

RISCOS DIGITAIS DE SEGUNDA ORDEM

o PL 2628/2022 sob a ótica da Teoria dos Sistemas Sociais

Eloisa Samy Santiago¹
Universidade Federal do Rio de Janeiro
esamyrtj@gmail.com

Resumo

O avanço das tecnologias digitais e a centralidade das plataformas de interação no cotidiano de crianças e adolescentes instauram um cenário de riscos que desafia os modelos tradicionais de proteção jurídica. O Projeto de Lei nº 2.628/2022, conhecido como “ECA Digital”, propõe atualizar o marco normativo brasileiro com o objetivo de resguardar os direitos da infância no ambiente virtual. A análise de suas disposições, à luz da teoria dos sistemas sociais de Niklas Luhmann, evidencia tensões entre a complexidade algorítmica e a capacidade do Direito de estabilizar expectativas sociais. O estudo examina os riscos digitais de segunda ordem, especialmente aqueles derivados da manipulação algorítmica e do vício comportamental, e problematiza os limites do ordenamento jurídico diante da opacidade e da mutabilidade das arquiteturas digitais. Sustenta-se que a eficácia protetiva não depende apenas da positivação de regras, mas da articulação entre regulação estatal, deveres de responsabilidade das plataformas e a incorporação de mecanismos técnicos voltados à mitigação de danos. A investigação, assim, contribui para uma reflexão crítica acerca dos limites e possibilidades do Direito diante das transformações digitais, oferecendo subsídios teóricos e práticos para o debate sobre a regulação da infância e da adolescência na sociedade em rede.

Palavras-chave: plataformas digitais; direitos da criança e do adolescente; manipulação algorítmica; vício comportamental; Teoria dos Sistemas Sociais.

SECOND-ORDER DIGITAL RISKS

Bill 2628/2022 from the perspective of Social Systems Theory

Abstract

The advancement of digital technologies and the centrality of interaction platforms in the daily lives of children and adolescents establish a landscape of risks that challenges traditional models of legal protection. Bill No. 2,628/2022, known as the “Digital ECA,” seeks to update the Brazilian legal framework with the purpose of safeguarding children’s rights in the virtual environment. An analysis of its provisions, in light of Niklas Luhmann’s social systems theory, reveals tensions between algorithmic complexity and the law’s ability to stabilize social expectations. This study examines second-order digital risks, particularly those arising from algorithmic manipulation and behavioral addiction, and problematizes the limits of the legal system in the face of the opacity and mutability of digital architectures. It argues that the effectiveness of protective measures depends not only on the enactment of rules but also on the articulation between state regulation, the responsibility of platforms, and the incorporation of technical mechanisms aimed at mitigating harm. The investigation thus contributes to a critical reflection on the limits and possibilities of law in the context of digital transformations, offering theoretical and practical insights for the debate on the regulation of childhood and adolescence in the network society.

Keywords: digital platforms; children’s rights; algorithmic manipulation; behavioral addiction; Social Systems Theory.

¹ Mestre em Direito pela Universidade Federal do Rio de Janeiro – UFRJ; Pós-graduada com Especialização em Gênero e Direito pela Escola da Magistratura do Estado do Rio de Janeiro – EMERJ; Advogada. Lattes: <http://lattes.cnpq.br/0827871638853240>. ORCID: <https://orcid.org/0009-0002-8739-7866>.



Esta obra está licenciada sob uma licença

Creative Commons Attribution 4.0 International (CC BY-NC-SA 4.0).

P2P & INOVAÇÃO, Rio de Janeiro, v. 12, n. 1, p. 1-22, e-7736, jul./dez. 2025.

RIESGOS DIGITALES DE SEGUNDO ORDEN

Proyecto de Ley 2628/2022 desde la perspectiva de la Teoría de Sistemas Sociales

Resumen

El avance de las tecnologías digitales y la centralidad de las plataformas de interacción en la vida cotidiana de niños, niñas y adolescentes crean un escenario de riesgos que desafía los modelos tradicionales de protección jurídica. El Proyecto de Ley n.º 2628/2022, conocido como "ECA Digital", propone actualizar el marco regulatorio brasileño con el objetivo de salvaguardar los derechos de la infancia en el entorno virtual. Un análisis de sus disposiciones, a la luz de la teoría de sistemas sociales de Niklas Luhmann, destaca las tensiones entre la complejidad algorítmica y la capacidad del derecho para estabilizar las expectativas sociales. El estudio examina los riesgos digitales de segundo orden, especialmente los derivados de la manipulación algorítmica y el sesgo conductual, y problematiza los límites del sistema jurídico ante la opacidad y la mutabilidad de las arquitecturas digitales. Se argumenta que la eficacia de la protección depende no solo del establecimiento de normas, sino también de la articulación de la regulación estatal, las obligaciones de rendición de cuentas de las plataformas y la incorporación de mecanismos técnicos destinados a mitigar el daño. Por lo tanto, la investigación contribuye a una reflexión crítica sobre los límites y las posibilidades del derecho ante las transformaciones digitales, ofreciendo perspectivas teóricas y prácticas para el debate sobre la regulación de la infancia y la adolescencia en la sociedad en red.

Palabras clave: plataformas digitales; derechos de niños, niñas y adolescentes; manipulación algorítmica; sesgo conductual; teoría de sistemas sociales.

1 INTRODUÇÃO

A expansão da vida social para ambientes digitais transformou de maneira profunda as formas de comunicação, de acesso à informação e de construção da subjetividade, atingindo de modo particularmente sensível crianças e adolescentes. Redes sociais, serviços de *streaming*, jogos online e aplicativos de entretenimento converteram-se em espaços privilegiados de aprendizagem, expressão e convivência, mas também configuram cenários de exposição a riscos inéditos, cuja natureza difere substancialmente das vulnerabilidades reconhecidas em contextos analógicos. Essa realidade interpela o Direito, enquanto sistema vocacionado a organizar expectativas sociais, exigindo a formulação de respostas capazes de assegurar direitos fundamentais sem sufocar o dinamismo próprio das tecnologias emergentes.

O Projeto de Lei nº 2.628/2022, aprovado pelo Congresso Nacional e denominado “ECA Digital”, insere-se nesse processo de atualização normativa. Inspirado no princípio do melhor interesse da criança, estabelece deveres de transparência, de mitigação de riscos e de suporte ao controle parental, articulando-se com debates internacionais sobre regulação de plataformas digitais, como o *Digital Services Act* da União Europeia, bem como com legislações específicas voltadas à salvaguarda de direitos infantojuvenis no espaço virtual. A positivação dessas regras, entretanto, não basta para garantir a efetividade da tutela almejada. Conforme adverte Niklas Luhmann, o Direito reduz a complexidade social mediante a estabilização de expectativas, mas não dispõe de meios diretos para controlar condutas individuais ou para intervir na evolução autônoma de sistemas tecnológicos. Essa constatação ganha acuidade no campo digital, em que algoritmos processam dados e ajustam parâmetros em frações de segundo, orientando fluxos de informação e induzindo engajamento de maneira invisível, enquanto as normas jurídicas mantêm estrutura relativamente estática, com ritmos de revisão incompatíveis com a velocidade de mutação das práticas algorítmicas.

Nesse horizonte surgem os chamados riscos digitais de segunda ordem, expressão utilizada para designar danos de caráter estrutural e cumulativo que derivam de escolhas de design, de modelos econômicos e de mecanismos de recomendação algorítmica. Diferenciam-se dos riscos clássicos, como a exposição direta a conteúdos ilícitos, porque se instalam de modo difuso, silencioso e persistente, moldando preferências, hábitos e padrões de comportamento. A manipulação das escolhas do usuário, a indução a estados de compulsão e o consequente vício comportamental digital resultam de arquiteturas persuasivas que exploram vulnerabilidades cognitivas e emocionais, especialmente agudas na infância e na adolescência. A opacidade desses processos, associada à sua capacidade de adaptação constante, desafia a

eficácia de instrumentos jurídicos tradicionais e reclama respostas regulatórias sofisticadas, capazes de integrar saberes técnicos, econômicos e sociológicos.

O presente artigo parte da hipótese de que o Projeto de Lei nº 2.628/2022, embora represente avanço normativo importante, enfrenta limitações substanciais no enfrentamento dos riscos digitais de segunda ordem. O ordenamento jurídico, tal como se estrutura, não alcança plenamente os mecanismos de manipulação algorítmica nem os efeitos psicossociais derivados do vício comportamental. A investigação, por conseguinte, busca responder à seguinte questão: até que ponto o Direito pode regular com eficácia a atuação das plataformas digitais diante da opacidade e da mutabilidade de seus algoritmos?

A relevância do tema justifica-se em diferentes planos. No plano jurídico, a proteção integral de crianças e adolescentes, consagrada no artigo 227 da Constituição Federal, demanda atualização contínua diante de novas formas de vulnerabilidade social. No plano social, os impactos da manipulação algorítmica e do vício digital incidem diretamente sobre o desenvolvimento psíquico e sobre a formação identitária de sujeitos em processo de amadurecimento. No plano teórico, a aplicação da teoria dos sistemas sociais de Niklas Luhmann oferece um quadro conceitual robusto para compreender os limites estruturais do Direito e propor alternativas regulatórias mais ajustadas à complexidade dos ambientes digitais.

O objetivo geral deste estudo consiste em analisar o Projeto de Lei nº 2.628/2022 à luz da teoria dos sistemas sociais autopoieticos, identificando seus alcances e restrições no enfrentamento dos riscos digitais de segunda ordem. Para tanto, estabelecem-se quatro objetivos específicos: investigar os fundamentos da complexidade digital e suas implicações para o Direito; caracterizar os mecanismos de manipulação algorítmica e de indução ao vício comportamental; examinar práticas técnicas que ampliam riscos e dificultam a responsabilização das plataformas; e avaliar, sob perspectivas teóricas e práticas, a viabilidade de um regime normativo mais responsivo às dinâmicas digitais.

A introdução cumpre, assim, a função de traçar o itinerário argumentativo que guiará o estudo. O texto desenvolve-se a partir da análise da complexidade digital e dos limites do código jurídico, discutindo a manipulação algorítmica e o vício digital sob o prisma da vulnerabilidade peculiar de crianças e adolescentes, e examinando práticas técnicas que potencializam riscos, tratando a proteção da infância como construção social. Por fim, confronta o Projeto de Lei nº 2.628/2022 com a teoria dos sistemas sociais de Luhmann, destacando limites e potencialidades de sua implementação.

2 O DIREITO E OS DESAFIOS DA REGULAÇÃO ALGORÍTMICA NO AMBIENTE DIGITAL

O ambiente digital apresenta uma complexidade estrutural que desafia profundamente as categorias jurídicas forjadas para realidades sociais mais estáveis e tecnicamente menos dinâmicas. A lógica algorítmica, que se apoia na mineração e no processamento de enormes volumes de dados em intervalos ínfimos de tempo, altera os contornos das interações sociais, reorganizando a maneira como preferências, hábitos e relações são constituídos. Cada clique, curtida, comentário ou segundo de permanência em uma plataforma transforma-se em dado valioso para sistemas de recomendação que, muitas vezes de forma opaca, moldam escolhas, condicionam comportamentos e criam perfis de vulnerabilidade e dependência.

Esse cenário coloca o Direito diante de um paradoxo: de um lado, a Constituição e o Estatuto da Criança e do Adolescente impõem a obrigação de conferir proteção especial a grupos em situação de maior fragilidade. De outro, a velocidade de transformação e a sofisticação das arquiteturas digitais excedem a capacidade dos instrumentos normativos clássicos, concebidos para ambientes sociais de mutação lenta ou previsível. Surge, então, uma tensão permanente entre a necessidade de tutela jurídica e a plasticidade dos sistemas tecnológicos, cujo ritmo de inovação torna obsoletos, em pouco tempo, mecanismos que pareciam adequados.

A teoria dos sistemas sociais de Niklas Luhmann oferece um referencial conceitual valioso para compreender a relação entre Direito e tecnologia. Para o autor, o Direito não regula condutas de maneira direta e individualizada; sua função consiste em estabilizar expectativas sociais por meio da distinção binária entre o lícito e o ilícito, criando condições de previsibilidade para a ação (Luhmann, 2016). Esse enfoque desloca o olhar da norma isolada para o funcionamento do sistema jurídico como rede autopoietica de comunicações, relativamente fechada, mas estruturalmente acoplada a outros sistemas, inclusive o tecnológico.

Luhmann observa que os sistemas sociais não se organizam primariamente como associações de indivíduos, mas como conjuntos de operações comunicativas. A sociedade reproduz-se por meio dessas operações e o fechamento operacional constitui elemento essencial de sua definição. A fronteira entre sistema social e ambiente corresponde, portanto, à distinção entre comunicações e não comunicações. A informação não ingressa de maneira bruta no sistema; ela é produzida internamente, segundo códigos e critérios próprios (Baxter, 2013).

Luhmann refere-se aos sistemas não primariamente como abertos, mas como fechados operacionalmente ou normativamente - embora, para complicar as coisas, também como cognitivamente abertos. Consideremos primeiro o que Luhmann entende por

fechamento operacional ou normativo. Ele vê o sistema social e seus subsistemas não como associações entre indivíduos - a concepção tradicional de sociedade -, mas como uma rede de operações. Essas operações são comunicações. Através da comunicação, a sociedade se mantém e se reproduz como um sistema. Dada a definição de Luhmann de sociedade como uma rede de comunicações, a ideia de que ela é fechada por essas operações chamadas comunicações é uma tautologia. A fronteira entre o sistema social e o ambiente não social é a fronteira entre comunicações e não-comunicações. Segundo Luhmann, a informação não entra do ambiente para o sistema; em vez disso, a informação é sempre produzida internamente, dentro do sistema, de acordo com procedimentos, padrões e critérios próprios desse sistema. (Baxter, 2013, p. 169). (Tradução nossa).

Nessa perspectiva, os sistemas algorítmicos - elementos centrais da arquitetura digital - podem ser analisados como estruturas autopoieticas e autorreferenciais, em analogia aos sistemas sociais descritos por Luhmann. Essas estruturas apresentam organização operacional fechada, sustentada por processos internos contínuos e recursivos. Cada operação gera insumos para as seguintes, alimentando ciclos que conferem estabilidade e autonomia. Embora interajam com dados externos, filtram o que lhes é relevante, garantindo consistência em suas operações. A autorreferência manifesta-se na capacidade de utilizar sua própria estrutura informacional para orientar decisões e gerar resultados, ajustando parâmetros e reproduzindo a lógica interna de funcionamento sem depender de intervenções imediatas (Totaro; Mangiante, 2025).

A característica autopoietica e autorreferencial dos algoritmos impõe ao Direito desafios singulares. A temporalidade normativa, mais lenta e vinculada a procedimentos deliberativos, não acompanha com facilidade operações que se renovam de forma ininterrupta, orientadas por critérios internos que escapam ao controle regulatório direto. Dessa defasagem surgem zonas de cegueira normativa, em que práticas de manipulação ou de indução ao vício permanecem fora do alcance de regras positivadas.

Nesse contexto, torna-se pertinente diferenciar riscos digitais de primeira e de segunda ordem. Os primeiros referem-se à exposição direta a conteúdos ilícitos ou manifestamente inadequados, passíveis de enquadramento por institutos jurídicos tradicionais. Os segundos resultam da própria estrutura técnica e econômica das plataformas, traduzindo-se em processos cumulativos de influência sutil sobre preferências e em dinâmicas de estímulo compulsivo ao uso. Não se apresentam como episódios isolados, mas como fluxos persistentes e difusos, que afetam um número indeterminado de usuários e exigem respostas voltadas à arquitetura de funcionamento e aos incentivos econômicos que sustentam essas tecnologias.

O Projeto de Lei nº 2.628/2022, ao enumerar práticas vedadas e impor obrigações de transparência e mitigação, expressa o esforço legislativo de transformar um fenômeno volátil em categorias jurídicas aptas a produzir efeitos normativos. Essa tentativa, contudo, revela o caráter inevitavelmente simplificador da regulação: para operar, toda norma precisa estabilizar

dinâmicas sociais e tecnológicas em formas relativamente fixas, deixando fora de seu escopo aspectos relevantes da realidade. Assim, modalidades mais refinadas de manipulação - como a exploração da atenção infantil por meio de *dark patterns* ou o emprego de estímulos intermitentes destinados a prolongar o engajamento - frequentemente permanecem fora do alcance imediato do Direito.

Experiências estrangeiras ajudam a ilustrar o tratamento regulatório do problema. A California Privacy Rights Act definiu *dark patterns* como interfaces projetadas para subverter a autonomia ou prejudicar a tomada de decisões do usuário. O Digital Services Act da União Europeia conceituou-os como práticas capazes de distorcer escolhas livres e informadas, proibindo expressamente seu uso. O European Data Protection Board, por sua vez, emitiu diretrizes para orientar o reconhecimento e a eliminação dessas técnicas enganosas.

Paralelamente, a economia comportamental, por meio de pesquisas sobre nudges, demonstrou que a arquitetura de escolhas pode influenciar decisões sem eliminar a liberdade formal de opção. O Age Appropriate Design Code do Reino Unido incorpora essas preocupações ao restringir o uso de nudges que induzam crianças a decisões de privacidade inadequadas, recomendando, ao contrário, aqueles voltados à proteção de dados, saúde e bem-estar (Kidron; Rudkin, 2024).

7

DARK PATTERNS

A *California Privacy Rights Act*, aprovada em 2020, é considerada a primeira legislação a fornecer uma definição de *dark patterns*, da seguinte forma: “uma interface de usuário projetada ou manipulada com o efeito substancial de subverter ou prejudicar a autonomia, a tomada de decisão ou a escolha do usuário.” A *Digital Services Act* (DSA) da União Europeia define *dark patterns* como “práticas que distorcem ou prejudicam materialmente, seja intencionalmente ou de fato, a capacidade dos destinatários do serviço de tomar decisões ou escolhas autônomas e informadas.” A DSA proíbe expressamente que serviços online utilizem *dark patterns*, apresentem escolhas de forma não neutra ou subvertam a autonomia, a tomada de decisão ou a livre escolha dos usuários. O *European Data Protection Board* também publicou diretrizes sobre padrões de design enganosos em interfaces de plataformas de mídia social, oferecendo recomendações para controladores de mídia social sobre como reconhecer e evitar esses padrões.

TÉCNICAS DE NUDGE

As técnicas de *nudge* se baseiam no conceito da economia comportamental de que o design de “ambientes de decisão”, também conhecido como “arquitetura de escolha”, influencia a tomada de decisão individual e coletiva. Sem privar os tomadores de decisão de escolha, essas técnicas influenciam as decisões que eles tomam. Essa teoria foi popularizada por dois acadêmicos americanos da Universidade de Chicago, o economista comportamental Richard Thaler e o jurista Cass Sunstein, que em 2008 publicaram o livro *Nudge: Improving Health, Wealth and Happiness*. Eles definem um *nudge* como “qualquer aspecto da arquitetura de escolha que altera o comportamento das pessoas de forma previsível, sem proibir opções ou alterar significativamente seus incentivos econômicos.”

O *Age Appropriate Design Code* do Reino Unido faz referência às técnicas de *nudge* em seus padrões de proteção de dados de crianças. Define essas técnicas como “recursos de design que conduzem ou incentivam os usuários a seguir os caminhos preferidos pelo projetista na tomada de decisão do usuário.” Serviços provavelmente acessados por crianças têm proibido o uso de técnicas de *nudge* para induzir decisões de privacidade inadequadas, de acordo com o AADC. Também são incentivados a utilizar *nudges* pró-privacidade e *nudges* projetados para promover saúde e bem-estar. O AADC foi o primeiro código legal a fazer referência ao uso de *nudges*, incorporando o design persuasivo firmemente no âmbito de atuação dos reguladores de privacidade. (Kidron; Rudkin, 2024, p. 11). (Tradução nossa).

O descompasso entre a rapidez das transformações tecnológicas e o ritmo mais lento dos processos legislativos, administrativos e judiciais intensifica a vulnerabilidade de crianças e adolescentes. Plataformas inovam constantemente, testando novas interfaces e estratégias de engajamento, enquanto a elaboração normativa e o controle institucional requerem prazos extensos de análise, debate e implementação. Não raro, práticas prejudiciais consolidam-se ou são substituídas por mecanismos ainda mais sofisticados antes mesmo que ocorra sua proibição formal. Essa realidade expõe a insuficiência dos instrumentos tradicionais para acompanhar o ciclo acelerado da inovação digital.

A análise sistêmica da relação entre Direito e tecnologia revela que, embora o sistema jurídico seja operacionalmente fechado, ele se acopla estruturalmente aos sistemas tecnológicos, que operam segundo códigos e lógicas próprios. Todavia, a sanção jurídica, ainda que essencial para estabelecer fronteiras e proibir condutas, não penetra nos processos internos que regulam algoritmos e códigos-fonte. A eficácia regulatória depende, portanto, de instrumentos flexíveis e dialógicos, capazes de interagir com a evolução das tecnologias e de adaptá-las aos imperativos de proteção.

Nesse cenário, a tutela de crianças e adolescentes demanda auditorias independentes e periódicas, a responsabilização efetiva das plataformas e a fixação de parâmetros técnicos mínimos para o desenho e a operação de sistemas digitais (Frazão, 2021). A efetividade jurídica não resulta apenas da precisão das regras, mas da criação de uma interface operacional entre Direito, sociedade e tecnologia, sustentada por cooperação intersetorial e monitoramento permanente. A regulação digital requer, assim, criatividade normativa e um deslocamento epistemológico: de uma atuação meramente reativa para um posicionamento prospectivo, atento aos riscos e potencialidades trazidos pela digitalização da vida social.

O Supremo Tribunal Federal, em reiteradas decisões, tem reconhecido que os direitos fundamentais irradiam efeitos diretos sobre relações privadas, independentemente de delegação legislativa específica. Parte da Corte fundamenta essa incidência no princípio da dignidade da pessoa humana e na força normativa da Constituição (Figueiredo, 2009). Essa compreensão reforça a ideia de que uma regulação que se limite a esquemas formais, ignorando as

singularidades das práticas sociais e tecnológicas, corre o risco de produzir novos erros e injustiças. Impõe-se, por isso, um esforço interpretativo que conjugue princípios normativos e sensibilidade às transformações concretas do ambiente digital.

3 RISCO ALGORÍTMICO: MANIPULAÇÃO E VÍCIO DIGITAL

A centralidade que as plataformas digitais adquiriram na vida cotidiana de crianças e adolescentes configura um desafio que transcende a preocupação restrita com a exposição a conteúdos ilícitos ou inadequados. O núcleo do problema reside na própria lógica de funcionamento dos sistemas algorítmicos, cujas operações não apenas refletem preferências individuais, mas também as condicionam de maneira sistemática. O que se apresenta sob a aparência de “personalização” (suposta adaptação de conteúdos às escolhas autônomas do usuário) revela-se, no plano interno, um processo de condicionamento progressivo, orientado por critérios objetivos de maximização da atenção e de rentabilidade econômica (Zuboff, 2021).

Um estudo sobre plataformas de mídia social com algoritmos de personalização, focado no TikTok, revela como esses sistemas não só decidem o que os usuários veem, mas também transformam profundamente sua experiência, comportamento e percepções. Os algoritmos, projetados para maximizar o engajamento, geram picos de dopamina, induzem o uso excessivo e fazem os usuários perderem a noção do tempo. Muitos acreditam que controlam o conteúdo que consomem, mas essa sensação de autonomia é uma ilusão. Na prática, os algoritmos ditam o fluxo de informações, manipulando preferências e mantendo os usuários presos em um ciclo de consumo contínuo. O controle, quando existe, é limitado e altamente direcionado pela própria plataforma (Koç, 2023).

A manipulação algorítmica manifesta-se, assim, como um processo invisível, cumulativo e adaptativo. Ela redefine a percepção do sujeito, delimitando o campo de possibilidades a partir de parâmetros econômicos e comportamentais estabelecidos pelo design da plataforma. A teoria dos sistemas sociais de Luhmann oferece instrumento hermenêutico para compreender essa dinâmica: o algoritmo deve ser pensado não apenas como ferramenta técnica, mas como subsistema capaz de criar expectativas próprias e de ajustá-las de modo recursivo, recalibrando, a cada interação, o que é considerado relevante. O risco de segunda ordem, portanto, reside na estrutura mesma do ambiente digital, configurado para capturar atenção e induzir padrões específicos de comportamento.

O vício digital surge como efeito direto dessa arquitetura algorítmica. Dependendo de seu desenho intencional, induz a uma dependência comportamental, alicerçada na exploração

deliberada de mecanismos neuropsicológicos. Recompensas intermitentes, notificações constantes e o recurso da rolagem infinita ativam circuitos cerebrais de recompensa, fomentando ciclos compulsivos de uso. A situação é particularmente grave no caso de crianças e adolescentes, cuja vulnerabilidade é agravada pelo estágio imaturo do córtex pré-frontal - região cerebral responsável pela regulação do autocontrole -, o que favorece reações imediatas em detrimento de reflexões ponderadas (Costello *et al.*, 2023).

Outro fenômeno relevante é a proliferação das chamadas *loot boxes* em jogos eletrônicos, cuja estrutura simula dinâmicas de aposta. Esses dispositivos operam com base na promessa de ganhos aleatórios, estimulando expectativas ilusórias de recompensa e favorecendo padrões de comportamento semelhantes aos observados em jogos de azar. Pesquisas indicam correlação significativa entre o uso de *loot boxes* e comportamentos problemáticos entre adolescentes, evidenciando o impacto econômico e psicológico dessa forma de design digital (Hadlac *et al.*, 2023). A monetização das interações infantis, portanto, não constitui efeito colateral, mas elemento intrínseco à lógica empresarial que sustenta tais plataformas.

A opacidade que caracteriza os sistemas de recomendação amplifica o problema. A maior parte dos usuários não dispõe de informações suficientes para compreender os critérios que determinam a seleção e a hierarquização dos conteúdos que consomem. Essa assimetria informacional compromete a autonomia e cria obstáculos para a responsabilização das empresas, que muitas vezes alegam desconhecimento sobre o funcionamento detalhado de seus próprios modelos, dada a complexidade e a plasticidade de processos internos em constante evolução (Szymielewicz *et al.*, 2024).

A tutela da infância e da adolescência não pode, nesse contexto, restringir-se à repressão de atos ilícitos pontuais, pois o risco decorre de uma lógica estrutural que orienta o design e a operação das plataformas. Tentar enquadrar a manipulação algorítmica em figuras jurídicas tradicionais - como publicidade enganosa ou abuso de poder econômico - revela-se insuficiente, porque ignora a persistência e a sistematicidade dessas práticas. A manipulação encontra-se entranhada na economia da atenção e é funcional aos modelos de negócio que priorizam engajamento e retenção.

A proteção integral assegurada pelo Estatuto da Criança e do Adolescente abrange, entre outros, o direito ao respeito, compreendido como inviolabilidade da integridade física, psíquica e moral, e o direito de acesso a produtos e serviços compatíveis com a condição peculiar de pessoa em desenvolvimento (Brasil, 1990, arts. 17 e 71). Nessa perspectiva, os riscos digitais de segunda ordem devem ser compreendidos como efeitos sistêmicos, associados

à mercantilização da atenção e ao aproveitamento de fragilidades cognitivas. A eliminação desses riscos requer revisão crítica dos instrumentos jurídicos disponíveis e a formulação de mecanismos capazes de incidir sobre a arquitetura das plataformas.

O Projeto de Lei nº 2.628/2022 representa avanço relevante ao impor obrigações às empresas e ao fixar parâmetros mínimos de proteção, mas sua eficácia depende da incorporação de medidas técnicas, como auditorias periódicas, aplicação do princípio *safe by default* e previsão de sanções capazes de modificar incentivos econômicos. A ausência desses instrumentos compromete o alcance normativo do diploma e ameaça reduzi-lo a elemento simbólico, sem efetiva ingerência sobre os fatores estruturais que sustentam a manipulação e o vício digital.

O vício comportamental digital pode ser definido como um padrão recorrente de uso compulsivo, caracterizado pela dificuldade de interrupção voluntária e pela interferência na vida cotidiana. Diferentemente das dependências químicas, resulta da exploração intencional de circuitos de recompensa por meio de estímulos constantes e calibrados. Essa dependência é inseparável da arquitetura persuasiva das plataformas, que recorre a elementos de design voltados à maximização do tempo de permanência e do engajamento (Lumen Learning, 2025). Recompensas variáveis, notificações incessantes e retorno social imediato instauram um sistema de reforço positivo, propiciando adesão continuada. A compulsividade digital constitui resultado previsto e explorado economicamente.

A literatura recente também discute a rolagem infinita como mecanismo que prolonga a exposição do usuário e provoca arrependimento pelo tempo despendido. Estudos mostram que *feeds* de notícias e funcionalidades de entretenimento estão entre os elementos mais associados ao prolongamento involuntário do uso, o que evidencia seu papel na criação de experiências negativas e na perda de controle (Rixen *et al.*, 2023). Entre crianças e adolescentes, a vulnerabilidade é agravada por fatores neuropsicológicos: maior sensibilidade a recompensas imprevisíveis, predominância de decisões rápidas e imaturidade de estruturas cerebrais ligadas ao autocontrole (Costello *et al.*, 2023). Essa combinação favorece padrões compulsivos e explica por que técnicas de reforço contínuo têm efeitos mais profundos nessa faixa etária.

Do ponto de vista do Direito do Consumidor, tais constatações exigem revisão das categorias protetivas, historicamente orientadas para fraudes explícitas ou abusos contratuais. É necessário incorporar à dogmática a indução comportamental sutil promovida por *dark patterns* e interfaces persuasivas, reconhecendo a formação de designs que induzem à adicção como prática que compromete a autonomia e instrumentaliza vulnerabilidades psicológicas.

A teoria dos sistemas sociais permite, enfim, compreender que o vício comportamental

digital não deriva de ato ilícito isolado, mas do funcionamento integrado de um ambiente técnico-econômico estruturado para capturar atenção e extrair valor.

O Direito, alicerçado na distinção lícito/ilícito, encontra dificuldades para enquadrar condutas difusas, cuja eficácia depende da exploração de brechas cognitivas em larga escala. A conceituação jurídica do vício digital, portanto, deve ultrapassar a constatação de danos individuais, reconhecendo-o como risco político que ameaça a formação da autonomia, a saúde mental e o desenvolvimento social de crianças e adolescentes. A resposta normativa deve alcançar a própria configuração das plataformas, impondo padrões técnicos, limites explícitos e regras que impeçam a exploração sistemática de fragilidades cognitivas e emocionais.

4 PRÁTICAS TÉCNICAS AMPLIFICANDO O RISCO INFANTIL

O ambiente digital intensifica significativamente a exposição de crianças e adolescentes às plataformas online, configurando um risco específico e agravado, distinto daquele amplamente enfrentado por usuários adultos. A literatura atual mostra que certas práticas técnicas adotadas por essas plataformas potencializam a atenção e o engajamento infantojuvenil e também geram riscos psicológicos, comportamentais e econômicos, colocando o Direito diante de um desafio regulatório e ético de elevada complexidade.

Destaca-se, em primeiro plano, a frequente adoção dos chamados testes A/B, método consistente na experimentação simultânea de múltiplas versões de interfaces, fluxos e funcionalidades, cujo propósito é aferir quais variantes incrementam a permanência e interação do usuário. Quando dirigidos ao público infantil, tais experimentos convertem-se em instrumentos de manipulação comportamental, pois operam sem a observância de critérios éticos adequados, aproveitando-se da vulnerabilidade cognitiva peculiar à infância (Harrington, 2023). As alterações recorrentes nas interfaces, além de prejudicarem a percepção crítica da criança quanto à experiência digital vivida, facilitam a consolidação de hábitos compulsivos, com potenciais danos duradouros à atenção e à capacidade de autocontrole.

Outra prática com impacto direto sobre o risco infantil reside na otimização pautada por métricas econômicas. As plataformas digitalizam e monetizam a atenção de seus usuários mediante a coleta e análise de dados como tempo de uso, número de cliques e frequência de interações, transformando o *feed* digital em uma verdadeira máquina de captura de atenção infantil (Szymielewicz *et al.*, 2024). Esse *modus operandi* converge com modelos de negócio voltados à receita publicitária e às microtransações, elevando substancialmente a possibilidade de exploração econômica de menores. Nessa lógica, a atenção da criança passa a ser tratada

como um insumo monetizável, tornando inexorável a responsabilização das plataformas frente ao potencial de prejuízo.

No espectro das estratégias de reforço comportamental, o uso sistemático de recompensas intermitentes e microtransações, entre as quais moedas virtuais, bônus aleatórios e conquistas digitais, reproduz programas clássicos de condicionamento psicológico. Tais mecanismos estimulam o hábito repetitivo e o consumo contínuo de conteúdos e produtos digitais, configurando, segundo a perspectiva neuropsicológica, riscos comparáveis aos de padrões aditivos (Lumen Learning, 2025).

A imprevisibilidade do benefício advinda da intermitência das recompensas assegura o engajamento persistente, enquanto a monetização direta incute vulnerabilidades financeiras tanto na esfera infantil quanto familiar. A consequência jurídica é evidente: decisões técnicas de engenharia de produto extrapolam a experiência digital, adentrando o domínio de danos comportamentais e econômicos de notório relevo. Também a personalização hipersegmentada figura como vetor relevante de riscos infantis. Mediante a coleta massiva e detalhada de dados, as plataformas ajustam conteúdos e anúncios às preferências e vulnerabilidades psicológicas individuais das crianças para maximizar seu engajamento (Szymielewicz *et al.*, 2024). Tal prática, frequentemente ocultada aos pais e a órgãos reguladores, amplia o potencial de exploração dos desejos e impulsos infantis, ao mesmo tempo em que dificulta a responsabilização empresarial pelo impacto cumulativo dessas escolhas de design. Este quadro torna imperativa a adoção de normas que vedem expressamente a utilização de dados sensíveis para fins de manipulação comportamental de menores.

A fragmentação organizacional e a terceirização de decisões estratégicas compõem outro fator que agrava o risco infantil. A dispersão das responsabilidades e a complexidade estrutural das organizações intensificam a dificuldade de realização de auditorias efetivas, tornando mais nebulosa a identificação do responsável pelos impactos adversos na criança. Tal opacidade operacional compromete não apenas a responsabilização judicial, mas prejudica também a capacidade estatal de formular e executar políticas regulatórias preventivas eficazes.

A arquitetura do produto digital, ao priorizar métricas de engajamento e rentabilidade, tende a normalizar como externalidade legítima os danos causados à criança. As escolhas de design que provocam prejuízos à infância são incorporadas como custos aceitáveis dentro do modelo de negócio, e não como riscos a serem mitigados. Esse fenômeno demanda uma compreensão jurídica crítica capaz de aferir de que modo as normas de proteção à criança e ao adolescente podem ser internalizadas no processo de desenvolvimento tecnológico, convertendo a tutela infantil em parâmetro central da concepção digital.

Com base em nossas avaliações de risco abrangentes, essas ferramentas de IA apresentam riscos inaceitáveis para crianças e adolescentes menores de 18 anos e não devem ser utilizadas por menores. Recomendamos:

Nenhum companheiro social de IA para jovens menores de 18 anos.

Os desenvolvedores devem implementar mecanismos robustos de verificação de idade além da autodeclaração.

As plataformas devem ser examinadas quanto a possíveis manipulações relacionais e à criação de dependência emocional.

A conscientização dos pais e o diálogo com os adolescentes são essenciais.

São necessárias pesquisas adicionais sobre os impactos emocionais e psicológicos.

[...]

Adolescentes, cujos cérebros ainda estão em desenvolvimento, podem ter dificuldade em separar relacionamentos humanos de vínculos com a IA. Em nossos testes, os companheiros sociais de IA frequentemente afirmaram ser “reais”, possuíam sentimentos e participavam de atividades humanas como comer ou dormir. Esse comportamento enganoso aumenta o risco de que jovens usuários se tornem dependentes desses relacionamentos artificiais (Common Sense Media, 2025). (Tradução nossa).

14

Para que a eficácia normativa na redução do risco infantil seja alcançada, é imprescindível a incidência sobre escolhas de design, processos de desenvolvimento e mecanismos de responsabilização. Entre as medidas indicadas na literatura destacam-se: (1) a proibição de mecânicas de aposta para menores; (2) a implementação compulsória de padrões protetivos por padrão (tais como *privacy by design* e *safety by design*); (3) a mensuração contínua de indicadores de risco infantil; (4) a realização periódica de auditorias independentes; e (5) o condicionamento da oferta e comercialização dos produtos digitais à demonstração efetiva de mitigação de danos (Szymielewicz *et al.*, 2024). Este conjunto de medidas reconhece que a proteção da infância demanda regulação proativa, integrada e antecipatória.

A conjugação dessas práticas demonstra que o risco infantil não é contingente ou decorrente de mau uso ocasional, mas estrutural e inseparável da própria concepção e operação das plataformas digitais. Ao entrelaçar incentivos econômicos, engenharia comportamental e opacidade organizacional, as plataformas ampliam as vulnerabilidades cognitivas e emocionais dos menores, impondo ao Direito o imperativo de formular respostas regulatórias robustas e fundamentadas.

A tutela eficaz do risco infantil exige, portanto, um modelo jurídico que articule proteção por design, responsabilização clara e auditoria contínua, prevenindo a banalização e naturalização da exposição das crianças a danos evitáveis, e enfrentando os desafios da nova economia digital em sua raiz.

5 RESPONSABILIZAÇÃO DIGITAL INFANTIL E SOLUÇÕES TECNOLÓGICAS DE PROTEÇÃO

A proteção da criança e do adolescente no ambiente digital constitui uma construção social na qual normas, tecnologia e práticas empresariais devem ser articuladas para eliminar riscos previsíveis e estruturalmente produzidos. Diante dessa realidade, o ordenamento jurídico deve impor um dever de responsabilidade proporcional ao poder exercido pelas grandes plataformas digitais, responsáveis por decisões de design e infraestrutura que condicionam o uso e a experiência infantojuvenil no espaço digital.

Instala-se um dos problemas centrais na efetividade dessa proteção na fragilidade dos métodos tradicionais de verificação etária. Sistemas que dependem da mera autodeclaração, por meio do preenchimento de formulários ou da indicação de data de nascimento, demonstraram-se vulneráveis a contornos e fraudes. O resultado são brechas significativas que comprometem a eficácia de mecanismos legais e contratuais de salvaguarda da infância no ciberespaço.

Em resposta a esses desafios, tecnologias emergentes - notadamente o uso do *blockchain* -, apresentam soluções promissoras. A implementação de *tokens* digitais para registro criptográfico do consentimento parental viabiliza a prova irrefutável da autorização, sem expor dados pessoais sensíveis, ampliando a proteção da privacidade infantil e assegurando conformidade com a regulação aplicável (Crypto ID, 2025). Experiências práticas nessa seara, como exemplificado pelo projeto TrustNFT (2025) indicam que tais mecanismos tecnológicos podem ser plenamente integrados à infraestrutura das plataformas digitais. Essa integração assegura rastreabilidade, autenticidade do consentimento parental e alinhamento às previsões do Projeto de Lei nº 2.628/2022, à Lei Geral de Proteção de Dados (Brasil, 2018) e a marcos regulatórios internacionais, como o *Digital Services Act* (UE, 2024). Assim se fortalece a legitimidade jurídica e a operacionalização da tutela digital da infância por meio de soluções tecnológicas inovadoras e conformes ao ordenamento jurídico vigente.

O *Estudo Técnico sobre Sandbox Regulatório*, elaborado pela Autoridade Nacional de Proteção de Dados (Brasil, 2023), constitui um marco significativo no debate acerca da regulação ágil e inovadora no contexto do tratamento de dados pessoais, especialmente quando voltado à proteção de grupos em situação de vulnerabilidade, como crianças e adolescentes. Ao propor a criação de um ambiente controlado de experimentação (*sandbox* regulatório) o documento abre caminho para a implementação de soluções tecnológicas e jurídicas que conciliem o fomento à inovação com a garantia dos direitos fundamentais de proteção de dados. No que tange à proteção de crianças e adolescentes no ambiente digital, o estudo oferece um

terreno promissor para o desenvolvimento e teste de mecanismos capazes de assegurar, de forma eficaz e segura, o consentimento dos responsáveis legais, sem, contudo, comprometer a privacidade dos titulares. Nesse sentido, uma das possibilidades mais promissoras reside na experimentação de sistemas de consentimento digital verificável, nos quais a autenticação da condição de responsável possa ser realizada por meio de identidade digital certificada, como a plataforma Gov.br, garantindo assim a legitimidade da autorização conforme exigido pelo artigo 12, inciso III, da Lei Geral de Proteção de Dados (LGPD).

Nesse modelo, o uso de tecnologias como *tokens* digitais assinados criptograficamente pode permitir o registro inequívoco da anuência, sem que os dados pessoais sensíveis, como documentos completos ou informações biométricas, sejam armazenados ou expostos desnecessariamente, alinhando-se aos princípios da minimização e da limitação de finalidade. Ademais, o estudo incentiva a adoção de uma abordagem de *privacy by design*, isto é, a incorporação de medidas de proteção de dados desde as fases iniciais de desenvolvimento de produtos e serviços digitais. No caso de plataformas voltadas ao público infantil, isso implica na implementação de controles técnicos, como anonimização e pseudo anonimização, e na concepção de interfaces adequadas à idade e ao grau de maturidade das crianças, de modo a promover uma compreensão clara e acessível sobre o uso de seus dados. Esse cuidado reflete o dever de transparência reforçado previsto na Recomendação nº 2/2021 da ANPD, que orienta os agentes de tratamento a adotarem mecanismos claros e adequados para informar crianças sobre o processamento de suas informações pessoais.

Outro aspecto de grande relevância diz respeito à verificação de idade (*age assurance*), um desafio central para a aplicação efetiva das normas protetivas no ambiente online. O sandbox regulatório permite a testagem de soluções que equilibrem precisão e proteção da privacidade, como o uso de provas de conhecimento zero (*zero-knowledge proofs*), nas quais a idade do usuário pode ser confirmada sem a necessidade de revelar dados sensíveis, como a data completa de nascimento. Trata-se de um avanço significativo, pois evita a coleta excessiva de informações e reduz os riscos associados ao tratamento indevido de dados de crianças em plataformas que não deveriam ser acessadas por esse público. Ainda, a supervisão contínua por parte da ANPD durante o período experimental assegura que eventuais impactos negativos sejam identificados e mitigados prontamente, reforçando o regime de responsabilidade e prestação de contas (*accountability*) exigido pela LGPD.

O design das plataformas é intencional, não neutro. Interfaces, fluxos e algoritmos são projetados para capturar e prender a atenção dos usuários de forma sistemática, gerando riscos estruturais que não podem ser ignorados como meros efeitos colaterais. Dentre tais riscos,

sobressaem a exposição precoce a conteúdos impróprios, a potencialização de comportamentos aditivos mediante recompensas intermitentes e microtransações, e a coleta intensiva de dados pessoais para fins de segmentação e hiper personalização (Szymielewicz *et al.*, 2024; Lumen Learning, 2025).

Essa combinação de fatores configura um ambiente de influência deliberada sobre crianças, capaz de comprometer negativamente sua autoestima, desenvolvimento psicossocial e hábitos de consumo, impactos com consequências jurídicas que exigem uma resposta regulatória integrada e proporcional.

A insuficiência do arcabouço jurídico atual torna-se ainda mais evidente diante do impacto dos sistemas decisórios automatizados sobre crianças e adolescentes. Essa deficiência manifesta-se em três níveis críticos: (i) ausência de deveres específicos de transparência e auditabilidade voltados à proteção de sujeitos em fase de desenvolvimento; (ii) carência de mecanismos acessíveis e eficazes de participação, escuta e contestação frente a decisões algorítmicas que afetam diretamente a educação, saúde, segurança e inclusão social de crianças e adolescentes; (iii) fragilidade institucional das estruturas estatais responsáveis por supervisionar tecnicamente e regular normativamente esses sistemas, especialmente na garantia dos direitos fundamentais *infantojuvenis*. Somadas, essas falhas configuram um déficit de legitimidade democrática e um risco grave à base ético-jurídica da prioridade absoluta assegurada às crianças e adolescentes no Estado de Direito.

Diante disso, o reconhecimento jurídico dos riscos estruturais exige que a tecnologia deixe de ser vista como infraestrutura neutra e passe a ser entendida como espaço regulatório, onde interações sociais e econômicas significativas ocorrem e que, por isso, demanda responsabilidades proporcionais ao poder exercido pelas plataformas. Neste cânone, a responsabilização demanda uma atuação proativa, com a imposição de obrigações proporcionais ao porte, poder econômico e domínio tecnológico dessas corporações.

6 CONSIDERAÇÕES FINAIS

A análise desenvolvida neste trabalho, buscou-se evidenciar que o design das plataformas digitais não é neutro no contexto da experiência online de crianças e adolescentes. Ao estruturar fluxos, interfaces e algoritmos, esses sistemas atuam de forma deliberada e sistemática para capturar a atenção dos usuários, gerando riscos que não podem ser tratados como efeitos colaterais fortuitos, mas como consequências diretas da configuração técnica e econômica das plataformas. Nesse cenário, destacam-se riscos estruturais de alta gravidade:

exposição precoce a conteúdos inadequados, intensificação de comportamentos viciantes e coleta massiva de dados pessoais, todos elementos de uma influência premeditada.

A constante exposição a padrões idealizados de aparência, sucesso e comportamento exerce impacto negativo sobre a autoestima, o desenvolvimento psicossocial e a formação de limites saudáveis nesse público. A literatura científica demonstra que tais efeitos surgem estruturalmente das escolhas técnicas e econômicas voltadas à maximização do engajamento e da monetização, em um quadro que reforça a urgência de intervenção regulatória direcionada, contínua e eficaz.

A proteção integral de crianças e adolescentes, assegurada constitucionalmente como prioridade absoluta, exige reconhecer que a arquitetura algorítmica e as plataformas digitais não operam em um espaço neutro ou privado de comunicação, mas constituem a infraestrutura do espaço público contemporâneo. Ao controlar fluxos informacionais, dinâmicas de visibilidade e formas de interação social, essas estruturas tecnológicas assumem função pública, ainda que sob gestão privada. Tal condição impõe-lhes deveres reforçados de governança e regulação, compatíveis com o mandamento constitucional de proteção prioritária à infância e à juventude. Assim, a proteção efetiva desses sujeitos em formação não pode ser dissociada da regulação da própria arquitetura digital. A configuração técnica dos sistemas molda, condiciona e, em muitos casos, expõe vulnerabilidades cognitivas, emocionais e psicológicas, exigindo uma atuação jurídica que vá além da mera correção de danos.

No contexto do poder concentrado que as plataformas exercem sobre a infraestrutura digital, impõe-se um imperativo jurídico: o dever de responsabilidade proporcional ao grau de influência que detêm. A imposição de sanções e mecanismos de responsabilização não deve ser vista apenas como instrumento punitivo *ex post*, mas como ferramenta essencial para compelir ajustes tecnológicos alinhados às normas jurídicas, promovendo a convergência entre design, algoritmos e regulação. Essa responsabilidade implica supervisão e cuidado compatíveis com o impacto potencial dessas plataformas sobre o desenvolvimento infantil e juvenil, afinal, o poder de moldar comportamentos exige deveres acrescidos de proteção.

Nesse quadro, destaca-se o papel do Projeto de Lei nº 2.628/2022, avanço legislativo necessário que estabelece regras para limitar a exposição de crianças a conteúdos prejudiciais e define parâmetros claros para a coleta e tratamento de seus dados pessoais. Contudo, é fundamental reconhecer que as limitações inerentes ao Direito nem sempre alcançam a complexidade dinâmica dos sistemas algorítmicos. A opacidade, a velocidade de mutação e a capacidade crescente de influenciar decisões individuais ampliam o risco de danos cumulativos e invisíveis, que escapam aos mecanismos tradicionais de fiscalização e responsabilização.

Para garantir proteção efetiva, torna-se indispensável uma articulação integrada entre normas jurídicas, plataformas digitais, desenvolvimento tecnológico e atuação estatal de fiscalização. Somente por meio dessa convergência será possível recalibrar a complexidade digital em favor do interesse superior da criança e do adolescente, prevenindo manipulações sutis, exploração de vulnerabilidades cognitivas e consequências psicológicas decorrentes do engajamento algorítmico. A proteção integral, portanto, exige uma abordagem proativa, na qual design ético, auditoria contínua e responsabilização jurídica atuem de forma coordenada e sinérgica.

A proteção eficaz desse grupo vulnerável depende da incorporação, desde a concepção dos produtos, dos princípios de segurança e ética - materializados nos conceitos de *safety by design* e *privacy by design* -, aliada a normas jurídicas consistentes e a mecanismos de fiscalização e responsabilização proporcionais ao poder das plataformas. Apenas assim será possível mitigar danos cumulativos, preservar a autonomia em formação e garantir que a experiência digital respeite, de modo efetivo, os direitos fundamentais das crianças e adolescentes.

REFERÊNCIAS

BAXTER, Hugh. *Niklas Luhmann's Theory of Autopoietic Legal Systems*. **Annual Review of Law and Social Science**, v. 9, p. 167–184, 2013.

BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). **Estudo Técnico sobre Sandbox Regulatório**. Brasília, DF, 2023. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/estudo_tecnico_sandbox_regulatorio_versao_publica.pdf. Acesso em: 30 ago. 2025.

BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). **Recomendação nº 2/2021**: diretrizes para a proteção de dados pessoais de crianças e adolescentes. Brasília, DF, 23 set. 2021. Disponível em:

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: 28 ago. 2025.

BRASIL. **Lei nº 13.709**, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em: 28 ago. 2025.

BRASIL. **Lei nº 8.069**, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Diário Oficial da União, Brasília, 16 jul. 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 30 ago. 2025.

BRASIL. **PL 2628/2022**. Projeto de Lei que dispõe sobre a proteção de crianças e adolescentes no ambiente digital, 2025. Disponível em: https://www.senado.leg.br/materias/legislacao/PL_2628_2022.pdf. Acesso em: 26 ago. 2025.

COMMON SENSE MEDIA. *Social AI Companions*. Pub.: July 16, 2025. Disponível em: <https://www.commonsemmedia.org/ai-ratings/social-ai-companions?gate=riskassessment>. Acesso em: 26 ago. 2025.

COSTELLO, N., SUTTON, R., JONES, M., ALMASSIAN, M., RAFFOUL, A., OJUMU, O., SALVIA, M., SANTOSO, M., KAVANAUGH, J. R., & AUSTIN, S. B. (2023). *ALGORITHMS, ADDICTION, AND ADOLESCENT MENTAL HEALTH: An Interdisciplinary Study to Inform State-level Policy Action to Protect Youth from the Dangers of Social Media*. **American journal of law & medicine**, 49(2-3), 135–172. Disponível em: <https://www.cambridge.org/core/journals/american-journal-of-law-and-medicine/article/algorithms-addiction-and-adolescent-mental-health-an-interdisciplinary-study-to-inform-statelevel-policy-action-to-protect-youth-from-the-dangers-of-social-media/EC9754B533553BDD56827CD9E34DFC25>. Acesso em: 26 ago. 2025.

CRYPTO ID. Verificação etária e consentimento digital via blockchain. [S.l.], 2025. Disponível em: <https://cryptoid.com.br/id-identidade-digital/verificacao-etaria-no-brasil-e-no-mundo-avancos-legislativos-e-solucoes-tecnologicas/>. Acesso em: 26 ago. 2025.

FIGUEIREDO, Fernanda Mendonça. *Supremo Reconhece a Aplicabilidade Direta dos Direitos Fundamentais às Relações Privadas*. **Direito Público**, [S. l.], v. 6, n. 30, 2011. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/1665>. Acesso em: 30 ago. 2025.

FRAZÃO, Ana. *Dever geral de cuidado das plataformas diante de crianças e adolescentes*. **Instituto ALANA**. Publicado em São Paulo, em novembro de 2021. Disponível em: <https://criancaconsumo.org.br/wp-content/uploads/2021/11/dever-geral-de-cuidado-das-plataformas.pdf>. Acesso em: 28 ago. 2025.

HADLAC, Peter; BROWN, Sarah; GIBSON, Rhiannon; et al. *Loot boxes use, video gaming, and gambling in adolescents: Results from a national survey*. *Addiction*, [S.l.], v. 118, n. 10, p. 1843–1852, 2023. Disponível em: https://pmc.ncbi.nlm.nih.gov/articles/PMC9551606/?utm_source=chatgpt.com. Acesso em: 26 ago. 2025.

HARRINGTON, Tristan. *Testimony: The Role of Persuasive Technology in the Attention Economy*. **Center for Humane Technology**, 2023. Disponível em: <https://www.commerce.senate.gov/services/files/96e3a739-dc8d-45f1-87d7-ec70a368371d>. Acesso em: 26 ago. 2025.

<https://www.gov.br/anpd/pt-br/acompanhe-a-anpd/assuntos/noticias/anpd-aprova-recomendacao-com-diretrizes-para-protecao-de-dados-pessoais-de-criancas-e-adolescentes>. Acesso em: 30 ago. 2025.

KIDRON, Beeban; RUDKIN, Angharad. *Disrupted Childhood: The cost of persuasive design*. 2. ed. Londres: **5Rights Foundation**, 2024. Disponível em: https://5rightsfoundation.com/wp-content/uploads/2024/08/5rights_DisruptedChildhood_G.pdf?utm_source=chatgpt.com. Acesso em: 26 ago. 2025.

KOÇ, Birkan. *The Role of User Interactions in Social Media on Recommendation Algorithms: Evaluation of TikTok's Personalization Practices From User's Perspective*. **Researchgate**, 2023. Disponível em: https://www.researchgate.net/publication/375775130_The_Role_of_User_Interactions_in_Social_Media_on_Recommendation_Algorithms_Evaluation_of_TikTok's_Personalization_Practices_From_User's_Perspective. Acesso em: 26 ago. 2025.

LUHMANN, Niklas. **Sistemas sociais**: esboço de uma teoria geral. São Paulo: Vozes, 2016.

LUMEN LEARNING. *Reinforcement Schedules*. **General Psychology**, 2025. Disponível em: <https://pressbooks.online.ucf.edu/lumenpsychology/chapter/reading-reinforcement-schedules/>. Acesso em: 26 ago. 2025.

LUMEN LEARNING. *Reinforcement schedules*. **Introduction to Psychology**, 2025. Disponível em: <https://courses.lumenlearning.com/waymaker-psychology/chapter/reading-reinforcement-schedules/>. Acesso em: 26 ago. 2025.

RIXEN, Jan; MEINHARDT, Luca Maxim; GLÖCKLER, Michael; ZIEGENBEIN, Marius-Lukas; et al. *The Loop and Reasons to Break It: Investigating Infinite Scrolling Behaviour in Social Media Applications and Reasons to Stop*. **Proceedings of the ACM on Human-Computer Interaction**, v. 7, n. MHCI, p. 1–22, 2023. Disponível em:

https://www.researchgate.net/publication/373906218_The_Loop_and_Reasons_to_Break_It_Investigating_Infinite_Scrolling_Behaviour_in_Social_Media_Applications_and_Reasons_to_Stop. Acesso em: 26 ago. 2025.

SZYMIELEWICZ, Katarzyna; O'CARROLL, Tanya; FADDOUL, Marc; GŁOWACKA, Dorota; MARSH, Oliver. *Safe by Default: Moving away from engagement-based rankings towards safe, rights-respecting, and human-centric recommender systems*. **Panoptikon Foundation**; People vs Big Tech, mar. 2024. Disponível em: https://panoptikon.org/sites/default/files/2024-03/panoptikon_peoplevsbigtech_safe-by-default_briefing_03032024.pdf. Acesso em: 26 ago. 2025.

TOTARO, Paolo; MANGIANTE, Alberto. *Conceptual and design principles for a self-referential algorithm mimicking neuronal assembly functions*. **Cornell University**, arXiv, 18 jul. 2025. Disponível em: <https://arxiv.org/abs/2507.14011>. Acesso em: 28 ago. 2025.

TRUSTNFT. *TrustNFT develops age verification via token*. **BitcoinBlog.de**, 2025. Disponível em: <https://bitcoinblog.de/2025/06/04/trustnft-develops-age-verification-via-token/>. Acesso em: 26 ago. 2025.

UNIÃO EUROPEIA. **DSA - Digital Services Act**, 2024. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32022R2065>. Acesso em: 26 ago. 2025.

ZUBOFF, SHOSHANA. **A Era do Capitalismo de Vigilância**. Tradução de George Schlesinger. Rio de Janeiro: Intrínseca, 2021[edição digital].