

IX ENCONTRO VIRTUAL DO CONPEDI

**DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS
IV**

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

Diretoria - CONPEDI

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

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

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

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

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

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

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

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

Conselho Fiscal:

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

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

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

Prof. Dr. Fernando Passos - UNIARA - São Paulo

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

Secretarias

Relações Institucionais:

Prof. Dra. Claudia Maria Barbosa - PUCPR - Paraná

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

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

Comunicação:

Prof. Dr. Robison Tramontina - UNOESC - Santa Catarina

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

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

Relações Internacionais para o Continente Americano:

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

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

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

Relações Internacionais para os demais Continentes:

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

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

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

Educação Jurídica

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

Prof. Dr. Rubens Beçak - USP - SP

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

Eventos:

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

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

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

Comissão Especial

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

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

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

Prof. Dr. Rogério Borba - UNIFACVEST - SC

D597

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

Coordenadores: Irineu Francisco Barreto Junior; Diogo de Almeida Viana dos Santos – Florianópolis: CONPEDI, 2026.

Inclui bibliografia

ISBN: 978-65-5274-588-0

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

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

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

CDU: 34



IX ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS IV

Apresentação

Os trabalhos que integram esta publicação foram apresentados no Grupo de Trabalho “Direito, Governança e Novas Tecnologias IV”, realizado virtualmente no dia 25 de junho de 2026, como parte da programação do IX Encontro Virtual do Conselho Nacional de Pesquisa e Pós-graduação em Direito (CONPEDI). Esta edição do evento reafirma o compromisso histórico desta sociedade científica, que há décadas promove a excelência na pesquisa jurídica, adaptando-se às novas realidades de interação digital para garantir a continuidade do diálogo acadêmico em nível nacional e internacional.

O presente Grupo de Trabalho consolidou-se como um espaço privilegiado de interlocução, destacando-se não apenas pela densidade teórica dos trabalhos expostos, mas também pelo perfil de seus participantes, composto por professores pesquisadores, doutores, mestres e alunos de pós-graduação, que trouxeram o frescor de suas investigações institucionais para o debate coletivo. A dinâmica das apresentações, conduzida em ambiente virtual, propiciou uma interação instigante entre os autores e o público, permitindo que a pesquisa jurídica fosse discutida sob o prisma da transdisciplinaridade e do enfrentamento dos desafios contemporâneos.

A temática central deste GT, focada na governança e nas novas tecnologias, reflete a inquietude necessária diante das constantes transformações da sociedade da informação. Cientes da complexidade desses fenômenos, os pesquisadores buscaram articular respostas jurídicas para uma realidade que se apresenta em fluxo permanente, onde a técnica e o Direito se entrelaçam. Nesse sentido, as discussões perpassaram por eixos fundamentais que estruturam o debate acadêmico atual, tais como:

Tecnologias Emergentes e Sociedade: A investigação sobre os impactos da cibercultura na esfera pública, o uso da tecnologia como ferramenta de persuasão e os desafios éticos impostos pela biotecnologia e pela segurança pública.

Os trabalhos selecionados para esta coletânea são o resultado de pesquisas rigorosas desenvolvidas em diversos Programas de Pós-graduação em Direito do país. Ressalte-se que todos os artigos foram submetidos a um criterioso processo de seleção, por meio do sistema de dupla avaliação cega por pares (double blind peer review), garantindo o rigor científico e a adequação temática aos propósitos deste Grupo de Trabalho.

Ao apresentar estes anais ao público, os coordenadores manifestam a expectativa de que estas reflexões contribuam efetivamente para o fortalecimento do diálogo interdisciplinar e para o avanço da ciência jurídica brasileira. O objetivo é oferecer aos leitores um panorama crítico e atualizado sobre como o Direito pode e deve mediar as relações em um mundo cada vez mais pautado pela inovação tecnológica, assegurando sempre a prevalência da dignidade humana e dos valores democráticos.

Desejamos a todos uma leitura proveitosa e inspiradora.

Os Coordenadores

Prof. Dr. Irineu Francisco Barreto Junior (Mestrado em Direito das Faculdades Metropolitanas Unidas - FMU-SP)

Prof. Dr. Diogo de Almeida Viana dos Santos (Universidade Estadual do Maranhão; Universidade CEUMA-PPG em Direito e Afirmação de Vulneráveis)

DO CONTROLE REATIVO AO DESIGN PREVENTIVO: A URGÊNCIA DO SAFETY BY DESIGN NO CONTEXTO DO ECA DIGITAL

FROM REACTIVE CONTROL TO PREVENTIVE DESIGN: THE URGENCY OF SAFETY BY DESIGN IN THE CONTEXT OF THE DIGITAL CHILD AND ADOLESCENT STATUTE (ECA DIGITAL)

Bruno Passos Terlizzi ¹

Resumo

O presente artigo examina a incorporação do princípio do safety by design pelo ordenamento jurídico brasileiro por meio da Lei nº 15.211/2025, analisando seus fundamentos normativos, suas expressões operacionais e seus limites de implementação no contexto nacional. Partindo do caso emblemático da "Revolta do Roblox", ocorrida em março de 2026, o trabalho demonstra como a tensão entre proteção infantojuvenil e liberdade de interação digital condensou, em um episódio singular, os desafios estruturais que a nova legislação foi chamada a enfrentar. O artigo sustenta que o safety by design representa uma inflexão paradigmática na regulação do ambiente digital: ao deslocar o eixo da proteção do comportamento individual para a responsabilização estrutural dos provedores, a lei converte a segurança de crianças e adolescentes em elemento constitutivo da arquitetura das plataformas. São analisados casos de falha regulatória — o escândalo Hytalo Santos e as mecânicas de loot boxes — e de implementação bem-sucedida — as experiências do Grupo LEGO e da ONG ReachOut; que iluminam, respectivamente, os custos do modelo reativo e as possibilidades do modelo preventivo. O trabalho identifica, ainda, três paradoxos centrais da implementação brasileira: a tensão entre verificação de idade e minimização de dados; o risco de sobrecumprimento e censura algorítmica; e a barreira socioeconômica que ameaça produzir um ambiente digital de duas classes. Conclui-se que a efetividade do ECA Digital dependerá não apenas de sua força normativa, mas de sua capacidade de se articular com políticas complementares de inclusão digital e de interpretação jurisdicional comprometida com seus fins protetivos.

freedom of digital interaction condensed, in a singular episode, the structural challenges that the new legislation was called upon to address. The article argues that safety by design represents a paradigmatic shift in the regulation of the digital environment: by displacing the axis of protection from individual behavior to the structural accountability of providers, the law transforms the safety of children and adolescents into a constitutive element of platform architecture. It analyzes cases of regulatory failure (the Hytalo Santos scandal and the mechanics of loot boxes) as well as successful implementation (the experiences of the LEGO Group and the NGO ReachOut) which illuminate, respectively, the possibilities of the preventive model. The study further identifies three central paradoxes of Brazilian implementation: the tension between age verification and data minimization; the risk of over-compliance; and the socioeconomic barrier that threatens to produce a two-tier digital environment. It concludes that the effectiveness of the ECA Digital will depend not only on its normative force, but also on its capacity to articulate with complementary digital inclusion policies and with a jurisdictional interpretation committed to its protective purposes.

Keywords/Palabras-claves/Mots-clés: Eca digital, Safety by design, Comprehensive protection, Children and adolescents, Digital platforms

Introdução

Poucas plataformas digitais ilustram com tanta clareza os paradoxos do ecossistema infantojuvenil contemporâneo quanto o Roblox¹ — e poucas, por essa mesma razão, concentram de maneira tão eloquente os desafios que o ECA Digital foi chamado a enfrentar. Trata-se, em sua configuração mais elementar, de um ambiente que reúne milhares de jogos e experiências interativas criadas pelos próprios usuários; mas reduzir o Roblox à categoria de plataforma de jogos seria subestimar sua natureza mais profunda e, justamente por isso, mais inquietante. O que ele efetivamente constitui é uma rede social de geometria proteica — um espaço de sociabilidade contínua, mediada por chat de texto e de voz em tempo real, no qual crianças e adolescentes não apenas jogam, mas conversam, constroem vínculos, compartilham experiências e, não raro, interagem com interlocutores cuja identidade e intenções permanecem completamente opacas. Mas o que foi o recente caso de protestos ocorridos na plataforma Roblox?

Em março de 2026, algo inédito aconteceu nos servidores do Roblox: crianças e adolescentes brasileiros foram às ruas — virtuais. Com seus avatares segurando cartazes digitais e ocupando praças e avenidas simuladas dentro da própria plataforma, eles protestavam contra uma mudança que, para muitos, soou como perda de liberdade: as novas restrições de comunicação impostas pelo Roblox, que passou a exigir verificação de idade — inclusive por estimativa facial ou documento — para liberar recursos de chat, e criou barreiras de interação escalonadas por faixa etária. Para os menores de 9 anos, o chat dentro dos jogos foi simplesmente desativado por padrão, salvo consentimento expresso dos responsáveis (MIGALHAS, 2026)

O episódio, que rapidamente ganhou o nome de "Revolta do Roblox", revelou uma tensão que está no coração do debate sobre segurança digital: para milhões de jovens usuários, o Roblox não é apenas um jogo — é uma rede social, um ponto de encontro, um espaço de sociabilidade tão real quanto qualquer praça física. Restringir o chat, portanto, não era apenas uma medida técnica; era alterar a geografia afetiva de uma geração inteira. Daí a reação: intensa, organizada e, à sua maneira, politicamente eloquente.

¹ O Roblox é uma plataforma on-line disfarçada de playground. A plataforma reúne milhares de experiências criadas por usuários e atrai, sobretudo, crianças e adolescentes — que ali não apenas jogam, mas conversam em tempo real por texto e voz com pessoas que, muitas vezes, não conhecem. É exatamente essa combinação — alcance massivo entre os mais jovens e interação irrestrita com desconhecidos — que torna o Roblox um dos ambientes digitais que mais preocupam especialistas em proteção infantil.

O que os jovens manifestantes talvez não soubessem — ou não quisessem saber — é que as mudanças da plataforma não surgiram do acaso. Elas chegaram às vésperas da entrada em vigor da Lei nº 15.211/2025, o chamado ECA Digital, que passou a vigorar em 17 de março de 2026 e impõe às plataformas digitais uma postura radicalmente diferente diante da presença infantojuvenil em seus ambientes: verificação de idade, ferramentas de supervisão parental, restrição de contato entre crianças e adultos desconhecidos e controle de mecanismos que estimulem uso excessivo ou exponham os mais jovens a riscos. Em outras palavras, o Roblox não endureceu suas regras por vontade própria — foi compelido a redesenhar sua arquitetura para se adequar a uma legislação que chegou com força normativa e sanções proporcionais (*Idem*, 2026).

É precisamente aí que entra o conceito de *safety by design* — segurança pela arquitetura, e não pela reação ao dano já consumado. A lógica é simples, ainda que sua execução seja complexa: uma plataforma verdadeiramente segura não espera que a criança seja assediada para então tomar providências; ela constrói, desde o início, um ambiente onde esse risco é estruturalmente reduzido. No Roblox, isso se traduziu em bloqueios padrão, filtros por faixa etária, restrições ao chat e ampliação do controle parental — medidas que, do ponto de vista da proteção, fazem sentido inequívoco (SANTOS, 2026).

A controvérsia, porém, não se dissipou com a boa intenção regulatória. Especialistas em privacidade e proteção de dados levantaram uma objeção de peso: a verificação facial, quando aplicada a crianças e adolescentes, envolve a coleta de dados biométricos sensíveis — e os riscos associados a esse tipo de tratamento são, eles próprios, uma forma de vulnerabilidade que a lei pretende combater. Para além do debate técnico-jurídico, houve ainda um episódio que, a seu modo, resumiu as limitações do sistema: relatos de usuários tentando enganar a verificação facial com desenhos de barba e bigode — imagem que seria cômica se não fosse reveladora. Ela expôs, com ironia involuntária, a distância que ainda separa a ambição protetiva da lei e a confiabilidade real dos instrumentos disponíveis para implementá-la (*Idem*, 2026).

A Revolta do Roblox configura-se, assim, como um caso exemplar — não porque os jovens estivessem errados ao protestar, nem porque a plataforma estivesse errada ao restringir, mas porque o episódio iluminou, de maneira vívida e incomum, o campo de tensões onde o ECA Digital precisará operar: entre proteção e liberdade, entre segurança e privacidade, entre

a arquitetura do sistema e a criatividade daqueles que sempre encontram uma forma de contorná-la.

Isto posto, o sinal de alerta que o Roblox acende não deriva de qualquer característica isolada de seu design, mas da combinação entre seu alcance massivo junto ao público infantojuvenil e a ausência, até recentemente, de mecanismos robustos de verificação etária e moderação de interações — uma combinação que transformou a plataforma em um dos territórios digitais onde a fronteira entre entretenimento e vulnerabilidade mais frequentemente se dissolve².

1. Princípio da proteção integral e seus desdobramentos

O denominado ECA Digital — positivado na Lei nº 15.211/2025, em vigor desde 17 de março de 2026 — não rompe com a lógica protetiva do ECA (Estatuto da Criança e do Adolescente - Lei 8.069/90), mas a projeta para o ambiente digital, adaptando princípios clássicos da tutela da infância e da adolescência aos riscos, dinâmicas e deveres próprios das plataformas, aplicativos, jogos e demais serviços tecnológicos.

Vale mencionar que o Comentário Geral n.º 25 de 2021 da Organização das Nações Unidas (ONU) já reconhecia expressamente que os valores da doutrina da proteção integral preconizados pela Convenção da ONU sobre os Direitos da Criança, os quais foram incorporados no ECA, aplicam-se plenamente também no ambiente digital.

Dentre as vigias mestras que sustentam os dois edifícios e que funcionam como vasos comunicantes que se retroalimentam e garantem a efetivação de um estatuto para o outro está o princípio da Proteção integral. Esta constitui o ponto de continuidade mais evidente entre o ECA e o ECA Digital, na medida em que ambos os diplomas partem da premissa de que

² As reflexões e resultados publicados neste artigo têm como origem o diverso trabalho de pesquisa desenvolvida no âmbito do Grupo de Estudos “Cidadania plena da criança e do adolescente”, vinculado à Linha de Pesquisa “Intervenção Econômica Estatal e Relações de Trabalho”, sob coordenação e orientação da Prof^a. Dr^a. Denise Auad, professora livre-docente de Direito Constitucional da Faculdade de Direito de São Bernardo do Campo. Nesse contexto, o trabalho dialoga com um conjunto de problemáticas contemporâneas que articulam os direitos fundamentais infantojuvenis à crescente digitalização da vida social, abordando, de modo particular, os princípios da proteção integral e do melhor interesse da criança e do adolescente, bem como categorias correlatas como o direito ao cuidado, o direito ao brincar e a preservação de um meio ambiente — também digital — saudável. Ao situar tais temas no cenário da hiperconexão, marcado pela centralidade das plataformas digitais e pela intensificação das mediações tecnológicas, o artigo propõe como recorte analítico a investigação da efetivação desses direitos no contexto do ECA Digital, buscando compreender em que medida a nova legislação é capaz de responder às transformações estruturais que reconfiguram as condições de desenvolvimento, sociabilidade e vulnerabilidade de crianças e adolescentes na contemporaneidade. Em outras palavras, trata-se de examinar como o direito, diante da digitalização da vida, rearticula seus instrumentos de tutela para assegurar, em chave atualizada, a cidadania plena infantojuvenil.

crianças e adolescentes demandam tutela jurídica reforçada em razão de sua condição peculiar de pessoas em desenvolvimento.

No Estatuto da Criança e do Adolescente, esse princípio comparece já no art. 1º e ganha densidade no art. 3º, ao assegurar todos os direitos fundamentais necessários ao desenvolvimento físico, mental, moral, espiritual e social; no ECA Digital, por sua vez, essa mesma gramática protetiva é deslocada para o ambiente on-line, de modo a reconhecer que a vida digital também se converteu em espaço decisivo de socialização, vulnerabilidade e formação subjetiva.

Assim, o que a nova legislação realiza não é uma ruptura com o paradigma anterior, mas sua atualização histórica diante de um ecossistema tecnológico em que riscos, interações e mediações passaram a incidir diretamente sobre a infância e a adolescência. Por essa razão, ao impor aos fornecedores o dever de estruturar produtos e serviços compatíveis com esse padrão elevado de tutela, o ECA Digital reafirma que a proteção integral não se limita ao mundo físico, mas deve acompanhar as transformações dos espaços em que a experiência infantojuvenil efetivamente se produz.

2. Sentido e significado de *safety by design*

O conceito de *safety by design* — segurança pela arquitetura, como se poderia traduzir com alguma liberdade — representa uma das inflexões mais significativas no modo como o direito, a tecnologia e as políticas públicas têm buscado equacionar o problema da proteção de usuários no ambiente digital. Em sua formulação mais precisa, trata-se de uma abordagem proativa que recusa a lógica reparatória que até então predominava no setor: a de que bastava reagir aos danos após sua ocorrência, moderando conteúdos, banindo perfis e respondendo a denúncias — como se a segurança fosse uma questão de gestão de crises, e não de responsabilidade estrutural. A ruptura operada por esse princípio é, portanto, de natureza paradigmática: ao postular que os riscos devem ser antecipados e eliminados na origem, ele eleva a proteção ao estatuto de condição constitutiva do produto digital e a posiciona, ao lado da privacidade e da segurança cibernética, como o "terceiro pilar" do desenvolvimento tecnológico (SCHERTEL, 2018).

Três princípios fundamentais sustentam essa arquitetura: a responsabilidade ativa do provedor, que retira do usuário o ônus de sua própria proteção e o transfere para quem detém os meios técnicos de prevenir o dano; o empoderamento e a autonomia do usuário, que

pressupõe interfaces respeitosas da dignidade humana e ferramentas genuinamente acessíveis de controle da experiência; e a transparência e a responsabilidade pública, que obriga as plataformas a demonstrar, de maneira verificável e periódica, a eficácia real de seus mecanismos de proteção — e não apenas a proclamá-la (HALFELD; COELHO, 2026).

A consequência mais operacional desse conjunto de princípios — e aquela que mais diretamente dialoga com o ECA Digital brasileiro — é o que se convencionou chamar de *Safety by Default*: a segurança não como configuração a ser ativada pelo usuário diligente, mas como estado natural e automático do sistema. Mais do que uma opção técnica, trata-se de uma decisão política incorporada ao produto: ao identificar um usuário menor de idade, a plataforma deve aplicar, de maneira imediata e sem necessidade de qualquer intervenção adicional, as configurações mais protetivas disponíveis em matéria de privacidade, restrição de contato e limitação de funcionalidades de risco — invertendo, assim, a lógica que por décadas governou o setor e que o mantra do Vale do Silício resumia com desconcertante candura: "mover-se rápido e quebrar coisas".

O *safety by design* é, em certa medida, a antítese exata dessa filosofia: ele postula que a velocidade de lançamento de um produto jamais pode justificar a exposição de usuários vulneráveis a riscos que uma arquitetura mais cuidadosa poderia ter prevenido, e que a criança que acessa uma plataforma digital pela primeira vez não deve chegar a um território neutro à espera de configuração, mas a um ambiente já calibrado, de antemão, para sua proteção. A distância entre esse modelo e o que prevaleceu durante décadas é considerável; e é precisamente essa distância — entre a segurança como exceção e a segurança como ponto de partida — que o ECA Digital, ao incorporar o *safety by design* como princípio estruturante, se propõe, finalmente, a abolir.

Sob uma perspectiva analítica, a noção de *safety by design* sinaliza uma inflexão de natureza estrutural no modo de enquadramento do problema: abandona-se o eixo normativo centrado na conduta individual — isto é, nas prescrições acerca de “como os sujeitos devem agir” — para privilegiar uma abordagem institucional e infraestrutural, voltada a indagar “como os próprios sistemas devem ser concebidos e operados”. Esse deslocamento, longe de ser meramente retórico, insere-se no horizonte mais amplo da responsabilidade compartilhada — categoria que organiza o ECA Digital —, mas o faz sublinhando a desigual distribuição de

poder entre usuários e plataformas digitais, cuja capacidade de moldar ambientes e comportamentos não pode ser ignorada (*Idem*, 2026).

Nesse sentido, a incorporação do *safety by design* pelo ECA Digital indica uma tentativa de reconfiguração das condições de experiência no espaço digital brasileiro: a proteção de crianças e adolescentes deixa de depender, em primeiro plano, de mecanismos reativos ou de decisões informadas de difícil operacionalização, passando a ser inscrita, desde a origem, nas próprias arquiteturas que estruturam a interação digital. Em outras palavras, trata-se de converter a proteção em pressuposto do sistema, e não em resposta contingente a seus efeitos.

2.1. O ponto onde ainda estamos: NO *safety by design*

Um caso recente que ilustra sintomaticamente a crueza e os limites do modelo regulatório vigente é o escândalo que, no Brasil, ficou associado ao nome do influenciador digital Hytalo Santos — episódio que expôs, de maneira incontornável, a extensão em que plataformas de vídeo como o YouTube haviam se tornado vetores de adultização, sexualização e exploração de crianças, gerando, ao mesmo tempo, milhões de visualizações e receita publicitária mensurável para seus operadores. O que o caso revelou não foi apenas a existência de conteúdos inadequados em circulação — fenômeno que, lamentavelmente, não surpreende a quem acompanha o debate sobre proteção infantil no ambiente digital —, mas algo estruturalmente mais grave: a arquitetura das plataformas não apenas tolerava esses conteúdos, mas os monetizava ativamente, distribuindo receita publicitária a canais cujo produto era, em última análise, a imagem sexualizada de crianças reais.

A falha não era, portanto, de moderação; era de design. O modelo operacional das plataformas repousava sobre o princípio do "notificar e remover" — uma lógica reativa que pressupunha o dano já consumado como condição de intervenção, e que, na prática, permitia que vídeos inadequados circulassem livremente, acumulassem visualizações e gerassem receita antes que qualquer mecanismo de proteção fosse acionado. Não havia, na arquitetura do serviço, nenhum dispositivo proativo capaz de detectar a propagação desses conteúdos ou de proteger, preventivamente, a imagem dos menores envolvidos — o que equivalia a construir uma praça pública sem iluminação e depois culpar os transeuntes por não enxergarem o perigo (LEMOS, 2016).

As consequências do escândalo foram proporcionais à gravidade da falha que ele expôs. O caso gerou repercussão nacional e colocou em evidência a insuficiência do ordenamento jurídico então vigente para lidar com violações dessa natureza e dessa escala — violações que, convém sublinhar, não eram episódicas, mas sistêmicas. Os dados documentados entre janeiro e julho de 2025 são, a esse respeito, perturbadores: quase 77 mil violações de direitos humanos foram registradas no ambiente online nesse período, e 64% delas envolviam material de abuso sexual infantil (CRUZ, 2025).

Diante dessa constatação, o debate sobre o ECA Digital — que até então avançava em ritmo parlamentar ordinário — ganhou uma urgência que os dados estatísticos, por si sós, dificilmente teriam produzido: o caso Hytalo Santos deu rosto e escândalo ao que os números descreviam em abstrato, e foi, por essa razão, o principal propulsor da aprovação acelerada da nova legislação. Posto isso, o que o episódio deixou como legado mais duradouro não foi apenas a reforma legal que ajudou a precipitar, mas a demonstração empírica de um princípio que o *Safety by Design* já postulava em teoria: que a proteção de crianças no ambiente digital não pode depender da boa vontade das plataformas nem da vigilância posterior ao dano, mas deve estar inscrita na própria arquitetura dos serviços — antes que a câmera grave, antes que o vídeo seja carregado, antes que o algoritmo decida amplificá-lo.

O segundo caso que merece exame detido é o das mecânicas de apostas embutidas em jogos eletrônicos — as chamadas loot boxes, gachas e roletas virtuais —, fenômeno que, a diferença do anterior, opera de maneira mais silenciosa e, justamente por isso, com maior dificuldade de ser identificado e combatido. Trata-se de sistemas de recompensa aleatória mediante pagamento que, incorporados a jogos de ampla circulação entre crianças e adolescentes, exploram um princípio psicológico há muito estudado pela literatura comportamental: o da recompensa variável intermitente, mecanismo que produz padrões de engajamento compulsivo precisamente porque a incerteza do resultado — e não a certeza da recompensa — é o que sustenta o comportamento.

Ao projetar jogos com essas características sem restrições de idade eficazes, as empresas do setor não cometeram um erro de avaliação; tomaram uma decisão de negócios. A arquitetura dessas mecânicas foi deliberadamente construída para maximizar o engajamento e o gasto dos usuários — e a ausência de salvaguardas etárias robustas não foi uma omissão

técnica, mas a condição de funcionamento de um modelo que depende, estruturalmente, da participação do público mais jovem para atingir a escala de receita pretendida. Ignorar o impacto dessas escolhas de design no desenvolvimento psicológico de crianças e adolescentes não era, portanto, descuido; era, nos termos mais precisos, uma externalidade negativa deliberadamente não contabilizada (EL KHATIB, 2024).

As consequências dessa arquitetura de exploração mostraram-se, com o tempo, suficientemente documentadas para fundamentar uma resposta legislativa inequívoca. Especialistas em psicologia do desenvolvimento e em medicina das dependências passaram a descrever as loot boxes como uma porta de entrada para o vício em jogos de azar na infância — não por analogia retórica, mas por identidade funcional: os circuitos neurológicos ativados por uma caixa de recompensa aleatória em um jogo eletrônico são, em larga medida, os mesmos que sustentam a dependência do jogo patológico em adultos (*Idem*, 2024).

A partir daí, o mosaico de consequências foi se tornando cada vez mais legível: danos psicológicos previsíveis em usuários que ainda não completaram o desenvolvimento das estruturas cerebrais responsáveis pelo controle de impulsos; dependência algorítmica reforçada por notificações, recompensas temporárias e mecânicas de progressão cuidadosamente calibradas para impedir o abandono; e exploração financeira de famílias que, muitas vezes, sequer tinham consciência de que seus filhos estavam realizando transações monetárias dentro de ambientes que se apresentavam, externamente, como jogos infantis (BILENSKY, 2026).

Foi diante desse quadro que o ECA Digital optou por uma solução radical em sua simplicidade: o banimento total das *loot boxes* para menores — decisão que, ao interditar não apenas o acesso ao mecanismo, mas o próprio mecanismo em si quando o usuário for criança ou adolescente, afirma que há formas de design que são, por sua própria natureza, incompatíveis com a proteção integral da infância.

2.2. O ponto onde se quer chegar: experiências positivas em *safety by design*

Entre os casos que a literatura sobre Safety by Design mais frequentemente mobiliza como exemplos de implementação bem-sucedida, o do Grupo LEGO ocupa um lugar de destaque — e não apenas pela notoriedade global da marca, mas pela coerência com que a empresa soube traduzir seus princípios de proteção infantil em escolhas concretas de

arquitetura digital. A plataforma LEGO Life, voltada especificamente ao público infantil, constitui, nesse sentido, uma janela privilegiada para observar como a segurança pode ser incorporada ao design de um serviço não como camada adicional de restrição, mas como elemento constitutivo da experiência do usuário — algo que a criança encontra desde o primeiro momento de contato com o ambiente, antes mesmo de realizar qualquer interação (eSAFETY COMMISSIONER, 2019).

O processo de registro é, a esse respeito, exemplar: ao se cadastrarem, os pequenos usuários passam por um percurso de indução que inclui tutoriais sobre as regras da comunidade e a assinatura de um "Compromisso de Segurança" — dispositivo que, longe de ser uma formalidade burocrática, funciona como um ritual de pertencimento que confere à criança o senso de responsabilidade sobre o ambiente que está prestes a habitar.

A essa pedagogia inicial, a LEGO acrescenta um elemento de design particularmente engenhoso: um personagem especial que se apresenta como o "primeiro amigo" da criança na plataforma e que reaparece de maneira contextual — quando a criança tenta carregar uma fotografia, por exemplo — para oferecer orientações em tempo real sobre práticas seguras, convertendo o que poderia ser uma intervenção restritiva em um momento de aprendizado mediado por uma figura de identificação afetiva (*Idem*, 2019). Completa esse mosaico de iniciativas o treinamento interno obrigatório de todos os funcionários e afiliados da empresa em segurança digital infantil — sinal de que a proteção não é, para a LEGO, uma política de produto, mas uma cultura organizacional.

As consequências dessa arquitetura de cuidado são, a um só tempo, práticas e simbólicas. Do ponto de vista prático, o uso de personagens, tutoriais e lembretes contextuais demonstrou ser capaz de aumentar significativamente a compreensão das regras de convivência por parte das crianças — não porque as regras sejam mais simples, mas porque são apresentadas em uma linguagem e por meio de mediadores com os quais o público infantil é capaz de estabelecer vínculo.

Do ponto de vista simbólico — e talvez mais duradouro —, o modelo LEGO oferece uma prova de conceito que desafia a narrativa, largamente difundida no setor, de que segurança e experiência do usuário são objetivos naturalmente antagônicos. O que o caso demonstra é o oposto: que a segurança, quando integrada ao design com inteligência e sensibilidade, pode tornar a experiência mais rica, mais confiante e mais propícia ao

desenvolvimento de uma cidadania digital genuína — aquela que não se limita a obedecer regras impostas de fora, mas as compreende e as incorpora como parte de uma identidade de usuário responsável. Justamente por isso, o modelo LEGO tem sido citado por reguladores e pesquisadores como referência para o que o ECA Digital, em seu horizonte mais ambicioso, busca generalizar: não a segurança como policiamento, mas a segurança como cultura (LIVINGSTONE, 2012).

O segundo caso que merece exame detido é o da ONG australiana ReachOut³, plataforma de saúde mental voltada a jovens, cuja abordagem de *safety by design* se distingue por uma característica que a torna particularmente relevante para o debate sobre proteção infantojuvenil no ambiente digital: a aposta na autogestão comunitária e na moderação por pares como instrumentos centrais de construção de um ambiente seguro. A premissa que orienta o modelo é, em sua aparente simplicidade, bastante sofisticada: jovens em situação de vulnerabilidade emocional respondem de maneira distinta a diferentes fontes de autoridade, e a figura do moderador adulto externo — ainda que tecnicamente competente — carrega uma assimetria relacional que pode inibir a participação ou reduzir a percepção de pertencimento ao ambiente (eSAFETY COMMISSIONER, 2019).

Partindo dessa constatação, a ReachOut optou por um design que coloca moderadores treinados pertencentes ao mesmo grupo etário dos usuários no centro da dinâmica comunitária — não como fiscais invisíveis operando nos bastidores, mas como participantes visíveis que exemplificam, em suas próprias interações públicas, o tipo de comportamento que as diretrizes da comunidade prescrevem. Trata-se, em outros termos, de uma aposta na modelagem por pares como vetor de normatização social: em lugar de comunicar as regras de cima para baixo, a plataforma as encarna em sujeitos com os quais os demais usuários podem se identificar — transformando a norma em comportamento observável e, por essa via, em referência desejável.

Com o tempo, essa estratégia de design produziu um efeito que a literatura sobre comunidades online raramente documenta com tanta clareza: a autorregulação espontânea. Observou-se que os próprios jovens usuários passaram, progressivamente, a chamar a atenção uns dos outros de maneira proativa diante de comportamentos inadequados — assumindo,

³ REACHOUT AUSTRALIA. ReachOut: when life doesn't go as planned. [S.l.]: ReachOut Australia, c2024. Disponível em: <https://au.reachout.com/>. Acesso em: [data de acesso].

sem que isso lhes fosse formalmente exigido, uma responsabilidade pelo clima comunitário que antes cabia exclusivamente à moderação institucional (LIVINGSTONE, 2020).

Esse deslocamento da responsabilidade — do gestor para a comunidade, do externo para o interno, do punitivo para o colaborativo — é, do ponto de vista do *safety by design*, um resultado de alta relevância, pois demonstra que ambientes digitais podem ser arquitetados de modo a cultivar, e não apenas a disciplinar, o comportamento de seus usuários. A redução das intervenções punitivas não foi, nesse caso, consequência da ausência de problemas, mas da constituição de uma cultura de suporte mútuo suficientemente robusta para absorver os conflitos antes que eles se tornassem casos de moderação. Diante disso, o modelo ReachOut oferece ao debate brasileiro sobre o ECA Digital uma lição que transcende o âmbito da saúde mental: a de que a proteção mais eficaz não é aquela que se impõe sobre a comunidade, mas aquela que a própria comunidade, devidamente arquitetada para isso, aprende a exercer sobre si mesma.

3. Limites e paradoxos do *safety by design* hoje no Brasil.

A implementação do Safety by Design sob os auspícios do ECA Digital não é uma empreitada isenta de tensões — e o mais honesto a fazer, do ponto de vista analítico, é reconhecê-las sem que esse reconhecimento se converta em argumento contra a regulação. O primeiro e talvez mais agudo desses paradoxos reside precisamente no núcleo do dispositivo que a lei considera mais urgente: os mecanismos de verificação de idade. Para proibir a autodeclaração — ficção jurídica que, como se buscou demonstrar, nunca protegeu ninguém além das próprias plataformas —, o ECA Digital pode compelir essas mesmas plataformas a coletar volumes muito maiores de dados sensíveis do que fariam ordinariamente, incluindo documentos de identidade e biometria facial de crianças e adolescentes (COLOMBO; FALEIROS; ENGELMANN, 2022).

O paradoxo é, nesse ponto, de uma ironia considerável: para proteger menores dos riscos do ambiente digital, a lei pode estar criando novos vetores de vulnerabilidade — bancos de dados biométricos infantis que, se mal gerenciados ou vazados, representam uma ameaça à privacidade de dimensão potencialmente mais grave e duradoura do que aquela que se pretendia prevenir. Isso implica reconhecer uma tensão estrutural que o legislador não pode simplesmente ignorar: a obrigação de "verificação confiável" imposta pelo ECA Digital

colide, em pontos não triviais, com o princípio de minimização de dados consagrado pela LGPD, que exige o uso do menor volume possível de informações pessoais para a consecução de qualquer finalidade (*Idem*, 2022).

Resolver essa colisão não é tarefa de interpretação ordinária; exige que reguladores e juristas desenvolvam, de maneira criativa e urgente, soluções técnicas e normativas capazes de verificar sem acumular — de garantir a idade sem fazer da infância um arquivo biométrico permanente.

O segundo paradoxo é de natureza distinta, pois não opõe dois direitos de proteção entre si, mas coloca em tensão o dever de cuidado proativo que o *safety by design* exige e a liberdade de expressão que qualquer democracia constitucional deve salvaguardar. A linha que separa o design que "protege" da intervenção que censura é, por definição, uma linha disputada — e o ECA Digital, ao empregar categorias como "conteúdo prejudicial" ou "dano psicológico previsível" sem densificá-las com a precisão técnica que sua aplicação exigiria, abre espaço para um risco que os críticos da legislação não deixaram de apontar: o do sobrecumprimento (SCHERTEL, 2014).

Diante de multas de até cinquenta milhões de reais por infração e da presunção de culpa em caso de falha de segurança, as plataformas têm todos os incentivos econômicos para adotar uma postura de remoção preventiva e excessiva de conteúdos, retirando do ar materiais legítimos — debates sobre saúde, educação sexual, representações artísticas de temas difíceis — tão somente para evitar a incerteza regulatória.

Ora, esse resultado seria não apenas juridicamente problemático, mas antitético ao espírito do próprio ECA Digital, que não foi concebido como instrumento de censura, mas de proteção. A superação desse paradoxo dependerá, em larga medida, da capacidade do Poder Judiciário e da ANPD de enquadrar as obrigações da lei como normas de segurança do produto e de saúde pública — analogamente ao que se faz com a regulação de medicamentos ou de equipamentos elétricos —, e não como restrições à liberdade de expressão, o que implicaria um padrão de escrutínio constitucional muito mais severo e uma tendência interpretativa de sentido inverso ao que a legislação persegue (COLOMBO; FALEIROS; ENGELMANN, 2022).

O terceiro limite é, provavelmente, o mais silencioso dos três — e, por essa razão, o mais propenso a ser subestimado no debate público. O ECA Digital aplica-se, em seu escopo

mais abrangente, a qualquer serviço digital com "acesso provável" por menores, o que expande suas obrigações para a quase totalidade do ecossistema digital brasileiro; mas o Brasil não é um país socialmente homogêneo, e as soluções técnicas que a lei prescreve — contas vinculadas a responsáveis, verificação biométrica, dispositivos compatíveis com sistemas de controle parental — pressupõem condições materiais de acesso que uma parcela significativa da população simplesmente não possui (eSAFETY COMMISSIONER, 2019).

No contexto de um país onde milhões de crianças acessam a internet por meio de smartphones compartilhados entre vários membros do mesmo núcleo familiar, onde a conectividade doméstica ainda é limitada nas regiões mais vulneráveis e onde a literacia digital dos responsáveis legais frequentemente não alcança o nível necessário para operar os dispositivos de supervisão que a lei prevê, as exigências do *safety by design* correm o risco de produzir um efeito perverso: o de excluir digitalmente exatamente as crianças mais vulneráveis, aquelas que mais necessitariam da proteção que a lei se propõe a garantir. Há, nessa possibilidade, o germe de um ambiente digital de duas classes — no qual crianças de famílias com maior capital econômico e tecnológico navegam em plataformas plenamente adequadas às normas, enquanto as demais ficam à margem ou são empurradas para ambientes menos regulados e, portanto, menos seguros.

Enfrentar esse risco não é opcional; é condição de legitimidade do próprio projeto regulatório — e exige que o ECA Digital seja acompanhado de políticas públicas complementares de inclusão digital, formação de responsáveis e subsídio tecnológico que, até o momento, ainda aguardam a atenção que merecem.

Conclusão

O cenário, portanto, já conhecido. O uso de ambientes digitais por crianças e adolescentes, aliado a falhas de moderação, algoritmos de recomendação e práticas de design nocivas, contribuiu para situações graves, como: a) divulgação de bets e cassinos on-line nas redes sociais, inclusive dirigida a crianças e adolescentes; b) conteúdos de abuso e exploração sexual infantojuvenil, ampliados por recomendações automáticas; c) erotização precoce e adultização, com crianças e adolescentes incentivados a reproduzir comportamentos ou imagens sexualizadas ou típicas de adultos; d) discursos de ódio e bullying intenso, que permanecem on-line por falhas na moderação desses conteúdos; e) recomendação de

conteúdos hiperviolentos por sistemas automatizados, mesmo sem intenção consciente dos usuários.

O ECA Digital introduz, no âmbito da regulação das redes sociais, plataformas, jogos e demais infraestruturas digitais, uma reorientação normativa ancorada no princípio da proteção integral e na primazia dos direitos de crianças e adolescentes, tal como enunciado no artigo 4º. Esse movimento, longe de se limitar à reafirmação de diretrizes já conhecidas, implica a densificação de deveres jurídicos dirigidos aos fornecedores de produtos e serviços digitais, agora compelidos a internalizar, em suas práticas, a prevenção e a mitigação de riscos inerentes à violação desses direitos. Trata-se, portanto, de um deslocamento que amplia o alcance da responsabilidade regulatória: as obrigações deixam de incidir exclusivamente sobre a fase de uso e operação e passam a alcançar a própria lógica de concepção dos sistemas. Desse modo, como indicam leituras contemporâneas sobre governança digital e arquitetura regulatória (MENDES, 2021; DONEDA, 2020), o direito projeta-se sobre o design, convertendo a proteção de direitos fundamentais em elemento constitutivo — e não meramente corretivo — das tecnologias digitais. Em outras palavras, a tutela jurídica deixa de ser reativa para se tornar estrutural, inscrita nas condições mesmas de produção e funcionamento dos ambientes digitais.

No plano normativo, o dispositivo em questão estabelece que os fornecedores de produtos e serviços digitais devem adotar “medidas razoáveis” orientadas à prevenção e à mitigação de riscos, especialmente aqueles associados ao acesso, à exposição, à recomendação ou à facilitação de contato com conteúdos e práticas potencialmente lesivos. Essa formulação, embora aberta, delineia um campo de incidência bastante preciso: abrange desde situações de exploração e abuso sexual até dinâmicas de violência, intimidação e assédio, passando por mecanismos de indução ou estímulo a condutas prejudiciais à saúde física e psíquica, bem como pela exposição a jogos de azar, substâncias nocivas — como tabaco e álcool — e estratégias publicitárias de caráter predatório ou enganoso dirigidas ao público infantojuvenil. Ademais, inclui-se nesse espectro a restrição a conteúdos de natureza pornográfica, consolidando um rol de riscos que orienta a atuação preventiva dos agentes econômicos (ECA Digital, art. 6º).

A partir daí, como sugere a literatura contemporânea sobre regulação de plataformas (LIVINGSTONE, 2019), a noção de “razoabilidade” opera menos como indeterminação e

mais como um critério de adaptação contextual, capaz de exigir respostas proporcionais à posição estrutural dos provedores e à vulnerabilidade dos usuários. Em outras palavras, trata-se de converter a gestão de riscos em dever jurídico contínuo, inscrito na própria lógica de funcionamento das infraestruturas digitais.

A preservação desses direitos imporá aos fornecedores avaliar riscos, controlar conteúdos, oferecer processos padronizados que dificultem o acesso a conteúdo ou relacionamentos danosos ou ameaçadores para crianças e adolescentes (artigo 8º). A nova legislação dispõe ainda sobre a criação de mecanismos de aferição de idade para acesso a serviços e produtos, impondo inclusive a necessidade de vinculação das contas de crianças e adolescentes com menos de 16 anos à conta de um responsável. Houve toda uma preocupação com o acesso aos jogos eletrônicos, às violações graves e à publicidade no meio digital que explorassem a hipervulnerabilidade de crianças e adolescentes.

Quando transposta, então, ao contexto do chamado ECA Digital (Lei nº 15.211/2025), o *safety by design* adquire densidade normativa específica: trata-se de deslocar o eixo da proteção de crianças e adolescentes do comportamento individual (controle parental isolado) para a responsabilização estrutural dos provedores e plataformas. Nesse sentido, o *safety by design* funciona como uma técnica de efetivação do princípio da proteção integral, já consagrado no Estatuto da Criança e do Adolescente. Em outras palavras, a segurança deixa de ser um “remendo posterior” e passa a constituir um parâmetro originário de arquitetura, influenciando decisões de interface, algoritmos, fluxos de uso e modelos de negócio (HALFELD, COELHO, 2026).

Em termos analíticos, o *safety by design* marca uma inflexão importante: ele desloca o debate do plano moral (“como os indivíduos devem se comportar”) para o plano institucional e infraestrutural (“como os sistemas devem ser construídos”). Tal deslocamento está em consonância com a ideia de responsabilidade compartilhada — núcleo do ECA Digital —, mas com um acento claro na assimetria de poder entre usuários e plataformas. Em suma, ao incorporar o *safety by design*, o ECA Digital procura transformar o ambiente digital brasileiro em um espaço em que a proteção de crianças e adolescentes não dependa primordialmente de vigilância posterior ou de escolhas informadas difíceis, mas seja pré-configurada nas próprias condições de possibilidade da experiência digital.

Além disso, é importante lembrar que o ECA Digital impõe responsabilização ativa dos fornecedores sobre o design e funcionamento dos seus serviços, prevenindo riscos estruturais associados à forma como recursos e telas são apresentados aos usuários mais jovens. Isso inclui limites a práticas de design aditivo, ligadas a vício, ansiedade e uso excessivo de telas. Estão explicitamente proibidos recursos que induzam ao uso compulsivo, exemplificados como reprodução automática de mídia, recompensas vinculadas ao tempo de permanência, notificações insistentes e mecânicas semelhantes. Promover a educação midiática dos usuários também se torna uma obrigação ativa (art. 8º., IV; art. 17, §4º., II e IV). Ainda, as loot boxes, caixas de recompensas aleatórias que simulam jogos de azar, comuns em plataformas de games, passam a ser reguladas com restrições específicas. O ECA Digital proíbe a sua oferta para crianças e adolescentes, de acordo com a classificação indicativa, devido ao risco de exposição precoce a estímulos de apostas.

Por fim, seria um equívoco reduzir o *safety by design* a uma exigência de conformidade legal — como se sua adoção representasse, para as empresas de tecnologia, nada mais do que o custo inevitável de operar em um ambiente regulatório mais exigente. A experiência acumulada pelos casos que a literatura especializada mais documenta aponta em direção oposta: a incorporação genuína desses princípios tende a gerar, para as empresas que os adotam com seriedade, um conjunto de benefícios estratégicos que transcendem em muito o mero cumprimento da norma.

O primeiro e talvez mais contraintuitivo desses benefícios é o da vantagem competitiva: em um mercado cujas expectativas de consumo estão sendo paulatinamente reconfiguradas — especialmente entre as gerações mais jovens, que demonstram crescente sensibilidade às práticas éticas das plataformas que frequentam —, a empresa que incorpora a segurança como valor central de sua proposta de produto ocupa uma posição diferenciada que seus concorrentes dificilmente podem replicar sem uma transformação cultural igualmente profunda. A esse diferencial se soma o do aumento da confiança: plataformas que comunicam com transparência como tratam a segurança de seus usuários — e que, sobretudo, demonstram essa transparência por meio de escolhas de design verificáveis e não apenas de declarações institucionais — constroem com famílias e usuários um vínculo de lealdade que nenhuma campanha publicitária é capaz de produzir artificialmente, porque ele repousa sobre a experiência concreta de ser respeitado e protegido (eSAFETY COMMISSIONER, 2019).

O terceiro benefício — e aquele de consequências mais imediatas para o modelo de negócios das empresas — é o da mitigação proativa de riscos. A lógica econômica subjacente ao Safety by Design é, nesse ponto, de uma clareza difícil de contestar: "projetar a saída" dos riscos na fase de arquitetura do produto é, invariavelmente, muito menos custoso do que remediar, a posteriori, os danos gerados por uma falha de design que se tornou pública — seja na forma de um escândalo de violação de dados, de uma investigação regulatória ou de um processo judicial de grandes proporções (*Idem*, 2019).

As soluções de remendo — o que a literatura técnica designa pelo termo *retrofit* —, além de financeiramente onerosas, carregam um custo reputacional que raramente se dissipa por completo: a imagem de uma plataforma que precisou ser forçada a se tornar segura dificilmente se equipara, aos olhos do mercado e da opinião pública, à de uma plataforma que escolheu sê-lo desde o princípio. Diante desse quadro, a conclusão que se impõe é menos uma prescrição normativa do que uma constatação pragmática: no ecossistema digital contemporâneo, segurança e sustentabilidade empresarial deixaram de ser objetivos concorrentes para se tornarem, crescentemente, as duas faces de uma mesma escolha estratégica — e as empresas que ainda não perceberam isso estão, a rigor, acumulando um passivo que o tempo e a regulação tornarão cada vez mais caro postergar (*Ibid*, 2019).

O ECA Digital e o *safety by design* não são, em última análise, instrumentos paralelos que se encontram por conveniência regulatória; são expressões contemporâneas de um mesmo imperativo civilizacional — o de que a sociedade tem o dever de construir, em cada época e nos territórios que cada época inaugura, ambientes onde a infância possa existir com dignidade e segurança. Se o Estatuto de 1990 inscreveu esse imperativo no espaço físico da vida social brasileira, cabe ao ECA Digital e à arquitetura de proteção que ele exige inscrevê-lo também no espaço digital — não como utopia, mas como obrigação jurídica exigível, auditável e, quando descumprida, sancionável. O futuro dirá se a lei foi suficiente. O presente exige, ao menos, que ela seja levada a sério.

Referências bibliográficas

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, [2025].

AUAD, Denise. O tempo como um Direito Fundamental e sua relação com a proteção da infância e juventude. In: Luiz Nelson Porto Araujo e Arsenio Eduardo Corrêa. (Org.). Ensaio sobre a Constituição de 1988. 1ª ed. São Paulo: Editora LiberArs, 2019, v. 1, p. 185-196.

AUAD, Denise. A Importância dos Princípios para a Efetivação dos Direitos Fundamentais da Criança e do Adolescente, em especial do Princípio da Dignidade Humana sob o enfoque da Alteridade. In: AUAD, Denise e OLIVEIRA, Bruno Batista da Costa de. Direitos Humanos, Democracia e Justiça Social: Uma Homenagem à Professora Eunice Prudente – Da militância à academia. São Paulo: Letras Jurídicas, 2017, p. 361-386.

BILENKY, Thais. “Uma brecha na polarização política” in ALANA. Crianças e adolescentes primeiro: como o ECA Digital virou o jogo da proteção on-line no Brasil. São Paulo: Instituto Alana, 2026. pp.29-30

BROCHADO TEIXEIRA, Ana Carolina; FALEIROS JÚNIOR, José Luiz de Moura, DENSA, Roberta (coord.). Infância, adolescência e tecnologia - o Estatuto da Criança e do Adolescente na sociedade da informação. Indaiatuba: Editora Foco, 2022.

COLOMBO, Cristiano; FALEIROS JR., José Luiz de Moura; ENGELMANN, Wilson (org.). Tutela jurídica do corpo eletrônico: novos desafios ao direito digital. Indaiatuba: Editora Foco, 2022.

CRUZ, Elaine Patricia. Mais de 60% das denúncias de crimes na internet são de abuso infantil. Agência Brasil, São Paulo, 20 ago. 2025. Disponível em: <https://agenciabrasil.ebc.com.br/direitos-humanos/noticia/2025-08/mais-de-60-das-denuncias-de-crimes-na-internet-sao-de-abuso-infantil>. Acesso em: 20 de abril de 2026.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados. 3. ed. São Paulo: Revista dos Tribunais, 2021.

_____. A proteção dos dados pessoais como um direito fundamental. Espaço Jurídico Journal of Law [EJL], Joaçaba, v. 12, n. 2, p. 91-108, 2011. Disponível em: <https://periodicos.unoesc.edu.br/espacojuridico/article/view/1315>. Acesso em: 20 de abril de 2026.

EL KHATIB, Ahmed Sameer. Diversão ou armadilha? Um estudo exploratório das apostas esportivas (bets) entre universitários brasileiros sob a lente da Teoria do Comportamento Planejado (TCP). SciELO Preprints, versão 1, 18 out. 2024. Preprint. DOI: <https://doi.org/10.1590/SciELOPreprints.10133>. Acesso em: 31 mar. 2026.

eSAFETY COMMISSIONER (Austrália). Safety by Design: overview. [Sydney]: eSafety Commissioner, May 2019. 27 p. Disponível em: <https://www.esafety.gov.au/sites/default/files/2019-10/SBD%20-%20Overview%20May19.pdf>. Acesso em: 5 maio 2026.

HALFELD, Emanuella; COELHO, João Francisco de Aguiar. “Antes e depois: o que muda com a lei?” In ALANA. *Crianças e adolescentes primeiro: como o ECA Digital virou o jogo da proteção on-line no Brasil*. São Paulo: Instituto Alana, 2026. p. 166.

LEMOS, Ronaldo; SOUZA, Carlos Affonso Pereira de. Marco Civil da Internet: construção e aplicação. Rio de Janeiro: ed. Editor, 2016.

LIVINGSTONE, Sonia. Children and the Internet: Great Expectations, Challenging Realities. Polity Press, 2009.

_____. Children, Risk and Safety on the Internet. Policy Press, 2012.

_____. Parenting for a Digital Future: How Hopes and Fears about Technology Shape Children's Lives. Oxford University Press, 2020.

MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor. São Paulo: Saraiva, 2014.

_____. MENDES, Laura Schertel; DONEDA, Danilo Cesar Maganhoto; SOUZA, Carlos Affonso Pereira de; ANDRADE, Norberto Nuno Gomes de. Considerações iniciais

sobre inteligência artificial, ética e autonomia pessoal. Pensar - Revista de Ciências Jurídicas, Fortaleza, v. 23, n. 4, p. 1-17, 2018. DOI: <https://doi.org/10.5020/2317-2150.2018.8257>. Disponível em: <https://ojs.unifor.br/rpen/article/view/8257>. Acesso em: 02 de maio de 2026.

MIGALHAS. Roblox restringe chat e verifica idade; medida antecipa o ECA Digital. Migalhas, São Paulo, 22 jan. 2026. Atualizado em 21 jan. 2026. Disponível em: <https://www.migalhas.com.br/quentes/448269/roblox-restringe-chat-e-verifica-idade-medida-antecipa-o-eca-digital>. Acesso em: 4 de maio de 2026.

RODOTÀ, Stefano. A vida na sociedade da vigilância: a privacidade hoje. Organização, seleção e apresentação: Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SANTAELLA, Lucia. Navegar no ciberespaço: o perfil cognitivo do leitor imersivo. São Paulo: Paulus, 2004.

_____. Linguagens líquidas na era da mobilidade – Coleção Comunicação. São Paulo: Paulus, 2007.

SANTOS, Marco Aurelio Fernandes dos. Roblox e a insuficiência do aparato jurídico e policial brasileiro. Migalhas, São Paulo, 10 fev. 2026. Disponível em: <https://www.migalhas.com.br/depeso/449575/roblox-e-a-insuficiencia-do-aparato-juridico-e-policial-brasileiro>. Acesso em: 02 de maio de 2026

VIEIRA, Oscar Vilhena. “ECA Digital, preenchendo lacunas” In ALANA. Crianças e adolescentes primeiro: como o ECA Digital virou o jogo da proteção on-line no Brasil. São Paulo: Instituto Alana, 2026. p. 150.