26º ENANCIB
Encontro Nacional de Pesquisa e Pós-Graduação em Ciência da Informação
A Amazônia na sociedade global em rede: assimetrias e potencialidades informacionais, tecnológicas e ambientais
Belém, Pará, 09 a 13 de novembro de 2026
Universidade Federal do Pará

XXVI ENCONTRO NACIONAL DE PESQUISA E PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO - XXVI ENANCIB

2177-3688

GT 5 – Política e Economia da Informação

DA BURLA AO LIMITE À BURLA COMO LIMITE: AFERIÇÃO E PROTEÇÃO INFANTOJUVENIL NO *ETHOS* DA DIGITALIDADE CAPITALISTA

FROM CIRCUMVENTION TO THE LIMIT, TO CIRCUMVENTION AS A LIMIT: *AGE VERIFICATION AND YOUTH PROTECTION IN THE ETHOS OF CAPITALIST DIGITALITY*

Ingrid Rocha Guimarães – Instituto Brasileiro de Informação em Ciência e Tecnologia (IBICT)
Gustavo Silva Saldanha – Instituto Brasileiro de Informação em Ciência e Tecnologia (IBICT)

Modalidade: Trabalho Completo

Resumo: A exigência de verificação etária no ambiente digital impõe novas tensões ao campo informacional brasileiro. Esta pesquisa investiga em que medida a agenda regulatória de proteção à infância e à adolescência, ao fundamentar-se em barreiras estritamente técnicas, pode aprofundar a exploração algorítmica. Qualitativo, exploratório e documental, o estudo examina o cenário regulatório nacional recente à luz do caso precursor da Austrália. O referencial teórico articula o pensamento de Bernd Frohmann, Luciano Floridi, Maria Nélida González de Gómez e Rafael Capurro. Os resultados demonstram que soluções pautadas no determinismo tecnológico não apenas falham, mas ampliam a superfície de vigilância sobre o cidadão. Conclui-se que preservar a responsabilidade compartilhada na proteção infantil exige integrar auditorias independentes, escrutínio humano e letramento informacional às soluções técnicas.

Palavras-chave: Estatuto Digital da Criança e do Adolescente (ECA Digital); economia política da informação; proteção; ética; responsabilidade compartilhada.

Abstract: The requirement for age verification in the digital environment creates new tensions within the Brazilian information landscape. This study investigates the extent to which the regulatory agenda for the protection of children and adolescents, by relying on strictly technical barriers, exacerbates algorithmic exploitation. Qualitative, exploratory, and document-based in nature, the study examines the recent national regulatory landscape in light of the pioneering case in Australia. The theoretical framework draws on the work of Bernd Frohmann, Luciano Floridi, Maria Nélida González de Gómez, and Rafael Capurro. The results demonstrate that solutions based on technological determinism not only fail but also expand the scope of surveillance over citizens. This study concludes that preserving shared responsibility in child protection requires integrating independent audits, human scrutiny, and information literacy into technical solutions.

Keywords: Estatuto Digital da Criança e do Adolescente (ECA Digital); political economy of information; protection; ethics; shared responsibility.

1 INTRODUÇÃO AO DILEMA DA ÉTICA ETÁRIA NA DIGITALIDADE

Em 10 de dezembro de 2025, entrou em vigor na Austrália a "*Online Safety Amendment (Social Media Minimum Age) Act 2024*", legislação que altera a "*Online Safety Act 2021*" para impor a idade mínima obrigatória de 16 anos na criação e manutenção de contas em redes sociais (Austrália, 2025). Ao instituir um modelo de proteção à infância e à adolescência em ambientes digitais fundamentado, essencialmente, na imposição de uma barreira etária, a Austrália assumiu a dianteira na aplicação de bloqueios dessa magnitude (Livingstone, 2026). O posicionamento adotado representa uma ruptura com o próprio histórico regulatório australiano, até então pautado por maior cautela (Hu, 2025).

Embora a formulação de barreiras etárias avance por projetos de lei na União Europeia, no Reino Unido, na Nova Zelândia e na Espanha, e países como Malásia, Turquia e Emirados Árabes Unidos já tenham fixado suas legislações (Reuters, 2026), o pioneirismo australiano em um cenário mais proibitivo coloca o país como um estudo de caso relevante sobre os limites do controle de acesso no meio digital. O debate está em pauta e é controverso, especialmente no campo jurídico, como exemplificado pela recente rejeição de um projeto de lei que proibia o uso de redes sociais por menores de 15 anos pelo Conselho Constitucional da França (Reuters, 2026), sob o argumento de violação à liberdade de expressão.

No Brasil, a busca por uma internet mais segura tomou forma com o Estatuto Digital da Criança e do Adolescente (ECA Digital), instituído pela Lei nº 15.211/2025 (Brasil, 2025a), vigente desde 17 de março de 2026. Esse marco legal reconfigura o cenário regulatório nacional ao estabelecer obrigações específicas de proteção em ambientes digitais, exigindo, precipuamente, a implementação de mecanismos de aferição de idade confiáveis para assegurar a adequação entre o ambiente e o público-alvo.

Diante dessa conjuntura, discute-se aqui um quadro analítico de parte das tensões inerentes ao processo de assegurar a segurança de crianças e jovens na digitalidade por meio de infraestruturas tecnológicas controladas pelo mercado. A depender de como essas salvaguardas forem desenhadas e aplicadas, o Estado corre o risco de, colateralmente, chancelar a expansão de sistemas de monitoramento e de perfilamento de dados. Isso ocorre porque a limitação do acesso infantojuvenil a ambientes e conteúdos de risco passa a exigir,

inevitavelmente, procedimentos de aferição ou verificação etária que ampliam a vigilância sobre os sujeitos. Nesse cenário, o problema de pesquisa que orienta este estudo é: em que medida a agenda regulatória sobre "mecanismos confiáveis de aferição de idade", conforme formulada pela Autoridade Nacional de Proteção de Dados, aprofunda a invasividade da mediação algorítmica na digitalidade?

A justificativa da pesquisa ancora-se na premência do debate na conjuntura brasileira, no fato de que o mercado tecnológico e a sociedade civil encontram-se em fase de adequação ao ECA Digital, bem como nas questões sensíveis vinculadas ao fenômeno da realidade informacional de exposição de crianças e adolescentes ao espaço privado das plataformas digitais. A recente normativa confronta práticas enraizadas durante o período em que a expansão do acesso digital infantojuvenil sobrepujou a efetividade da proteção jurídica. Sob essa ótica, evidencia-se que prescrições estritamente técnicas se revelam inócuas ao serem dissociadas das dinâmicas sociais de resistência e das táticas de burla operadas pelos sujeitos. Esta condição manifesta-se em uma estrutura de mediação sociotécnica marcada pela opacidade e pela diretriz da mercantilização, e não por princípios éticos estruturantes. Em outras palavras, concebe-se uma pseudo-ética da mediação pretensamente neutra da técnica, em detrimento do crivo humano de autoridade(s) epistêmica(s).

Há uma equivocada atribuição de autonomia à tecnologia, como se o artefato pudesse existir independentemente da agência humana, quando, factualmente, resulta de sua intencionalidade. E, para além disto, como se, no caso da "eventual" atuação do artefato – ou de sua artificialidade -, a criatura, pudesse antecipar, condicionar e reproduzir comportamentos da agência criadora, do *ethos* humano. Trata-se de um "jogo", sob o pseudoprincípio da neutralidade, onde burla e limite de usos éticos de uma fonte, por exemplo, fossem objeto de juízo da máquina, "reprodutora" de juízos humanos previamente programados para sua ação artefactual. A cidadania é colocada em risco na digitalidade quando se atribui a algoritmos supostamente infalíveis a responsabilidade por decisões no processo educativo. Essa ilusão de uma ética da máquina eclipsa o dever do Estado, da família e da sociedade, agentes de tal juízo demarcados na Constituição brasileira (Brasil, 1988).

Em face do exposto, o objetivo deste estudo é analisar, no plano teórico-político, parte das tensões que atravessam o processo de aferição de idade, investigando como os atritos entre a proteção embasada em atributos técnicos e a agência digital dos jovens não apenas explicitam os limites da eficácia normativa, mas também reconfiguram a própria mediação em

um ambiente submetido à crescente automação e ao uso de metadados para mercantilização das relações sociais em meio digital. O intuito é oferecer subsídios críticos para a atualização de marcos regulatórios nacionais, utilizando a análise das contradições do modelo proibitivo australiano como parâmetro para antecipar os limites da implementação brasileira.

Para o alcance dos objetivos propostos, a pesquisa caracteriza-se como teórica, embasada em pesquisa qualitativa de natureza exploratória e documental estruturada em *corpora* selecionados pela atualidade geopolítica sobre a temática. O *corpus* documental reúne marcos do ordenamento jurídico brasileiro vigente, destacando-se o ECA Digital (Brasil, 2025a), as diretrizes da ANPD (Brasil, 2026a) e a consulta pública do Ministério da Justiça e Segurança Pública (Brasil, 2026b). No âmbito internacional, foram levantadas as diretrizes australianas sobre o tema, o *Social media minimum age regulatory guidance* (Austrália, 2025), o relatório *Age Assurance Technology Trial* (Age Check Certification Scheme, 2025) e os estudos de Tengyue Hu (2025) e Woodley *et al.* (2025), que avaliam os impactos da nova legislação naquele país, tomado como caso precursor. A adoção dessa restrição na Austrália, ocorrida meses antes da vigência do ECA Digital, oferece um horizonte empírico para a prospecção dos impactos, das limitações e da eficácia dos mecanismos de aferição de idade já utilizados, embora Austrália e Brasil adotem matrizes regulatórias distintas.

Para debater a dimensão ética do fenômeno, a pesquisa mobiliza Frohmann (2000; 2008) para observar as tensões inerentes à subjetividade; Floridi (2014), para alicerçar a crítica da mercantilização ontológica na infoesfera; González de Gómez (2002), para balizar a análise das micropolíticas infraestruturais; e Capurro (2016), para fundamentar as contradições éticas da cidadania digital frente ao risco de controle absoluto exercido por conglomerados tecnológicos. Articulados, esses autores demonstram como a delegação da proteção infantil a sistemas algorítmicos reconfigura estruturalmente as regras da cidadania digital. Nesse sentido, a pesquisa estabelece critérios intencionais de seleção das fontes, afastando-se de abordagens sistemáticas. Embora reconheça os limites de inferência desse recorte, a pesquisa alicerça-se em conceitos consolidados no debate sobre o capitalismo de plataformas e a mercantilização da esfera pública digital.

2 DO SUJEITO AO ATRIBUTO: A PROTEÇÃO INFANTOJUVENIL FRAGMENTADA NA DIGITALIDADE

A trajetória de proteção infantojuvenil no Brasil estruturou-se sob a premissa da responsabilidade compartilhada, cujo alicerce está posto desde a Constituição de 1988, que instituiu a proteção integral a esse público como prioridade absoluta ao estabelecer um dever compartilhado entre família, sociedade e Estado (Brasil, 1988, art. 227). Esse pressuposto ganhou densidade com o Estatuto da Criança e do Adolescente (ECA) (Brasil, 1990, art. 240), legislação que, ao reforçar o sistema de garantias, antecipou desafios da era digital ao tipificar crimes em meios telemáticos. A massiva transposição das interações sociais para o espaço digital exigiu uma atualização do pacto protetivo, processo delineado inicialmente pelo Marco Civil da Internet (Brasil, 2014, art. 29), que assegurou o direito ao controle parental e reforçou o compromisso multissetorial com a educação para inclusão digital desse público. Posteriormente, a Lei Geral de Proteção de Dados (Brasil, 2018, art. 14) subordinou o tratamento de dados de menores ao princípio do "melhor interesse" e estabeleceu a obrigatoriedade do consentimento específico dos responsáveis.

A despeito do avanço promovido pelos referidos marcos legais, a natureza predominantemente reativa dessas normas foi insuficiente diante da atuação cada vez mais acentuada de algoritmos que impulsionam a exposição precoce a conteúdos impróprios e estimulam comportamentos compulsivos. Nessa conjuntura, o ECA Digital foi concebido para superar essa limitação ao substituir a resposta reativa a crimes no ambiente digital por uma tutela preventiva, que obriga lojas de aplicativos, sistemas operacionais e plataformas a incorporar a aferição etária como condição vinculante de operação (Brasil, 2025a).

O regramento também fomenta o engajamento dos provedores de aplicação no arranjo de responsabilidade compartilhada (cujo *ethos* na digitalidade nasce e se sustenta sob o fundamento do lucro a partir de meios de produção concentrados no topo da pirâmide econômica), atribuindo a essas corporações o dever de atuar ativamente na proteção do público infantojuvenil em seus ecossistemas digitais. Sob a lógica da corresponsabilidade, a legislação admite a insuficiência da barreira técnica quando operada de forma isolada e consagra a educação e o acompanhamento tutelar como dimensões indissociáveis da experiência infantojuvenil, delegando aos responsáveis o dever de cuidado contínuo (Brasil,

2025a). Alinhado a essa diretriz, o artigo 24 do ECA Digital impõe a vinculação obrigatória das contas de redes sociais de jovens de até 16 anos às de um responsável legal (Brasil, 2025a).

As medidas de proteção direcionadas ao público infantojuvenil no ambiente digital exigem, intrinsecamente, a certificação prévia da faixa etária. Todavia, a implementação de tais salvaguardas enfrenta o desafio de isolar o atributo etário sem promover a identificação do usuário. No cenário atual, a coleta desse dado tem ocorrido por meio de mecanismos que, ao aferirem a idade, revelam simultaneamente a identidade civil, sujeitando tanto jovens quanto adultos a uma exposição invasiva de sua esfera de privacidade. Até o momento, plataformas de grande alcance têm recorrido à identificação biométrica ou documental (Kaufman; Bhatia, 2026), métodos classificados como altamente sensíveis sob a ótica da LGPD.

A análise de Floridi (2014) evidencia que esse tipo de cenário ilustra a crise contemporânea da privacidade, provocada pela erosão das barreiras naturais e das dificuldades técnicas que antes tornavam o cruzamento de dados lento e oneroso, gerando a necessária fricção. Quanto mais fácil se torna a correlação de dados, mais céleres e rentáveis operam os sistemas de mercado; porém, nessa mesma proporção, eleva-se a exposição do indivíduo e os riscos de mercantilização de seus dados e reusos para controle, persuasão e exploração de suas afecções. Assim sendo, a obrigatoriedade de comprovação de idade acaba por instituir, na prática, um rastreamento que viola diretamente as garantias da LGPD.

Diante desse tensionamento, o ECA Digital estabeleceu um modelo regulatório pautado pelos princípios do risco e da proporcionalidade. A regulamentação exige dos fornecedores uma identificação e avaliação prévia de duas categorias de ameaças. A primeira refere-se aos riscos inerentes ao uso do serviço, como a exposição a conteúdos impróprios, enquanto a segunda vincula-se aos riscos decorrentes do próprio mecanismo de aferição, o qual pode ensejar o tratamento indevido de dados e o aprofundamento da vigilância (Brasil, 2026a). Sob essa lógica, ambientes de alto risco, como *sites* adultos, com conteúdos pornográficos ou imagens sensíveis a diferentes contextos e culturas, exigem protocolos rigorosos, enquanto serviços de menor periculosidade devem priorizar a privacidade, limitando a coleta ao estritamente necessário para a confirmação da faixa etária (Brasil, 2025a; Brasil, 2026a).

Em resposta às exigências do ECA Digital, plataformas privadas de acesso provável, tais como *Google*, *Tik Tok* e o *YouTube*, implementam modelos de estimativa de idade (*age inference*), extraindo o atributo etário a partir da telemetria comportamental, histórico de buscas, dados declarados e natureza do conteúdo produzido (Redação G1, 2026). Na mesma

esteira, a *Meta* passou a integrar metadados extraídos de sistemas operacionais e lojas de aplicativos (Redação G1, 2026). Uma vez estimada a faixa etária, a arquitetura de rede aciona restrições proativas e automatizadas, tais como o bloqueio de aplicações, a ativação de filtros de busca e a exclusão de conteúdos voltados ao público adulto (Redação G1, 2026). Faz-se relevante enfatizar que, independentemente de tais posicionamentos nos processos de identificação etária, o foco das empresas está na obtenção do lucro através dos metadados produzidos pelo uso de seus usuários; logo, quanto menos acessos, menos vantagem para cada plataforma privada em sua concorrência no *ethos* da digitalidade, reforçando a descrição weberiana de construção das formas de mercantilização do espírito através do capitalismo (Weber, 2004). Nesse caso, coloca-se em cena a participação pretensamente ajuizada de crianças e adolescentes na esfera pública, espaço que, no entanto, é desenhado por empresas focadas no uso intensivo de seus serviços e produtos, e não nos riscos à saúde e à dignidade humana, por exemplo, de uma pessoa com cinco anos de idade.

A adequação regulatória alcança a atuação do Estado, que intensificou a análise de riscos em plataformas de redes sociais e jogos eletrônicos. Recentemente, serviços como *TikTok*, *WhatsApp* e *Pinterest* tiveram a classificação indicativa elevada em razão dos conteúdos veiculados (Lopes, 2026). O ordenamento jurídico brasileiro dispõe de uma política de classificação indicativa pautada em critérios objetivos para definir a faixa etária adequada, a qual abrange também as empresas responsáveis por plataformas e aplicações de internet. A base legal dessa prerrogativa existe desde a implementação do ECA (Brasil, 1990) e foi expandida pelo ECA Digital (Brasil, 2025a). Sob essa base, a classificação indicativa digital é validada pelo Ministério da Justiça e Segurança Pública (MJSP), que avalia os conteúdos com base em sexo, nudez, drogas, violência e interatividade, ponderando o contexto para mensurar o impacto no público (Brasil, 2025b). Essa filtragem segmenta os materiais em acesso livre ou faixas etárias restritas de 6, 10, 12, 14, 16 e 18 anos (Brasil, 2025b).

3 O MERCADO DIGITAL DA INFÂNCIA E DA ADOLESCÊNCIA NA DIGITALIDADE CAPITALISTA

A adaptação ao ECA Digital avança com o objetivo de mitigar as tensões regulatórias ao estabelecer a distinção entre aferição e verificação de identidade. Conforme as diretrizes formuladas pela ANPD, o processo padrão deve se limitar à aferição, modelo que abrange procedimentos de checagem, estimativa ou inferência de faixa etária focados estritamente na confirmação binária de um atributo etário, isto é, uma resposta de sim ou não (Brasil, 2026a).

A aferição garante que a plataforma confirme exclusivamente a elegibilidade do usuário, resguardando seu anonimato. Com isso, efetiva os princípios da privacidade por padrão (*privacy by default*) e desde a concepção (*privacy by design*), assegurando a minimização de dados como regra intrínseca à arquitetura de qualquer sistema, durante todo o seu ciclo de vida. Em contrapartida, a verificação de identidade, imposta em ambientes digitais mais sensíveis, exigiria a comprovação de quem é o cidadão, ou seja, a identificação, um método considerado excessivo para o controle de acesso ordinário (Brasil, 2026a).

Seguindo o princípio da responsabilidade compartilhada, o ECA Digital determina que provedores de lojas de aplicações e sistemas operacionais viabilizem, por meio de Interfaces de Programação de Aplicações (APIs), o fornecimento de sinal de idade aos provedores de conteúdo. Sob esse arranjo, os provedores recebem apenas a confirmação da condição etária necessária, sem acesso aos dados brutos. Embora isso não desonere as plataformas de conteúdo do dever de realizar a própria conferência final, essa interoperabilidade mitiga coletas redundantes (Brasil, 2025a).

Alinhada a essa diretriz, a ANPD (2026a) adota como referencial técnico os mecanismos criptográficos, como provas de conhecimento zero (*Zero-Knowledge Proofs* - ZKP) e credenciais verificáveis, que permitem ao usuário comprovar a maioridade a partir de uma fonte fidedigna sem que o serviço receba ou armazene dados identificáveis adicionais. Para plataformas de acesso provável, como as redes sociais, a Secretaria Nacional de Direitos Digitais (Brasil, 2026b), sob recomendação do Instituto Alana, prescreve o método de cascata (*waterfall*) para validação sucessiva. A abordagem prioriza a inferência etária por comportamento e o uso de sinais interoperáveis via *APIs* de lojas de aplicativos, acionando a verificação documental apenas diante de indícios iniciais inconclusivos. A exigência de verificação documental ou estimativa biométrica facial a cada acesso restringe-se a ambientes de risco crítico, cuja oferta seja proibida a menores de 18 anos, como material pornográfico e jogos de azar, cenários nos quais a autodeclaração é expressamente vedada (Brasil, 2025a). A legislação proíbe expressamente que essa governança venha a “impor, autorizar ou resultar na implantação de mecanismos de vigilância massiva” (Brasil, 2025a, art. 37).

No entanto, a desvinculação entre a identidade civil e o atributo etário, concebida para preservar a privacidade, baseia-se na falsa premissa de que a segurança pode ser garantida por uma eficácia tecnológica autônoma, isolada do escrutínio humano direto, dos contextos sociais e históricos de recepção e da própria construção ética que antecede, se dá e prossegue

no contexto pré-uso (identificação ou entrada no sistema), uso e lastro de uso. Ao determinar que a aferição de idade deve ocorrer de modo "proporcional, auditável e tecnicamente seguro" (Brasil, 2025a), sem exigir a revisão humana nos processos de análise e validação, o ECA Digital delega o poder de certificação a um regime opaco de processamento automatizado, centralizado em *APIs* e na troca de sinais etários entre as grandes plataformas de tecnologia. A delegação transfere o monopólio da certificação para infraestruturas privadas que, para minimizar a fricção de acesso e assegurar o fluxo econômico, privilegiam estimativas estatísticas (faciais e comportamentais) em detrimento de uma mediação construída e mantida por agenciamentos humanos diretos e permanentes.

Nesse sentido, o princípio do "melhor interesse da criança", que deveria ser objeto do contrato social de um *ethos* fundado na proteção conforme asseguram a Constituição e a LGPD, é capturado pela lógica do mercado e reduzido a métricas algorítmicas de gerenciamento de risco e mercantilização de metadados. É precisamente nessa ausência de supervisão do agenciamento humano, quando a proteção se resume ao cálculo automatizado, que a criatividade e a agência infantojuvenil encontram brechas para contornar esses mecanismos de segurança por meio de táticas de burla. Corpo e afetos de crianças e adolescentes restam, pois, expostos à exploração por cálculos corporativos de aferição etária, suprimindo-se a ação direta dos agentes formalmente incumbidos dessa proteção pelo princípio constitucional (Estado, família e sociedade).

Na realidade sociotécnica, o perigo da burla entrelaça-se ao próprio modelo de negócios do ente privado, ator que detém o poder infraestrutural efetivo para induzir comportamentos na digitalidade. Se o princípio existencial da empresa é a sua viabilidade por meio do lucro, e não o compromisso ético permanente de regular o espaço público por ela controlado, torna-se ingênuo esperar que essa corporação coloque o risco de violência contra uma criança acima do risco financeiro de limitação do seu próprio negócio.

Embora as diretrizes da ANPD e o Artigo 6º do ECA Digital determinem que os fornecedores de tecnologia incorporem a lógica de privacidade e proteção de dados tomando medidas razoáveis "desde a concepção" da plataforma, a margem de "razoabilidade" apresenta-se como um parâmetro regulatório frágil. Ao delegar ao próprio ente privado a baliza de conformidade moral e técnica de suas aplicações ainda nas etapas de desenvolvimento, o legislador transfere uma responsabilidade pública a *priori* para a esfera corporativa. Como consequência, a vasta gama de dados sensíveis que tocam diretamente a

dignidade e a existência de crianças e adolescentes acaba submetida a um ambiente em que a proteção concorre, de forma assimétrica, com o imperativo estrutural da mercantilização.

Esse arranjo não se restringe ao Brasil. Na Austrália, avaliações sobre a implementação de garantias de idade embutidas diretamente nas camadas de *hardware* e rede indicam uma tendência global de compartimentalização das salvaguardas e, consequentemente, da descentralização da responsabilidade. Conforme elucida a análise da Age Check Certification Scheme (2025), a dispersão das funções de controle pela infraestrutura tecnológica dilui a responsabilização entre diversos atores, uma vez que, nesse cenário, a ausência de fronteiras contratuais claras propicia uma ambiguidade jurídica que enfraquece tanto a fiscalização estatal quanto o estabelecimento de mecanismos diretos de reparação ao usuário.

A própria estrutura do ecossistema digital está submetida a interesses abertamente conflitantes. Enquanto, potencialmente, Estados, famílias e sociedades se mobilizam para assegurar a proteção da infância, a infraestrutura privada opera sob a premissa do lucro. Uma vez que o ECA Digital (Brasil, 2025a), por exemplo, proíbe a reutilização de dados obtidos durante processos de aferição e verificação de idade para qualquer finalidade de publicidade comercial, bem como a utilização de técnicas de perfilamento para o direcionamento de anúncios a crianças e adolescentes, a conformidade regulatória impõe um severo estrangulamento ao modelo de negócios das plataformas. Ao interditar a conversão do atributo etário em ativo mercadológico circulante, a legislação fratura a engrenagem de monetização hipersegmentada que sustenta redes sociais, jogos digitais, plataformas de apostas e serviços de *streaming*, colocando o arcabouço regulatório em atrito direto com a economia política da fase atual do capitalismo. Diante dessa conjuntura, o zoneamento técnico corre o risco de ser mobilizado como um subterfúgio para ocultar falhas de privacidade e blindar as empresas contra o seu próprio dever de reparação.

A dispersão em camadas de *hardware* e rede também impõe uma neutralização do julgamento moral humano. Uma vez inscritas no próprio desenho técnico, as normativas padronizadas antecipam relações preferenciais de forma prescritiva e coordenam a cadeia de produção da informação (González de Gómez, 2002). Na prática, a infraestrutura redefine as condições de acesso e os limites da interação, reconfigurando os direitos basilares da cidadania digital. A infraestrutura técnica opera como um dispositivo de opacidade que converte decisões éticas, políticas e penais intrincadas em uma operação protocolar e ilusoriamente neutra, reforçando a inimputabilidade das empresas nas relações sociais da

digitalidade, ambiente por elas desenhado e controlado conforme os potenciais de rendimento financeiro de seus modelos algorítmicos.

Para além das questões de opacidade, a auditoria solicitada pelo governo australiano revelou que alguns fornecedores de tecnologia de verificação de idade, em uma suposta antecipação a demandas estatais, desenvolveram mecanismos de rastreabilidade para reguladores e forças policiais, retendo dados biométricos completos ou documentos de identidade de todos os usuários, mesmo quando tal retenção não era necessária ou solicitada (Age Check Certification Scheme, 2025). O relatório *Age Assurance Technology Trial* enfatiza que, embora a maioria dos provedores siga as boas práticas de minimização de metadados, a infraestrutura privatizada atua como um vetor de monitoramento assimétrico, enquanto a opacidade facilita o desvio de finalidade e exige uma fiscalização estatal incisiva para proteger a cidadania (Age Check Certification Scheme, 2025). O documento descarta a hipótese de falência técnica sistêmica, mas demostra como a racionalidade mercadológica pode cooptar a proteção infantil como pretexto para a expansão de infraestruturas de vigilância e a captura de metadados excedentes, assentando o lucro sobre qualquer princípio ético.

Na regulação brasileira, a operacionalização da verificação etária exigida pelo ECA Digital tenta equilibrar a eficácia protetiva e a garantia da privacidade. O dissenso está presente nos debates da consulta pública conduzida pelo Ministério da Justiça e Segurança Pública (Brasil, 2026b). De um lado, a proposta de centralizar a custódia da identidade digital em uma estrutura governamental única, via *Gov.br*, recebeu objeções na consulta pública em função do risco de constituir repositórios massivos de dados sob controle estatal (Brasil, 2026b). Por outro lado, a descentralização dessa governança em favor das plataformas privadas compromete a soberania digital do país, uma vez que aliena a custódia da identificação de brasileiros a atores corporativos estrangeiros, vulnerabilidade que expõe dados pessoais de cidadãos a ataques e vazamentos direcionados, bem como à exploração não autorizada de metadados para o treinamento de modelos de inteligência artificial (Brasil, 2026b). Diante disso, o desafio para 2027, marco da fiscalização efetiva (Almeida, 2026), consiste em garantir a eficácia do ordenamento estatal de forma que impeça tanto o monitoramento invasivo por parte do Estado quanto a exploração algorítmica das grandes corporações.

O diagnóstico formulado por Floridi (2014) estabelece que os sujeitos se tornaram indissociáveis do ambiente informacional, existindo de forma ubíqua e integrados a agentes artificiais (como algoritmos) e a multiagentes híbridos (entidades humanas e artificiais, como

as próprias plataformas digitais). Nesse sentido, reduzir o debate regulatório à escolha do aparato técnico que centralizará o controle de acesso privilegia a mecânica da ferramenta em detrimento da compreensão política da infraestrutura e de suas assimetrias de poder e vigilância. Ao circunscrever o cidadão à condição de consumidor passivo das regras de mercado, essa abordagem favorece a eficiência tecnológica e a mercantilização dos metadados. A delegação desse controle sabota a premissa constitucional da responsabilidade compartilhada (Brasil, 1988), bem como destitui o corpo social de sua agência pedagógica. Ao permitir que a validação de direitos se dê primariamente pela imposição de barreiras tecnológicas, o Estado corre o risco de ver seu ordenamento jurídico reduzido a um dispositivo de opacidade, controlado por atores corporativos cujas lógicas operacionais refletem as condições econômicas de sua própria emergência (González de Gómez, 2002).

Para González de Gómez (2002), as infraestruturas informacionais não apenas regulam o acesso, mas prescrevem as próprias condições de existência e de cidadania digital. Esse processo de subsunção infraestrutural mapeado pela autora reverbera a advertência de Capurro (2016) sobre o esvaziamento da identidade e a perda de consciência sobre a liberdade no ambiente informacional contemporâneo, alertando para a vigilância inerente à sua faceta digital. Com efeito, na digitalidade, o cidadão perde cada vez mais a consciência de sua dimensão cognitiva no contexto da materialidade das relações sociais, incluindo a compreensão de seu corpo como agente da realidade, e passa a confundir o seu próprio ser com os seus rastros quantificáveis. Essa compressão reduz a complexidade da subjetividade de indivíduos e de sociedades inteiras a meras variáveis de intercâmbio comercial (Capurro, 2016). Ao operar sob essa racionalidade mercadológica, a validação delegada ao código técnico usurpa as forças sociais de representação, o que expõe a governança pública à apropriação por esses sistemas e expande uma moderação algorítmica opaca.

A condição da infância e da juventude no ambiente digital brasileiro é reduzida a um sinal de idade interoperável, processado por APIs sem a consciência do sujeito. Imperceptível ao usuário, essa articulação fragmenta o sujeito em amostras de comportamento e o perfila, o que confirma a denúncia de Frohmann (2008) sobre como os sistemas documentais de informação constroem e configuram materialmente a subjetividade humana. O controle corporativo dos algoritmos retira do indivíduo o domínio sobre sua presença na rede, atuando para ditar ativamente quais conteúdos cada pessoa deve consumir e como deve se comportar.

A ilusão de controle é desmontada pela crítica de Frohmann (2000; 2008) aos limites da *cyber ethics*. O autor recusa a existência de uma ética da informação em sentido especial, denunciando que a simples aplicação de princípios éticos gerais aos serviços de informação mascara as relações de dominação exercidas pelas infraestruturas materiais invisíveis. O ambiente digital instaura uma ética dos *bytes*, na qual as infraestruturas tecnológicas utilizam os corpos infantojuvenis como matrizes produtoras de lucro. Esse processo de exploração e controle do comportamento, focado no sequestro dos fluxos de afeto sob a lógica de mercado, desemboca na transfiguração ontológica descrita por Floridi (2014) anteriormente. No interior do ambiente informacional contemporâneo, no qual a dicotomia entre o *online* e o *offline* deixou de existir, o indivíduo é destituído de sua cidadania e convertido em uma mercadoria informacional, um sujeito reificado e exaustivamente precificado no mercado publicitário global. Sob a denúncia política de Capurro (2016), a mercantilização absoluta enclausura a subjetividade em um espaço no qual as oportunidades de agência e de liberdade real são sacrificadas em nome da hegemonia dos grandes monopólios tecnológicos.

A convergência entre a fabricação da identidade e a extração econômica demonstra que a preocupação com vazamentos de dados é secundária frente à captura ontológica estrutural. Nesse cenário, a proteção técnica pretendida pela lei corre o risco de tornar a verificação de idade em uma ferramenta de exploração, cujo objetivo final subordina-se ao lucro e ao gerenciamento de riscos empresariais. Nesse sentido, o esvaziamento da corresponsabilidade não decorre da apatia social, mas da imposição de um regime de modulação contínua que escapa ao crivo da consciência, operando de forma pervasiva mediante a própria arquitetura digital. Como o monitoramento avança em segundo plano por meio de infraestruturas corporativas opacas e inacessíveis às famílias, o sistema suprime o espaço da mediação ética humana. Esse arranjo institucionaliza a tecnocratização da proteção por meio do controle algorítmico sobre a subjetividade, o que anula a agência consciente da sociedade civil.

4 CONSIDERAÇÕES FINAIS: A AGÊNCIA INFANTOJUVENIL CAPTURADA NA TEIA DA DIGITALIDADE

A presente investigação evidenciou que a transição para modelos de aferição de idade, embasados em atributos técnicos, enfrenta limites frente à agência infantojuvenil e à racionalidade mercadológica das plataformas digitais. Embora Austrália e Brasil reconheçam a ineficácia da autodeclaração etária para obstar o acesso infantojuvenil a ambientes de alto

risco, ambos centraram o controle de garantia de idade (*age assurance*) na conta do usuário. Não obstante, os tensionamentos divergem. Enquanto o modelo australiano centralizou o controle nas plataformas e na tecnologia, chegando a vedar a autorização parental como exceção para o acesso a redes sociais (Austrália, 2025), o ECA Digital contrapesou a mediação tecnológica ao reafirmar a família e a sociedade civil como indispensáveis à presença infantojuvenil no ambiente digital (Brasil, 2025a).

A estratégia regulatória australiana de proibir o acesso de menores de 16 anos às redes sociais colidiu frontalmente com as práticas sociais de apropriação da digitalidade. Em vez de ceder, a agência infantojuvenil fraturou a infraestrutura limitadora mediante a burla. O repertório de evasões documentado por Hu (2025), Woodley et al. (2025) e Livingstone (2026) abrange desde táticas elementares, como o uso de credenciais e documentos de adultos ou simulações biométricas que ludibriam o reconhecimento facial, até técnicas mais sofisticadas, a exemplo de Redes Privadas Virtuais (*Virtual Private Networks* — VPNs), filtros e linguagens cifradas para enganar a moderação de conteúdo.

A postura dos jovens australianos demonstra que as tentativas de controle da *internet*, ainda que sob pretexto protetivo, fracassam ao desconsiderar a agência e as práticas de apropriação dos próprios sujeitos. A experiência do país evidencia não apenas a falência de restrições puramente técnicas, mas também reafirma a agência infantojuvenil perante o avanço daquilo que Capurro (2016) caracteriza como um Leviatã só que dessa vez é algorítmico, um poder infraestrutural privado que usurpa as funções tradicionais do Estado de Direito. Esse poder é exercido tanto de forma *ad intra* (ao colonizar as forças afetivas e comportamentais do usuário por meio de modulações algorítmicas) quanto *ad extra* (ao contornar jurisdições e fronteiras geopolíticas, impondo seus "Termos de Consentimento" privados como se fossem leis soberanas). Conforme adverte Capurro (2016, p. 74) sobre os riscos desse arbítrio, "se um Leviatã abusa de seu poder *ad intra* e/ou *ad extra*, e alguns delatores corajosos desvendam tais contradições, que tipo de mecanismos internacionais devem ser criados, a fim de lidar com estas questões, para evitar os mecanismos de cinismo".

Conforme demonstrado ao longo deste estudo, delegar a proteção infantojuvenil a infraestruturas privadas opacas desestrutura o arranjo constitucional de responsabilidade compartilhada (Brasil, 1988). Para impedir a captura do ECA Digital por esse Leviatã, a agenda regulatória deve rejeitar o determinismo tecnológico. Isso exige integrar o escrutínio humano às revisões de bloqueio algorítmico e impor auditorias independentes de impacto, coibindo

abusos na infraestrutura de aferição e verificação etária, nos moldes do que já é previsto tanto pela legislação (Brasil, 2025a) quanto pelo regulador (Brasil, 2026a). Do mesmo modo, ações de letramento informacional devem capacitar famílias e jovens para a avaliação crítica das ferramentas de controle parental, em detrimento da interação acrítica com a automação corporativa. Em última análise, as salvaguardas brasileiras em ambientes digitais só superarão os vícios da moderação privatizada mediante a harmonização entre a padronização de protocolos criptográficos que preservem o anonimato e uma fiscalização efetiva do Estado.

REFERÊNCIAS

AGE CHECK CERTIFICATION SCHEME. **Age assurance technology trial**: Part A – main report (n 13). Stockport: Age Check Certification Scheme, 19 ago. 2025. Projeto financiado pelo Australian Government. Disponível em: https://www.infrastructure.gov.au/sites/default/files/documents/aatt_part_a_digital.pdf Acesso em: 27 abr. 2026.

ALMEIDA, Daniella. Cronograma prevê fiscalização efetiva do ECA Digital pela ANPD em 2027. **Agência Brasil**, Brasília, 20 mar. 2026. Disponível em: https://agenciabrasil.ebc.com.br/direitos-humanos/noticia/2026-03/cronograma-preve-fiscalizacao-efetiva-do-eca-digital-pela-anpd-em-2027 Acesso em: 17 maio 2026.

AUSTRÁLIA. eSafety Commissioner**. Social media minimum age regulatory guidance**. Canberra: eSafety Commissioner, 16 set. 2025. Disponível em: https://www.esafety.gov.au/sites/default/files/2025-09/eSafety-SMMA-Regulatory-Guidance.pdf?v=1777485893446 Acesso em: 29 abr. 2026.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**. Brasília, DF: Presidente da República, 1988.

BRASIL. Autoridade Nacional de Proteção de Dados. **Mecanismos confiáveis de aferição de idade**: orientações preliminares. 1. versão. Brasília: ANPD, 20 mar. 2026a. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/eca-digital/mecanismos-confiaveis-de-afericao-de-idade-orientacoes-preliminares.pdf/view Acesso em: 27 abr. 2026.

BRASIL. Lei nº 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. **Diário Oficial da União**, seção 1, Brasília, DF, ano 128, n. 135, p. 13563, 16 jul. 1990.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil**. Diário Oficial da União**, seção 1, Brasília, DF, ano 151, n. 77, 24 abr. 2014.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**, seção 1, Brasília, DF, n. 157, p. 59, 15 ago. 2018.

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). **Diário Oficial da União**, seção 1, Brasília, DF, ano 163, n. 177-A, edição extra, p. 1, 17 set. 2025a.

BRASIL. Ministério da Justiça e Segurança Pública. Gabinete do Ministro. Portaria MJSP nº 1.048, de 15 de outubro de 2025. Regulamenta o processo de classificação indicativa [...] da Lei nº 15.211, de 17 de setembro de 2025. **Diário Oficial da União**, seção 1, Brasília, DF, n. 198, p. 70, 16 out. 2025b.

BRASIL. Ministério da Justiça e Segurança Pública. Secretaria Nacional de Direitos Digitais. **Mecanismos de aferição de idade**: análise das contribuições à consulta pública e subsídios para regulamentação da Lei nº 15.211/2025. Brasília: MJSP, janeiro de 2026b. Disponível em: www.gov.br/mj/pt-br/assuntos/noticias/relatorio-sedigi-consulta-de-afericao-de-idade.pdf Acesso em: 07 set. 2026.

CAPURRO, Rafael. Cidadania na era digital. *In.*: CABRAL, Adilson; CABRAL, Eula (eds.). **Comunicação, cultura, informação e democracia**: tensões e contradições. Porto: Media XXI, 2016. p. 49-75.

FLORIDI, Luciano. Privacy: Informational Friction. *In*: FLORIDI, Luciano. **The fourth revolution**: how the infosphere is reshaping human reality. Oxford: Oxford University Press, 2014. p. 101-128.

FROHMANN, Bernd. Cyber Ethics: Bodies or Bytes? **Intl. Inform. & Libr. Rev.**, Inglaterra (RU), v. 32, p. 423-435, 2000.

FROHMANN, Bernd. Subjectivity and information ethics. **Journal of the American Society for Information Science and Technology**, Nova Jersey (EUA), v. 59, n. 2, p. 267-277, 2008. Disponível em: https://ideas.repec.org/a/bla/jamist/v59y2008i2p267-277.html Acesso em: 07 set. 2026.

GONZÁLEZ DE GÓMEZ, Maria Nélida. Novos cenários políticos para a informação. **Ciência da Informação**, Brasília, v. 31, n. 1, p. 27-40, jan./abr. 2002. Disponível em: https://revistas.usp.br/pbcib/pt_BR/article/view/259379 Acesso em: 07 set. 2026.

HU, Tengyue. The role of age verification systems in protecting minors from harmful online content in Australia. **International Journal of Social Sciences and Public Administration**, [*s. l.*], v. 6, n. 2, p. 134-141, 2025.

KAUFMAN, Matt; BHATIA, Rajiv. Uma nova era de segurança: verificações de idade facial passaram a ser necessárias para usar o chat na Roblox. **Roblox**, [*s.l.*], 7 jan. 2026. Disponível em: https://about.roblox.com/pt-br/newsroom/2026/01/roblox-age-checks-required-to-chat Acesso em: 5 maio 2026.

LIVINGSTONE, Helen. Australia has banned social media for kids under 16: how does it work? **BBC News**, Sydney, 22 jan. 2026. Disponível em: https://www.bbc.com/news/articles/cwyp9d3ddqyo Acesso em: 29 abr. 2026.

LOPES, Raquel. Governo aumenta classificação indicativa de oito redes sociais. **Folha de São Paulo**, Brasília, 19 mar. 2026. Disponível em: https://www1.folha.uol.com.br/cotidiano/2026/03/governo-aumenta-classificacao-indicativa-de-oito-redes-sociais.shtml Acesso em: 11 set. 2026.

REDAÇÃO G1. ECA Digital: Google, Meta e TikTok explicam como verificam idade de usuários no Brasil. **G1**, Rio de Janeiro, 17 mar. 2026. Disponível em: https://g1.globo.com/tecnologia/noticia/2026/03/17/eca-digital-plataformas-verificacao-idade.ghtml Acesso em: 5 maio 2026.

REUTERS. Da Austrália à Europa: veja países que restringem acesso de crianças às redes sociais. **G1**, [*s. l.*], 29 ago. 2026. Disponível em: https://g1.globo.com/tecnologia/noticia/2026/08/29/da-australia-a-europa-veja-paises-que-restringem-acesso-de-criancas-as-redes-sociais.ghtml Acesso em: 05 set. 2026.

WEBER, Max. **A ética protestante e o espírito do capitalismo**. São Paulo: Cia das Letras, 2004.

WOODLEY, Giselle; SEE, Harrison W.; O'NEILL, Brian; GREEN, Lelia; STAKSRUD, Elisabeth; HASKELL-DOWLAND, Paul. Australian Teen Voices on Age Verification and Age Assurance Measures. **Policy & Internet**, Sydney, v. 17, p. 1-11, 2025. Disponível em: https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=8294&context=ecuworks2022-2026 Acesso em: 05 set. 2026.

AGRADECIMENTOS

O presente trabalho foi realizado com apoio da Fundação Coordenação de Aperfeiçoamento de Pessoal de Nível Superior, Brasil (CAPES) – Código de Financiamento 001, e do Conselho Nacional para o Desenvolvimento Científico e Tecnológico (CNPq).