GAZETA DO POVO
Quarta-feira, 26 de Novembro de 2025

Artigo

A proteção de menores no ambiente digital

Por Cristiane Manzueto e Carolina Cesarini 26/11/2025 às 09:27

Em 17 de setembro de 2025, foi sancionada a Lei 15.211/2025, oriunda do Projeto de Lei 2.628/2022, que institui o Estatuto Digital da Criança e do Adolescente (ECA Digital). A nova legislação estabelece diretrizes inéditas para a proteção de crianças e adolescentes no ambiente digital, com foco em plataformas digitais, redes sociais, aplicativos e jogos eletrônicos. A *vacatio legis* foi fixada em seis meses, conforme a Medida Provisória nº 1.319/2025, de modo que sua entrada em vigor ocorrerá em março de 2026.

O ECA Digital representa uma atualização normativa significativa do Estatuto da Criança e do Adolescente (Lei 8.069/1990), constituindo um marco regulatório histórico na proteção da infância e da juventude frente à hiperconectividade e aos desafios tecnológicos contemporâneos, além de ser oficialmente a primeira legislação da América Latina dedicada exclusivamente à proteção de crianças e adolescentes no ambiente digital.

O ECA Digital tem como escopo a mitigação de riscos digitais, tais como publicidade emocional, perfilamento comportamental e exposição a conteúdos inadequados. Reforça-se, assim, o princípio da proteção integral previsto no artigo 1º do ECA, em consonância com o artigo 227 da Constituição Federal, que impõe à família, à sociedade e ao Estado o dever de assegurar, com prioridade absoluta, os direitos fundamentais da criança e do adolescente. No contexto digital, esse dever se concretiza por meio de obrigações específicas impostas às plataformas tecnológicas, que passam a ser responsabilizadas pela exposição indevida de menores. Entre as proibições expressas na norma estão a publicidade direcionada com base em perfil emocional ou comportamental de menores, o uso de caixas de recompensa (*loot boxes*) em jogos eletrônicos voltados ao público infantojuvenil, a monetização de funcionalidades que incentivem o uso compulsivo, a exposição a conteúdos ilícitos ou manifestamente inadequados – como pornografia, apologia ao suicídio, bullying e jogos de azar – e a coleta de dados pessoais sem consentimento expresso dos responsáveis legais, inclusive para fins de verificação de idade.

Adicionalmente, plataformas, aplicativos e sistemas operacionais passam a ter o dever jurídico de incorporar salvaguardas por padrão, tais como configurações de privacidade restritivas, classificação de conteúdo por faixa etária (*privacy by design*), ferramentas obrigatórias de supervisão familiar, mecanismos de mitigação de riscos à saúde mental e canais acessíveis de denúncia e moderação. A supervisão parental deve ser disponibilizada de forma efetiva, permitindo aos responsáveis legais limitar o tempo de uso, ajustar recomendações e desativar funcionalidades sensíveis, como a geolocalização.

> ***Em caso de incidentes de segurança envolvendo dados pessoais de crianças e adolescentes, a LGPD impõe obrigações rigorosas. O controlador deve comunicar à ANPD e aos titulares dos dados (ou a seus responsáveis legais) no prazo de até três dias úteis, caso haja risco ou dano relevante***

Sob a perspectiva da proteção de dados pessoais, o ECA Digital se articula com a Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018), especialmente com o artigo 14, que determina que o tratamento de dados de crianças e adolescentes deve observar o princípio do melhor interesse do titular. A Autoridade Nacional de Proteção de Dados (ANPD) já publicou enunciados interpretativos e guias orientativos que reforçam esse entendimento, destacando que o melhor interesse do menor deve prevalecer sobre qualquer finalidade comercial. A verificação de idade, por exemplo, deve ser realizada com uso mínimo de dados, exclusivamente para fins de checagem etária, sendo vedada a reutilização ou o compartilhamento das informações coletadas.

A responsabilização das plataformas digitais é reforçada pela previsão de sanções administrativas, que podem alcançar o montante de R$ 50 milhões. A legislação prevê medidas graduais, que vão desde advertências até a suspensão de atividades, além da exigência de relatórios periódicos de riscos e de moderação. A atuação do órgão regulador deve preservar o equilíbrio entre proteção e liberdade de expressão, vedando práticas de vigilância massiva.

Importante destacar que a Lei Geral de Proteção de Dados Pessoais (LGPD) já previa cuidados específicos no tratamento de dados de menores, especialmente no artigo 14. O Enunciado CD/ANPD 1/2023 reforça a interpretação de que o melhor interesse da criança e do adolescente deve prevalecer em qualquer operação de tratamento de dados. O *Guia da ANPD sobre Hipóteses Legais de Tratamento de Dados Pessoais* (fev./2024) estabelece que o legítimo interesse pode ser utilizado como base legal inclusive para dados de crianças e adolescentes, desde que seja realizado um teste de balanceamento, avaliando a necessidade do tratamento, a expectativa legítima do titular (ou de seu responsável legal), os direitos e liberdades fundamentais envolvidos, bem como a transparência e o registro das operações. Além disso, deve ser observada a prevalência do melhor interesse do menor, conforme exigido pelo artigo 14 da LGPD.

O mencionado Guia da ANPD também esclarece que o legítimo interesse somente pode ser aplicado quando houver relação direta entre o controlador e o titular dos dados, e desde que não haja riscos desproporcionais aos seus direitos fundamentais. O controlador deve documentar a análise e, se necessário, elaborar um Relatório de Impacto à Proteção de Dados Pessoais (RIPD).

Quanto à verificação de idade, a norma determina que o uso de dados pessoais deve ser mínimo, com finalidade exclusiva de checagem etária, sendo proibida a reutilização ou o compartilhamento das informações coletadas. O procedimento deve ser transparente e apresentado em linguagem acessível aos responsáveis legais.

Em caso de incidentes de segurança envolvendo dados pessoais de crianças e adolescentes, a LGPD impõe obrigações rigorosas. O controlador deve comunicar à ANPD e aos titulares dos dados (ou a seus responsáveis legais) no prazo de até três dias úteis, caso haja risco ou dano relevante. A comunicação deve conter, no mínimo, a descrição do incidente, os tipos de dados afetados, o número de titulares envolvidos, as medidas de segurança adotadas, o plano de mitigação e os dados de contato do encarregado e do controlador.

Cristiane Manzueto *e* ***Carolina Peyres da Silveira Cesarini*** *são advogadas do escritório Montaury Pimenta, Machado & Vieira de Mello.*