idade na Internet, especialmente no que se refere à proteção de crianças e adolescentes. Em especial destacam-se:

+ **Privacidade e proteção de dados por padrão e desde a concepção**, como eixo estruturante de todos os sistemas de aferição de idade;

+ **Proporcionalidade**, que exige que o nível de verificação seja adequado ao risco do serviço acessado, evitando excessos na coleta de dados;

+ **Minimização e limitação da finalidade**, limitando a coleta de dados ao estritamente necessário para o objetivo de verificação de idade, e vedando usos secundários;

+ **Transparência e responsabilidade**, exigindo que os usuários, especialmente os responsáveis legais, tenham clareza sobre os métodos utilizados e seus impactos;

+ **Gestão de riscos e segurança da informação**, garantindo a integridade, confidencialidade e disponibilidade dos dados utilizados nos processos de verificação;

+ **Inclusão e acessibilidade**, assegurando a participação das crianças e adolescentes nas decisões e evitando a exclusão digital de crianças sem documentos oficiais ou com limitações socioeconômicas;

+ **Direitos humanos, não discriminação e equidade**, como garantia de que os métodos utilizados não gerem tratamentos desiguais injustificados; e

+ **Interoperabilidade e robustez técnica**, que facilitam a padronização, o cumprimento normativo e a escalabilidade das soluções.

Além disso, observa-se uma crescente valorização da escuta ativa de crianças e adolescentes nos processos regulatórios e da construção de soluções centradas na criança, que respeitem seus direitos digitais em sua integralidade, conforme a Convenção sobre os Direitos da Criança da ONU e os padrões emergentes da ISO/IEC FDIS 27566-1 (ISO; IEC, 2025). Essa convergência global indica que os esforços regulatórios caminham não apenas para impedir o acesso de crianças a conteúdos inadequados, mas para fomentar um ecossistema digital seguro, ético e inclusivo, em que o respeito aos direitos da infância seja o ponto de partida para a inovação tecnológica.

‹ a aferição de idade no contexto brasileiro ›

No Brasil, com a promulgação da Lei nº 15.211, de 17 de setembro de 2025, conhecida como Estatuto Digital da Criança e do Adolescente, o Brasil consolidou um marco normativo específico para a proteção de crianças e adolescentes em ambientes digitais. O Capítulo IV da Lei dispõe de forma detalhada sobre os mecanismos de aferição de idade, estabelecendo obrigações e parâmetros que dialogam diretamente com a noção de aferição de idade. Entre as inovações da lei, destacam-se:

+ A exigência de que provedores de aplicações e serviços digitais adotem mecanismos robustos e auditáveis de aferição de idade, de modo a impedir o acesso de crianças e adolescentes a conteúdos, produtos e serviços inadequados a sua faixa etária, sendo vedada a autodeclaração;

+ A previsão de que os mecanismos de verificação devem ser pautados pela proteção da privacidade, minimização de dados e proporcionalidade, vedando a coleta excessiva ou o uso dos dados para finalidades diversas da aferição de idade;

+ A possibilidade de o poder público atuar como regulador, certificador ou promotor de soluções técnicas de verificação de idade, garantindo que tais mecanismos sejam confiáveis, transparentes e seguros;

+ O estabelecimento de regras para a fiscalização, responsabilização e sanção de fornecedores que descumprirem as normas de aferição de idade, fortalecendo a atuação coordenada entre ANPD e demais órgãos competentes.

Diversos avanços têm sido empreendidos na criação da legislação da proteção de crianças e adolescentes em ambientes digitais. Destacam-se as resoluções do Conselho Nacional dos Direitos da Criança e do Adolescente (CONANDA): a Resolução nº 245 (Brasil, 2024a), que dispõe sobre os

direitos das crianças e adolescentes em ambiente digital; e a Resolução nº 257 (Brasil, 2024b), que estabelece as diretrizes gerais da Política Nacional de Proteção dos Direitos da Criança e do Adolescente (PNPDCAAD), com o objetivo de "[…] assegurar a prioridade absoluta dos direitos de crianças e adolescentes no ambiente digital" (Brasil, 2024b). Em particular, sob a ótica da privacidade e da proteção de dados, a política estabelece os princípios da garantia à proteção de dados pessoais, autodeterminação informativa e do direito à privacidade e a prevenção do uso excessivo como elementos a serem considerados desde a fase de concepção de produtos e serviços digitais (*privacy by design*) e por padrão (*privacy by default*), com a adoção das configurações mais protetivas disponíveis (Brasil, 2024b).

No mesmo sentido, art. 17, §3º da Resolução nº 245 do CONANDA (Brasil, 2024a) estabelece que "as empresas provedoras devem criar e aprimorar mecanismos que previnam o uso de serviços e ambientes digitais por crianças e adolescentes sempre que seus serviços não sejam adequados e seguros a esse público". Por sua vez, o art. 19 afirma que

> *mecanismos efetivos de verificação etária nos serviços e ambientes digitais acessíveis a crianças e adolescentes devem ser disponibilizados para impedir que crianças e adolescentes tenham acesso a plataformas, produtos, serviços e conteúdos ilícitos ou incompatíveis com sua idade (Brasil, 2024a).*

No art. 19, parágrafo único, a Resolução nº 245 estabelece que "os dados de crianças e adolescentes obtidos pelos mecanismos e sistemas de verificação etária não poderão ser utilizados para quaisquer outros fins, a não ser a verificação etária" (Brasil, 2024a).

A PNPDCAAD está estruturada em dez eixos temáticos (Brasil, 2024b, art. 4º). Em especial, destacamos o eixo da definição e publicação de diretrizes e referências de mecanismos de mediação parental a provedores de aplicação para utilização de produtos ou serviços de tecnologia, junto à Coordenação de Política de Classificação Indicativa do Ministério da Justiça e o Comitê Gestor da Internet.

Caso de processo de fiscalização da anpd sobre aferição de idade

Em março de 2021, a Coordenação-Geral de Fiscalização da ANPD iniciou uma ação de fiscalização sobre a coleta e o tratamento de dados pessoais pela plataforma TikTok. O processo teve origem em questionamentos sobre a funcionalidade denominada "feed sem cadastro", que permitia a navegação mesmo sem a criação de uma conta, e sobre o compartilhamento de dados previsto na própria Política de Privacidade da empresa. Com base nas informações fornecidas tanto pelo denunciante quanto pela plataforma, a ANPD avaliou a conformidade das práticas à luz da LGPD. Concluiu-se que, naquele momento e ainda em 2023, o mecanismo de verificação de idade adotado era frágil, permitindo navegação sem cadastro e resultando em tratamento indevido de dados pessoais de crianças e adolescentes. Além disso, foram avaliadas as medidas de aferição de idade aplicadas na versão com cadastro (*age gate*), e entendeu-se que, utilizadas de forma isolada, não eram suficientes, uma vez que a autodeclaração sozinha não se configura como mecanismo capaz de prevenir o acesso de crianças e adolescentes (ANPD, 2023b).

Como desdobramento do caso TikTok, em 2024 a ANPD realizou uma nova análise e concluiu que as irregularidades identificadas até aquele momento apresentavam indícios suficientes de infração aos dispositivos da LGPD, e justificavam a instauração de processo administrativo sancionador para a devida apuração dessas infrações. Entre as irregularidades identificadas, estavam falhas na verificação de idade durante e após o cadastro na plataforma e o tratamento de dados realizado na funcionalidade "*feed* sem cadastro". Determinou-se, assim, a suspensão integral da funcionalidade "*feed* sem cadastro" enquanto não houver mecanismos de verificação de idade adequados, e a elaboração de um plano de conformidade nos termos do art. 36 da LGPD, que seja claro e abrangente, detalhe os objetivos específicos, os prazos para

execução, as ações corretivas necessárias para reverter as irregularidades identificadas, os critérios de acompanhamento e monitoramento das medidas adotadas, bem como a trajetória prevista para alcançar os resultados esperados. Os detalhes dessa última nova análise estão na Nota Técnica nº 50 de 2024 (ANPD, 2024b).

‹ perspectivas de futuro ›

O uso de mecanismos de aferição de idade de crianças e adolescentes em ambientes digitais é um requisito essencial para a garantia da idade, para o controle da segurança, da privacidade e da proteção de dados desse público nos ambientes digitais. A aferição de idade está na pauta de diversas agências reguladoras e governos no mundo todo, para que provedores de serviços digitais se adequem a seus princípios e requisitos de conformidade. Esse movimento vem impulsionando a indústria de identificação digital a desenvolver aplicações aderentes às exigências dos usuários, do mercado e principalmente dos governos. Por isso, o mercado de produtos e serviços na Internet deve buscar soluções que adotem a aferição de idade e que estejam em conformidade com os padrões existentes e marcos regulatórios, ao mesmo tempo em que viabilizam uma experiência segura dos usuários nesses ambientes. As aplicações atuais são bastante variadas, não existindo uma tecnologia ou mecanismo universal que sirva para todos os contextos.

A Lei nº 15.211 (Brasil, 2025c), o Estatuto Digital da Criança e do Adolescente (EDCA), marco regulatório publicado em 2025, coloca em evidência a necessidade de padronização de requisitos técnicos voltados ao desenvolvimento de aplicações certificadas de aferição de idade, que combinem segurança, proteção de dados pessoais e acessibilidade. A lei também reforça o papel do poder público e sua atuação como regulador, certificador e promotor de tecnologias, fortalecendo os mecanismos de

governança de plataformas digitais. Além disso, sua integração à sistemática de aplicação da LGPD corrobora a complementaridade desses quadros normativos e das funções regulatórias da ANPD.

No plano internacional, também merecem destaques dois documentos lançados recentemente. Primeiramente, o *The legal and policy landscape of age assurance online for child safety and well-being* (OCDE, 2025) analisa o contexto legal e político em países membros da OCDE. Leis sobre aferição de idade foram agrupadas em três categorias principais: i) entrega de serviços apropriados à idade, que aplicam proteções para diferentes grupos etários em serviços de audiência mista (muitas vezes em leis de segurança online); ii) limites de idade rígidos, que proíbem o acesso abaixo de uma certa idade (como a pornografia online ou a compra de produtos restritos); e iii) regulamentações de privacidade e proteção de dados, que exigem consentimento parental ou criam proteções especiais para dados de crianças.

De acordo com o estudo (OCDE, 2025), apesar da crescente regulamentação, o contexto jurídico é complexo e muitas vezes confuso, com requisitos de aferição de idade que podem ser expressos (uso obrigatório de mecanismos) ou implícitos (inferidos da necessidade de proteger crianças, mas sem exigir um mecanismo específico). Embora 27 países da OCDE exijam proteção especial de dados para crianças e 33 requeiram consentimento parental, a idade para esses limites varia amplamente (entre 13 e 18 anos). Para a categoria de limites rígidos, as proteções são irregulares: embora quase todos os países proíbam o acesso à pornografia, apenas 23 têm leis específicas para o online, e só cinco delas incluem requisitos detalhados de aferição de idade. Há uma falta generalizada de especificidade em como cumprir esses requisitos, mas guias de implementação estão emergindo de reguladores de segurança online e privacidade.

Em segundo lugar, o *Social Media Minimum Age: Regulatory Guidance* (Australia, 2025b), elaborado pelo *Office of the eSafety Commissioner*, autoridade australiana independente responsável pela aplicação do *Online Safety Act*, de 2021. O documento dá concretude à alteração promovida pelo *Social Media Minimum Age Amendment*, de 2024, que fixou em 16 anos a idade mínima para manutenção de contas em plataformas de redes sociais. A partir de dezembro de 2025, esses serviços estão

obrigados a adotar "passos razoáveis" (*reasonable steps*) para impedir que pessoas com idade inferior a 16 anos usem esses ambientes.

Para além da definição de métodos técnicos, o guia (Australia, 2025b) estabelece diretrizes baseadas em princípios orientadores como confiabilidade, proporcionalidade, privacidade desde a concepção, acessibilidade e transparência, reforçando a ideia de que a aferição de idade não deve ser concebida como solução isolada, mas como parte de um sistema de governança digital articulado com avaliações de risco sistêmico, relatórios de transparência e salvaguardas de direitos fundamentais. Entre as inovações relevantes apresentadas no guia ressaltam-se três:

1. a adoção do princípio da validação sucessiva (*successive validation*), que incentiva o uso combinado e sequencial de múltiplos métodos de aferição de idade (verificação documental, estimativa biométrica, inferência comportamental) para reduzir falhas e enviesamentos;

2. a proibição de exigir exclusivamente documento governamental ou credenciais do sistema nacional de identidade digital, obrigando sempre a oferta de alternativas proporcionais; e

3. a introdução de sanções severas, incluindo multas, publicização de violações e responsabilização direta de executivos.

Ao priorizar auditorias independentes, métricas objetivas de desempenho e salvaguardas contra tentativas de evasão, o documento australiano (Australia, 2025b) marca uma inflexão relevante, ou seja, desloca o debate de uma abordagem centrada apenas em soluções técnicas para um modelo regulatório integrado, no qual inovação tecnológica, proteção de dados pessoais e responsabilização corporativa se articulam de forma sistêmica. Tal arranjo evidencia uma mudança de paradigma, aproximando a aferição de idade de um regime de governança regulatória contínua, capaz de inspirar futuros desenvolvimentos normativos no Brasil.

Em síntese, a aferição de idade tende a evoluir de diretriz meramente programática para um dever jurídico plenamente exigível e sujeito à fiscalização. Esse movimento transformará a aferição de idade em requisito

estrutural do ecossistema digital, impactando diretamente o desenho, o desenvolvimento e a oferta de produtos e serviços voltados a crianças e adolescentes, em consonância com os princípios de proteção integral e o seu melhor interesse.

A privacidade desde a concepção é uma das soluções para a aferição de idade que irá direcionar o desenvolvimento de novos produtos e serviços. Espera-se que ferramentas e soluções sejam incorporadas aos ambientes digitais com tecnologias que garantam a segurança e a confidencialidade de dados utilizados para a verificação de idade.

Com relação às normas técnicas ou padrões internacionais, destacam-se também os trabalhos do IEEE (2024) e da ISO (2025) sobre a garantia de idade, que vão inspirar e guiar todo o mercado de desenvolvimento de soluções com esse propósito. Com o lançamento dessas normas, outras complementares tendem a surgir e abordar questões cada vez mais específicas.

A União Europeia disponibilizou um modelo de solução de verificação de idade, chamado de "mini carteira", que está em fase piloto de testes (Comissão Europeia, 2025a). Essa solução permite que os usuários provem que têm mais de 18 anos sem compartilhar outras informações pessoais. Além disso, é compatível e interoperável com a *EU Digital Identity Wallet*, identidade continental para ser usada por todos os cidadãos europeus, com previsão de lançamento até o fim de 2026 (Comissão Europeia, 2025b). Porém, o EDRI estimou que a eID *wallet* poderá excluir 20% de usuários (EDRI, 2023, p. 30).

‹ considerações finais ›

A complexidade do ambiente digital exige um esforço contínuo e multifacetado para garantir a segurança e o bem-estar de crianças e adolescentes. Conforme demonstrado, a proteção desse público não se restringe a uma única medida, mas sim a um conjunto de ações que envolvem legislação, tecnologia e políticas públicas.

Contudo, a implementação desses mecanismos de proteção não está isenta de desafios. O principal deles reside na necessidade de conciliar a segurança com a proteção de dados pessoais e a privacidade. A busca por soluções de aferição de idade precisa respeitar princípios como a minimização de dados, evitando a coleta desnecessária de informações sensíveis, como a biometria. O desafio, portanto, é desenvolver tecnologias que sejam eficazes na proteção de crianças e adolescentes, ao mesmo tempo em que preservam seus direitos fundamentais.

Nesse contexto, as iniciativas de comitês consultivos e a colaboração internacional são cruciais para aprimorar os requisitos de mecanismos de aferição de idade. O trabalho conjunto entre o poder público, a sociedade civil e as empresas é essencial para criar um ambiente digital que promova o desenvolvimento pleno de crianças e adolescentes, permitindo-lhes desfrutar dos benefícios da Internet de forma segura. A aferição de idade, assim, emerge como uma peça-chave nesse ecossistema, funcionando como a principal ferramenta para garantir que a cidadania digital seja exercida de maneira responsável e protegida.

‹ referências ›

5RIGHTS FOUNDATION. **Child online safety toolkit**. London: 5Rights Foundation, 2023. Disponível em: https://childonlinesafetytoolkit.5rightsfoundation.com/wp-content/uploads/2022/05/5Rights-Child-Online-Safety-Toolkit-English.pdf. Acesso em: 5 mai. 2025.

ACCS. **Summit Comuniqué Final**: Global Age Assurance Standards Summit – Summit Communiqué. Amsterdam: ACCS, 2025. Disponível em: https://accscheme.com/wp-content/uploads/Summit-Communique-Final-Document-May-2025.pdf. Acesso em: 1 jul. 2025.

AEPD. **Decálogo de principios: verificación de edad y protección de personas menores de edad ante contenidos inadecuados**. Madrid: AEPD, 2023. Disponível em: https://www.aepd.es/guias/decalogo-principios-verificacion-edad-proteccion-menores.pdf. Acesso em: 25 jan. 2025.

ALANA. **Glossário**: Sharenting. c2025. Disponível em: https://alana.org.br/glossario/sharenting/ Acesso em: 06 out. 2025.

ANPD. **Enunciado CD/ANPD nº 1, de 22 de maio de 2023**. Brasília, DF: ANPD, 2023a. Disponível em https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-enunciado-sobre-o-tratamento-de-dados-pessoais-de-criancas-e-adolescentes/Enunciado1ANPD.pdf. Acesso em: 30 abr. 2025.

ANPD. **Guia orientativo hipóteses legais de tratamento de dados pessoais – legítimo interesse**. Brasília, DF: ANPD, 2024a. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_legitimo_interesse.pdf. Acesso em: 22 jan. 2025.

ANPD. **Nota Técnica nº. 6/2023/CGF/ANPD**. Brasília, DF: ANPD, 2023b. Disponível em https://www.gov.br/anpd/pt-br/centrais-de-conteudo/tiktok-nota_tecnica_6_versao_publica.pdf. Acesso em: 30 abr. 2025.

ANPD. **Nota Técnica nº. 50/2024/FIS/CGF/ANPD**. Brasília, DF: ANPD, 2024b. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/nt-50-pub.pdf. Acesso em: 30 abr. 2025.

ANPD. **Portaria ANPD nº 35, de 4 de novembro de 2022**. Torna pública a Agenda Regulatória para o biênio 2023-2024. Brasília, DF: ANPD, 2024c. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-anpd-n-35-de-4-de-novembro-de-2022-442057885. Acesso em: 8 jan. 2025.

ANPD. **Resolução CD/ANPD nº 2, de 27 de janeiro de 2022**. Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte. Brasília, DF: ANPD, 27 jan. 2022. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no-2-de-27-de-janeiro-de-2022. Acesso em: 30 abr. 2025.

ANPD. **Resolução CD/ANPD nº 10, de 05 de dezembro de 2023**. Aprova o Mapa de Temas Prioritários para o biênio 2024-2025 e dispõe sobre a periodicidade do Ciclo de Monitoramento. Brasília, DF: ANPD, 2023c. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-10-de-5-de-dezembro-de-2023-530258528. Acesso em: 30 abr. 2025.

ARCOM. **Pratiques médias des mineurs et exposition aux contenus inappropriés**. Paris: ARCOM, 2024a. Disponível em: https://www.arcom.fr/sites/default/files/2024-11/Arcom-Pratiques-medias-des-mineurs-et-exposition-aux-contenus-inappropries-etude-qualitative-resultats-detailles.pdf. Acesso em: 15 jan. 2025.

ARCOM. **Référentiel déterminant les exigences techniques minimales applicables aux systèmes de vérification de l'âge mis en place pour l'accès à certains services de communication au public en ligne et aux plateformes de partage de vidéos qui mettent à disposition du public des contenus pornographiques**. Paris: ARCOM, 2024b. Disponível em: https://www.arcom.fr/sites/default/files/2024-10/Arcom-Referentiel-technique-sur-la-verification-de-age-pour-la-protection-des-mineurs-contre-la-pornographie-en-ligne.pdf. Acesso em: 15 jan. 2025.

AUSTRALIA. Department of Infrastructure, Transport, Regional Development, Communications and the Arts. **Age Assurance Technology Trial**: Part A: Main Report. Stockport: Age Check Certification Scheme, 2025a. Disponível em: https://www.infrastructure.gov.au/sites/default/files/documents/aatt_part_a_digital.pdf. Acesso em: 1 set. 2025.

AUSTRALIA. E-Safety Commissioner. **Roadmap for age verification and complementary measures to prevent and mitigate harms to children from online pornography**. Austrália: Australian Government, 2023. Disponível em: https://www.esafety.gov.au/sites/default/files/2023-08/Roadmap-for-age-verification_2.pdf. Acesso em: 8 mai. 2025.

AUSTRALIA. E-Safety Commissioner. **Social Media Minimum Age**: Regulatory Guidance. Australia: Australian Government, 2025b. Disponível em: https://www.esafety.gov.au/sites/default/files/2025-09/eSafety-SMMA-Regulatory-Guidance.pdf?v=1757990720895. Acesso em: 29 set. 2025.

AVPA. **Definitions**. c2025. Disponível em: https://avpassociation.com/definitions/. Acesso em: 7 mai. 2025.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Diário Oficial da União, Brasília, DF, 11 jan. 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 9 jun. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 20 dez. 2024.

BRASIL. **Lei nº 15.211, de 17 de setembro de 2025**. Dispõe sobre a proteção de crianças e adolescentes em ambientes digitais (Estatuto Digital da Criança e do Adolescente). Brasília, DF: Presidência da República, 2025c. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/Lei/L15211.htm. Acesso em: 22 set. 2025.

BRASIL. Ministério da Justiça e Segurança Pública. **Crescer em Paz: Estratégia de Justiça e Segurança Pública para Proteção de Crianças e Adolescentes**. Brasília, DF: MJSP, 2025b. Disponível em: https://criaprevencao.com.br/wp-content/uploads/2025/04/Crescer-em-Paz-Estrategia-de-Justica-e-Seguranca-Publica-para-Protecao-de-Criancas-e-Adolescentes_Versao-Digital-.pdf. Acesso em: 22 mai. 2025.

BRASIL. Ministério da Justiça e Segurança Pública. **Portaria MJSP nº 925, de 10 de abril de 2025**. Institui o Comitê Consultivo para formulação de proposta de metodologia e requisitos mínimos de verificação etária em serviços digitais que podem ser acessados por crianças e adolescentes. Brasília: Imprensa Nacional, Seção 1, 2025e. Disponível em: https://dspace.mj.gov.br/bitstream/1/14869/2/PRT_GM_2025_925.pdf Acesso em: 22 mai. 2025.

BRASIL. Ministério da Justiça e Segurança Pública. Secretaria de Direitos Digitais. **Nota Técnica nº 4/2025/SEDIGI/MJ** – Verificação Etária em Serviços Online. Brasília: Ministério da Justiça e Segurança Pública, 2025d. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/drci-seleciona-chefe-de-divisao-para-cooperacao-jurid… Acesso em: 22 mai. 2025.

BRASIL. Ministério dos Direitos Humanos e da Cidadania. **Resolução nº 245, de 05 de abril de 2024**. Dispõe sobre os direitos das crianças e adolescentes em ambiente digital. Brasília, DF: MDHC, 2024a. Disponível em: https://www.gov.br/participamaisbrasil/blob/baixar/48630. Acesso em: 8 jan. 2025.

BRASIL. Ministério dos Direitos Humanos e da Cidadania. **Resolução nº 257, de 12 de dezembro de 2024**. Estabelece as diretrizes gerais da Política Nacional de Proteção dos Direitos da Criança e do Adolescente no Ambiente Digital. Brasília, DF: MDHC, 2024b. Disponível em: https://www.gov.br/participamaisbrasil/blob/baixar/61597. Acesso em: 8 jan. 2025.

BRASIL. Secretaria de Comunicação Social. **Crianças, adolescentes e telas: Guia sobre usos de dispositivos digitais**. Brasília, DF: SECOM, 2025a. Disponível em: https://www.

gov.br/secom/pt-br/assuntos/uso-de-telas-por-criancas-e-adolescentes/guia/guia-de-telas_sobre-usos-de-dispositivos-digitais_versaoweb.pdf. Acesso em: 19 mai. 2025.

BSI. **PAS 1296:2018: Online age checking. Provision and use of online age check services. Code of Practice**. Londres, 31mar. 2018. Disponível em: https://knowledge.bsigroup.com/products/online-age-checking-provision-and-use-of-online-age-check-services-code-of-practice?version=standard. Acesso em: 10 jul. 2025.

CAGLAR, Cansu; NAIR, Abhilash. **EU Member State Legal Framework**. [*S.l.*]: euCONSENT, 2021. Disponível em: https://euconsent.eu/download/eu-member-state-legal-framework/. Acesso em: 02 set. 2025.

CNIL. **Online age verification**: balancing privacy and the protection of minors. Paris, 22 set. 2022. Disponível em: https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors. Acesso em: 27 nov. 2024.

CNIL. **Recommendation 7**: check the age of the child and parental consent while respecting the child's privacy. Paris, 9 ago. 2021. Disponível em: https://www.cnil.fr/en/recommendation-7-check-age-child-and-parental-consent-while-respecting-childs-privacy. Acesso em: 27 nov. 2024.

COMISSÃO EUROPEIA. **eIDAS Regulation**. Brussels: 2025c. Disponível em: https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation. Acesso em: 23 set. 2025.

COMISSÃO EUROPEIA. **EU Age Verification Solution**. Brussels, c2025a. Disponível em: https://ageverification.dev/. Acesso em: 16 jun. 2025.

COMISSÃO EUROPEIA. **Overall Architecture – European Age Verification Solution: Operational, Security, Product and Architecture Specifications**. Brussels: European Commission, Directorate-General for Communications Networks, Content and Technology (DG CNECT), 2025d. Disponível em: https://ageverification.dev/av-doc-technical-specification/docs/architecture-and-technical-specifications/. Acesso em: 06 out. 2025.

COMISSÃO EUROPEIA. **The EU approach to age verification**. Brussels, 2025b. Disponível em: https://digital-strategy.ec.europa.eu/en/policies/eu-age-verification. Acesso em: 9 set. 2025.

EDPB. **Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act, 2018 and Articles 60 and 65 of the General Data Protection Regulation**. Brussels: EDPB, 2023. Disponível em: https://www.edpb.europa.eu/system/files/2023-09/final_decision_tiktok_in-21-9-1_-_redacted_8_september_2023.pdf. Acesso em: 2 set. 2025.

EDPB. **Joint Opinion 4/2022**: on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse. Brussels: EDPB, 2022. Disponível em: https://www.edps.europa.eu/system/files/2022-07/22-07-28_edpb-edps-joint-opinion-csam_en.pdf. Acesso em: 2 set. 2025.

EDPB. **Statement 1/2025 on Age Assurance**. Brussels: EDPB, 2025. Disponível em: https://www.edpb.europa.eu/system/files/2025-04/edpb_statement_20250211ageassurance_v1-2_en.pdf. Acesso em: 5 mai. 2025.

EDRI. **Online age verification and children's rights**. Brussels: EDRI, 2023. Disponível em: https://edri.org/wp-content/uploads/2023/10/Online-age-verification-and-childrens-rights-EDRi-position-paper.pdf. Acesso em: 27 nov. 2024.

EFA. **Age Assurance Technology Trial Final Report Released**. Camberra: EFA, 2025. Disponível em: https://efa.org.au/age-assurance-technology-trial-final-report-released/. Acesso em: 13 set. 2025.

ESPANHA. Ministerio de Juventud e Infancia. Comité de personas expertas para el desarrollo de un entorno digital seguro para la juventud y la infancia. **Informe del comité de personas expertas para el desarrollo de un entorno digital seguro para la juventud y la infancia**. Madrid: Ministerio de Juventud e Infancia, 2024. Disponível em: https://www.juventudeinfancia.gob.es/sites/default/files/noticias/Informe%20del%20comit%C3%A9%20de%20personas%20expertas%20para%20el%20desarrollo%20de%20un%20entorno%20digital%20seguro%20para%20la%20juventud%20y%20la%20infancia.pdf. Acesso em: 5 abr. 2025.

FERNANDES, Elora. Direitos de crianças e adolescentes por design: uma agenda regulatória para a ANPD. *In*: LATERÇA, Priscilla Silva; FERNANDES, Elora; TEFFÉ, Chiara Spadaccini de; BRANCO, Sérgio (coord.). **Privacidade e Proteção de Dados de Crianças e Adolescentes**. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro; Obliq, 2021. *E-book*. Disponível em: https://itsrio.org/wp-content/uploads/2021/10/Privacidade-e-Protecao-de-Dados-de-Crian%C3%A7as-e-Adolescentes-ITS.pdf. Acesso em: 5 out. 2025.

FOSI. **Coming to Terms with Age Assurance**. Washington: FOSI, 2023. Disponível em: https://global-uploads.webflow.com/5f4dd3623430990e705ccbba/64b0011a158eea37fb7796c4_FOSI%20White%20Paper%20Coming%20to%20Terms%20with%20Age%20Assurance%20FOR%20WEBSITE.pdf. Acesso em: 5 mai. 2025.

GORIN, Jérôme; BIÉRI, Martin; BROCAS, Côme. **Demonstration of a privacy-preserving age verification process**. França: Laboratoire d'Innovation Numérique de la CNIL, 2022. Disponível em: https://linc.cnil.fr/demonstration-privacy-preserving-age-verification-process. Acesso em: 03 set. 2025.

ICO. **Age appropriate design**: a code of practice for online services. Wilmslow: ICO, 2022. Disponível em: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/. Acesso em: 28 nov. 2024.

ICO. **Age assurance for the children's code**. Wilmslow: ICO, 2024b. Disponível em: https://ico.org.uk/about-the-ico/what-we-do/information-commissioners-opinions/age-assurance-for-the-children-s-code/. Acesso em: 12 jun. 2025.

ICO; IFF RESEARCH. **How online businesses are using age assurance**: Research findings. Wilmslow: ICO, 2024. Disponível em: https://ico.org.uk/media2/migrated/4030926/20240704-ico-age-assurance-report.pdf. Acesso em: 11 jun. 2025.

IEEE. **IEEE 2089.1-2024**: IEEE Standard for Online Age Verification. New York: IEEE, 2024. Disponível em: https://standards.ieee.org/ieee/2089.1/10700/. Acesso em: 5 out. 2025.

ISO; **IEC. ISO/IEC FDIS 27566-1**: Information security, cybersecurity and privacy protection — Age assurance systems: Part 1: Framework. Geneva: ISO, 2025. Disponível em: https://www.iso.org/standard/88143.html#lifecycle. Acesso em: 5 out. 2025.

LIVINGSTONE, Sonia; STOILOVA, Mariya; RAHALI, Miriam. **Realising children's rights in the digital age**: The role of digital skills: Principle 4: Age appropriate: Develop policies and products that are age appropriate by design and consider using age assurance. Leuven: KU Leuven; ySKILLS, 2023. Disponível em: https://eprints.lse.ac.uk/121075/1/4_Age_appropriate.pdf. Acesso em: 16 jun. 2025.

LIVINGSTONE, Sonia; POTHONG, Kruakae. **Child rights by design: guidance for innovators of digital products and services used by children**. London: Digital Futures Commission; 5Rights Foundation, 2023. Disponível em: https://eprints.lse.ac.uk/119724/. Acesso em: 4 nov. 2024.

NACIMENTO, Natália Castro Reis; BERNARDES, Rochele Juliane Lima Firmeza. Perfis Infantis no Instagram: A Responsabilidade Civil dos Pais e da Plataforma Diante da Violação dos Direitos Personalíssimos. Teresina, **Revista FSA**, v. 22, n. 2, fev. 2025. Disponível em: http://www4.unifsa.com.br/revista/index.php/fsa/article/view/3095/491494663 Acesso em: 30 de abr. 2025.

NIC.BR. **TIC Kids Online Brasil 2023**: Pesquisa sobre o uso da Internet por crianças e adolescentes no Brasi. São Paulo: NIC.br, 2024. Disponível em: https://cetic.br/media/docs/publicacoes/2/20240913124019/tic_kids_online_2023_livro_eletronico.pdf. Acesso em: 5 dez. 2024.

NIC.BR. **TIC Kids Online Brasil 2024**: Pesquisa sobre o uso da Internet por crianças e adolescentes no Brasil. São Paulo: NIC.br, 2025. Disponível em: https://cetic.br/media/docs/publicacoes/2/20250512154312/tic_kids_online_2024_livro_eletronico.pdf. Acesso em: 25 abr. 2025.

OCDE. **The legal and policy landscape of age assurance online for child safety and well-being**: Technical paper. Paris: OECD, 2025. Disponível em: https://www.oecd.org/en/publications/the-legal-and-policy-landscape-of-age-assurance-online-for-child-safety-and-well-being_4a1878aa-en.html. Acesso em: 1 jul. 2025.

OCDE. **Towards digital safety by design for children**. Paris: OECD, 2024. Disponível em: https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/06/towards-digital-safety-by-design-for-children_f1c86498/c167b650-en.pdf. Acesso em: 2 set. 2024.

OFCOM. **Guidance on age assurance and other Part 5 duties for service providers publishing pornographic content on online services**: Annex 2. London: OFCOM, 2023. Disponível em: https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/272586-consultation-guidance-for-service-providers-publishing-pornographic-content/associated-documents/annex-2-guidance-for-service-providers-publishing-pornographic-content-online?v=368675. Acesso em: 5 mai. 2025.

OFCOM. **Guidance on highly effective age assurance**: For Part 3 services. London: OFCOM, 2025. Disponível em: https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/statement-age-assurance-and-childrens-access/part-3-guidance-on-highly-effective-age-assurance.pdf?v=395680. Acesso em: 5 mai. 2025.

OFCOM. **Quick guide to children's access assessments**. Londres: Ofcom, 2024. Disponível em: https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/quick-guide-to-childrens-access-assessments. Acesso em: 5 mai. 2025.

OLSZEWSKI, Bruna Dezevecki. **Overshareting e Responsabilidade Parental**: a necessidade de proteção da criança no ambiente digital e da conscientização sobre o uso das redes sociais. São Paulo: Dialética, 2025. Disponível em: https://books.google.com.br/books?id=8cxJEQAAQBAJ&lpg=PR97&dq=lgpd%20garantia%20de%20idade%20crian%C3%A7as%20e%20adolescentes&lr&hl=pt-BR&pg=PP5#v=onepage&q=lgpd%20garantia%20de%20idade%20crian%C3%A7as%20e%20adolescentes&f=false. Acesso em: 30 de abr. 2025.

ONU. Committee on the Rights of the Child. **General comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration *(art. 3, para. 1)***. Geneva: United Nations, 2013. Disponível em: https://www2.ohchr.org/english/bodies/crc/docs/gc/crc_c_gc_14_eng.pdf. Acesso em: 2 mai. 2025.

ONU. Committee on the Rights of the Child. **General comment No. 25 (2021) on children's rights in relation to the digital environment (seção E)**. Geneva: ONU, 2021. Disponível em: https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=ZFIB6YHG%2FGsPZWN0RxLScHq9GiMBdnF6%2FJbmpI3osWkgGhvw49aL7h%2B8Vn0mCi2e0q8gmJS2YdjNrWEF706%2FDw%3D%3D. Acesso em: 2 mai. 2025.

PENTEL, Avar. Predicting user age by keystroke dynamics. In: COMPUTER SCIENCE ON-LINE CONFERENCE, 7., 2018, [s.l.]. **Proceedings** [...]. Cham: Springer, 2018. p.

336-343. Disponível em: https://link.springer.com/chapter/10.1007/978-3-319-91189-2_33#citeas. Acesso em: 5 out. 2025.

PEREN. **Détection des mineurs en ligne**: peut-on concilier efficacité, commodité et anonymat? França: Pôle d'expertise de la régulation numérique, 2022. Disponível em: https://www.peren.gouv.fr/rapports/2022-05-20%20-%20Eclairage-sur-detection-mineurs_FR.pdf Acesso em: 06 out. 2025.

SAFERNET. **O que é ciberbullying?**. [2019?]. Disponível em: https://new.safernet.org.br/content/o-que-e-ciberbullying Acesso em: 06 out. 2025.

SAS, Martin; MÜHLBERG, Jan Tobias. **Trustworthy Age Assurance?** A risk-based evaluation of available and upcoming age assurance technologies from a fundamental rights perspective. Brussels: The Greens/EFA in the European Parliament, 2024. Disponível em: https://www.greens-efa.eu/en/article/document/trustworthy-age-assurance. Acesso em: 20 ago. 2025.

SHAFFIQUE, Mohammed Raiz; HOF, Simone van der. **Research report**: Mapping age assurance typologies and requirements: Executive summary. Luxembourg: European Commission, 2024. Disponível em: https://digital-strategy.ec.europa.eu/en/library/research-report-mapping-age-assurance-typologies-and-requirements. Acesso em: 5 out. 2025.

STEINBERG, Stacey. Sharenting: Children's privacy in the age of social media. [*S.l.*], **Emory Law Journal**, v. 66, n. 4, p. 839-884, 2017. Disponível em: https://scholarlycommons.law.emory.edu/elj/vol66/iss4/2/. Acesso em: 13 de maio de 2025.

UNIÃO EUROPEIA. **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016** [...]. Brussels, 2016. Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng. Acesso em: 5 out. 2025.

W3C. **Verifiable Credentials Data Model 2.0**. W3C Recommendation, 15 mai. 2025. [*S.l.*]: W3C, 2025. Disponível em: https://www.w3.org/TR/vc-data-model/. Acesso em: 20 ago. 2025.

www.gov.br/anpd

ANPD

Agência Nacional de
Proteção de Dados