

IX ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

Todos os direitos reservados e protegidos. Nenhuma parte destes anais poderá ser reproduzida ou transmitida sejam quais forem os meios empregados sem prévia autorização dos editores.

Diretoria - CONPEDI

Presidente - Profa. Dra. Samyra Haydêe Dal Farra Napolini - FMU - São Paulo

Diretor Executivo - Prof. Dr. Orides Mezzaroba - UFSC - Santa Catarina

Vice-presidente Norte - Prof. Dr. Jean Carlos Dias - Cesupa - Pará

Vice-presidente Centro-Oeste - Prof. Dr. José Querino Tavares Neto - UFG - Goiás

Vice-presidente Sul - Prof. Dr. Leonel Severo Rocha - Unisinos - Rio Grande do Sul

Vice-presidente Sudeste - Profa. Dra. Rosângela Lunardelli Cavallazzi - UFRJ/PUCRio - Rio de Janeiro

Vice-presidente Nordeste - Prof. Dr. Raymundo Juliano Feitosa - UNICAP - Pernambuco

Representante Discente: Prof. Dr. Abner da Silva Jaques - UPM/UNIGRAN - Mato Grosso do Sul

Conselho Fiscal:

Prof. Dr. José Filomeno de Moraes Filho - UFMA - Maranhão

Prof. Dr. Caio Augusto Souza Lara - SKEMA/ESDHC/UFMG - Minas Gerais

Prof. Dr. Valter Moura do Carmo - UFERSA - Rio Grande do Norte

Prof. Dr. Fernando Passos - UNIARA - São Paulo

Prof. Dr. Ednilson Donisete Machado - UNIVEM/UENP - São Paulo

Secretarias

Relações Institucionais:

Prof. Dra. Claudia Maria Barbosa - PUCPR - Paraná

Prof. Dr. Heron José de Santana Gordilho - UFBA - Bahia

Profa. Dra. Daniela Marques de Moraes - UNB - Distrito Federal

Comunicação:

Prof. Dr. Robison Tramontina - UNOESC - Santa Catarina

Prof. Dr. Liton Lanes Pilau Sobrinho - UPF/Univali - Rio Grande do Sul

Prof. Dr. Lucas Gonçalves da Silva - UFS - Sergipe

Relações Internacionais para o Continente Americano:

Prof. Dr. Jerônimo Siqueira Tybusch - UFSM - Rio Grande do sul

Prof. Dr. Paulo Roberto Barbosa Ramos - UFMA - Maranhão

Prof. Dr. Felipe Chiarello de Souza Pinto - UPM - São Paulo

Relações Internacionais para os demais Continentes:

Profa. Dra. Gina Vidal Marcilio Pompeu - UNIFOR - Ceará

Profa. Dra. Sandra Regina Martini - UNIRITTER / UFRGS - Rio Grande do Sul

Profa. Dra. Maria Claudia da Silva Antunes de Souza - UNIVALI - Santa Catarina

Educação Jurídica

Profa. Dra. Viviane Coêlho de Séllos Knoerr - Unicuritiba - PR

Prof. Dr. Rubens Beçak - USP - SP

Profa. Dra. Livia Gaigher Bosio Campello - UFMS - MS

Eventos:

Prof. Dr. Yuri Nathan da Costa Lannes - FDF - São Paulo

Profa. Dra. Norma Sueli Padilha - UFSC - Santa Catarina

Prof. Dr. Juraci Mourão Lopes Filho - UNICHRISTUS - Ceará

Comissão Especial

Prof. Dr. João Marcelo de Lima Assafim - UFRJ - RJ

Profa. Dra. Maria Creusa De Araújo Borges - UFPB - PB

Prof. Dr. Antônio Carlos Diniz Murta - Fumec - MG

Prof. Dr. Rogério Borba - UNIFACVEST - SC

D597

Direito, governança e novas tecnologias I [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Rubens Beçak; Aires Jose Rover; Ana Elisa Silva Fernandes Vieira – Florianópolis: CONPEDI, 2026.

Inclui bibliografia

ISBN: 978-65-5274-592-7

Modo de acesso: www.conpedi.org.br em publicações

Tema: Constituição, Processo e Justiça Social: o papel da jurisdição constitucional na efetivação de direitos

2. Direito. 3. Governança e novas tecnologias. IX Encontro Virtual do CONPEDI (2: 2026: Florianópolis, Brasil).

CDU: 34



IX ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

Apresentação

Os encontros nacionais do Conselho Nacional de Pesquisa e Pós-graduação em Direito (CONPEDI) têm se consolidado como referência na disseminação de pesquisas que abordam os novos fenômenos envolvendo o direito, e o Grupo de Trabalho "Direito, Governança e Novas Tecnologias" é um exemplo vivo desse compromisso. Nesta edição, o evento destacou-se não apenas pela qualidade dos trabalhos apresentados, mas pela presença de renomados professores pesquisadores em instigante debate com seus alunos de pós-graduação.

Como de praxe, houve uma diversidade muito grande de temas e abordagens. Numa tentativa de dar unidade temática e facilitar a compreensão dessa complexa teia de inovações, os coordenadores organizaram os artigos desta publicação em três grandes grupos de reflexão.

O primeiro bloco abordou o tema da "Inteligência Artificial, Viés Algorítmico e Responsabilidade Tecnológica". As reflexões apresentadas neste eixo evidenciam a tensão constante entre a rápida expansão da inteligência artificial - que transforma desde o papel da advocacia e o uso de "smart contracts" até a governança das plataformas digitais - e os profundos riscos sociais intrínsecos a essas tecnologias. Os debates trouxeram à tona denúncias contundentes sobre o racismo estrutural e algorítmico, demonstrando como projetos de cidades inteligentes e ferramentas de reconhecimento facial podem operar sob uma lógica de necropolítica se não houver um olhar crítico. Consequentemente, os pesquisadores debruçaram-se sobre a urgência de estabelecer novos marcos de regulação, modelos de responsabilidade civil e robustos mecanismos de "compliance" e segurança da informação para frear a discriminação e garantir proteção contratual.

destaque para a urgência de uma identidade digital segura e a afirmação de um Estatuto da Criança e do Adolescente (ECA) no ambiente virtual.

Por fim, o terceiro bloco englobou "Direitos Humanos, Processo Judicial, Economia Digital e Governança Institucional". Este eixo refletiu de forma abrangente as complexas interseções entre a Revolução 4.0 e a proteção da dignidade humana. Foram problematizados fenômenos contemporâneos alarmantes, como a precarização das relações na "gig economy", o abandono parental no ambiente virtual e a violação do direito ao esquecimento infantil decorrente do "oversharenting". Em paralelo a essas vulnerabilidades, os estudos investigaram a modernização das estruturas institucionais e econômicas. Discutiu-se desde a responsabilidade civil frente à tokenização e financeirização de terras no agronegócio, até o esforço contínuo para democratizar o sistema de justiça. Para isso, foram apresentadas análises valiosas sobre a implantação municipal do processo eletrônico, a aplicação do "design thinking" no direito e o aprimoramento da transparência e da participação democrática sob a ótica do direito comparado.

Os artigos que ora são apresentados ao público têm a finalidade de fomentar a pesquisa e fortalecer o diálogo interdisciplinar em torno das respostas que o Direito precisa dar a uma realidade em constante e veloz transformação.

Enfim, os coordenadores do GT convidam os leitores para desfrutarem do teor integral dos artigos, expressando imensa gratidão pela participação dos autores pesquisadores desta edição.

Os Coordenadores

Prof. Dr. Aires José Rover, Universidade Federal de Santa Catarina

Prof. Dr. .Rubens Beçak, Universidade de São Paulo - USP

VERIFICAÇÃO ETÁRIA E IDENTIDADE DIGITAL: AVANÇOS E LIMITES DO ECA DIGITAL NA REGULAÇÃO DAS PLATAFORMAS

AGE VERIFICATION AND DIGITAL IDENTITY: ADVANCES AND LIMITS OF THE DIGITAL ECA IN PLATFORM REGULATION

Cássia Luize Ferreira da Silva ¹
Greice Patricia Fuller ²

Resumo

O presente trabalho analisa a exigência de mecanismos obrigatórios de verificação de idade em redes sociais, à luz da Lei nº 15.211/2025 (ECA Digital), examinando seus avanços regulatórios e seus limites no contexto da governança da identidade digital. Parte-se da constatação de que as plataformas digitais historicamente se estruturaram sobre modelos frágeis de autenticação, fundamentados na autodeclaração e na ausência de mecanismos efetivos de verificação identitária, circunstância que favoreceu a proliferação de perfis falsos, a prática de ilícitos digitais e a exposição de crianças e adolescentes a conteúdos inadequados e situações de risco. Nesse cenário, a vedação da autodeclaração representa relevante inflexão normativa ao impor às plataformas o dever de adotar métodos confiáveis de verificação etária. O estudo analisa os impactos dessa mudança legislativa e demonstra que, embora a nova regulamentação fortaleça a proteção infantojuvenil e amplie os deveres de controle das plataformas, a verificação de idade não se confunde com identificação civil plena, permanecendo a dissociação entre identidade digital e identidade civil dos usuários.

Palavras-chave: Identidade digital, Redes sociais, Verificação de idade, Crimes virtuais, Eca digital

Abstract/Resumen/Résumé

This paper analyzes the requirement for mandatory age verification mechanisms on social media platforms in light of Law No. 15,211/2025 (“Digital Child and Adolescent Statute” – ECA Digital), examining its regulatory advances and limitations within the context of digital identity governance. The study is based on the understanding that digital platforms have

adopt reliable age verification methods. The paper analyzes the impacts of this legislative change and demonstrates that, although the new regulation strengthens the protection of minors and expands platform oversight duties, age verification does not amount to full civil identification, thus maintaining the dissociation between digital identity and users' civil identity.

Keywords/Palabras-claves/Mots-clés: Digital identity, Social media, Age verification, Cybercrime, Digital eca

INTRODUÇÃO

O crescimento exponencial das redes sociais nas últimas décadas promoveu profunda transformação nas formas de comunicação, interação e organização social, consolidando essas plataformas como espaços centrais da vida contemporânea. Para além do entretenimento, passaram a desempenhar funções econômicas, informativas, políticas e culturais de elevada relevância. Não obstante sua importância, esse desenvolvimento ocorreu sob bases tecnológicas e regulatórias marcadas por fragilidades relacionadas à identificação dos usuários.

Historicamente, o modelo de criação de contas nas plataformas digitais estruturou-se sobre a autodeclaração de dados, sem exigência de validação documental ou mecanismos efetivos de verificação identitária. Na prática, isso permitiu o ingresso de usuários mediante simples fornecimento de informações cuja veracidade não é aferida, favorecendo a baixa rastreabilidade das interações digitais, a multiplicidade de identidades e a criação de perfis falsos.

As consequências desse modelo manifestam-se tanto no crescimento da criminalidade digital, frequentemente associada ao uso de identidades fictícias, quanto na exposição de crianças e adolescentes a conteúdos inadequados, diante da insuficiência dos mecanismos tradicionais de restrição etária. Evidencia-se, assim, uma dissonância entre a realidade tecnológica das plataformas digitais e os parâmetros jurídicos de proteção de direitos fundamentais, especialmente no âmbito da tutela infantojuvenil.

Nesse contexto, a Lei nº 15.211/2025, conhecida como “ECA Digital”, introduziu relevante alteração no cenário normativo brasileiro ao estabelecer a obrigatoriedade da adoção de métodos confiáveis de verificação de idade pelas plataformas digitais, superando, ao menos em perspectiva normativa, o modelo de autodeclaração até então predominante.

Diante dessa mudança, o presente trabalho propõe-se a examinar os mecanismos tradicionalmente adotados para a criação de contas em redes sociais, analisando os impactos decorrentes da ausência de verificação identitária no contexto da criminalidade digital e da vulnerabilidade infantojuvenil, bem como os avanços e limites do modelo regulatório introduzido pela Lei nº 15.211/2025.

O objetivo geral da pesquisa consiste em analisar os mecanismos de verificação de identidade e idade em redes sociais, considerando sua evolução no contexto regulatório brasileiro e suas implicações na proteção de usuários, especialmente crianças e adolescentes. Como objetivos específicos, pretende-se: (i) examinar os procedimentos tradicionalmente

exigidos para a criação de contas nas principais plataformas digitais; (ii) analisar os impactos da ausência de mecanismos efetivos de verificação identitária e etária no contexto da criminalidade digital e da vulnerabilidade infantojuvenil; e (iii) investigar os avanços e os limites do modelo regulatório introduzido pela Lei nº 15.211/2025.

Para o desenvolvimento deste trabalho, adota-se a metodologia dedutiva, partindo de premissas gerais acerca da proteção de direitos fundamentais, da responsabilidade digital e do dever de cuidado estatal e parental, para examinar o modelo tradicional de identificação nas redes sociais e a recente inflexão normativa promovida pela legislação brasileira.

1. PROCEDIMENTOS TRADICIONALMENTE EXIGIDOS PARA A CRIAÇÃO DE CONTAS NAS PRINCIPAIS PLATAFORMAS DIGITAIS

A ascensão das redes sociais como pilares da vida contemporânea reconfigurou profundamente as dinâmicas de interação humana, projetando para o ambiente digital esferas antes restritas ao convívio físico.

De acordo com estudo publicado no Instituto de Pesquisa Econômica Aplicada IPEA (Neto, Chiarini e Ribeiro, 2024, p. 47), a partir de 2010 consolidou-se um novo padrão empresarial baseado em plataformas digitais, por meio do qual empresas passaram a conectar diferentes grupos de usuários e agregar valor pela ampliação contínua de participantes em ambientes virtuais sob seu controle.

Plataformas como *Instagram*, *TikTok*, *Facebook* e *X* (antigo *Twitter*), deixaram de exercer funções meramente comunicacionais, consolidando-se como ecossistemas multifuncionais voltados ao consumo, produção de conteúdo, prestação de serviços, formação de opinião e circulação de informações com elevado impacto social e econômico. A socialização, antes mediada por instituições presenciais, passou a ocorrer, em grande medida, em ambientes virtuais. (Coneglian, Santarem e Sant'ana, 2017, p. 63).

Apesar dessa centralidade, o ingresso nas plataformas digitais historicamente ocorreu sob mecanismos frágeis de identificação. O modelo tradicional de cadastro sempre esteve baseado na autodeclaração de dados, sem validação documental ou verificação efetiva da identidade dos usuários. Na prática, a simples criação de um endereço eletrônico, que pode ser gerado em questão de segundos em provedores como *Google* ou *Microsoft*, permite o acesso às principais redes sociais.

No ambiente institucional de suporte da *Google*, consta resposta a questionamento: “Quantas contas *Google* posso criar?”. A empresa esclarece que “você pode criar quantas contas quiser, entretanto, precisa colocar um endereço de e-mail e uma senha diferente para cada uma das contas” (*Google*, 2020, *online*). A orientação evidencia a inexistência de limitações materiais ou etárias (conteúdo da programação) à criação de contas, condicionando o cadastro apenas à utilização de credenciais distintas.

Não obstante, a criação de contas de e-mail na *Google* exige apenas o preenchimento de formulários simplificados, compostos por informações autodeclaradas, como nome, data de nascimento e telefone (Shimabukuro e Toledo, 2023, *online*). Conforme apontam Charleaux e Lima, em publicação no *Tecnoblog*, o *Instagram* “permite criar até 25 contas usando o mesmo e-mail” (Charleaux; Lima, 2023, *online*), circunstância que viabiliza a multiplicação de perfis mediante simples criação de novos endereços eletrônicos.

Diante da ausência de mecanismos consistentes de verificação identitária nas redes sociais, consolidou-se cenário em que um único indivíduo pode manter múltiplos perfis sob identidades distintas, sem vinculação eficaz à sua identidade civil.

No que concerne especificamente à verificação etária, as fragilidades do modelo mostravam-se ainda mais graves. Embora as plataformas previssem idade mínima para criação de contas, geralmente fixada em 13 anos, tal exigência baseava-se exclusivamente na autodeclaração do usuário, sem mecanismos técnicos de aferição. Isso permitia que crianças e adolescentes acessassem livremente esses ambientes mediante simples inserção de data de nascimento fictícia.

Nesse sentido, pesquisa conduzida pelo Comitê Gestor da Internet no Brasil (CGI.br) e pelo Núcleo de Informação e Coordenação do Ponto BR (NIC.br) apontou que 84% das plataformas digitais mais acessadas por crianças no país não realizavam verificação de idade no momento do registro (CETIc.br, 2025, p. 12-20):

Maioria dos serviços (21/25) não utiliza aferição no momento do cadastro (inclusive serviços destinados a adultos, com exceção dos serviços de apostas [2/2] e pornografia [1/2]) [...] Poucos serviços (8/25) declaram atuar proativamente na identificação de usuários abaixo da idade mínima [...] Redes Sociais - 13 anos para acesso e uso / sem aferição no cadastro / uso de autodeclaração / supervisão parental para funcionalidades e conteúdos até usuário completar 18 anos [...] Pornografia - apenas autodeclaração para usuários espectadores (1/2) ou aferição em todos os casos (1/2) / aferição etária para upload de conteúdos e busca por conteúdos ilegais (material de abuso sexual infantil) [...] Jogos - sem aferição no cadastro / proteção em grande medida baseada em supervisão parental / configurações de proteção diferenciadas por faixas etárias / discrepâncias entre idades mínimas (serviço, lojas de apps e Classificação Indicativa)

A ausência de validação da idade expunha crianças e adolescentes ao acesso a conteúdos inadequados, à interação com terceiros desconhecidos e à atuação de agentes envolvidos em práticas ilícitas. Nesse contexto, a fragilidade dos métodos de cadastro ultrapassava a esfera meramente técnica, alcançando a proteção de direitos fundamentais da infância.

Diante desse cenário, evidencia-se que os métodos de cadastro historicamente adotados pelas plataformas digitais, embora eficientes sob a ótica da expansão e acessibilidade, mostravam-se insuficientes para assegurar autenticidade identitária, segurança das interações e proteção de direitos fundamentais, especialmente no que se refere à tutela infantojuvenil. A naturalização da ausência de verificação identitária, longe de constituir uma contingência técnica inevitável, representou escolha consciente que privilegiou o crescimento das plataformas em detrimento da segurança jurídica e da proteção dos usuários.

2. CRIMINALIDADE DIGITAL E VULNERABILIDADE DE MENORES

A fragilidade dos métodos de cadastro historicamente adotados pelas plataformas digitais projeta efeitos relevantes sobre a dinâmica das interações no ambiente virtual. A dissociação entre identidade digital e identidade civil, aliada à ausência de mecanismos eficazes de verificação, contribuiu para a consolidação de um ambiente marcado pela baixa rastreabilidade e pela dificuldade de responsabilização dos usuários. Nesse contexto, tais características favoreceram tanto a prática de ilícitos quanto a ampliação dos riscos a que estão expostos grupos vulneráveis, especialmente crianças e adolescentes.

De um lado, a facilidade de criação de perfis não verificados viabilizou a utilização de identidades falsas para a prática de crimes digitais. De outro, a inexistência de mecanismos efetivos de verificação etária possibilitou o ingresso irrestrito de menores em ambientes potencialmente nocivos, marcados pela circulação de conteúdos inadequados e interações de risco.

É a partir dessa dupla dimensão, qual seja, a criminalidade digital e a vulnerabilidade infantojuvenil, que se desenvolve o presente capítulo, examinando, inicialmente, o papel dos perfis falsos na prática de ilícitos virtuais e, posteriormente, os riscos decorrentes do acesso precoce e descontrolado de crianças e adolescentes às redes sociais.

2.1 Crescimento exponencial de perfis falsos para práticas criminosas

A ausência de mecanismos robustos de verificação de identidade nas redes sociais constitui um dos principais fatores associados ao crescimento da criminalidade digital. Inseridas em ambiente marcado pela fluidez identitária e pela baixa rastreabilidade dos usuários, as plataformas digitais passaram a permitir a criação de perfis desvinculados da identidade civil de seus titulares. Nesse contexto, a utilização de identidades falsas deixou de representar exceção para se tornar elemento recorrente da dinâmica digital contemporânea. Nesse sentido:

outro fator em relação à privacidade nas publicações analisadas é a possibilidade de criação de perfis falsos, ou de vários perfis por um mesmo sujeito (multiperfil), não sendo necessário uma verificação que confirme a veracidade dos dados, como ocorre, por exemplo, com o registro de abertura de conta em uma instituição financeira. Os perfis falsos podem ser utilizados para obter informações sobre outros sujeitos ou empresas por meio de técnicas de engenharia social. As estruturas dos SRSOs permitem a criação deste tipo de perfil, permitindo um certo anonimato e dificultando a sua identificação. Sujeitos com esses perfis se aproveitam da invisibilidade ou do uso de multiperfis para acessar páginas pessoais com a intenção de perseguir (cyberstalking) um sujeito, obter dados pessoais para promover golpes e hackeamento ou propagar discursos de ódio. (Fonteles e Rodrigues, 2024, p. 166).

Os perfis falsos, constituídos a partir de dados fictícios, indevidamente apropriados de terceiros ou gerados automaticamente por sistemas computacionais, consolidaram-se como instrumentos centrais para a prática de ilícitos no ambiente virtual. Sua principal funcionalidade reside na dissociação entre a conduta praticada e a identidade real do agente, dificultando sua identificação e responsabilização. Deslandes e Arantes (2017, p. 175) esclarecem:

Pessoas se conhecem e se relacionam pelas redes sociais, em uma velocidade que talvez jamais fosse mensurada há uma década. Neste mesmo contexto e velocidade crescem também os crimes virtuais, principalmente os relacionados às redes sociais. Tais crimes aumentaram muito, devido à facilidade encontrada para praticá-lo [...].

Embora praticadas no ambiente virtual, tais condutas produzem efeitos concretos e reais no mundo fenomênico, incluindo prejuízos financeiros, danos reputacionais, abalos psicológicos e desestabilização de relações sociais e institucionais. Apesar disso, a responsabilização dos agentes encontra obstáculos relevantes relacionados à fragilidade dos mecanismos de identificação e da engenharia social empreendida para o cometimento da criminalidade digital.

Conforme destacam Rodrigues, Ferreira e Aguiar (2025, *online*), o anonimato viabilizado pelo ambiente digital permite que agentes criminosos ocultem sua identidade por meio do uso de ferramentas que dificultam a rastreabilidade de suas condutas. O problema se agrava quando as práticas ilícitas ocorrem em plataformas hospedadas fora do território

nacional, hipótese em que a persecução investigativa depende de mecanismos de cooperação internacional, frequentemente marcados por morosidade, limitações legais, especialmente, referentes à tipicidade e medidas processuais penais referentes à persecução penal, e reduzida eficácia na obtenção de dados e identificação dos responsáveis.

Mesmo quando determinado perfil é identificado e removido, a facilidade de criação de novas contas permite a rápida reiteração das condutas ilícitas.

O crescimento exponencial de perfis falsos, portanto, não constitui fenômeno isolado, mas consequência direta de uma arquitetura digital que privilegiou a expansão das plataformas e a redução de barreiras de ingresso, favorecendo a opacidade identitária e a desresponsabilização dos agentes. A ausência de mecanismos eficazes de verificação não apenas possibilitou a prática de ilícitos, mas ampliou sua escalabilidade, permitindo que um mesmo indivíduo opere múltiplas identidades simultaneamente, favorecendo um rompimento da estrutura clássica dos crimes, nos quais, vê-se a figura individualizada e bem delineada do sujeito ativo (Fuller, 2020, p. 217).

Sousa e Marini (2025, p. 13) apontam:

O uso de perfis falsos em redes sociais representa um dos maiores obstáculos à imputação criminal eficaz, criando complexidades técnicas e jurídicas que comprometem a responsabilização penal dos infratores.

Diante desse cenário, evidencia-se que a proliferação de perfis falsos constitui vetor central da criminalidade digital contemporânea, diretamente associado às insuficiências dos métodos de cadastro historicamente adotados pelas plataformas digitais.

2.2 Vulnerabilidade infantojuvenil no ambiente digital: limites do modelo tradicional de acesso às plataformas digitais

A proteção de crianças e adolescentes no ambiente digital consolidou-se como um dos principais desafios regulatórios contemporâneos, especialmente diante da crescente centralidade das redes sociais na formação de comportamentos e padrões de interação. Nesse contexto, o acesso de menores a conteúdos impróprios passou a ser reconhecido como problema diretamente relacionado aos modelos de ingresso e circulação de conteúdo nas plataformas digitais.

Conforme demonstrado anteriormente, o acesso às redes sociais estruturou-se sobre a ausência de verificação etária efetiva, permitindo que a idade autodeclarada operasse como único critério de controle. Sem mecanismos de validação, tornava-se inviável distinguir

usuários adultos e menores, comprometendo a eficácia das restrições etárias formalmente previstas pelas plataformas.

O problema revela-se ainda mais complexo diante da inexistência de mecanismos eficazes de verificação identitária. Não se trata apenas da ausência de controle sobre a idade do usuário, mas da impossibilidade de vincular a conta digital a pessoa física identificável, ampliando os riscos inerentes às interações virtuais.

A conjugação dessas fragilidades produziu ambiente de acesso irrestrito, no qual crianças e adolescentes ingressavam facilmente nas plataformas ao mesmo tempo em que interagiam com perfis cuja autenticidade não podia ser aferida. Estabeleceu-se, assim, dinâmica de vulnerabilidade bilateral: de um lado, menores expostos a conteúdos inadequados; de outro, agentes potencialmente mal-intencionados operando sob identidades fictícias.

Essa arquitetura favoreceu a exposição precoce de crianças e adolescentes a conteúdos incompatíveis com seu estágio de desenvolvimento físico, cognitivo e emocional, incluindo material violento, sexualizado, autodestrutivo, discursos de ódio e desafios de risco elevado. Santos, Rodrigues, Mota e Lima (2026, p. 15), asseveram:

Nos desafios decorrentes da facilidade de acesso às mídias por meio da internet, destaca-se, em primeiro lugar, a exposição de crianças e adolescentes a conteúdos impróprios, sejam eles de cunho sexual, violento ou discriminatório. A ausência de mecanismos eficazes de fiscalização e controle do uso desses materiais configura um relevante obstáculo à inibição do acesso dos jovens aos conteúdos inadequados.

A circulação desses conteúdos não se apresentava como fenômeno periférico. Até a superveniência da Lei nº 15.211/2025, tais materiais integravam a própria dinâmica das plataformas digitais, sendo amplificados por sistemas automatizados de recomendação orientados por métricas de engajamento e retenção. Nesse modelo, a lógica algorítmica operava dissociada de critérios de adequação etária, privilegiando conteúdos de maior apelo emocional.

Teixeira e Coutinho (2024, p. 7) explicam que os algoritmos consistem em conjuntos de instruções responsáveis por regular o funcionamento das redes sociais e modular as interações entre usuários, agrupando perfis conforme interesses comuns e influenciando padrões de engajamento e comportamento.

A exposição de menores a conteúdos potencialmente lesivos muitas vezes independia de busca ativa consistente. Os próprios sistemas de recomendação amplificavam o fenômeno ao direcionar conteúdos com base em interações superficiais ou circunstanciais.

A ausência de diferenciação efetiva entre perfis adultos e infantojuvenis comprometia a implementação de políticas adequadas de filtragem e moderação. Sem identificação segura da idade do usuário, tornava-se inviável estabelecer mecanismos eficazes de proteção voltados à infância e adolescência. Além disso, a inexistência de verificação identitária favorecia a atuação de agentes que se valiam do anonimato para estabelecer contato com menores, criando ambiente propício para práticas como aliciamento, manipulação psicológica e outras formas de violência digital.

No plano jurídico, esse cenário evidencia tensão significativa com o regime de proteção integral da infância. A Constituição Federal, em seu artigo 227, estabelece prioridade absoluta à proteção da criança e do adolescente, dever que se projeta também sobre o ambiente digital. O Estatuto da Criança e do Adolescente (Lei nº 8.069/1990), por sua vez, reforça essa diretriz ao assegurar condições para o desenvolvimento físico, mental, moral, espiritual e social dos menores:

Art. 3º A criança e o adolescente gozam de todos os direitos fundamentais inerentes à pessoa humana, sem prejuízo da proteção integral de que trata esta Lei, assegurando-se-lhes, por lei ou por outros meios, todas as oportunidades e facilidades, a fim de lhes facultar o desenvolvimento físico, mental, moral, espiritual e social, em condições de liberdade e de dignidade. (Brasil, 1990, *online*).

No âmbito da proteção de dados, a Lei nº 13.709/2018 já previa, em seu artigo 14, §1º, a necessidade de consentimento específico de responsável legal para o tratamento de dados de crianças: “§ 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal” (Brasil, 2018, *online*).

Entretanto, na ausência de instrumentos técnicos adequados, essa exigência encontrava obstáculos relevantes de implementação, evidenciando que o problema não decorria apenas da insuficiência normativa, mas da incapacidade prática de operacionalização pelas plataformas digitais.

Em síntese, a inexistência de mecanismos eficazes de verificação identitária operou como vetor de vulnerabilidade ao permitir o ingresso irrestrito de menores em ambientes inadequados e dificultar a identificação dos responsáveis pelas interações digitais.

É nesse contexto que se insere a Lei nº 15.211/2025, ao introduzir a exigência de métodos confiáveis de verificação de idade e superar o modelo fundado exclusivamente na autodeclaração. A norma promove reorientação do paradigma protetivo ao atribuir às plataformas responsabilidade ativa na conformação de ambientes digitais mais seguros.

3. A VERIFICAÇÃO ETÁRIA NO ECA DIGITAL: AVANÇOS NORMATIVOS E LIMITES ESTRUTURAIS DO MODELO REGULATÓRIO

A partir do diagnóstico das fragilidades historicamente presentes no ambiente digital, especialmente quanto à ausência de controle etário efetivo e à dissociação entre identidade digital e identidade civil, impõe-se a análise da resposta normativa introduzida pela Lei nº 15.211/2025. O diploma representa marco regulatório relevante ao estabelecer diretrizes voltadas à restrição de acesso de crianças e adolescentes a conteúdos inadequados e à imposição de deveres concretos às plataformas digitais.

O presente capítulo examina os avanços promovidos pela exigência de verificação confiável de idade e, posteriormente, os limites estruturais do modelo adotado, especialmente quanto à persistência da dissociação entre identidade digital e identidade civil.

3.1. A verificação rígida de idade: superação da autodeclaração e dever de controle efetivo

A Lei nº 15.211/2025 introduz novo paradigma regulatório no controle de acesso de crianças e adolescentes ao ambiente digital. Ao disciplinar a vedação de acesso a conteúdos e serviços impróprios, inadequados ou proibidos, o legislador reconhece a insuficiência dos modelos anteriormente adotados e estabelece regime jurídico estruturado de verificação etária, com repercussões diretas sobre a atuação das plataformas digitais.

O ponto de partida dessa inflexão normativa encontra-se no art. 9º da lei, que impõe aos fornecedores de produtos ou serviços de tecnologia da informação o dever de adotar medidas eficazes para impedir o acesso de menores a conteúdos incompatíveis com sua faixa etária (Brasil, 2025, online). A norma desloca a atuação das plataformas de lógica permissiva para modelo de controle ativo orientado por critérios de adequação etária.

A obrigação é reforçada pelo §1º do mesmo dispositivo, ao estabelecer a necessidade de adoção de “mecanismos confiáveis de verificação de idade a cada acesso do usuário ao conteúdo, produto ou serviço de que trata o caput deste artigo, vedada a autodeclaração” (Brasil, 2025, online).

A vedação da autodeclaração afasta a validade jurídica de práticas baseadas na simples inserção de data de nascimento. Ao exigir verificação “a cada acesso”, o legislador impõe lógica contínua de validação etária, afastando mecanismos meramente iniciais de controle. A exigência normativa evidencia que a lei institui verdadeiro dever de eficácia. Não basta a mera

declaração de adoção de mecanismos de controle; exige-se que eles sejam aptos, concretamente, a reduzir o risco de acesso indevido por menores.

Nesse sentido, Gonçalves, Lara e Silva (2026, p. 15-17) esclarecem:

No tocante à verificação etária, a lei impõe aos fornecedores de produtos e serviços de tecnologia da informação o dever de aferir a idade de seus usuários, a fim de assegurar experiências compatíveis com a respectiva faixa etária e obstar o acesso a conteúdos, produtos ou serviços considerados impróprios, inadequados ou vedados a menores de 18 (dezoito) anos. Dentre as inovações de maior relevo está a proibição de que a autodeclaração constitua o único método de aferição etária para serviços acessíveis a menores de dezoito anos. A medida busca superar a notória ineficácia dos sistemas autodeclaratórios, impondo às plataformas a adoção de mecanismos mais confiáveis.

Os arts. 10 a 14 aprofundam a disciplina da verificação etária e estabelecem diretrizes para sua implementação. O art. 10 determina que os fornecedores adotem mecanismos aptos a proporcionar experiências adequadas à idade, evidenciando que a verificação etária constitui instrumento voltado à proteção do público infantojuvenil (Brasil, 2025, online).

Particular relevância assume o art. 12, que estabelece obrigações específicas para provedores de lojas de aplicações e sistemas operacionais. O inciso I determina a adoção de medidas “proporcionais, auditáveis e tecnicamente seguras” para aferição da idade, observando os princípios previstos no art. 6º da Lei Geral de Proteção de Dados Pessoais (Brasil, 2025, online). A previsão busca compatibilizar controle etário e proteção de dados pessoais.

O inciso III do mesmo dispositivo prevê a possibilidade de fornecimento de “sinal de idade” por meio de APIs seguras, permitindo o compartilhamento apenas das informações estritamente necessárias à verificação etária. O §1º reforça essa lógica ao determinar observância ao princípio da minimização de dados, vedando compartilhamento contínuo e irrestrito de informações pessoais (Brasil, 2025, online).

O art. 13 estabelece que os dados coletados para verificação de idade somente poderão ser utilizados para essa finalidade:

Art. 13. 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, 2025, *online*)

No mesmo sentido, o art. 14 impõe aos fornecedores o dever de adotar medidas técnicas e organizacionais para garantir o correto recebimento das informações de idade, sem afastar a obrigação das plataformas de implementar mecanismos próprios para impedir acessos indevidos. A previsão consolida regime de corresponsabilidade entre os agentes da cadeia digital.

Essa lógica é reforçada pelo art. 15, que estabelece a responsabilidade solidária dos agentes envolvidos na proteção de crianças e adolescentes, evidenciando que a verificação etária constitui dever compartilhado, e não isolado.

No âmbito específico das redes sociais, o art. 24 introduz obrigações adicionais de elevada relevância. Destaca-se, nesse ponto, a exigência de vinculação de contas de usuários com até 16 anos aos seus responsáveis legais, o que representa avanço significativo na integração entre verificação etária e supervisão parental:

Art. 24. 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 (dezesesseis) anos de idade estejam vinculados ao usuário ou à conta de um de seus responsáveis legais. (Brasil, 2025, *online*)

Além disso, o dispositivo, em seu parágrafo 2º, impõe às plataformas o dever de aprimorar continuamente seus mecanismos de verificação de idade, submetendo sua efetividade à avaliação por autoridade administrativa competente (Brasil, 2025, *online*).

O §3º do art. 24, autoriza, ainda, que plataformas solicitem confirmação de identificação em casos de indícios de uso indevido por menores, permitindo a utilização de métodos complementares de verificação (Brasil, 2025 *online*). Tal previsão reforça a natureza dinâmica e adaptativa do sistema, permitindo respostas proporcionais a situações de risco.

A análise conjunta desses dispositivos revela que a Lei nº 15.211/2025 adota um modelo regulatório que combina três elementos centrais: (i) a superação expressa da autodeclaração como mecanismo válido de controle etário; (ii) a imposição de um dever de verificação efetiva, pautado por critérios de eficácia, proporcionalidade e auditabilidade; e (iii) a adoção de uma arquitetura tecnologicamente aberta, que permite a utilização de múltiplas soluções técnicas, desde que compatíveis com os parâmetros legais.

Nesse sentido, embora a legislação não estabeleça um rol taxativo de tecnologias, seu desenho normativo admite, em termos práticos, a utilização de diferentes métodos de verificação, tais como validação documental, biometria com estimativa etária, sistemas de verificação por terceiros e modelos híbridos. A escolha entre esses mecanismos deverá observar, necessariamente, os princípios da proteção de dados, da minimização de informações e da adequação ao risco.

Em síntese, a verificação rígida de idade instituída pelo ECA Digital representa avanço normativo substancial ao substituir um modelo meramente formal por um regime de controle efetivo, estruturado e juridicamente exigível. Ao redefinir o papel das plataformas digitais e

estabelecer parâmetros claros para a implementação de mecanismos de aferição etária, a lei inaugura um novo estágio na regulação do ambiente digital.

3.2. Os limites da verificação etária: a persistência da dissociação entre identidade digital e identidade civil

A introdução de mecanismos obrigatórios de verificação de idade pela Lei nº 15.211/2025 representa, como visto, avanço significativo na mitigação dos riscos associados ao acesso indevido de crianças e adolescentes ao ambiente digital. Todavia, a análise mais detida do modelo normativo revela que a verificação etária, embora essencial, não se confunde, nem se destina, à implementação de um sistema de identificação identitária plena dos usuários.

Essa distinção não possui caráter meramente terminológico, mas traduz um limite estrutural do próprio desenho regulatório instituído pelo legislador. A verificação etária, em sua essência, constitui um mecanismo de classificação, voltado à determinação de uma condição objetiva, a idade ou faixa etária do usuário, ao passo que a identificação identitária pressupõe a vinculação inequívoca entre a conta digital e a pessoa natural, com todas as consequências jurídicas daí decorrentes. Enquanto a primeira responde à pergunta “o usuário é maior ou menor de idade?”, a segunda busca responder “quem é o usuário?”.

Trata-se, portanto, de operações distintas, com finalidades, níveis de intrusão e implicações jurídicas substancialmente diferentes. A Lei nº 15.211/2025, ao priorizar a verificação etária, opta deliberadamente por um modelo que não exige, de forma generalizada, a identificação civil completa dos usuários.

Essa conclusão decorre da própria ordem normativa. O art. 9º, §1º, ao exigir mecanismos confiáveis de verificação de idade, limita o escopo da obrigação à aferição etária, sem impor, em momento algum, a necessidade de coleta ou validação de dados identificadores completos. Essa diretriz é reforçada pelo art. 13, ao estabelecer que os dados coletados para verificação de idade devem ser utilizados exclusivamente para essa finalidade, vedando sua utilização para quaisquer outros propósitos. (Brasil, 2025, *online*).

Tal limitação funcional indica que a verificação etária deve operar, sempre que possível, sob uma estrutura de minimização informacional, compatível com os princípios previstos na Lei Geral de Proteção de Dados Pessoais. Nesse sentido, o próprio art. 12, §1º, ao disciplinar o fornecimento de “sinal de idade” por meio de APIs, veda o compartilhamento

contínuo e irrestrito de dados pessoais, evidenciando que o legislador buscou evitar a criação de sistemas massivos de identificação civil:

Art. 12. Os provedores de lojas de aplicações de internet e de sistemas operacionais de terminais deverão:

I – tomar 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);

II – permitir que os pais ou responsáveis legais configurem mecanismos de supervisão parental voluntários e supervisionem, de forma ativa, o acesso de crianças e de adolescentes a aplicativos e conteúdos; e

III – possibilitar, por meio de Interface de Programação de Aplicações (*Application Programming Interface* – API) segura e pautada pela proteção da privacidade desde o padrão, o fornecimento de sinal de idade aos provedores de aplicações de internet, exclusivamente para o cumprimento das finalidades desta Lei e com salvaguardas técnicas adequadas.

§ 1º O fornecimento de sinal de idade por meio de APIs **deverá observar o princípio da minimização de dados, vedado qualquer compartilhamento contínuo, automatizado e irrestrito de dados pessoais** de crianças e de adolescentes.

Essa opção normativa abre espaço para a adoção de modelos de verificação que não implicam, necessariamente, a identificação do usuário. Tecnologias de estimativa etária por biometria facial, por exemplo, permitiriam inferir a idade aproximada de um indivíduo sem revelar sua identidade civil. Da mesma forma, sistemas de verificação por terceiros podem fornecer apenas a confirmação da condição etária (“maior de idade” ou “menor de idade”), sem transferência de dados identificadores.

Desse modo, a resposta à indagação acerca da produção de identificação identitária pelos mecanismos previstos na lei é necessariamente contingente: depende do método técnico adotado. Enquanto soluções baseadas em validação documental tendem a gerar identificação civil direta, outras, estruturadas sob lógica de anonimização, permitem o cumprimento da exigência legal sem a vinculação explícita da identidade do usuário.

Essa flexibilidade, contudo, implica uma consequência relevante: a verificação etária, ainda que rigorosa, não elimina a dissociação entre identidade digital e identidade civil. A conta pode ser classificada corretamente quanto à idade do usuário e, ainda assim, permanecer desvinculada de sua identidade jurídica. Em outras palavras, é possível saber que o usuário é adulto sem saber quem ele é.

Essa característica revela um dos principais limites do modelo instituído pelo ECA Digital. Ao concentrar-se na proteção etária, a legislação não enfrenta, de forma direta, o problema da rastreabilidade identitária no ambiente digital, questão que se encontra na base de

fenômenos como a proliferação de perfis falsos, a multiplicidade de contas por um mesmo indivíduo e a dificuldade de responsabilização por condutas ilícitas.

A persistência desse cenário decorre, em grande medida, de uma escolha regulatória consciente. A imposição de um regime de identificação identitária plena, aplicável a todos os usuários de plataformas digitais, implicaria a coleta massiva de dados pessoais, com potenciais impactos sobre direitos fundamentais como a privacidade, a liberdade de expressão e a proteção de dados. O legislador, ao optar por um modelo centrado na verificação etária, buscou equilibrar a proteção da infância com a preservação desses direitos.

Não se trata, portanto, de omissão legislativa, mas de delimitação do escopo regulatório. A Lei nº 15.211/2025 resolve, de maneira significativa, a fragilidade relacionada ao controle de idade, mas preserva espaços de anonimato funcional no ambiente digital. As implicações dessa escolha são relevantes. A possibilidade de criação de múltiplas contas por um mesmo usuário não é, em princípio, eliminada; o anonimato, ou a sua percepção, continua a viabilizar a atuação de agentes que se beneficiam da dificuldade de identificação; e a responsabilização jurídica permanece dependente, em muitos casos, de mecanismos posteriores de investigação, como requisição de dados, análise de registros de acesso e cooperação internacional.

É justamente nesse ponto que emerge, no debate público e legislativo, a perspectiva de adoção de mecanismos obrigatórios de verificação de identidade civil, inspirados em práticas já consolidadas em setores regulados, como o financeiro. Tais sistemas envolvem, por exemplo, reconhecimento facial dinâmico, capaz de atestar a presença real do usuário e distinguir imagens autênticas de reproduções estáticas, e a vinculação dos cadastros a documentos oficiais, com validação cruzada em bases governamentais, de modo a assegurar a correspondência entre a conta digital e um indivíduo real e identificável:

Para afastar a ação de fraudadores e minimizar o acesso por terceiro não autorizado, além da validação do dispositivo móvel em uso, tem-se ampliado a utilização de captura de biometria facial nos procedimentos antifraude. É considerada um dos meios mais seguros para se auferir a autenticidade da operação realizada no âmbito eletrônico. [...] Além da possibilidade de captura da biometria facial enquanto fator de autenticação, tem-se verificado a ampliação do seu uso como forma de assinatura, na contratação de serviços no ambiente *online*, seja para a criação de uma conta corrente ou até mesmo a contratação de um financiamento. (Pinheiro, 2023, *online*)

Essa perspectiva já se materializa em iniciativas legislativas em tramitação. Em 2025, a Comissão de Comunicação da Câmara dos Deputados aprovou projeto de lei que altera o Marco Civil da Internet para tornar obrigatório o reconhecimento facial dos usuários no acesso

a redes sociais, com o objetivo de “fortalecer a segurança das contas e combater a disseminação de perfis falsos, frequentemente associados a episódios de difamação, assédio, *bullying* virtual e golpes financeiros” (USP, 2025, *online*).

De autoria do deputado Jorge Goetten (Republicanos-SC), o Projeto de Lei nº 1.380/2025 recebeu substitutivo do relator Alex Manente (Cidadania-SP), que transferiu a responsabilidade pela verificação facial das plataformas de redes sociais para os provedores de sistemas operacionais. No voto do relator, destaca-se que a proposta busca enfrentar uma das principais fragilidades do ambiente digital contemporâneo, a ausência de mecanismos eficazes de identificação, ao mesmo tempo em que reconhece os riscos associados à implementação inadequada desses sistemas, especialmente no que se refere à proteção de dados pessoais (Câmara dos Deputados, 2025, p. 2).

A alteração proposta pretende evitar a fragmentação de bancos de dados sensíveis, centralizando a verificação em agentes com maior capacidade técnica em segurança da informação. O substitutivo também prevê a correspondência entre o rosto do usuário e a fotografia constante em documento oficial, bem como a obrigatoriedade de recadastramento das contas no prazo de até um ano após a entrada em vigor da norma, além de promover a atualização conceitual do Marco Civil da Internet quanto a dados biométricos e reconhecimento facial, em consonância com a Lei Geral de Proteção de Dados Pessoais (Câmara dos Deputados, 2025, *online*).

Tal iniciativa evidencia que a agenda regulatória relacionada à identidade digital permanece em evolução. Como observa Juliano Maranhão (USP, 2025, *online*), trata-se de um campo marcado pela tensão entre valores constitucionais concorrentes, no qual a proteção da segurança pública pode entrar em conflito com direitos fundamentais, especialmente a privacidade e a liberdade de expressão, impondo ao legislador o desafio de construir soluções equilibradas.

Diante desse cenário, a verificação etária instituída pelo ECA Digital deve ser compreendida como uma resposta parcial, ainda que relevante, dentro de um problema mais amplo relacionado à governança da identidade no ambiente digital. Trata-se de avanço significativo no plano da proteção infantojuvenil, mas que não esgota os desafios associados à autenticidade das identidades e à responsabilização dos agentes.

Em síntese, a Lei nº 15.211/2025 corrige, de forma consistente, a falha estrutural relacionada à ausência de controle etário, mas não elimina a dissociação entre identidade digital

e identidade civil. Ao preservar espaços de anonimato, o modelo normativo mantém, ainda que de forma mitigada, riscos associados à desresponsabilização, à multiplicidade de identidades e à opacidade das interações digitais, evidenciando a necessidade de desenvolvimento contínuo de soluções jurídicas e tecnológicas capazes de enfrentar, de maneira mais abrangente, os desafios do ambiente digital contemporâneo.

CONCLUSÃO

A presente pesquisa demonstrou que o modelo historicamente adotado pelas plataformas digitais, fundado na autodeclaração e na ausência de verificação identitária efetiva, contribuiu de forma decisiva para a consolidação de um ambiente digital marcado pela baixa rastreabilidade, pela multiplicidade de perfis e pela ampliação de riscos associados à criminalidade virtual e à exposição indevida de crianças e adolescentes. A dissociação entre identidade digital e identidade civil revelou-se, nesse contexto, elemento estrutural de vulnerabilidade, tanto sob a perspectiva da responsabilização quanto da proteção de direitos fundamentais.

A superveniência da Lei nº 15.211/2025 representa uma inflexão relevante nesse cenário, ao vedar expressamente a autodeclaração e impor a adoção de mecanismos confiáveis de verificação de idade. Ao fazê-lo, o legislador desloca o eixo do controle de acesso de um modelo meramente formal para um regime orientado pela efetividade, estabelecendo deveres concretos às plataformas digitais e reforçando sua responsabilidade na conformação de ambientes mais seguros, especialmente no que se refere à tutela da infância e da adolescência.

Não obstante, a análise do novo marco normativo estabelece que a verificação etária não se confunde com identificação identitária plena. A legislação, ao privilegiar soluções compatíveis com a minimização de dados e a proteção da privacidade, não impõe a vinculação obrigatória entre contas digitais e a identidade civil dos usuários. Como consequência, permanece a dissociação entre identidade digital e pessoa natural, o que preserva, ainda que de forma mitigada, espaços de anonimato funcional e limitações quanto à rastreabilidade e à responsabilização.

Dessa forma, conclui-se que a Lei nº 15.211/2025 corrige, de maneira consistente, a falha estrutural relacionada ao controle etário, especialmente no tocante à proteção de crianças e adolescentes, mas não esgota os desafios inerentes à governança da identidade no ambiente digital. A persistência de lacunas no plano da identificação civil mostra que o avanço normativo,

embora significativo, é parcial e demanda complementação por meio de futuros desenvolvimentos regulatórios e tecnológicos.

A construção de um ambiente digital seguro, portanto, não se limita à aferição da idade dos usuários, exigindo a reflexão contínua sobre mecanismos que conciliem, de forma equilibrada, proteção de dados pessoais, liberdade de expressão, segurança das interações e efetividade na responsabilização jurídica. Nesse cenário, a verificação etária deve ser compreendida como etapa relevante, mas não definitiva, no processo de estruturação de um modelo de regulação digital capaz de responder, com coerência e proporcionalidade, às complexidades da sociedade em rede.

REFERÊNCIAS

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm. Acesso em: 21 abr. 2026.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm. Acesso em: 21 abr. 2026.

BRASIL. **Lei nº 15.211, de 17 de setembro de 2025**. Estatuto Digital da Criança e do Adolescente. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm. Acesso em: 21 abr. 2026.

BRASIL. **Lei nº 8.069, de 13 de julho de 1990**. Estatuto da Criança e do Adolescente. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm. Acesso em: 21 abr. 2026.

CÂMARA DOS DEPUTADOS. **Substitutivo ao Projeto de Lei nº 1.380, de 2025**. Altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), para dispor sobre o uso de reconhecimento facial para o cadastro e autenticação de usuários em sistemas operacionais. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2993156&filename=SBT+1+CCOM+%3D%3E+PL+1380/2025. Acesso em: 21 abr. 2026.

CETIc.br. **Práticas de aferição de idade em 25 serviços digitais usados por crianças no Brasil**. São Paulo: CETIc.br, 2025. Disponível em: https://cetic.br/media/analises/Ceticbr_Estudo_Afericao_Idade_Servicos_Digitais_Criancas.pdf. Acesso em: 21 abr. 2026.

CHARLEAUX, Lupa; LIMA, Lucas. **Como criar outra conta no Instagram com o mesmo e-mail**. Tecnoblog, 22 dez. 2024. Disponível em: <https://tecnoblog.net/responde/como-criar-outra-conta-no-instagram-com-o-mesmo-e-mail/>. Acesso em: 21 abr. 2026.

CONEGLIAN, Caio Saraiva. SANTAREM SEGUNDO, José Eduardo. SANT'ANA, CESAR GONÇALVES. Big Data: fatores potencialmente discriminatórios em análise de dados. **Em Questão**. Porto Alegre. v. 23. n. 1. p. 62-86. 2017. Disponível em: <https://seer.ufrgs.br/index.php/EmQuestao/article/view/62122>. Acesso em: 21 abr. 2026.

DESLANDES, Maria S. S.; ARANTES, Álisson R. Os perigos dos crimes virtuais nas redes sociais. **Sinapse Múltipla**, v. 6, n. 2, p. 175-178, 2017. Disponível em: <https://periodicos.pucminas.br/sinapsemultipla/article/view/16488/12745>. Acesso em: 21 abr. 2026.

FONTELES, Débora Matni; RODRIGUES, Fernando de Assis. Pesquisas brasileiras da ciência da informação sobre serviços de redes sociais e privacidade digital. **Comunicação & Informação**, Goiânia, GO, v. 27, p. 153-177, 2024. Disponível em: <https://revistas.ufg.br/ci/article/view/81050/41903>. Acesso em: 21 abr. 2026.

FULLER, Greice Patricia. Os delitos e as novas tecnologias em face da relação dialógica com os direitos humanos. In: **Direitos Humanos e Fundamentais na era da Informação**. Sarlet, Ingo Wolfgang; Waldman, Ricardo (Coords). Porto Alegre: Ed. Fundação Fenix, 2020.

GONÇALVES, Ana Paula; LARA, Célia Regina; SILVA, Rafael Fernandes da. A proteção de crianças e adolescentes no ambiente digital: Lei n. 15.211/2025. **Contribuciones a las Ciencias Sociales**, São José dos Pinhais, v. 19, n. 3, p. 1-28, 2026. Disponível em: <https://ojs.revistacontribuciones.com/ojs/index.php/clcs/article/view/23994/13772>. Acesso em: 15 maio 2026.

GOOGLE. **Quantas contas Google posso criar?** Central de Ajuda Google, 2024. Disponível em: <https://support.google.com/accounts/thread/26613177/quantas-contas-google-posso-criar?hl=pt-BR>. Acesso em: 21 abr. 2026.

PINHEIRO, Patricia Peck. **Biometria facial: utilização por instituições financeiras na prevenção a fraudes**. 2023. Disponível em: <https://febrabantech.febraban.org.br/especialista/patricia-peck-pinheiro/biometria-facial-utilizacao-por-instituicoes-financeiras-na-prevencao-a-fraudes>. Acesso em: 21 abr. 2026.

RODRIGUES, Vanessa Costa; FERREIRA, Rafaela Oliveira da Costa; AGUIAR, Vera Mônica Queiroz Fernandes. A eficácia da legislação brasileira no combate aos crimes cibernéticos, os desafios enfrentados na investigação e as dificuldades na responsabilização penal dos infratores. **Ciências Sociais Aplicadas**, v. 29, ed. 151, out. 2025. DOI: 10.69849/revistaft/ch10202510181202.

SANTOS, E. V. B. et al. Proteção de Crianças e Adolescentes no Ambiente Digital: Desafios e Limites do Estatuto Digital da Criança e do Adolescente (Lei Nº 15.211/2025). **Revista Tópicos**, Rio de Janeiro, v. 4, n. 31, p. 1-28, 2026. ISSN: 2965-6672.

SHIMABUKURO, Igor; TOLEDO, Victor. **Como criar um e-mail gratuito no Gmail pelo celular ou PC**. Tecnoblog, 2024. Disponível em: <https://tecnoblog.net/responde/como-criar-um-e-mail-gratuito-no-gmail-pelo-celular-ou-pc/>. Acesso em: 21 abr. 2026.

SILVA NETO, Victo José da; CHIARINI, Tulio; RIBEIRO, Leonardo Costa. Economia de plataformas: a eclosão de empresas brasileiras controladoras de plataformas digitais. In:

KUBOTA, Luis Claudio (org.). Digitalização e tecnologias da informação e comunicação: oportunidades e desafios para o Brasil. Rio de Janeiro: **Instituto de Pesquisa Econômica Aplicada (Ipea)**, 2024. v. 1, p. 49-72. Disponível em: <http://dx.doi.org/10.38116/9786556350660cap2>. Acesso em: 21 abr. 2026.

SOUSA, Lucas Silva de; MARINI, Bruno. **Crimes digitais: desafios na identificação do sujeito ativo diante de perfis falsos nas redes sociais para a imputação de penalidade**. Campo Grande: Universidade Federal de Mato Grosso do Sul, 2025. Disponível em: <https://repositorio.ufms.br/jspui/retrieve/ed2e1fc2-eb36-45c1-a0a7-32d0c10f242f/32433.pdf>. Acesso em: 21 abr. 2026.

TEIXEIRA, Lucia; COUTINHO, Mariana. Redes sociais, algoritmos e responsabilidade social: questões de enunciação na era digital. *Revista ENTRELETRAS*, v. 15, n. Especial, 2024. ISSN 2179-3948. Disponível em: <https://periodicos.ufmt.edu.br/index.php/entreletras/article/view/19229/22455>. Acesso em: 21 abr. 2026.

USP. **Reconhecimento facial nas redes sociais como forma de combater a disseminação de perfis falsos**. 2025. Disponível em: <https://jornal.usp.br/radio-usp/reconhecimento-facial-nas-redes-sociais-como-forma-de-combater-a-disseminacao-de-perfis-falsos/>. Acesso em: 21 abr. 2026.