QUEM PROVA QUE A PLATAFORMA É SEGURA?

O dever de segurança demonstrável e o encargo regulatório residual de produção no ECA Digital

WHO PROVES THE PLATFORM IS SAFE? THE DUTY OF DEMONSTRABLE SAFETY AND THE RESIDUAL REGULATORY BURDEN OF PRODUCTION UNDER BRAZIL'S DIGITAL STATUTE OF THE CHILD AND ADOLESCENT (ECA DIGITAL)

Jandislei Antonio Genova[1]

Resumo: O artigo investiga quem deve produzir a evidência de segurança exigida na fiscalização de produtos e serviços digitais acessíveis a crianças e adolescentes. Por método jurídico-dogmático, comparativo-funcional e documental, reconstrói o regime formado pela Constituição, pela legislação de proteção integral, pelo ECA Digital e por sua regulamentação, distinguindo o âmbito próprio do procedimento da Agência Nacional de Proteção de Dados na LGPD e as lacunas procedimentais transitórias do novo estatuto. O resultado separa quatro categorias: dever material de segurança; deveres positivos de documentação e cooperação; encargo regulatório residual de produção; e ônus processual da prova. Sustenta-se que "segurança demonstrável" é síntese interpretativa, não expressão literal da lei. Por controlar arquitetura, dados e registros, o fornecedor deve produzir evidência proporcional apta a avaliação independente nas condições legais de acesso. Esse encargo não exonera a autoridade do ônus de demonstrar a infração, não cria inversão judicial automática nem autoriza sanção baseada apenas em incerteza. O caso ANPD–Discord, sem decisão de mérito na data de corte, ilustra a centralidade da instrução documental. Como contribuição, propõe-se matriz de nove dimensões que explicita o núcleo jurídico vigente, os instrumentos interpretativos ou propostos e as salvaguardas aplicáveis.

Palavras-chave: ECA Digital; segurança demonstrável; encargo regulatório residual de produção; auditoria de plataformas; direitos de crianças e adolescentes.

Abstract: This article examines who must produce the safety evidence required to supervise digital products and services accessible to children and adolescents. Using doctrinal, comparative-functional, and documentary legal methods, it reconstructs the framework formed by the Constitution, comprehensive child-protection law, Brazil's Digital Statute of the Child and Adolescent (ECA Digital), and its implementing rules, distinguishing the proper scope of the National Data Protection Agency's LGPD procedure from the statute's transitional procedural gaps. The analysis separates four categories: substantive safety duties; positive documentation and cooperation duties; a residual regulatory burden of production; and the procedural burden of proof. "Demonstrable safety" is an interpretive synthesis, not statutory wording. Because providers control system architecture, data, and records, they should produce proportionate evidence enabling independent assessment under legally defined access conditions. This burden does not relieve the authority of proving the alleged infringement, create an automatic reversal of the judicial burden of proof, or permit sanctions based solely on uncertainty. The ANPD–Discord case, still without a merits decision at the cutoff date, illustrates the central role of documentary fact-finding. The article proposes a nine-dimension matrix that makes explicit the applicable positive-law core, interpretive or proposed instruments, and safeguards.

Keywords: ECA Digital; demonstrable safety; residual regulatory burden of production; platform auditing; children's rights.

[1]Advogado e pesquisador independente. São Paulo, SP, Brasil. E-mail: jandislei.genova@gmail.com. Site: https://jandisleigenova.com.

1 INTRODUÇÃO

A pergunta do título é alocativa, não retórica. Em sistemas digitais, quem projeta a arquitetura também escolhe quais eventos serão registrados, quais indicadores serão destacados, quais grupos serão agregados e quais falhas permanecerão invisíveis. Se a mesma organização define o risco, seleciona a métrica, conduz o teste e oferece a conclusão, a conformidade pode tornar-se epistemicamente fechada: terceiros não conseguem reconstruir o caminho entre a alegação de segurança e os dados que supostamente a sustentam. O problema jurídico não é apenas se o fornecedor declara observar a lei, mas se sua afirmação pode ser testada e contraditada por evidência independente.

A questão tornou-se imediata no Brasil com a vigência, em 17 de março de 2026, da Lei nº 15.211/2025, conhecida como ECA Digital. O diploma alcança fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e adolescentes ou de acesso provável por eles, e não apenas plataformas em sentido estrito. “Plataforma”, no título, é síntese comunicativa do problema mais amplo: o controle privado sobre arquitetura, métricas e registros relevantes para a supervisão pública.

A prática institucional inicial confirma a centralidade da prova. Em junho de 2026, no monitoramento de lojas de aplicações e sistemas operacionais, a Agência Nacional de Proteção de Dados (ANPD) requisitou informações e documentos sobre arquitetura, fluxos de dados, mecanismos de aferição etária, políticas internas e outros elementos aptos a demonstrar conformidade (ANPD, 2026a). Em 7 de agosto, a Agência instaurou o processo de fiscalização nº 00261.004804/2026-54 para apurar indícios relacionados ao Discord e concedeu cinco dias úteis para que a empresa apresentasse seus mecanismos de proteção (ANPD, 2026b; ANPD, 2026c). A instauração não equivale a constatação de infração: na data de corte, inexistia decisão de mérito. O episódio serve apenas como caso contemporâneo de instrução dependente de informações que estão, em grande parte, sob domínio do regulado.

O problema de pesquisa é o seguinte: como o direito brasileiro pode impedir que o fornecedor controle simultaneamente a definição, a medição e a prova de sua própria segurança sem presumir ilicitude, exigir risco zero ou substituir o devido processo? A pergunta se desdobra em cinco: quem fixa os parâmetros de segurança; qual evidência é materialmente adequada; quem a verifica; como grupos afetados e instituições independentes podem contestá-la; e que efeitos jurídicos podem decorrer de demonstração insuficiente.

A hipótese possui dois níveis, cada um com estatuto explícito. No primeiro, propõe-se uma reconstrução interpretativa: a combinação entre prevenção, segurança desde a concepção, gestão de riscos, documentação, monitoramento e transparência permite descrever uma

dimensão demonstrável dos deveres materiais do ECA Digital. A lei não emprega a locução "dever de segurança demonstrável"; a categoria sintetiza comandos positivos dispersos. No segundo nível, sustenta-se que a assimetria informacional justifica um encargo regulatório residual de produção: para sustentar determinada alegação de conformidade ou a adequação de uma alternativa técnica, quem controla os meios probatórios suporta o risco de não apresentar suporte verificável. Esse encargo residual convive com deveres documentais expressos e não se confunde com o ônus processual da prova.

O método é jurídico-dogmático, comparativo-funcional e documental. A etapa dogmática reconstrói a cadeia de premissas normativas do regime brasileiro e separa texto vigente, interpretação, boa prática técnica e proposta regulatória. A etapa comparativa seleciona instrumentos europeus pela função — avaliação de risco, auditoria, acesso a dados e prestação de contas — e registra os limites de equivalência institucional. A etapa documental examina atos e comunicações oficiais da ANPD e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD). Para a busca de anterioridade, foram consultados Google Scholar, SciELO, Biblioteca Digital Brasileira de Teses e Dissertações (BDTD) e SSRN, além de buscas por domínio, em português, inglês, espanhol e francês. O protocolo, as expressões, os critérios de inclusão e as limitações constam do Apêndice A. O corte temporal é 9 de agosto de 2026.

O corpus normativo compreende as fontes brasileiras e europeias integralmente enumeradas nas referências. O corpus documental inclui o relatório do Painel Especial Europeu, o relatório do GT2 do CNPD, orientações e atos da ANPD e as peças públicas do processo Discord. A literatura foi selecionada por pertinência direta a ônus da prova, processo administrativo sancionador, regulação baseada em risco, direitos da criança no ambiente digital, avaliações de impacto, *safety cases* e auditoria algorítmica. Foram excluídos resultados meramente promocionais, duplicados e textos sem relação funcional com demonstrabilidade ou alocação de produção informacional.

A contribuição é deliberadamente delimitada. A ideia de conformidade demonstrável antecede o ECA Digital: aparece na *accountability* da proteção de dados, em avaliações de impacto, na regulação de riscos sistêmicos e nos *assurance cases*. O CNPD já empregou a expressão "ônus argumentativo permanente" para a compatibilidade de fluxos de dados com o livre desenvolvimento de crianças e adolescentes (CNPD, 2026, p. 11). Ribera Martínez (2025) identifica transferência regulatória do ônus de produção informacional; Gilly (2026), em contexto constitucional norte-americano distinto, propõe deveres de verificação para distribuidores de plataformas. A originalidade aqui reivindicada é mais estreita: reconstruir o

problema no ECA Digital, estabilizar quatro categorias dogmáticas e convertê-las em matriz operacional com estatuto normativo declarado. O argumento prolonga, em ponto específico, investigação anterior sobre autonomia decisória e condicionamento arquitetural (Genova, 2026), sem pretender transformar obra do autor em fundamento de autoridade.

2 A EXPERIÊNCIA EUROPEIA: FUNÇÕES COMPARÁVEIS, REGIMES DISTINTOS

Em julho de 2026, os copresidentes do Painel Especial da Comissão Europeia sobre Segurança Infantil Online apresentaram o relatório *Child Safety Online: Protecting and Empowering Minors in a Digital World*. O documento formula duas recomendações relacionadas, mas não idênticas. Uma é específica: enquanto os provedores não demonstrarem que seus serviços são seguros desde a concepção, o acesso deveria ser restringido para crianças abaixo de treze anos (Comissão Europeia, 2026a, p. 5 e 108). A outra é geral e prospectiva: provedores deveriam demonstrar que produtos, serviços e novas funcionalidades são seguros para menores, inclusive antes da disponibilização no mercado (Comissão Europeia, 2026a, p. 18, 76 e 100).

Essa precisão importa. A primeira recomendação combina demonstração e limitação etária; a segunda projeta um modelo de controle anterior e contínuo. Nenhuma delas, em 9 de agosto de 2026, constituía regulamento, diretiva, decisão vinculante ou proposta legislativa formal. O painel era consultivo, e o relatório dos copresidentes destinava-se a informar ações posteriores da Comissão e dos Estados-membros (Comissão Europeia, 2026b). Seu valor para o Brasil é heurístico: torna explícita a ideia de que famílias e autoridades não deveriam arcar sozinhas com a prova posterior da nocividade de sistemas opacos.

O Regulamento de Serviços Digitais (Digital Services Act — DSA) oferece o pano de fundo vinculante, mas não cria uma regra universal de certificação prévia. O artigo 28 impõe às plataformas acessíveis a menores medidas apropriadas e proporcionais para assegurar elevado nível de privacidade, segurança e proteção. Para plataformas e motores de busca de muito grande dimensão, os artigos 34 e 35 exigem avaliação periódica e mitigação de riscos sistêmicos; o artigo 37 prevê auditoria independente anual; o artigo 40 disciplina acesso a dados por autoridades e pesquisadores credenciados; e o artigo 42 exige publicidade de relatórios, com ressalvas justificadas. As Diretrizes da Comissão de 2025 detalham medidas relativas a design, recomendação, contato, governança e aferição etária (Comissão Europeia, 2025).

Na proteção de dados, os artigos 5º, item 2, e 24 do Regulamento Geral sobre a Proteção de Dados (GDPR) atribuem ao controlador responsabilidade e capacidade de

demonstrar conformidade; o artigo 25 disciplina proteção de dados desde a concepção e por padrão; e o artigo 35 exige avaliação de impacto em tratamentos de alto risco. No Reino Unido, o *Age Appropriate Design Code* organiza padrões para serviços provavelmente acessados por crianças, entre eles melhor interesse, avaliação de impacto, alta privacidade por padrão, minimização e limites a técnicas de indução (ICO, 2020). Esses instrumentos não certificam segurança integral: incidem prioritariamente sobre dados pessoais ou sobre categorias específicas de intermediários.

O quadro comparativo registra funções e, simultaneamente, impede equivalências excessivas.

Quadro 1 — Equivalências funcionais e limites da comparação

Instrumento	Função comparável	Limite de equivalência com o ECA Digital
Relatório do Painel Especial de 2026	Recomenda deslocar aos provedores a demonstração de segurança, inclusive antes de lançamento, e restringir acesso de menores de treze anos enquanto ausente a demonstração	Fonte consultiva, não vinculante; critérios, procedimento e efeitos ainda dependem de decisão política e legislação
DSA, art. 28	Proteção proporcional de menores por plataformas acessíveis a eles	Dever amplo, mas não equivale a auditoria anual ou acesso a dados para todos os fornecedores
DSA, arts. 34–37, 40 e 42	Avaliação e mitigação de riscos, auditoria, acesso a dados e transparência	Regime reforçado concentrado em plataformas e buscadores de muito grande dimensão
GDPR, arts. 5º, 24, 25 e 35	*Accountability*, proteção desde a concepção e avaliação de impacto	Objeto principal é tratamento de dados pessoais, não toda a segurança infantojuvenil
Children's Code britânico	Padrões de design e privacidade adequados à idade	Código de proteção de dados em contexto jurídico e institucional próprio

Fonte: elaboração própria.

A comparação permite importar perguntas, não respostas prontas. Quatro funções são úteis: alocar a produção informacional a quem controla o sistema; exigir documentação produzida durante o ciclo de vida, e não apenas depois da fiscalização; combinar auditoria, pesquisa e transparência em níveis de acesso; e preservar a decisão final da autoridade. A transposição termina onde começam diferenças de competência, âmbito subjetivo, procedimento e sanção. A recomendação europeia não é fonte normativa brasileira nem resolve, por si, qual risco é aceitável ou como evitar que a aferição etária produza vigilância desproporcional.

3 A CADEIA NORMATIVA BRASILEIRA E SEUS LIMITES

A reconstrução parte de premissas em níveis. No primeiro, a Constituição e o Estatuto da Criança e do Adolescente fornecem os vetores gerais. O artigo 227 da Constituição impõe à família, à sociedade e ao Estado proteção com absoluta prioridade. Os artigos 4º e 70 do

Estatuto distribuem deveres de garantia e prevenção; os artigos 71 a 73 vinculam produtos, serviços, informação, cultura e lazer à condição peculiar de pessoa em desenvolvimento. Esses comandos qualificam a interpretação, mas não substituem a identificação de deveres específicos, sujeitos obrigados e consequências.

No segundo nível, diplomas setoriais oferecem fundamentos parciais. O Código de Defesa do Consumidor disciplina qualidade e segurança quando há relação de consumo. O artigo 6º, VIII, admite inversão judicial do ônus da prova sob pressupostos próprios; o artigo 14 trata da responsabilidade por defeito do serviço e de suas excludentes; e os artigos 36 a 38 exigem suporte fático da publicidade. A aproximação da prova a quem domina a cadeia técnica não autoriza uma inversão geral fora dessas hipóteses.

A Lei Geral de Proteção de Dados Pessoais (LGPD) incide quando há tratamento de dados pessoais. O artigo 6º, X, define responsabilização e prestação de contas como demonstração de medidas eficazes e capazes de comprovar observância; o artigo 14 impõe o melhor interesse no tratamento de dados de crianças e adolescentes; e o artigo 42, § 2º, permite inversão judicial em favor do titular mediante decisão fundamentada e requisitos legais. A LGPD fornece demonstrabilidade material e regra processual condicionada, mas não cobre todo risco digital nem mistura esses planos.

No terceiro nível, o ECA Digital densifica deveres próprios. O artigo 1º define incidência sobre produtos e serviços de tecnologia da informação direcionados ou de acesso provável por crianças e adolescentes. O artigo 3º exige medidas adequadas e proporcionais para assegurar elevado nível de privacidade, proteção de dados e segurança, sob o parâmetro do melhor interesse. O artigo 5º estabelece deveres de prevenção, proteção, informação e segurança. O artigo 6º determina medidas razoáveis, desde a concepção e ao longo da operação, para prevenir e mitigar riscos enumerados. O artigo 8º inclui gerenciamento de riscos de recursos, funcionalidades e sistemas e prevenção, por concepção e padrão, do uso compulsivo.

A lei cria deveres documentais delimitados. O artigo 12 exige de lojas de aplicações e sistemas operacionais medidas proporcionais, auditáveis e tecnicamente seguras para aferir idade ou faixa etária. O artigo 16 exige, em suas hipóteses, mapeamento de riscos ligados ao tratamento de dados de crianças e adolescentes, relatório de impacto, monitoramento e avaliação, com compartilhamento mediante requisição. O artigo 31 determina relatórios semestrais para provedores de aplicações que superem o patamar legal de usuários infantojuvenis e inclui métodos e resultados de avaliações de impacto e risco; seu parágrafo único prevê acesso gratuito a dados para pesquisa nos termos da lei.

O Decreto nº 12.880/2026 acrescenta critérios operacionais. Identifica expedientes de permanência compulsiva, descreve práticas manipulativas, estabelece salvaguardas para sistemas conversacionais e detalha segurança desde a concepção e por padrão. Seu artigo 47 exige avaliação de impacto sobre a segurança e a saúde de crianças e adolescentes e síntese pública, além de admitir que a ANPD discipline conteúdo mínimo, periodicidade, revisão e compartilhamento. A remissão do dispositivo ao artigo 31, caput, inciso VI, é tratada como aparente erro material, pois os métodos e resultados das avaliações constam do inciso VII; a análise preserva o texto vigente e se apoia cumulativamente no artigo 16 e no artigo 31, VII. O decreto torna a avaliação um processo de identificação, análise e tratamento de riscos, mas não define sozinho padrão universal de auditoria independente.[2]

A proporcionalidade também possui fundamento interno expresso. O artigo 39 do ECA Digital determina que diversas obrigações sejam moduladas conforme características e funcionalidades do serviço, grau de interferência do fornecedor, número de usuários e porte; os §§ 2º e 3º acrescentam capacidade de influência e critérios objetivos de intervenção. Esses parâmetros limitam tanto exigências documentais quanto eventual desenho regulatório.

3.1 Regime procedimental transitório e limites da Resolução nº 1/2021

A designação institucional é clara. O Decreto nº 12.622/2025 atribuiu à ANPD a função de autoridade administrativa autônoma do ECA Digital; a Lei nº 15.352/2026 transformou-a em agência reguladora; e o Decreto nº 12.881/2026 lhe conferiu competência para estabelecer processos e procedimentos de apuração e aplicação das sanções administrativas previstas no artigo 35. A competência para fiscalizar e sancionar, contudo, não resolve por si só qual rito deve ser observado.

O artigo 35, § 3º, do ECA Digital determina que a apuração de infrações e a aplicação das sanções se regerão pelas disposições do ECA sobre infrações administrativas. Os artigos 194 a 197 do ECA foram estruturados em torno de representação ou auto de infração, defesa e decisão da autoridade judiciária. A aplicação desse bloco ao processo administrativo da ANPD exige integração normativa e adaptação compatível com a nova competência, não simples transposição literal.

A Resolução CD/ANPD nº 1/2021 foi editada para fiscalizar o tratamento de dados e reprimir infrações à LGPD. Por isso, incide diretamente quando o fato examinado estiver em seu âmbito material. Em apurações fundadas exclusivamente no ECA Digital, ela não deve

[2] O art. 47 do Decreto nº 12.880/2026 remete ao art. 31, caput, inciso VI, da Lei nº 15.211/2025. O inciso VI trata de consentimento parental; os métodos e resultados das avaliações de impacto e risco constam do inciso VII. Até a data de corte, não foi localizada correção oficial. A análise trata a remissão como aparente erro material, sem alterar o texto vigente.

operar como fonte autônoma de tipificação, sanção ou ampliação de obrigações. Eventual utilização subsidiária de suas regras exige compatibilidade com o artigo 35, § 3º, prévia cognoscibilidade e fundamentação específica.

Enquanto não houver regulamento próprio, a Lei nº 9.784/1999 funciona como lei geral do processo administrativo federal: impõe legalidade, contraditório, ampla defesa, motivação e instrução de ofício. No âmbito em que a Resolução nº 1/2021 seja aplicável, seus artigos 5º, 6º, 48 e 50 reforçam cooperação, diligências e prova das alegações, sem dispensar a autoridade de demonstrar suficientemente a infração.

A própria ANPD reconhece a transição: seu cronograma prevê a atualização dos regulamentos de fiscalização e sanções do ECA Digital a partir de novembro de 2026. Até a data de corte, isso recomenda cautela com qualquer afirmação de rito consolidado, sem impedir monitoramento, orientação e medidas já sustentadas em base legal própria (ANPD, 2026d).

As competências sancionatórias também devem ser lidas sem expansão. O artigo 35 do ECA Digital prevê advertência e multa aplicáveis pela ANPD. Suspensão temporária e proibição de exercício das atividades são medidas de aplicação judicial, nos termos do § 5º. A autoridade pode fiscalizar, instruir, advertir e multar dentro das bases legais; não pode transformar a matriz proposta neste artigo em poder administrativo de impedir lançamentos sem norma habilitante. A proporcionalidade encontra apoio adicional no artigo 39 e nas competências de abordagem responsiva previstas no Decreto nº 12.881/2026.

Dessas premissas deriva uma conclusão intermediária. O direito vigente contém deveres materiais e documentais expressos, poderes de requisição e competência sancionatória delimitada. O procedimento específico do ECA Digital, porém, permanece em integração regulatória. “Segurança demonstrável” é o nome doutrinário da conexão funcional entre medida, registro, teste e fiscalização; não cria infração autônoma nem autoriza suprir lacunas procedimentais contra o regulado.

4 SEGURANÇA DESDE A CONCEPÇÃO COMO PROCESSO VERIFICÁVEL

Segurança desde a concepção não é atributo congelado no lançamento. Recursos de recomendação, contato, monetização, notificações, recompensas, chatbots e aferição etária mudam continuamente. Um produto pode iniciar com configuração protetiva e tornar-se mais arriscado depois de atualização, experimento ou mudança no perfil de uso. A unidade de análise deve ser o ciclo: identificar, priorizar, mitigar, testar, monitorar e corrigir.

Do direito vigente decorrem três exigências mínimas. A primeira é anterioridade razoável: os riscos previsíveis devem ser avaliados antes da implantação de funcionalidade relevante, sem prejuízo do monitoramento posterior. A segunda é proporcionalidade: gravidade, probabilidade, escala, reversibilidade e condição de desenvolvimento modulam a diligência. A terceira é adaptabilidade: incidentes, pesquisas e sinais de campo devem reabrir a avaliação. O artigo 6º e o artigo 8º do ECA Digital, combinados com o artigo 47 do Decreto, fornecem a base; a forma exata de cada teste depende do risco e da futura regulamentação.

As técnicas que seguem são boas práticas, não requisitos universais já positivados. Uma avaliação verificável pode registrar hipótese de dano, população exposta, método, amostra, limiares, incerteza, alternativas descartadas e risco residual. Testes pré e pós-implantação podem usar séries comparáveis, avaliações de acessibilidade, métodos qualitativos e, quando lícito e eticamente justificável, experimentos controlados. *Safety cases* organizam alegações, argumentos e evidências e permitem localizar saltos não sustentados (Kelly, 1998). Avaliações de impacto lembram que nenhum formulário compensa escopo estreito, participação tardia ou ausência de revisão (Watkins et al., 2021; Livingstone; Pothong, 2025).

A aferição etária ilustra a necessidade de equilíbrio. Um mecanismo pode reduzir exposição de menores e, ao mesmo tempo, aumentar coleta de dados, excluir usuários sem documentação ou criar pontos de vigilância. A ANPD recomenda abordagem baseada em risco, proporcionalidade, minimização, acurácia, segurança e possibilidade de revisão, e esclarece que a solução deve ser adequada ao contexto, não necessariamente idêntica para todos os serviços (ANPD, 2026e; ANPD, 2026f). A evidência pertinente inclui taxas de falso positivo e falso negativo, desempenho por faixa etária, dados coletados, retenção, alternativas de contestação e riscos de exclusão.

A participação de crianças e adolescentes integra a qualidade da avaliação, mas exige protocolo ético. O Comentário Geral nº 25 afirma que sua visão deve informar políticas e práticas digitais e que informação e mecanismos de reclamação precisam ser adequados à idade (ONU, 2021). Participação não significa expor menores a funcionalidades nocivas para produzir prova, transferir-lhes a responsabilidade por descobrir falhas ou extrair depoimentos sem consentimento, proteção e finalidade definidos. Ela pode ocorrer por testes protegidos, consulta a organizações representativas, pesquisa aprovada e canais acessíveis de contestação.

A arquitetura probatória deve preservar material adverso. Relatórios que registram apenas testes favoráveis produzem viés de sobrevivência. Histórico de versões, experimentos interrompidos, incidentes, reclamações, achados divergentes e justificativas para rejeitar

alternativas são parte do contexto. Preservar não significa publicar tudo: significa manter rastreabilidade suficiente para que a autoridade distinga avaliação genuína de narrativa retrospectiva.

5 QUATRO CATEGORIAS QUE NÃO DEVEM SER CONFUNDIDAS

A palavra "ônus" é intuitiva, mas pode ocultar regimes jurídicos diversos. Na teoria processual, ônus designa a necessidade prática de agir no próprio interesse para alcançar vantagem ou evitar desvantagem; difere de dever exigível em interesse alheio (Buzaid, 1962; Didier Jr.; Braga; Oliveira, 2026). A precisão é decisiva porque o ECA Digital contém comandos vinculantes, enquanto parte da operacionalização defendida neste artigo é interpretativa ou propositiva.

O primeiro plano é o dever material. Prevenir e mitigar riscos, adotar configurações protetivas, gerenciar recursos e evitar desenho compulsivo são condutas exigidas pela lei. Seu descumprimento pode constituir infração se estiverem presentes tipicidade, competência, imputação e demais requisitos aplicáveis. O fornecedor não apenas perde uma vantagem argumentativa: viola, em tese, um comando.

O segundo plano reúne deveres positivos de documentação e cooperação. Onde a lei, o decreto ou ato materialmente aplicável exige relatório, registro, informação, retenção, acesso ou atendimento à requisição, também há dever. A omissão pode ter consequência própria, inclusive caracterizar obstrução no âmbito efetivamente coberto pela Resolução nº 1/2021. Esses deveres não devem ser rebatizados como "ônus", pois isso enfraqueceria sua exigibilidade.

O terceiro é a categoria proposta neste artigo: encargo regulatório residual de produção. Nem todo artefato tecnicamente útil está enumerado em lei. Quando o fornecedor sustenta que uma métrica alternativa é equivalente, que uma mitigação foi efetiva ou que determinado acesso geraria risco concreto, ele suporta o risco regulatório de não oferecer suporte verificável para sua própria alegação. "Justificar", aqui, significa explicitar premissas, critérios, limites e rastreabilidade; não transferir ao regulado o poder de persuasão final. A autoridade pode rejeitar a alegação sem suporte, mas continua obrigada a instruir e provar os fatos constitutivos da infração que pretenda sancionar.

O quarto é o ônus processual da prova. No processo judicial ou administrativo, sua distribuição decorre de normas próprias. O artigo 373 do Código de Processo Civil, o artigo 6º, VIII, e o artigo 14 do Código de Defesa do Consumidor, o artigo 42, § 2º, da LGPD, a Lei nº 9.784/1999, o artigo 35, § 3º, do ECA Digital e a Resolução nº 1/2021, quando

materialmente aplicável, operam em âmbitos e com pressupostos distintos. A categoria regulatória proposta não altera silenciosamente nenhuma dessas regras.

Quadro 2 — Categorias dogmáticas do modelo probatório

Categoria	Natureza	Fonte típica	Efeito da inércia ou do descumprimento	Decisor
Dever material de segurança	Comando vinculante sobre concepção e operação	ECA Digital, especialmente arts. 5º, 6º e 8º	Apuração de infração e medida prevista em lei, com devido processo	ANPD dentro de sua competência; Judiciário nas medidas reservadas
Dever positivo de documentação e cooperação	Conduta exigível de registrar, preservar, informar ou permitir acesso	ECA Digital, arts. 12, 16 e 31; Decreto nº 12.880/2026, art. 47; ato procedimental aplicável	Complementação, apuração de omissão ou obstrução e consequência legal específica	ANPD, com controle judicial
Encargo regulatório residual de produção	Risco de não sustentar alegação técnica ou alternativa proposta pelo regulado	Reconstrução interpretativa baseada em controle probatório e assimetria informacional	Alegação pode ser desconsiderada; autoridade ainda deve instruir e provar eventual infração	Autoridade motivadamente; revisão judicial
Ônus processual da prova	Regra de julgamento e distribuição de risco probatório no processo	CPC, CDC, LGPD, art. 35, § 3º, do ECA Digital, Lei nº 9.784/1999 e Resolução nº 1/2021, quando materialmente aplicável	Consequência sobre fato controvertido individualizado, nunca presunção global automática	Juiz ou autoridade competente, com contraditório

Fonte: elaboração própria.

O título emprega “encargo regulatório residual de produção” porque essa categoria designa apenas o espaço ligado a alegações e escolhas sob domínio informacional do fornecedor. Parte da produção é dever positivo; outra parte integra o ônus processual disciplinado por normas próprias. A separação evita tanto a subproteção — tratar dever como faculdade — quanto a sobre-extensão — transformar assimetria em presunção de culpa.

6 DO DEVER DEMONSTRÁVEL AO ENCARGO RESIDUAL DE PRODUÇÃO

Define-se segurança demonstrável como a qualidade verificável de um processo pelo qual o fornecedor identifica riscos previsíveis, escolhe medidas proporcionais, registra critérios e alternativas, testa efetividade, monitora efeitos e corrige falhas ao longo do ciclo de vida. Trata-se de síntese interpretativa dos deveres do ECA Digital, não de padrão autônomo de responsabilidade civil ou garantia de ausência de dano.

O encargo residual de produção é mais estreito: diante de uma alegação técnica relevante cuja base permanece sob controle predominante do fornecedor, cabe a ele produzir e explicar evidência suficiente para que a autoridade avalie essa alegação. O encargo se apoia em quatro razões. A primeira é controle probatório: arquitetura, logs, experimentos e versões não estão ordinariamente disponíveis a crianças ou ao Estado. A segunda é prevenção: esperar

o dano pode tornar irreversível a afetação. A terceira é menor custo informacional: quem opera o sistema consegue documentá-lo com custo marginal inferior. A quarta é contestabilidade: a evidência precisa permitir teste por fonte distinta daquela que formulou a conclusão.

O conteúdo mínimo varia conforme o risco, mas pode ser organizado em sete campos: alegação de segurança; evidência que a suporta; responsável por produzi-la; verificador; momento e frequência; nível de acesso e publicidade; e efeito jurídico possível da insuficiência. Os campos não são checklist de conformidade. Uma alegação pode ser inadequada mesmo acompanhada de muitos documentos, e a ausência de um artefato proposto neste artigo não é infração sem base normativa.

6.1 Anterioridade e originalidade delimitada

A busca descrita no Apêndice A não localizou uso consolidado da locução exata "ônus regulatório de segurança demonstrável" como categoria do direito digital infantil brasileiro. Esse resultado é exploratório, depende de indexação e não prova inexistência universal. Quatro antecedentes funcionais foram retidos por proximidade: o "ônus argumentativo permanente" do CNPD (2026, p. 11); a transferência do ônus de produção descrita por Ribera Martínez (2025); a recomendação do Painel Especial Europeu (Comissão Europeia, 2026a); e o dever de verificação de distribuidores formulado por Gilly (2026).

As diferenças são substantivas. Ribera Martínez analisa leis digitais europeias e separa *burden of production* de *burden of persuasion*. Gilly se concentra na classificação e distribuição de plataformas em contexto constitucional norte-americano. O painel formula recomendação política abrangente. O CNPD trabalha principalmente com proteção de dados e devido processo informacional. Nenhum desses antecedentes, isoladamente, produz a reconstrução quadripartida aqui proposta para o ECA Digital.

Também há anterioridade técnica. *Safety cases* estruturam alegação, argumento e evidência (Kelly, 1998). Avaliações de impacto organizam antecipação e revisão; auditorias algorítmicas procuram testar governança, processo e resultados (Raji et al., 2020; Costanza-Chock; Raji; Buolamwini, 2022; Lam et al., 2024). A contribuição do artigo é jurídica e operacional: conectar essas técnicas a bases normativas brasileiras, declarar onde termina o direito vigente e impedir que demonstração seja confundida com autocertificação.

6.2 Consequências juridicamente possíveis

No direito vigente, cada consequência deve ser vinculada a base específica. A ANPD pode requisitar complemento e realizar diligências dentro de sua competência; pode avaliar se

houve violação de dever material ou documental; e, depois de contraditório e decisão motivada, aplicar advertência ou multa nos limites do artigo 35. Enquanto o rito específico estiver em integração, a autoridade deve identificar expressamente as normas procedimentais empregadas. Suspensão temporária e proibição de exercício das atividades dependem de aplicação judicial. A falta de suporte para uma alegação técnica permite que ela não seja acolhida, mas não prova automaticamente dano, nexo causal, dolo ou todas as elementares de uma infração.

Em juízo, retenção injustificada de evidência pode repercutir na exibição de documentos, na distribuição dinâmica quando cabível, na inversão legalmente autorizada e na valoração do conjunto probatório. O juiz deve individualizar o fato controvertido, a capacidade de produção e o efeito. O encargo regulatório pode aumentar a disponibilidade de evidência; não reescreve as regras de responsabilidade civil.

Medidas como aprovação prévia geral de lançamentos, auditoria independente anual para todo fornecedor, suspensão administrativa de funcionalidade e credenciamento universal de pesquisadores são propostas regulatórias, não descrições do direito atual. Elas exigem análise de competência, proporcionalidade, custo e desenho procedimental. A matriz as identifica pela classe “D”, evitando que recomendação apareça como comando já vigente.

7 AUTOAVALIAÇÃO PRIVADA E AUTONOMIA COGNITIVA DO REGULADOR

Autoavaliação é inevitável e útil. O fornecedor conhece o sistema, pode detectar incidentes cedo e deve incorporar segurança ao processo decisório. O risco surge quando relatório interno, métrica proprietária ou auditoria contratada funciona como conclusão autossuficiente, sem critério público, acesso suficiente ou possibilidade de contradita. “Autocertificação”, neste artigo, descreve esse efeito de fechamento; não um instituto geral criado pelo ECA Digital.

A independência do auditor não se resume a ausência formal de vínculo. Exige escopo não capturado pelo cliente, competência, acesso a material adverso, liberdade para registrar ressalvas, rotação proporcional e transparência sobre conflitos. Auditorias podem falhar por seleção do objeto, restrição de dados, materialidade estreita ou dependência econômica. Por isso, o parecer é fonte probatória, não decisão jurídica (Costanza-Chock; Raji; Buolamwini, 2022; Lam et al., 2024).

O regulador também precisa de autonomia cognitiva: capacidade de formular perguntas, obter fontes plurais, reproduzir amostras e decidir sem depender exclusivamente da taxonomia do regulado. Não se afirma captura institucional no sentido clássico. A expressão

designa dependência operacional de categorias e métricas que a própria empresa escolheu. Equipes técnicas, cooperação com universidades, procedimentos de acesso seguro e interoperabilidade de registros reduzem essa dependência.

Pesquisadores e organizações representativas acrescentam contestação, mas não substituem a autoridade. O acesso previsto no artigo 31, parágrafo único, do ECA Digital e detalhado pelo Decreto depende de credenciamento e salvaguardas. Crianças e adolescentes devem participar em formatos adequados à idade e ao risco, sem exposição indevida. A decisão final sobre licitude, medida e sanção permanece pública e motivada.

8 MATRIZ OPERACIONAL COM ESTATUTO NORMATIVO

A matriz abaixo transforma o argumento em perguntas verificáveis. Cada linha separa o núcleo jurídico vigente — marcado como “A” — das formas probatórias interpretativas (“B”), das boas práticas técnicas (“C”) e das propostas regulatórias (“D”). A separação evita que um único rótulo se projete sobre toda a linha. A coluna final não cria sanções: registra efeitos juridicamente possíveis e identifica os que dependem de nova norma.

Quadro 3 — Matriz operacional de demonstração de segurança

Dimensão	Alegação a testar	Núcleo jurídico vigente (A)	Forma probatória e estatuto (B/C/D)	Produção, verificação e acesso	Efeito possível da insuficiência
Inventário de riscos	Riscos previsíveis e populações expostas foram identificados.	Lei nº 15.211/2025, arts. 6º, 8º, I, 16 e 31, VII; Decreto nº 12.880/2026, art. 47.	B/C: taxonomia, cenários, fontes, incidentes, hipóteses descartadas e risco residual. D: validação externa geral ou aprovação prévia.	Fornecedor documenta; ANPD instrui e requisita nos limites legais; síntese pública e dossiê protegido conforme a base.	Complementação ou apuração de dever específico. Alegação sem suporte pode ser desconsiderada; aprovação prévia geral exige norma.
Probabilidade e gravidade	A priorização considera desenvolvimento, escala, probabilidade, reversibilidade e gravidade.	Lei nº 15.211/2025, arts. 3º, 5º, 6º, 8º e 39; Decreto nº 12.880/2026, art. 47.	B/C: método, amostra, limiares, incerteza e recortes etários pertinentes; não há fórmula universal positivada.	Fornecedor produz; autoridade ou especialista testa o método; publicidade apenas no grau legalmente exigido.	Requisitar esclarecimento ou novo teste. Sanção somente por infração individualizada e suficientemente demonstrada.
Escolha da mitigação	A medida é adequada e alternativas razoáveis foram consideradas.	Lei nº 15.211/2025, arts. 5º, 6º, 8º e 39; Decreto nº 12.880/2026, arts. 14 e 47.	B/C: decisão de design, alternativas, testes, limites e risco residual. D: aprovação externa prévia como regra geral.	Fornecedor registra o racional; ANPD verifica implementação e proporcionalidade; dossiê pode ter acesso restrito.	Correção dentro da competência legal; alegação de equivalência sem suporte pode ser rejeitada. Aprovação geral depende de norma.
Efetividade	A mitigação reduz o risco sem simples deslocamento do dano.	Lei nº 15.211/2025, arts. 6º, 16 e 31, VII; Decreto nº 12.880/2026, art. 47.	B/C: séries comparáveis, métricas adversas, método qualitativo e limitações. D: reprodução externa obrigatória em todo caso.	Fornecedor monitora; autoridade pode requisitar evidência; acesso independente depende da base e de salvaguardas.	Atualizar avaliação e corrigir violação. Alegação publicitária sem suporte sujeita-se ao regime aplicável do CDC.
Impactos diferenciados	A solução não agrava riscos para grupos específicos.	CF, art. 227; ECA, arts. 4º e 70 a 73; Lei nº 15.211/2025, arts. 3º a 6º; legislação antidiscriminatória aplicável.	B/C: testes de acessibilidade e análises por idade, deficiência e contexto, quando lícitos. D: recortes universais sem pertinência demonstrada.	Fornecedor produz; especialistas e grupos participam sob protocolo ético, seguro e proporcional.	Mitigação específica quando houver base. Exigência universal de recortes depende de pertinência e competência.
Monitoramento e correção	Incidentes são detectados, escalados, preservados e corrigidos.	Lei nº 15.211/2025, arts. 6º, 16, 31 e 34; Decreto nº 12.880/2026, art. 47; Resolução nº 1/2021 somente em seu âmbito material.	B/C: logs, alertas, prazos, histórico de versões, análise de causa e verificação pós-correção.	Fornecedor preserva; ANPD requisita amostras segundo base específica, finalidade, segurança e sigilo.	Diligência, complementação ou sanção se comprovada infração. Medida cautelar requer habilitação legal e motivação.
Auditoria	O exame cobre risco material com independência, competência e acesso suficientes.	Lei nº 15.211/2025, art. 12, e Decreto nº 12.880/2026, art. 24, XI, para aferição etária; LGPD e Decreto nº 12.881/2026, Anexo I, art. 2º, XVI, para tratamento de dados.	C: escopo, critérios, conflitos, amostra, limitações e resposta gerencial. D: auditoria independente geral ou anual para todo fornecedor.	Auditor produz parecer no escopo aplicável; ANPD preserva autonomia decisória; papéis de trabalho seguem níveis de acesso.	Parecer insuficiente pode ser desconsiderado. Auditoria complementar exige base; periodicidade geral depende de norma.
Contestação	Usuários podem questionar decisões abrangidas por dever legal de revisão.	Lei nº 15.211/2025, art. 30, para remoção de conteúdo; Decreto nº 12.880/2026, art. 25, § 2º, III, e art. 27, para aferição etária.	C: canal acessível, protocolo, prazo, motivação e registro de reversões. D: recurso técnico universal para toda avaliação.	Fornecedor mantém os canais exigidos; autoridade testa desempenho e acessibilidade dentro do escopo legal.	Correção do canal ou apuração da obrigação específica. Modelo universal depende de regulação própria.
Transparência	A síntese permite compreender risco, medida, resultado e limites sem exposição indevida.	Lei nº 15.211/2025, arts. 16 e 31, VII; Decreto nº 12.880/2026, art. 47.	C: versionamento, histórico, indicadores comparáveis e linguagem acessível. D: formato uniforme ampliado a todos os fornecedores.	Fornecedor publica a síntese legal; ANPD pode requisitar complemento; dados protegidos seguem acesso em camadas.	Retificação ou complementação; apuração de omissão material. Padronização adicional depende de norma competente.

Fonte: elaboração própria.

8.1 Acesso em três níveis

O primeiro nível é regulatório. A ANPD recebe documentos e dados necessários à fiscalização nos limites da competência e da requisição, sob regras de segurança e sigilo. Não se presume acesso irrestrito a "todo o sistema": pertinência, finalidade e proporcionalidade devem ser motivadas. A Resolução nº 1/2021 admite pedido de sigilo e limita as requisições ao exercício efetivo das atribuições, mas essas regras incidem diretamente apenas em seu âmbito material; fora dele, o acesso deve apoiar-se no ECA Digital, em sua regulamentação e na legislação administrativa aplicável.

O segundo nível é qualificado. Pesquisadores credenciados podem acessar dados nas condições do artigo 31, parágrafo único, e do artigo 48 do Decreto. A extensão desse nível a auditores independentes, peritos e organizações representativas pode ser útil, mas depende de base, credenciamento, minimização, ambiente controlado, logs e proibição de reidentificação.

O terceiro nível é público. A lei e o decreto já preveem informação a responsáveis, relatórios semestrais em hipóteses delimitadas e síntese pública de avaliação. Boas práticas incluem versionamento, linguagem adequada à idade, descrição de limites e indicadores comparáveis. Publicidade não é dumping de dados: deve permitir compreensão sem expor crianças, segurança do sistema ou segredo comercial legítimo.

8.2 Governança e proporcionalidade

A ANPD pode desenvolver taxonomias, modelos e protocolos dentro de sua competência regulamentar, observadas participação, análise de impacto, intervenção mínima e proporcionalidade. Um núcleo comum melhora comparação; módulos por serviço evitam que redes sociais, jogos, lojas de aplicações, sistemas operacionais e IA generativa sejam avaliados por métrica idêntica. Fornecedor que proponha alternativa deve explicar equivalência, limites e meio de validação — aplicação típica do encargo residual.

Metadados de versão, período, população, alteração metodológica e incerteza evitam comparações artificiais. Mudanças de métrica devem manter série histórica ou justificar ruptura. Indicadores não podem se tornar teto de proteção: sinais qualitativos e impactos raros, porém graves, exigem canais próprios. Regulação baseada em risco precisa responder ao comportamento do regulado e à performance do próprio instrumento, não apenas classificar o fornecedor uma vez (Black; Baldwin, 2010; OCDE, 2018).

9 LIMITES E SALVAGUARDAS

O primeiro limite é a inexistência de segurança absoluta. O objeto demonstrável é a diligência e a efetividade proporcional diante de riscos identificados e previsíveis, acompanhadas de incerteza e risco residual. Exigir prova de ausência universal de dano produziria paralisia ou documentação fictícia.

O segundo é a proporcionalidade regulatória. Pequenos fornecedores não devem reproduzir a estrutura de conglomerados globais. Modelos abertos, auditorias compartilhadas de componentes e cronogramas graduais podem reduzir custo. A diferenciação deve considerar risco, alcance, público e capacidade, não apenas faturamento: serviço pequeno exposto a dano grave pode justificar supervisão intensa (Black; Baldwin, 2010; OCDE, 2018).

O terceiro é a proteção de dados. Para provar que protege crianças, o fornecedor não pode criar base mais invasiva do que o risco exige. Minimização, agregação, retenção limitada, dados sintéticos quando adequados e ambientes seguros devem orientar a prova. A vedação do artigo 34 do ECA Digital a vigilância massiva, genérica ou indiscriminada limita tanto a solução privada quanto a fiscalização.

O quarto é o segredo empresarial. Fórmulas, pesos e estratégias antifraude podem merecer proteção. Isso justifica acesso em camadas, não imunidade à supervisão. O pedido de sigilo deve identificar o risco da divulgação; a autoridade deve motivar o tratamento e separar conteúdo público de material protegido.

O quinto é a qualidade da auditoria. Certificados genéricos, checklists adquiridos e escopos ditados pelo cliente podem criar falsa confiança. Independência, competência, materialidade, acesso, amostragem, achados divergentes e limitações precisam ser transparentes. O auditor não recebe delegação para definir direitos, risco aceitável ou sanção.

O sexto é a participação sem transferência de responsabilidade. Crianças, adolescentes, responsáveis e organizações podem revelar danos que métricas agregadas ocultam. Sua participação deve ser segura, inclusiva e eticamente governada. Não cabe a eles suportar o encargo de provar sozinhos falhas de arquiteturas que não controlam.

O sétimo é a não substituição do Estado. Padrões técnicos, co-regulação e auditorias ampliam capacidade, mas a decisão jurídica permanece pública. O Estado precisa de equipe, fontes plurais e possibilidade de reprodução para não enxergar o sistema apenas pelas métricas selecionadas pelo regulado.

O oitavo reúne garantias do processo administrativo sancionador. Enquanto o rito específico do ECA Digital estiver em integração, a autoridade deve indicar a norma procedimental aplicável e delimitar fato, período, base e formato da requisição; preservar

cadeia de custódia e integridade; admitir contraprova; enfrentar argumentos; e motivar a decisão. A instrução de ofício permanece dever público. O autuado prova os fatos que alega, mas a autoridade suporta a demonstração suficiente da conduta infrativa e de suas elementares. A insuficiência documental só gera efeito adverso próprio quando existe dever aplicável de produzir ou quando o regulado pretende sustentar uma alegação. Não há presunção irrefragável de culpa nem sanção por dúvida abstrata (Osório, 2025; Brasil, 1999; ANPD, 2021).

Sem pretender resolver neste artigo o alcance subjetivo e material do *nemo tenetur*, sustenta-se apenas que o encargo residual não autoriza compelir confissão nem dispensa a análise concreta da natureza, da origem e da finalidade do material requisitado. A exigibilidade de documentos preexistentes ou de registros associados a dever previamente constituído deve ser examinada à luz da base legal, do possível uso em outras esferas e das garantias do caso. Prova ilícita permanece inadmissível. Sigilo, acesso aos autos, assistência técnica e controle judicial completam o equilíbrio.

10 CONCLUSÃO

As conclusões de direito vigente são cinco. Primeira: o ECA Digital contém deveres materiais de prevenção, segurança, gestão de risco e configuração protetiva, além de deveres documentais em hipóteses delimitadas. Segunda: “segurança demonstrável” não é expressão literal da lei, mas reconstrução sistemática da conexão entre medida, registro, teste e fiscalização. Terceira: o artigo 39 exige modulação proporcional de parte relevante das obrigações. Quarta: a competência sancionatória da ANPD coexiste, nesta etapa, com a necessidade de integrar o artigo 35, § 3º, do ECA Digital, os artigos 194 a 197 do ECA, a Lei nº 9.784/1999 e o âmbito próprio da Resolução nº 1/2021; não há inversão automática do ônus da prova. Quinta: advertência e multa estão na esfera administrativa da ANPD, enquanto suspensão e proibição de atividades dependem de aplicação judicial.

A contribuição interpretativa é o encargo regulatório residual de produção. Quando a empresa formula alegação técnica baseada em dados, escolhas e registros sob seu controle — por exemplo, equivalência de métrica ou eficácia de mitigação —, ela suporta o risco de a alegação não ser acolhida se não oferecer suporte verificável. Esse encargo não substitui deveres documentais expressos nem exonera a autoridade de provar eventual infração.

As recomendações de política pública são separadas. A ANPD pode avaliar, dentro de sua competência, padronização proporcional de relatórios, taxonomias setoriais, interoperabilidade, critérios de auditoria, acesso seguro e versionamento. Auditoria anual

geral, aprovação prévia de lançamentos, suspensão administrativa de funcionalidade e extensão universal de acesso a terceiros exigem base normativa e análise própria; a matriz não as transforma em direito vigente.

O relatório europeu de 2026 torna visível a mesma intuição alocativa, mas permanece consultivo. DSA, GDPR, *Children's Code*, CNPD, literatura de regulação baseada em risco, avaliações de impacto, *safety cases* e auditoria oferecem antecedentes funcionais. A originalidade plausível do artigo está na reconstrução quadripartida para o ECA Digital e na matriz que identifica, em cada dimensão, o que é direito positivo, interpretação, boa prática ou proposta.

Quem prova que a plataforma é segura? O fornecedor cumpre deveres materiais e documentais e produz a evidência primária sob seu controle; auditores, pesquisadores e grupos afetados podem testá-la nas condições legais; a ANPD instrui e decide com autonomia; e o Judiciário controla competência, prova e medidas reservadas. A resposta não é uma certificação privada nem uma presunção pública de culpa. É uma arquitetura de demonstrabilidade contestável, proporcional e submetida ao devido processo.

APÊNDICE A — PROTOCOLO EXPLORATÓRIO DE BUSCA DE ANTERIORIDADE

A busca exploratória foi executada entre 8 e 9 de agosto de 2026, com corte final em 9 de agosto, nas bases Google Scholar, SciELO, BDTD e SSRN e por busca de domínio em repositórios institucionais. Foram empregados português, inglês, espanhol e francês. As expressões exatas foram: “ônus regulatório de segurança demonstrável”; “ônus de segurança demonstrável” plataforma; “regulatory burden of demonstrable safety” platform; “regulatory evidentiary burden” platform safety children; “carga regulatoria de seguridad demostrable” plataformas niños; “deber de seguridad demostrable” plataformas digitales menores; “charge réglementaire de sécurité démontrable” plateforme mineurs; e “obligation de sécurité démontrable” plateformes enfants. Buscas complementares combinaram burden of production, platform safety, children, age assurance, safety case, impact assessment e platform audit. O exercício não é revisão sistemática nem censo bibliométrico; seu objetivo é testar a ocorrência das locuções e identificar antecedentes funcionalmente próximos.

Foram incluídos trabalhos e documentos que: (a) alocassem ao fornecedor ou distribuidor a produção de informação sobre segurança ou conformidade; (b) estruturassem demonstração anterior ou contínua de risco; ou (c) tratassem de mecanismo funcionalmente equivalente de auditoria, avaliação de impacto ou assurance case. Foram excluídos duplicados, identificados por título, DOI ou URL; textos sem autoria ou origem identificável; páginas promocionais; resultados sobre segurança sem dimensão probatória; e estudos de idade sem relação com dever de verificação. As contagens dinâmicas das interfaces não foram usadas como evidência de inexistência ou originalidade.

Após a deduplicação, quatro antecedentes jurídicos ou institucionais foram retidos como mais próximos: CNPD (2026), Ribera Martínez (2025), Comissão Europeia (2026a) e Gilly (2026). A literatura técnica foi selecionada separadamente. Gilly (2026) é preprint/working draft sem revisão por pares. A busca dependeu de indexação, idioma, disponibilidade e estabilidade das interfaces. A ausência de ocorrência exata não prova ineditismo universal; sustenta apenas a formulação delimitada de originalidade apresentada no texto.

Quadro 4 — Registro mínimo da busca exploratória de anterioridade

Base ou repositório	Campo e estratégia	Limite de triagem	Antecedentes retidos
Google Scholar	Expressões exatas e combinações funcionais, em quatro idiomas, nos campos indexados pela plataforma.	Triagem por pertinência até cessarem novas categorias; contagens dinâmicas não foram usadas como prova de ausência.	Literatura técnica e jurídica de apoio; nenhum uso consolidado da locução exata localizado.
SciELO	Busca em todos os índices, com	Resultados relacionados ao problema e	Nenhum antecedente direto da

Base ou repositório	Campo e estratégia	Limite de triagem	Antecedentes retidos
	locuções exatas em português e espanhol e combinações sobre prova, segurança e plataformas.	à alocação informacional; deduplicação por título, DOI e URL.	categoria no recorte examinado.
BDTD	Busca em todos os campos, com locuções exatas e combinações em português.	Teses e dissertações com relação funcional a demonstrabilidade, auditoria ou ônus de produção.	Nenhum antecedente direto da categoria no recorte examinado.
SSRN	Título, resumo e palavras-chave, com combinações em inglês sobre burden of production, platform safety e age assurance.	Textos com argumento jurídico diretamente comparável; identificação separada do status editorial.	Ribera Martínez (2025) e Gilly (2026); este último é preprint/working draft sem revisão por pares.
Domínios institucionais	gov.br/anpd, commission.europa.eu e eur-lex.europa.eu, por título e termos funcionais.	Documentos oficiais pertinentes a prestação de contas, risco, auditoria, dados e segurança infantil.	CNPD (2026) e Comissão Europeia (2026a), além das fontes normativas de contexto.

Fonte: elaboração própria. A busca tem natureza exploratória e não constitui revisão sistemática.

REFERÊNCIAS

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **ANPD inicia monitoramento da adequação de lojas de aplicativos e sistemas operacionais ao ECA Digital**. Brasília, DF, 10 jun. 2026a. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/copy_of_anpd-monitoramento-lojas-de-aplicativos-sistemas-operacionais. Acesso em: 9 ago. 2026.

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **ANPD instaura processo de fiscalização contra o Discord para apurar falhas na proteção de crianças e adolescentes**. Brasília, DF, 7 ago. 2026b. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-instaura-processo-de-fiscalizacao-contra-o-discord-para-apurar-falhas-na-protecao-de-criancas-e-adolescentes. Acesso em: 9 ago. 2026.

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Despacho nº 0319773/2026/SFI/ANPD: processo nº 00261.004804/2026-54**. Brasília, DF, 7 ago. 2026c. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-instaura-processo-de-fiscalizacao-contra-o-discord-para-apurar-falhas-na-protecao-de-criancas-e-adolescentes/sei-processo-00261-004804_2026-54.pdf/@@display-file/file. Acesso em: 9 ago. 2026.

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **ECA Digital: cronograma**. Brasília, DF, 1 jun. 2026d. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/eca-digital. Acesso em: 9 ago. 2026.

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Mecanismos confiáveis de aferição de idade: orientações preliminares**. Brasília, DF, mar. 2026e. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/eca-digital/mecanismos-confiaveis-de-afericao-de-idade-orientacoes-preliminares.pdf/@@display-file/file. Acesso em: 9 ago. 2026.

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Perguntas e respostas sobre o ECA Digital**. Atualizado em 30 jul. 2026f. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/perguntas_respostas_eca_digital_18032026.pdf. Acesso em: 9 ago. 2026.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Resolução CD/ANPD nº 1, de 28 de outubro de 2021**. Aprova o Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da ANPD. Brasília, DF, 2021. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no1-2021. Acesso em: 9 ago. 2026.

BLACK, Julia; BALDWIN, Robert. Really responsive risk-based regulation. **Law & Policy**, Hoboken, v. 32, n. 2, p. 181–213, 2010. DOI: https://doi.org/10.1111/j.1467-9930.2010.00318.x.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 9 ago. 2026.

BRASIL. **Lei nº 8.069, de 13 de julho de 1990**. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Brasília, DF: Presidência da República, 1990a. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 9 ago. 2026.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Presidência da República, 1990b. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 9 ago. 2026.

BRASIL. **Lei nº 9.784, de 29 de janeiro de 1999**. Regula o processo administrativo no âmbito da Administração Pública Federal. Brasília, DF: Presidência da República, 1999. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9784.htm. Acesso em: 9 ago. 2026.

BRASIL. **Lei nº 13.105, de 16 de março de 2015**. Código de Processo Civil. Brasília, DF: Presidência da República, 2015. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105compilada.htm. Acesso em: 9 ago. 2026.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 9 ago. 2026.

BRASIL. **Lei nº 13.848, de 25 de junho de 2019**. Dispõe sobre a gestão, a organização, o processo decisório e o controle social das agências reguladoras. Brasília, DF: Presidência da República, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13848.htm. Acesso em: 9 ago. 2026.

BRASIL. **Decreto nº 12.622, de 17 de setembro de 2025**. Designa a ANPD como autoridade administrativa autônoma de proteção de crianças e adolescentes em ambientes digitais e estabelece competências para cumprimento de ordens judiciais de bloqueio. Brasília, DF: Presidência da República, 2025a. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/decreto/d12622.htm. Acesso em: 9 ago. 2026.

BRASIL. **Lei nº 15.211, de 17 de setembro de 2025**. Dispõe sobre a proteção de crianças e adolescentes em ambientes digitais (Estatuto Digital da Criança e do Adolescente). Brasília, DF: Presidência da República, 2025b. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/l15211.htm. Acesso em: 9 ago. 2026.

BRASIL. **Decreto nº 12.880, de 18 de março de 2026**. Regulamenta a Lei nº 15.211, de 17 de setembro de 2025. Brasília, DF: Presidência da República, 2026a. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/decreto/d12880.htm. Acesso em: 9 ago. 2026.

BRASIL. **Decreto nº 12.881, de 18 de março de 2026**. Aprova a Estrutura Regimental da Agência Nacional de Proteção de Dados. Brasília, DF: Presidência da República, 2026b. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/decreto/d12881.htm. Acesso em: 9 ago. 2026.

BRASIL. **Lei nº 15.352, de 25 de fevereiro de 2026**. Altera a LGPD para dispor sobre a Agência Nacional de Proteção de Dados e fixa a vigência do ECA Digital. Brasília, DF: Presidência da República, 2026c. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/lei/l15352.htm. Acesso em: 9 ago. 2026.

BUZAID, Alfredo. Do ônus da prova. **Revista da Faculdade de Direito, Universidade de São Paulo**, São Paulo, v. 57, p. 113–140, 1962. Disponível em: https://revistas.usp.br/rfdusp/article/viewFile/66398/69008. Acesso em: 9 ago. 2026.

COMISSÃO EUROPEIA. **Guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28(4) of Regulation (EU) 2022/2065**. Comunicação C/2025/6826. *Jornal Oficial da União Europeia*, C/2025/5519, 10 out. 2025. Disponível em: https://eur-lex.europa.eu/eli/C/2025/5519/oj/eng. Acesso em: 9 ago. 2026.

COMISSÃO EUROPEIA. **Child safety online: protecting and empowering minors in a digital world — Special Panel Report**. Bruxelas, 13 jul. 2026a. Disponível em: https://commission.europa.eu/document/download/d833504d-5ec3-4fac-945f-38e7d0bd5326_en?filename=Special-panel-report.pdf. Acesso em: 9 ago. 2026.

COMISSÃO EUROPEIA. **Special panel on child safety online**. Bruxelas, 2026b. Disponível em: https://commission.europa.eu/topics/digital-economy-and-society/special-panel_en. Acesso em: 9 ago. 2026.

CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE (CNPD). **Relatório consolidado do Grupo de Trabalho nº 2: proteção de dados de crianças e adolescentes**. Brasília, DF, 29 maio 2026. Disponível em: https://www.gov.br/anpd/pt-br/cnpd/grupos-de-trabalho/gt2-relatorio-final-cnpd.pdf/@@display-file/file. Acesso em: 9 ago. 2026.

COSTANZA-CHOCK, Sasha; RAJI, Inioluwa Deborah; BUOLAMWINI, Joy. Who audits the auditors? Recommendations from a field scan of the algorithmic auditing ecosystem. In: **ACM Conference on Fairness, Accountability, and Transparency (FAccT '22)**. New York: ACM, 2022. p. 1571–1583. DOI: https://doi.org/10.1145/3531146.3533213.

DIDIER JR., Fredie; BRAGA, Paula Sarno; OLIVEIRA, Rafael Alexandria de. **Curso de direito processual civil: teoria da prova, direito probatório, ações probatórias, decisão, precedente, coisa julgada e antecipação dos efeitos da tutela**. 21. ed. Salvador: JusPodivm, 2026. v. 2.

GENOVA, Jandislei Antonio. **Autonomia decisória na era da IA**. Belo Horizonte: Dialética, 2026.

GILLY, Travis. **The distributor's burden: platform verification duties, privacy-preserving age assurance, and the constitutional ceiling on online child-safety design**. Preprint/working draft não revisado por pares, versão 2, jul. 2026. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=7093359. Acesso em: 9 ago. 2026. DOI: https://doi.org/10.2139/ssrn.7093359.

INFORMATION COMMISSIONER'S OFFICE (ICO). **Age appropriate design: a code of practice for online services**. Wilmslow, [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: 9 ago. 2026.

KELLY, Timothy Patrick. **Arguing safety: a systematic approach to managing safety cases**. 1998. Thesis (Doctor of Philosophy) — Department of Computer Science, University of York, York, 1998.

LAM, Khoa et al. A framework for assurance audits of algorithmic systems. In: **ACM Conference on Fairness, Accountability, and Transparency (FAccT '24)**. New York: ACM, 2024. p. 1078–1092. DOI: https://doi.org/10.1145/3630106.3658957.

LIVINGSTONE, Sonia; POTHONG, Kruakae. Child rights impact assessment: a policy tool for a rights-respecting digital environment. **Policy & Internet**, Hoboken, v. 17, n. 3, e70008, 2025. DOI: https://doi.org/10.1002/poi3.70008.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). Comitê dos Direitos da Criança. **General Comment No. 25 (2021) on children's rights in relation to the digital environment**. Genebra, 2021. Disponível em: https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation. Acesso em: 9 ago. 2026.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO (OCDE). **OECD regulatory enforcement and inspections toolkit**. Paris: OECD Publishing, 2018. DOI: https://doi.org/10.1787/9789264303959-en.

OSÓRIO, Fábio Medina. **Direito administrativo sancionador**. 10. ed. São Paulo: Thomson Reuters Brasil, 2025.

RAJI, Inioluwa Deborah et al. Closing the AI accountability gap: defining an end-to-end framework for internal algorithmic auditing. In: **Conference on Fairness, Accountability, and Transparency (FAT* '20)**. New York: ACM, 2020. p. 33–44. DOI: https://doi.org/10.1145/3351095.3372873.

RIBERA MARTÍNEZ, Alba. The invisible burden: how digital regulations reverse the burden of proof. **European Business Organization Law Review**, artigo aceito, no prelo, 2025. Versão de autora disponível no SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5086779. Acesso em: 9 ago. 2026.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016** (Regulamento Geral sobre a Proteção de Dados). *Jornal Oficial da União Europeia*, L 119, 4 maio 2016. Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng. Acesso em: 9 ago. 2026.

UNIÃO EUROPEIA. **Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho, de 19 de outubro de 2022** (Regulamento dos Serviços Digitais). *Jornal Oficial da União Europeia*, L 277, 27 out. 2022. Disponível em: https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng. Acesso em: 9 ago. 2026.

WATKINS, Elizabeth Anne et al. Governing algorithmic systems with impact assessments: six observations. In: **AAAI/ACM Conference on AI, Ethics, and Society (AIES '21)**. New York: ACM, 2021. p. 1010–1022. DOI: https://doi.org/10.1145/3461702.3462580.