



ECA Digital: reflexões sobre a proteção de crianças e adolescentes na arquitetura digital

25/01/2026

Estamos a poucas semanas de um marco importante — o prazo prorrogado pela Agência Nacional de Proteção de Dados (ANPD) para a entrega dos relatórios de adequação ao ECA Digital, que se encerra em 13 de fevereiro. Diante desse cenário, é oportuno refletir com calma e clareza sobre os impactos dessa legislação, indo além das leituras mais imediatas e do óbvio.

O caminho não é “falar mais da lei”, mas compreender o que ela revela sobre a forma como redes sociais e games passaram a organizar a infância. A Lei nº 15.211/2025 (ECA Digital) não nasce apenas para “conter abusos”; ela surge porque o ambiente digital se tornou infraestrutura de socialização, consumo e identidade — e isso altera o tipo de proteção que a sociedade deve oferecer.

O fato de estarmos próximos do prazo de monitoramento estendido pela ANPD ajuda a trazer o tema do plano abstrato para o plano das escolhas concretas de produto e governança. Nesse sentido, algumas reflexões menos evidentes — e mais úteis — se impõem.

O debate real não é sobre “idade”, mas sobre “arquitetura de risco”. Em redes sociais e games, o dano raramente vem de um “conteúdo proibido” isolado; ele costuma surgir da combinação entre recomendação algorítmica, pressão do grupo, design persuasivo e captura de atenção (o famoso “só mais uma partida”, “só mais um vídeo”).

A verificação etária vira apenas um pedaço do quebra-cabeça — importante, mas insuficiente — e o próprio Comitê Gestor da Internet no Brasil (CGI.br) aponta que aferição de idade é central, porém não é o único mecanismo de proteção.

Nos games, a criança não é apenas usuária; muitas vezes é também uma espécie de “trabalhadora involuntária de dados”. Cada clique, partida, tempo de permanência, compra in-app e interação no chat alimentam modelos de personalização e monetização. Isso é parte do produto, não um efeito colateral. Quando o ECA Digital fala em proteção contra exploração comercial e impõe obrigações a serviços “direcionados ou de acesso provável” por menores, ele força a pergunta incômoda: o que, exatamente, está sendo extraído como valor — diversão ou previsibilidade comportamental?

Nesse contexto, privacidade não pode ser entendida apenas como sigilo de dados. Ela se conecta diretamente à liberdade de desenvolvimento. A lei menciona respeito à autonomia e ao desenvolvimento progressivo, o que aponta para uma leitura mais madura: a infância precisa de margem para experimentar sem ser permanentemente perfilada. Em redes sociais, isso tem impacto direto sobre recomendação, filtros, ranking de popularidade e até sobre como a plataforma “decide” o que o jovem verá repetidas vezes.

Por isso, a régua correta não é “o que a empresa consegue fazer”, mas “o que é proporcional ao risco”. O CGI.br defende proporcionalidade e necessidade: ambientes de maior risco pedem medidas mais fortes; ambientes de baixo risco não deveriam sofrer exigências excessivas. Essa chave é valiosa para tirar a conversa do moralismo (“rede social é ruim”, “game faz mal”) e colocá-la onde importa: quais funcionalidades aumentam risco e quais reduzem.

Algumas provocações práticas — do tipo que ajuda liderança de produto, jurídico e trust & safety — ajudam a visualizar este desafio. Em jogos com chat aberto ou comunicação por voz entre desconhecidos, o risco vai muito além de linguagem inadequada. Envolve grooming, assédio, manipulação e coação social em tempo real. A pergunta essencial é se o produto foi desenhado para maximizar interação a qualquer custo ou para maximizar interação segura.

Nos feeds das redes sociais, a lógica é semelhante: quando a plataforma aprende rapidamente o que prende o interesse, ela assimila também o que prende o interesse de um menor. Se o modelo é ótimo em amplificar emoção (raiva, ansiedade, comparação), a proteção não pode se limitar a remover conteúdo ilegal; precisa tratar recomendação e padrão de exposição repetida como parte do risco.

O mesmo vale para microtransações e economias internas em games, frequentemente ajustadas à impulsividade típica da adolescência: mesmo sem ilegalidade formal, há clara assimetria de maturidade — exatamente o tipo de desequilíbrio que estatutos protetivos buscam mitigar.

Engenharia social do produto

Do ponto de vista prático, a lei coloca pressão para que empresas façam três movimentos objetivos: mapear riscos reais por funcionalidade, escolher medidas proporcionais e auditáveis, e provar isso com transparência e governança — motivo pelo qual a ANPD está monitorando e pedindo informações sobre medidas técnicas e organizacionais adotadas. E, como o Comitê Gestor da Internet no Brasil ressalta, qualquer solução — inclusive verificação de idade — precisa ser compatível com privacidade e minimização de dados, para que não se resolva um problema criando outro.

O ECA Digital, em análise final, é um convite ao amadurecimento do debate: ele propõe abandonar a lógica superficial do “proibir ou liberar” e avançar para uma discussão de engenharia social do produto: quais escolhas de design ampliam vulnerabilidades e quais promovem desenvolvimento saudável. Redes sociais e games podem continuar sendo espaços de criatividade, amizade e diversão, desde que a proteção deixe de ser um apêndice burocrático

Spacca



e passe a funcionar como critério estruturante de projeto — especialmente quando o público é jovem.

Talvez a pergunta mais simples — e mais reveladora — seja esta: se amanhã essa plataforma fosse usada majoritariamente por crianças, o que mudaria no design? E por quê?

Fonte: <https://conjur.jumps.com.br/2026-jan-25/eca-digital-reflexoes-sobre-a-protecao-de-criancas-e-adolescentes-na-arquitetura-digital/>