O CONCEITO JURÍDICO DE ACESSO PROVÁVEL NO ECA DIGITAL

Carla Rodrigues
Eduardo Gomes Mendonça
Rafael A. F. Zanatta

DataPrivacyBR

Sobre a Data

A Data Privacy Brasil é uma organização que nasce da união entre uma escola e uma associação civil em prol da promoção da cultura de proteção de dados e direitos digitais no Brasil e no mundo. Fundada em 2018, a Data Privacy Brasil Ensino surgiu como um espaço para difundir e inovar no conhecimento sobre privacidade e proteção de dados no país. Com conteúdo adaptado para uma linguagem mais prática, com exercícios e estudos de caso, trata-se de uma escola para todos aqueles que se interessam e querem se aprofundar na temática da privacidade, proteção de dados e novas tecnologias.

A Associação Data Privacy Brasil de Pesquisa é uma organização da sociedade civil, sem fins lucrativos e suprapartidária, que promove a proteção de dados pessoais e outros direitos fundamentais a partir de uma perspectiva de justiça social e das assimetrias de poder.

A partir de 2023, as duas instituições se uniram para formar uma única organização, man tendo os mesmos princípios e atividades. Com o apoio de uma equipe multidisciplinar, realizamos formações, eventos, certificações, consultorias, conteúdos multimídia, pesquisas de interesse público e auditorias cívicas para a promoção de direitos em uma sociedade datificada marcada por assimetrias e injustiças. Por meio da educação, da sensibilização e da mobilização da sociedade, buscamos uma sociedade democrática em que as tecnologias estejam a serviço da autonomia e dignidade das pessoas.

Ficha técnica

Direção
Bruno Bioni, Mariana Rielli e Rafael Zanatta

Coordenação
Carla Rodrigues, Jaqueline Pigatto, Pedro Martins, Pedro Saliba e Victor Barcellos

Equipe
Barbara Yamasaki, Bianca Marques Eduardo Mendonça, Gabriela Vergili, Giovana Andrade, Isabelle Santos, João Paulo Vicente, Larissa Pacheco, Louise Karczeski, Luize Ribeiro, Matheus Arcanjo, Natasha Nóvoa, Pedro Henrique, Rafael Guimarães, Rennan Willian, Rodolfo Rodrigues e Vinicius Silva

Imprensa
Para esclarecimentos sobre o documento e entrevistas, entrar em contato pelo e-mail imprensa@dataprivacy.br.org

ÍNDICE

01. INTRODUÇÃO

A intensificação do uso de serviços digitais por crianças e adolescentes têm tensionado os limites dos modelos tradicionais de regulação, especialmente aqueles baseados em classificações formais de destinação etária e em declarações abstratas dos fornecedores. Em ambientes digitais estruturados pela coleta e pelo tratamento intensivo de dados, pela interação em larga escala e por mecanismos automatizados de engajamento, a distinção entre serviços "direcionados" e serviços efetivamente utilizados por crianças revela-se insuficiente para assegurar a proteção integral desse público.

É nesse contexto que a Lei nº 15.211/2025, o chamado ECA Digital, inaugura um novo paradigma normativo ao reposicionar a proteção da infância e da adolescência no centro da governança dos ambientes digitais. Partindo desse cenário, o artigo desenvolve uma leitura interpretativa do artigo 1º do ECA Digital, especialmente de seu parágrafo único, com foco nos critérios que delimitam o âmbito de aplicação da lei. A análise se orienta pela compreensão de que o conceito de "acesso provável" representa uma inflexão deliberada em relação a abordagens restritivas, ao deslocar o eixo da responsabilização da intenção declarada dos fornecedores para a realidade concreta de uso, atratividade e facilidade de acesso dos serviços digitais por crianças e adolescentes.

Nesse movimento, busca-se evidenciar que o "significativo grau de risco", previsto no inciso III, não se apresenta como um requisito autônomo ou excludente da incidência normativa, mas como uma consequência presumida do próprio acesso provável em contextos marcados por assimetrias estruturais e práticas intensivas de tratamento de dados.

Em síntese, argumentamos que o conceito jurídico de "acesso provável" não pode ser interpretado como se o "significativo grau de risco à privacidade, à segurança ou ao desenvolvimento biopsicossocial de crianças e de adolescentes" tivesse que ser demonstrado, caso a caso, para que ocorra a incidência da legislação em seu art. 1º. Essa tese é inconstitucional por colidir com as regras constitucionais de absoluta prioridade dos direitos fundamentais das crianças e adolescentes e com a doutrina jurídica dos direitos das crianças e adolescentes. A intenção do legislador é protetiva aos direitos fundamentais e presume situações de risco exaustivamente discutidas na elaboração do ECA Digital.[1] "Produtos ou serviços que tenham por finalidade permitir a interação social e o compartilhamento de informações em

1 Sobre a centralidade dos direitos fundamentais de crianças e adolescentes e a interpretação do Comentário Geral 25/2021, ver Ferreyra et al (2022). Sobre a orientação protetiva do ECA Digital e suas implicações para o direito de família e direito da responsabilidade civil, ver Santos Gomes (2025) e Faleiros Junior (2025). Sobre as contradições entre os modelos de negócios das Big Techs com o ECA Digital e a necessidade de uma abordagem transnacional ancorada no constitucionalismo digital, ver Henriques (2024) e Miolaro e Piovesan (2025).

larga escala entre usuários em ambiente digital" (art. 1º, § único, III, ECA Digital) presumem riscos a direitos fundamentais e dispensam demonstração de danos.

Por fim, com base na literatura técnica especializada e na experiência do Reino Unido, propomos uma adaptação da doutrina do "bom senso" utilizada no direito inglês. O teste jurídico para configuração do "acesso provável" reside em três elementos: (i) se há probabilidade de um serviço ser usado por crianças ou adolescentes, (ii) se há atratividade das arquiteturas da informação (incluindo o design de plataformas) e na divulgação do serviço do ponto de vista das crianças e adolescentes, e (iii) se há considerável facilidade de acesso de um produto ou serviço digital.

Argumentamos que o ECA Digital atribui o ônus argumentativo de não incidência da legislação para empresas que possam demonstrar, de antemão, que não há probabilidade de uso de seus serviços por crianças e adolescentes, de que não há intencionalidade nas escolhas de design e de arquitetura da informação para mirar crianças e adolescentes e de que há fricções suficientes para tornar o acesso difícil para crianças e adolescentes. O ECA Digital deliberadamente escolheu um padrão jurídico ex ante e não repressivo. Exigir uma prova empírica de dano, como se fosse equivalente de "grau significativo de risco", esvaziaria a função preventiva da norma jurídica, violando o princípio da proteção integral.[2]

2 Sobre o princípio da proteção integral aplicado ao direito contemporâneo das crianças e adolescentes, com fundamento em sua matriz na Constituição Federal de 1988, ver Henriques (2023).

02. A GENEALOGIA DO ACESSO PROVÁVEL NO DIREITO BRASILEIRO E NO DIREITO INGLÊS

A introdução do conceito jurídico de "acesso provável" no art. 1º ocorreu em 2025, na apresentação da primeira versão do substitutivo do Projeto de Lei 2628/2022 pelo deputado Jadyel Alencar no dia 12 de agosto de 2025. A versão original da norma jurídica previa o conceito de "provável acesso". Segundo argumentação do senador Alessandro Vieira, o projeto se aplicaria a todo produto ou serviço de tecnologia da informação "direcionado ou que possa ser utilizado por crianças e adolescentes, disponíveis em território nacional, independentemente de sua localização, desenvolvimento, fabricação, oferta, comercialização e operação". E essa abrangência, segundo o senador, "segue exemplo do que fez a autoridade britânica (ICO) em seu Age Appropriate Design Code, que condicionou a incidência da lei ao provável acesso de crianças e adolescentes ao produto ou serviço". Para o Senador, "uma vez que este tenha probabilidades significativas de ser acessado por crianças e adolescentes, ele deve ser mais protetivo, ainda que não seja declaradamente pensado para esse público" (Vieira, 2022, p. 14).

Como reconhecido pelo Senado Federal, a inspiração normativa para "provável acesso", no texto do PL 2628/2022, veio da jurisdição inglesa e da autoridade de proteção de dados pessoais (Information Commission's Officer - ICO). Jadyel Alencar, ao elaborar o seu substitutivo, acolheu uma sugestão do Instituto de Defesa do Consumidor (Idec) para garantir mais precisão ao texto, com o detalhamento dos incisos que explicitam atratividade e facilidade de acesso. Nas palavras do deputado Alencar em seu substitutivo:

> Em atendimento a sugestão apresentada pelo IDEC, optamos por delimitar com maior clareza o escopo dos agentes alcançados pela proposição, de modo a garantir maior segurança jurídica e mitigar dubiedades na interpretação da legislação que se pretende aprovar. Nesse sentido, sob a inspiração da terminologia empregada nas normas britânicas Online Safety Act e Age Appropriate Design Code, que adotam o modelo do "provável acesso", propomos a substituição, em todo o projeto, da expressão "produto ou serviço de tecnologia da informação direcionado ou que possa ser utilizado por crianças e adolescentes" por "produto ou serviço de tecnologia da informação direcionado ou de acesso provável por crianças e adolescentes". A medida considera a realidade material de utilização das plataformas, determinando a aplicação da legislação nos casos de uso provável ou significativo por crianças e adolescentes (Alencar, 2025, p. 39).

O quadro abaixo sintetiza as diferenças entre a versão apresentada pelo senador Alessandro Vieira em 2022 e a versão do substitutivo que, posteriormente, foi convertida na legislação federal (Lei 15.211/2025):

Quadro 01. Comparação do art. 1º da versão original do Senado Federal (2022) e substitutivo na Câmara dos Deputados (2025)

Versão do Senado Federal (outubro de 2022)	Versão da Câmara dos Deputados (agosto de 2025)
Art. 1º Esta Lei se aplica a todo produto ou serviço de tecnologia da informação direcionado ou de provável acesso por crianças e adolescentes, disponíveis em território nacional, independentemente de sua localização, desenvolvimento, fabricação, oferta, comercialização e operação. Parágrafo Único. A esta Lei aplicam-se os conceitos de crianças e adolescentes contidos no art. 2° da Lei nº 8.069, de 13 de Julho de 1990, o Estatuto da Criança e do Adolescente.	Art. 1º Esta Lei dispõe sobre a proteção de crianças e adolescentes em ambientes digitais e aplica-se a todo produto ou serviço de tecnologia da informação direcionado ou de acesso provável por crianças e adolescentes no Brasil, independentemente de sua localização, desenvolvimento, fabricação, oferta, comercialização e operação. Parágrafo único. Para fins desta lei, acesso provável por crianças e adolescentes será considerado quando houver: – suficiente probabilidade de uso e atratividade do produto ou serviço de tecnologia da informação por crianças e adolescentes; – considerável facilidade ao acesso e utilização do produto ou serviço de tecnologia da informação; e III – significativo grau de risco à privacidade, à segurança ou ao desenvolvimento biopsicossocial de crianças e adolescentes, especialmente no caso de produtos ou serviços que tenham por finalidade permitir a interação social e o compartilhamento de informações em larga escala entre usuários em ambiente digital

Fonte: Senado Federal e Câmara dos Deputados

Como bem evidenciado, o conceito jurídico de "acesso provável" no ECA Digital foi pensado a partir da experiência de regulação no Reino Unido, que é influente e crucial para uma correta interpretação dos sentidos jurídicos dessa expressão e sua implementação no direito brasileiro.

O ponto de inflexão na regulação internacional da proteção de dados de crianças e adolescentes ocorreu no Reino Unido, no processo de implementação do GDPR por meio do Data Protection Act 2018 (DPA 2018). Esse movimento consolidou a proteção de dados como linguagem de direitos fundamentais e, sobretudo, reposicionou o problema regulatório. Não basta proteger crianças e adolescentes do mundo digital. É preciso protegê-las dentro dele, garantindo que direitos fundamentais sejam respeitados por design e por padrão, à luz do princípio do melhor interesse (ONU, 1989, art. 3).

Esse enquadramento responde a um dado estrutural. Crianças e adolescentes participam intensamente do ecossistema digital, mas a infraestrutura de plataformas, serviços e dispositivos foi historicamente desenhada a partir de um utilizador implícito adulto, informado e plenamente autónomo. A consequência é uma assimetria persistente de poder e informação, na qual escolhas de design e modelos de negócio produzem riscos previsíveis que são deslocados para utilizadores em desenvolvimento e para as suas famílias. Em termos de direito público, consistente de uma disputa sobre alocação de deveres e sobre quem suporta os custos de uma economia orientada à captura de atenção.

A inovação decisiva aparece na Seção 123 do Data Protection Act de 2018, ao determinar que o Information Commissioner's Office (ICO) elaborasse um código estatutário de padrões de design apropriados à idade, aplicável a serviços relevantes da sociedade da informação provavelmente acessados por crianças e adolescentes (DPA 2018, s.123).[3] Com isso, o critério de incidência deixa de depender apenas da autodeclaração empresarial sobre o público-alvo e passa a considerar a realidade do uso social do serviço. Surge, assim, o acesso provável [likely to be accessed] como tecnologia regulatória de fechamento de lacunas. O gatilho não é o rótulo feito para crianças, mas a previsibilidade do acesso e do risco. Essa guinada é percebida na literatura jurídica inglesa, que reconhece que "serviços que possuem acesso provável por crianças devem enfrentar responsabilidades adicionais e devem conduzir avaliações de risco e agir para proteger usuários jovens de conteúdos danosos"[4].

O problema que essa mudança pretende resolver é, em primeiro lugar, de escopo. Quando a incidência depende de o serviço ser dirigido a crianças, a proteção

3 Conforme versão original da norma jurídica: "The Commissioner must prepare a code of practice which contains such guidance as the Commissioner considers appropriate on standards of age-appropriate design of relevant information society services which are likely to be accessed by children".

4 Nash & Falton (2024, p. 822)

pode falhar justamente nos ambientes generalistas onde crianças e adolescentes circulam de fato. Apesar de útil em cenários evidentes, como conteúdos e produtos claramente infantis, esse critério torna-se frágil em ecossistemas de grande escala, nos quais o acesso por crianças e adolescentes é previsível mesmo sem intenção declarada. Abre-se, assim, uma zona de sombra regulatória, em que a presença infantil é socialmente conhecida, mas juridicamente contestável.

Esse deslocamento responde, de forma explícita, aos limites de modelos tradicionais centrados no direcionamento do serviço. O contraste mais nítido é com o Children's Online Privacy Protection Act (COPPA), nos Estados Unidos, que aplica com uma lógica binária, serviços dirigidos a crianças ou serviços em que o operador tenha conhecimento real de utilizadores com menos de 13 anos. Na prática, essa arquitetura permitiu que plataformas amplamente utilizadas por crianças e adolescentes alegassem público-alvo adulto para reduzir deveres de proteção[5]. Além disso, a combinação de termos de uso, cortes etários formais e estratégias de não conhecimento pode funcionar como rota de fuga, mantendo o benefício econômico do uso de crianças e adolescentes e, ao mesmo tempo, mitigando obrigações. O standard do ICO procura romper com esse arranjo. Se o serviço tem atratividade para o público destinado a crianças e adolescentes, ou se há evidência de uso generalizado por essa faixa etária, a ausência de direcionamento explícito não afasta as obrigações regulatórias.

A partir dessa base, o Age Appropriate Design Code (AADC), também chamado Children's Code, amplia o olhar regulatório para além do tratamento de dados pessoais em sentido estrito. O foco recai sobre a arquitetura do serviço e sobre como funcionalidades, defaults e mecanismos de recomendação podem produzir riscos desproporcionais para pessoas em desenvolvimento (ICO, 2020). Nessa moldura, o acesso provável desloca o debate do marketing para o desenho do serviço e para os riscos previsíveis que esse desenho produz. O critério passa a funcionar como um operador de imputação. Se crianças e adolescentes estão, de forma previsível, no ecossistema, a organização deve justificar escolhas de design, configurar proteções por padrão e governar riscos de forma ex ante (DPA 2018, s.123; ICO, 2020).

Do ponto de vista operacional, o ICO adota um limiar de aplicação que procura evitar a inércia regulatória em serviços generalistas, ativando o standard quando há mais do que um número mínimo ou insignificante de crianças usando o serviço. A avaliação de probabilidade não se limita ao conteúdo com apelo infantojuvenil, mas também considera riscos inerentes ao processamento e ao modo de funcionamento do serviço. Nessa lógica, a conformidade exige governança preventiva, com avaliações de impacto voltadas a identificar riscos para crianças e adolescen-

5 Sobre as diferenças entre o COPPA e as novas legislações de proteção de crianças, como do Reino Unido e da Califórnia, ver Benson (2023). O autor também destaca o tensionamento dessas legislações com a doutrina de liberdade de expressão aplicada a corporações nos EUA.

tes e medidas protetivas implementadas antes do dano (ICO, 2020).

O eixo substantivo da inovação é a migração do debate de coleta de dados para arquiteturas de risco. O dano potencial passa a incluir manipulação comportamental, engajamento compulsivo e desenho viciante, muitas vezes realizado por padrões de interface e por incentivos de monetização. A lente do acesso provável permite enquadrar esses mecanismos sempre que houver risco previsível e desproporcional, ativando deveres de limitação por padrão e mitigação desde a concepção (ICO, 2020). Nesse mesmo campo entram discussões sobre caixas de recompensa e sistemas de recompensa variável, cuja qualificação jurídica pode variar entre jurisdições, mas cujo potencial de indução compulsiva e de dano financeiro ou psicológico justifica escrutínio reforçado quando há probabilidade de acesso por crianças e adolescentes.

A consolidação internacional do critério fica evidente com a sua incorporação na California Age Appropriate Design Code Act (CA-AADC), promulgada em 2022 e inspirada diretamente no modelo britânico. A lei californiana reage às lacunas do regime federal norte- americano e amplia o escopo de proteção para pessoas com menos de 18 anos, aplicando-se quando houver probabilidade razoável de acesso ao serviço, aferida pela demografia real de utilizadores e por semelhança com plataformas amplamente usadas por crianças e adolescentes. Assim como no Reino Unido, há exigência de avaliações de impacto orientadas ao melhor interesse e de privacidade por padrão, além da vedação de padrões manipulativos capazes de afetar a saúde física ou mental de utilizadores em desenvolvimento. As diferenças institucionais são relevantes. No Reino Unido, o AADC integra o ecossistema do UK GDPR sob supervisão do ICO. Na Califórnia, o CA-AADC é estatuto autônomo, com implementação atribuída à California Privacy Protection Agency e relação funcional com o CCPA, mas com escopo próprio. Ainda assim, a convergência é clara. Ambos os regimes tratam o acesso provável como gatilho de responsabilização e de deveres objetivos de cuidado.

Ao mesmo tempo, os elementos críticos do acesso provável não podem ser tratados como adendos. O critério não é neutro nem automático. A probabilidade é construída por indicadores, métricas e inferências, muitas vezes controladas pelas próprias plataformas. Isso cria risco de opacidade, em que operadores minimizam sinais de presença infantil para reduzir obrigações. Por essa razão, o acesso provável exige critérios verificáveis e expectativas claras sobre quais evidências contam, sob pena de transformar um teste material num formalismo administrável pela autorreferência empresarial.

Também há risco de respostas de alto custo social. Quando a conformidade é confundida com bloqueio, certas empresas podem optar por expulsar crianças e adolescentes do serviço, empurrando-as para circuitos menos seguros ou para estratégias de falsificação de idade. Além disso, quando a conformidade se apoia em mecanismos intensivos de garantia de idade, surgem tensões entre proteção

e vigilância. Tecnologias de verificação etária podem ampliar a recolha de dados, criar barreiras de acesso e afetar de modo desproporcional famílias com menos recursos, conectividade precária e menor literacia digital. Assim, uma política desenhada para reduzir riscos pode, paradoxalmente, criar novos riscos de privacidade e desigualdade.

Por fim, a categoria deve ser lida com atenção às desigualdades que atravessam infância e adolescência.[6] Crianças e adolescentes não formam um grupo homogêneo.[7] Raça, gênero, classe e território modulam exposição a assédio, exploração, perfis indevidos e dinâmicas de dependência, incluindo dependência de dispositivos partilhados e de acesso intermitente. Se a regulação não incorporar essa dimensão, corre-se o risco de proteger melhor quem já dispõe de mais mediação e recursos, deixando à margem os grupos que mais precisam de salvaguardas materiais.

No Brasil, a incorporação dessa lógica encontra fundamento constitucional no art. 227, que consagra a prioridade absoluta e a proteção integral, impondo um dever de prevenção também no ambiente digital. Somam-se a isso a proteção de dados como direito fundamental (EC 115/2022) e as regras da LGPD sobre tratamento de dados de crianças e adolescentes (art. 14), que reforçam a centralidade do melhor interesse e a necessidade de medidas reforçadas de proteção. O ECA Digital institucionaliza esse deslocamento ao prever incidência sobre produtos e serviços direcionados às crianças e adolescentes ou de acesso provável por esse público, rompendo com a lógica de autorreferência empresarial baseada apenas em não destinação.

Esse enquadramento afasta a ideia de que cláusulas contratuais ou avisos de não destinados a crianças e adolescentes bastariam para excluir responsabilidades. Se um serviço se beneficia economicamente da atenção e dos dados de um contingente significativo de adolescentes, a alegação de público-alvo adulto não elimina o dever de avaliar e mitigar riscos previsíveis. O critério de probabilidade funciona, portanto, como superação prática da ficção do consentimento plenamente esclarecido em ambientes digitais complexos, substituindo-a por deveres objetivos de cuidado e por uma abordagem de justiça de dados. A proteção deixa de ser apenas controle informacional e passa a abranger barreiras estruturais contra exploração e manipulação por design.

Em suma, no direito comparativo internacional, o acesso provável desloca a proteção infantil do rótulo do serviço ou dos tipos de dados coletados para a previsibilidade do uso e dos riscos, ampliando deveres de design, avaliação de impacto e governança. Ao mesmo tempo, a sua eficácia depende de como se prova o pro-

6 Sobre a temática das múltiplas infâncias, ver Henriques (2023).

7 Com relação a múltiplas infâncias e teorias pedagógicas contemporâneas aplicadas aos direitos digitais, ver Zanatta (2024).

vável, de como se evitam respostas excludentes e de como se limitam os efeitos colaterais de soluções tecnológicas intrusivas. É nessa tensão, entre expansão de escopo e disputa sobre evidências, que a categoria se consolida como ferramenta regulatória e como campo de controvérsia, preparando a análise das escolhas de implementação e da circulação internacional do modelo.

03. A INTERPRETAÇÃO DO ART. 1º E DO CONCEITO JURÍDICO DE ACESSO PROVÁVEL

A força normativa do ECA Digital começa, de forma decisiva, no art. 1º da Lei nº 15.211/2025, ao definir o seu âmbito de aplicação. O dispositivo rompe com a lógica restritiva que historicamente marcou a regulação de ambientes digitais ao afirmar que a lei se aplica não apenas a produtos ou serviços "direcionados" a crianças e adolescentes, mas também àqueles de "acesso provável" por esse público. Esse desenho normativo revela um movimento deliberado de fechamento de brechas interpretativas, inspirado nos modelos mais protetivos do direito comparado, como o Age Appropriate Design Code do Reino Unido e a California Age- Appropriate Design Code Act, apresentadas anteriormente.

O parágrafo único do art. 1º da Lei nº 15.211/2025 cumpre papel central nesse desenho ao densificar o conceito de acesso provável por meio de três incisos que devem ser lidos de forma conjunta e sistemática, e não como requisitos autônomos ou excludentes. Os incisos I e II incidem como verdadeiros "gatilhos de realidade", voltados à observação concreta do funcionamento dos serviços digitais. O inciso I refere-se à probabilidade de uso e atratividade do produto ou serviço por crianças e adolescentes. Aqui, a lei desloca o foco da intenção declarada do fornecedor para os efeitos reais do design, das funcionalidades, da linguagem visual e do apelo cultural do serviço.

Neste momento, não importa apenas para quem o serviço diz ser destinado, mas para quem ele efetivamente se torna atrativo no ecossistema digital contemporâneo[8]. Já o inciso II trata da considerável facilidade de acesso e utilização, evidenciando que a ausência de barreiras técnicas eficazes — como verificações de idade robustas ou fluxos diferenciados — contribui para a caracterização do acesso provável.

A ICO, na interpretação do Age Appropriate Design Code, utiliza a doutrina do "bom senso" para interpretar o conceito jurídico de likely to be acessed - o equivalente do conceito de "acesso provável".[9] Diz o informe da autoridade publicado em 2024:

8 ICO. Age appropriate design: a code of practice for online services. Disponível em: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/. Acesso em: 19 dez. 2025.

9 A autoridade utiliza a expressão common sense approach. Nós utilizamos a expressão doutrina do bom senso por ser uma expressão mais comum no Brasil. Essa concepção em nada se aproxima da crítica feita por Luis Alberto Warat sobre o "senso comum teórico" dos juristas (Warat, 1982). A "doutrina do bom senso" exige boa- fé e uma conduta proativa de comportamento no caso do ECA Digital.

> Consideramos que, para um serviço ser “provavelmente” acessado, a possibilidade de tal acontecer tem de ser mais provável do que improvável. Isso reconhece a intenção do Parlamento de abranger os serviços que as crianças utilizam na prática, mas não estende a definição a todos os serviços que as crianças possam acessar.
>
> Na prática, a probabilidade de seu serviço ser acessado por crianças dependerá de:
>
> 1. a natureza e o conteúdo do serviço e se ele é particularmente atraente para crianças; e
> 2. a forma como o serviço é acessado e quaisquer medidas que você implemente para impedir o acesso de crianças.
>
> Você deve adotar uma abordagem de bom senso em relação a essa questão. Se o seu serviço for do tipo que você não gostaria que crianças utilizassem em hipótese alguma, seu foco deve ser em como impedir o acesso (caso em que este código não se aplica), em vez de torná-lo adequado para crianças. Por exemplo, se for um serviço exclusivo para adultos, restrito ou inadequado para crianças. Este código não deve levar ao resultado perverso de que os provedores de serviços restritos tenham que tornar seus serviços adequados para crianças.
>
> Se o seu serviço não for direcionado a crianças, mas também não for inadequado para elas, então o seu foco deve ser avaliar o quão atraente ele será para esse público. Se a natureza, o conteúdo ou a apresentação do seu serviço fizerem você acreditar que crianças desejarão usá-lo, então você deve se adequar aos padrões deste código (ICO, 2024).

A ICO não tem um único “manual do bom senso” formalizado em um documento separado, mas o próprio código e as suas orientações complementares incorporam essa doutrina. A doutrina do bom senso, adotada pela ICO na interpretação do conceito de acesso provável, orienta que a análise não seja puramente abstrata ou formal, mas baseada em uma avaliação prática e realista de como o serviço funciona e de quem efetivamente tende a utilizá- lo. Segundo essa abordagem, um serviço é considerado “provavelmente acessado” por crianças quando, à luz do senso comum, é mais provável que elas o utilizem do que o contrário, considerando tanto a natureza e o apelo do conteúdo quanto as formas de acesso e as barreiras existentes.

No Brasil, os incisos I e II do parágrafo único do art. 1º do ECA Digital operam como balizas práticas da doutrina do bom senso. O teste jurídico para configuração do “acesso provável” reside em três elementos: (i) se há probabilidade de um serviço ser usado por crianças ou adolescentes, (ii) se há atratividade das arquiteturas da informação (incluindo o design de plataformas) e na divulgação do serviço do ponto de vista das crianças e adolescentes, e (iii) se há considerável facilidade de acesso de um produto ou serviço digital.

Tomemos dois exemplos claros que podem ser analisados à luz dos critérios propostos. O primeiro é uma plataforma profissional de gestão contábil ou fiscal (equivalente ao "Contabiliza"). Um sistema voltado à emissão de notas fiscais, apuração de impostos, escrituração contábil ou gestão tributária de empresas não é, pelo senso comum, algo que crianças tenderiam a acessar. O conteúdo é técnico, complexo e exige conhecimentos profissionais específicos, o acesso costuma exigir CNPJ, certificação digital ou credenciais profissionais, não há qualquer apelo lúdico, visual ou funcional voltado ao público infantil.

O segundo caso é uma plataforma corporativa interna de gestão de recursos humanos (equivalente ao "RH Gestor"). Nessa plataforma, o acesso é restrito a funcionários autenticados, o conteúdo trata de informações laborais e administrativas e não existe atratividade para crianças. Utilizando os critérios elaborados aqui, teríamos a seguinte matriz de análise para aplicação do teste de acesso provável:

Quadro 02. Aplicação do teste do "acesso provável" (art. 1º, par. ún., I e II – ECA Digital) em casos negativos

Critério do teste	*Plataforma de gestão contábil/fiscal*	*Sistema interno de RH corporativo*
(i) Probabilidade de uso por crianças ou adolescentes	**Muito baixa:** O serviço exige conhecimentos técnicos especializados, vocabulário contábil e finalidades incompatíveis com o universo infantil. Não há expectativa razoável de uso por crianças.	**Muito baixa:** Trata-se de ambiente profissional restrito a trabalhadores, sem qualquer função que faça sentido para crianças ou adolescentes.
(ii) Atratividade da arquitetura da informação e da divulgação	**Inexistente:** Interface técnica, linguagem formal, ausência de elementos lúdicos ou estéticos voltados a crianças. A comunicação institucional é dirigida a contadores, empresas e profissionais financeiros.	**Inexistente:** Design funcional e utilitário, voltado à gestão interna. A apresentação visual e discursiva não busca engajamento amplo nem apelo emocional típico de plataformas juvenis.
(iii) Facilidade de acesso ao serviço	**Baixa:** Normalmente exige cadastro com CNPJ, autenticação, certificados digitais ou contratos comerciais, o que constitui barreira efetiva de acesso.	**Muito baixa.** Acesso restrito a usuários previamente cadastrados pela organização, geralmente com autenticação corporativa.

Fonte: elaboração própria

Como visto, nesses dois exemplos, não haveria aplicação do ECA Digital e as duas empresas estariam fora de aplicação do art. 1º da legislação. Podemos repetir esse teste em casos exemplificativos de aplicação do ECA Digital em sentido oposto. Imagine, como terceiro caso, uma plataforma para celular que permite a troca virtual de figurinhas da Copa do Mundo e o direcionamento de mapas e pontos de encontro para troca presencial de figurinhas. Imagine, como quarto caso, uma plataforma de streaming de dicas de jogos. Nessa plataforma, jogadores profissionais de jogos como Roblox, Brawl Stars e Fortnite dão dicas de como ser um jogador bem sucedido, como melhorar sua performance e como participar de eventos presenciais com as principais estrelas do mundo dos jogos.

Quadro 02. Aplicação do teste do "acesso provável" (art. 1º, par. ún., I e II – ECA Digital) em casos positivos

Critério do teste	*Plataforma de troca de figurinhas da Copa do Mundo e organização de encontros presenciais*	*Plataforma de streaming com dicas de jogos (Roblox, Brawl Stars, Fortnite)*
(i) Probabilidade de uso por crianças ou adolescentes	**Alta:** A troca de figurinhas da Copa é uma prática culturalmente associada a crianças e adolescentes, ainda que adultos também participem. A própria lógica colecionável é fortemente vinculada à infância.	**Muito alta:** Os jogos mencionados têm base majoritariamente infanto-juvenil. É previsível, quase inevitável, que crianças e adolescentes constituam parcela significativa do público.
(ii) Atratividade da arquitetura da informação e da divulgação	**Alta:** O tema, a estética, a linguagem lúdica e o caráter social da plataforma são fortemente atrativos ao público infantojuvenil. O uso de mapas e encontros reforça a dimensão de engajamento típico desse público.	**Muito alta:** Linguagem visual, estética gamer, referências a influenciadores e promessa de melhoria de performance funcionam como fortes vetores de engajamento infantil.
(iii) Facilidade de acesso ao serviço	**Alta:** Aplicativos desse tipo tendem a ser de fácil acesso, com cadastro simples e uso intuitivo, muitas vezes sem mecanismos robustos de verificação etária.	**Alta:** Plataformas de streaming tendem a ser de fácil acesso, muitas vezes gratuitas ou com barreiras mínimas, o que reforça a previsibilidade de acesso por menores.

Fonte: elaboração própria

Nesses dois casos discutidos no quadro acima, configura-se claramente o "acesso provável" por crianças, exigindo não apenas adequação ao ECA Digital, mas atenção redobrada a práticas de design, publicidade, coleta de dados e incentivos comportamentais. Esses dois exemplos mostram como o teste do acesso provável não depende da intenção declarada do serviço, mas da leitura objetiva do ecossistema sociotécnico no qual ele opera.

Um ponto sensível da interpretação do art. 1º é o inciso III, que menciona o "significativo grau de risco à privacidade, à segurança ou ao desenvolvimento biopsicossocial" de crianças e adolescentes. Há um risco concreto de que esse dispositivo seja mobilizado por empresas como uma cláusula de escape interpretativa, sustentando que, embora seus serviços tenham (i) probabilidade de acesso, (ii) sejam atrativos do ponto de vista de design e arquitetura e (iii) sejam facilmente acessíveis, não apresentariam risco significativo e, portanto, estariam fora do alcance da lei.

Essa leitura, contudo, não se sustenta diante de uma interpretação sistemática, teleológica e constitucionalmente orientada do ECA Digital. O próprio texto do inciso III explicita que esse risco é inerente, "especialmente no caso de produtos ou serviços que tenham por finalidade permitir a interação social e o compartilhamento de informações em larga escala". Ao fazê-lo, o legislador reconhece que ambientes digitais baseados em interação massiva, circulação de dados e lógica de engajamento produzem, por sua própria natureza, riscos qualificados à privacidade, à segurança e ao desenvolvimento de pessoas em fase peculiar de formação.

Assim, o risco não é um elemento contingente a ser demonstrado caso a caso como condição para a incidência da lei. Ao contrário, trata-se de um risco presumido e estrutural, que decorre da própria configuração dos serviços digitais acessíveis a crianças e adolescentes (OCDE, 2024). Esse risco emerge da assimetria existente entre entre fornecedores de tecnologia (detentores de capacidade técnica, informacional e econômica amplamente superior) e usuários que são crianças e adolescentes, bem como das práticas sistemáticas de coleta e tratamento intensivo de dados pessoais, do perfilamento comportamental e da exposição contínua a dinâmicas de engajamento e recomendação potencialmente prejudiciais. Nesses termos, uma vez verificada a probabilidade de uso do serviço (inciso I), a atratividade do seu design (inciso I) e a facilidade de acesso e utilização por crianças e adolescentes (inciso II), o risco ao desenvolvimento biopsicossocial previsto no inciso III já se encontra configurado, independentemente da intenção declarada do fornecedor ou da ausência de danos imediatamente perceptíveis. Tal constatação aciona o regime protetivo do ECA Digital e desloca o foco regulatório para a exigência de salvaguardas preventivas e proporcionais, compatíveis com a prioridade absoluta assegurada constitucionalmente à infância e à adolescência.

Essa interpretação é substancialmente reforçada quando o Art. 1º do ECA Digital é lido à luz do Art. 227 da Constituição Federal, que consagra o princípio da prio-

ridade absoluta na proteção dos direitos da criança e do adolescente. Tal mandamento constitucional impõe ao Estado e à sociedade um dever qualificado de atuação preventiva, especialmente diante de contextos marcados por assimetrias estruturais de poder e informação.

O ECA Digital internaliza esse comando ao reconhecer, como fundamento expresso, a condição peculiar da criança e do adolescente como pessoas em desenvolvimento biopsicossocial, exigindo um nível elevado de proteção desde a concepção dos produtos e serviços digitais, e não apenas como resposta posterior a danos já verificados. A proteção integral exige antecipação regulatória, sobretudo em contextos tecnológicos marcados por opacidade, coleta massiva de dados e mecanismos automatizados de recomendação e engajamento.

É justamente nesse ponto que se situa o núcleo do debate em torno do inciso III do parágrafo único do Art. 1º, relativo ao "significativo grau de risco". Há uma tendência previsível de que empresas tentem mobilizar esse inciso como um argumento excludente, sustentando que, embora seus serviços sejam utilizados por crianças e adolescentes, eles não apresentariam riscos relevantes à privacidade, à segurança ou ao desenvolvimento biopsicossocial, razão pela qual a lei não lhes seria aplicável. Essa leitura, contudo, esvazia o sentido protetivo do dispositivo e contraria a lógica interna do ECA Digital.

O risco mencionado no inciso III não é contingente, eventual ou dependente de demonstração individualizada. Ao contrário, ele é presumido e inerente à própria dinâmica de interação digital em larga escala, como expressamente reconhece o dispositivo ao destacar, de forma enfática, os produtos e serviços que permitem interação social e compartilhamento de informações entre usuários. Plataformas digitais estruturadas a partir da coleta contínua de dados, do perfilamento comportamental e da maximização do engajamento produzem, por sua própria arquitetura, riscos qualificados ao desenvolvimento de crianças e adolescentes.

Nesse sentido, Zanatta, Valente e Mendonça (2021) evidenciam que os riscos a que crianças e adolescentes estão expostos no ambiente digital não se originam apenas de episódios pontuais ou de conteúdos explicitamente danosos, mas de práticas estruturais de coleta, tratamento e monitoramento contínuo de dados pessoais operadas por plataformas e aplicativos digitais. Ao analisarem a dinâmica de registros digitais e o funcionamento cotidiano desses serviços, os autores demonstram que a exposição infantil se dá em um contexto de vigilância permanente, no qual dados comportamentais são extraídos, correlacionados e utilizados para fins de perfilamento, recomendação e direcionamento de conteúdos. No mesmo sentido, Henriques (2023) demonstra, com base em diversos estudos conduzidos por Sonia Livingstone e por especialistas associados ao Comitê de Direitos das Crianças da Organização das Nações Unidas, que há uma intensificação dos riscos a direitos fundamentais em ambientes digitais, devendo existir um imperativo de proteção integral que afeta as escolhas de design e o modo como serviços

são tornados disponíveis para crianças e adolescentes.

Essa constatação empírica evidencia que a vulnerabilidade de crianças e adolescentes no ambiente digital não se restringe à exposição a conteúdos manifestamente ilícitos ou inadequados, mas decorre, de maneira mais profunda, da assimetria informacional, técnica e econômica que estrutura a relação entre usuários em desenvolvimento e fornecedores de serviços digitais. Verifica-se que há uma vulnerabilidade produzida pela própria lógica de funcionamento de plataformas que exercem modelos de negócio baseados na coleta, no tratamento e na exploração intensiva de dados pessoais, em contextos marcados por opacidade decisória, automatização de processos e capacidade assimétrica de influência sobre comportamentos e escolhas.

O "significativo grau de risco", portanto, não pode ser compreendido como um filtro excludente da incidência do ECA Digital - uma espécie de "carta da manga" que pode ser jogada pelas empresas para argumentar que não houve comprovação de danos a crianças em situações casuísticas -, mas como um vetor de calibração regulatória que organiza a aplicação proporcional e responsiva da lei. Nessa chave interpretativa, o risco não atua no plano da aplicabilidade da norma, mas no plano de sua concretização, definindo o nível de rigor regulatório, a densidade das salvaguardas exigidas e a extensão das responsabilidades exigidas atribuídas aos fornecedores em cada caso.

É justamente essa função moduladora que se encontra positivada no art. 39 da Lei nº 15.211/2025, ao estabelecer que as obrigações de prevenção, mitigação e governança devem ser graduadas conforme as características do serviço, o número de usuários e o porte econômico do agente regulado. O risco, assim, cumpre o papel de ajustar a intensidade e a complexidade das obrigações impostas, assegurando uma resposta regulatória adequada às especificidades de cada contexto, sem comprometer a incidência plena do seu regime protetivo.

Ao final, essa interpretação preserva a coerência sistêmica do ECA Digital, assegura sua efetividade normativa e reafirma seu alinhamento com o paradigma constitucional da proteção integral e da prioridade absoluta, previsto no Art. 227 da Constituição Federal. Mais do que um regime de responsabilização reativa, o ECA Digital consolida-se, assim, como um marco de governança preventiva, orientado à construção de ambientes digitais estruturalmente mais seguros, responsáveis e compatíveis com o pleno desenvolvimento de crianças e adolescentes.

04. CONCLUSÃO

O conceito jurídico de “acesso provável” no art. 1º do ECA Digital deve ser lido a partir das lentes de análise da teoria da proteção integral das crianças e adolescentes. Com base na literatura técnica especializada e na experiência do Reino Unido, propomos neste artigo uma adaptação da doutrina do “bom senso” utilizada no direito inglês. O teste jurídico para configuração do “acesso provável” do ECA Digital reside em três elementos: (i) se há probabilidade de um serviço ser usado por crianças ou adolescentes, (ii) se há atratividade das arquiteturas da informação (incluindo o design de plataformas) e na divulgação do serviço do ponto de vista das crianças e adolescentes, e (iii) se há considerável facilidade de acesso de um produto ou serviço digital.

A interpretação sistemática do art. 1º do ECA Digital conduz à conclusão de que o inciso III do parágrafo único não opera como uma cláusula de exclusão da incidência normativa, mas como um critério de modulação da intensidade regulatória. O risco ali mencionado não é um elemento contingente a ser comprovado caso a caso, tampouco um ônus probatório a ser deslocado para o poder público ou para os usuários. Trata-se, antes, de um risco estrutural e presumido, inerente à própria lógica de funcionamento de serviços digitais que envolvem coleta de dados, interações em larga escala e mecanismos de engajamento. Uma vez verificada a probabilidade de acesso por crianças, a atratividade do serviço e a facilidade de uso, o risco ao desenvolvimento biopsicossocial emerge como consequência lógica e normativa, acionando automaticamente o regime protetivo do ECA Digital.

Nesse sentido, o inciso III não autoriza uma leitura defensiva por parte dos fornecedores, mas opera como vetor de densificação das obrigações de cuidado, prevenção e governança. O “significativo grau de risco” não delimita o âmbito de incidência da lei, e sim orienta a intensidade das salvaguardas exigidas, em consonância com a prioridade absoluta assegurada pelo art. 227 da Constituição. A função do dispositivo é garantir que a resposta regulatória seja proporcional à assimetria estrutural existente entre plataformas e usuários em desenvolvimento, reafirmando o caráter preventivo, prospectivo e estrutural do ECA Digital. Trata-se, portanto, de um regime que não reage apenas a danos consumados, mas que busca conformar, desde a origem, ecossistemas digitais compatíveis com os direitos fundamentais de crianças e adolescentes.

REFERÊNCIAS

ALENCAR, Jadyel. Apresentação do Substitutivo do Projeto de Lei 2628/2022. Brasília: Câmara dos Deputados, 2025. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2970493&filenam e=PRL+1+C-COM+%3D%3E+PL+2628/2022. Acesso em: 19 dez. 2025.

BENSON, Peter J. NetChoice v. Bonta and First Amendment Limits on Protecting Children Online. Congressional Research Service (CRS) Reports and Issue Briefs, p. NA-NA, 2023.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/ConstituicaoCompilado.htm. Acesso em: 19 dez. 2025.

BRASIL. Emenda Constitucional n. 115, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Diário Oficial da União: seção 1, Brasília, DF, 11 fev. 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 19 dez. 2025.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei n. 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 19 dez. 2025.

FALEIROS JÚNIOR, José Luiz de Moura. Gamificação, exploração e vulnerabilidade infantil: a regulação das' loot boxes'e o desafio da responsabilidade civil no 'ECA Digital'. Revista IBERC, v. 8, n. 3, p. IV-IX, 2025.

FERREYRA, Eduardo et al. Dados e direitos na infância e adolescência no ambiente digital: caminhos para a proteção jurídica no Brasil e Argentina. Asociación por los Derechos Civiles; Data Privacy Brasil; Instituto Alana, 2022.

HENRIQUES, Isabella. Direitos Fundamentais da Criança no Ambiente Digital: o dever de garantia da absoluta prioridade. São Paulo: Revista dos Tribunais, 2023.

HENRIQUES, Isabella. Constitucionalismo digital e proteção da criança no ciberespaço. In: PIOVESAN, Flavia et al. Constitucionalismo Digital e Direitos Humanos: desafios da internet, inteligência artificial e neurotecnologia. São Paulo: Thomson Reuters Brasil, 2024.

ESTADOS UNIDOS. Califórnia. Assembly Bill No. 2273 (2021–2022 Reg. Sess.). Chapter 320, Statutes of 2022. The California Age-Appropriate Design Code Act. [S.l.]: California Legislative Information, 2022. Disponível em: https://legiscan.com/CA/text/AB2273/id/2599734. Acesso em: 19 dez. 2025.

ESTADOS UNIDOS. Children's Online Privacy Protection Act of 1998 (COPPA). 15 U.S.C. §§ 6501–6506, 1998. Disponível em: https://www.ftc.gov/legal- library/browse/rules/childrens-online-privacy-protection-rule-coppa. Acesso em: 19 dez. 2025.

ICO. Age appropriate design: a code of practice for online services. Disponível em: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of- practice-for-online-services/. Acesso em: 19 dez. 2025.

ICO. Age appropriate design: a code of practice for online services. Section "Services covered by this code". Londres: ICO, 2024. Disponível em: https://ico.org.uk/for- organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code- guidance-and-resources/age-appropriate-design-a-code-of-practice--for-online- services/services-covered-by-this-code/. Acesso em: 19 dez. 2025.

OCDE. Towards digital safety by design for children, nº 363, 2024. Disponível em: https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/06/towards-digital- safety-by-design-for-children_f1c86498/c167b650-en.pdf?. Acesso em: 18 dez. 2025.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Convenção sobre os Direitos da Criança. Nova York: ONU, 1989. Disponível em: https://www.unicef.org/brazil/convencao--sobre-os- direitos-da-crianca. Acesso em: 19 dez. 2025.

MIOLARO, Enzo; PIOVESAN, Flávia. O Estatuto Digital da Criança e do Adolescente (Lei 15.221/2025), Revista Contemporânea, v. 5, n. 12, p. e10022-e10022, 2025.

NASH, Victoria; FELTON, Lisa. Treating the symptoms or the disease? Analysing the UK Online Safety Act's approach to digital regulation. Policy & Internet, v. 16, n. 4, p. 818-832, 2024.

PRESIDÊNCIA DA REPÚBLICA FEDERATIVA DO BRASIL. Lei nº 15.211, de 17 de setembro de 2025. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/L15211.htm. Acesso em: 19 dez. 2025.

REINO UNIDO. Data Protection Act 2018 (c. 12). [S.l.]: legislation.gov.uk, 2018. Disponível em: https://www.legislation.gov.uk/ukpga/2018/12/contents. Acesso em: 19 dez. 2025.

REINO UNIDO. Information Commissioner's Office (ICO). Age appropriate design: a code of practice for online services. Wilmslow: ICO, 2020. Disponível em: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens- information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/. Acesso em: 19 dez. 2025.

SANTOS GOMES, Cárita Carolina. O Estatuto Digital da Criança e do Adolescente: Avanços e Implicações no Direito de Família. Revista Eletrônica da OAB-RJ, 2025.

VIEIRA, Alessandro. Apresentação do Projeto de Lei 2628/2022. Brasília: Senado Federal, 2022. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=9205520&ts=1758309711047&disposition=inline. Acesso em: 19 dez. 2025.

ZANATTA, Rafael; JONAS, Valente; JÚLIA, Mendonça. Entre o abusivo e o excessivo: Novos contornos jurídicos para o tratamento de dados pessoais de crianças e adolescentes na LGPD. Privacidade e Proteção de Dados de Crianças e Adolescentes. in: Priscilla Laterça, Elora Fernandes, Chiara Teffé and Sérgio Branco. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro, p. 396-426, 2021.

ZANATTA, Rafael A. F. Inteligências Artificiais, Infâncias e Direitos, in: HENRIQUES, Isabella (org.). Direitos de Crianças e Adolescentes: reflexões da advocacia do Estado de São Paulo. São Paulo: Editora Tirant lo Branch, 2024, p. 129-161.

WARAT, Luis Alberto. Saber crítico e senso comum teórico dos juristas. Seqüência: Estudos Jurídicos e Políticos, v. 3, n. 5, p. 48-57, 1982.