NOTA PÚBLICA do CGI.br sobre o Projeto de Lei nº 3.066, de 2025

O COMITÊ GESTOR DA INTERNET NO BRASIL – CGI.br, em sua 7ª Reunião Ordinária de 2026, realizada em 17 de julho, e no uso das atribuições que lhe confere o Decreto nº 4.829/2003, vem a público se manifestar, **em vista da aprovação, no Congresso Nacional, do Projeto de Lei nº 3.066 de 2025**, que institui medidas de enfrentamento e repressão ao crime de violência sexual contra criança ou adolescente, inclusive no ambiente digital; e altera os Decretos-Leis nºs 2.848/1940 (Código Penal), a Lei nº 8.069/1990 (Estatuto da Criança e do Adolescente), dentre outras legislações, para recrudescer o tratamento penal aos criminosos sexuais. O referido projeto de lei, aprovado na Câmara dos Deputados e no Senado Federal, foi encaminhado em 17 de julho de 2026 à Presidência da República para análise de sanção ou veto da matéria. Nesse sentido, o CGI.br,

CONSIDERANDO

1) A relevância em estabelecer iniciativas que visem a garantir a proteção de crianças e adolescentes contra a violência sexual, instituindo medidas diligentes de enfrentamento a

tais crimes, inclusive em ambiente digital;

2) Que o CGI.br tem se manifestado e se envolvido no debate sobre proteção a crianças e adolescentes no ambiente digital de maneira qualificada, produzindo posicionamentos públicos, recomendações e diretrizes estratégicas para o tema, a exemplo da *NOTA PÚBLICA sobre a proteção de crianças e adolescentes no ambiente digital****[1]*** e da *NOTA PÚBLICA sobre exploração sexual por uso indevido de inteligência artificial generativa*[2];

3) Que qualquer medida de responsabilização direcionada ao ambiente digital não deve ocorrer em prejuízo da promoção de uma Internet segura, estável e funcional, orientada pelos princípios da privacidade, inimputabilidade da rede e respeito aos direitos humanos, conforme os "Princípios para a governança e uso da Internet" do CGI.br (Resolução CGI.br/RES/2009/003/P);

4) Que o referido projeto de lei, ao prever alteração no Estatuto da Criança e do Adolescente com a inserção do artigo 226-A, **propõe aumento de pena** de 1/3 (um terço) a 2/3 (dois terços) se o agente comete os crimes dispostos pela lei **mediante** "utilização de modulador de proxy ou técnica de mascaramento, ocultação, falsificação, alteração ou anonimização de endereço IP ou de qualquer outro identificador digital, por meio de software, programa, ferramenta, navegador ou qualquer outro meio, com o objetivo de impedir ou dificultar sua identificação";

VEM A PÚBLICO

1) Apontar que o caput do artigo 226-A, ao mencionar "modulador de proxy" e "técnicas de mascaramento, ocultação, falsificação ou alteração de endereço IP" e "outros identificadores digitais", adota uma redação ampla que abrange **um conjunto extenso de tecnologias** cujo desincentivo pode fragilizar mecanismos essenciais de proteção a ameaças, afetando a segurança, privacidade e operação da Internet;

2) Reiterar que tais ferramentas, em alinhamento com os relatórios do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br)[3] e da ICANN[4], possuem diversos **usos legítimos.** Podem, por exemplo, ser essenciais à democracia, à privacidade, segurança e liberdade de expressão, atuando na proteção a redes corporativas e públicas contra ataques cibernéticos, espionagem, vazamentos de informações e de dados pessoais, além de contribuir para a proteção de jornalistas, ativistas e grupos vulneráveis;

3) Manifestar preocupação com a associação entre o conjunto de técnicas cobertos pelo caput do artigo 226-A e a medida de agravamento penal, o que estabelece o seu uso

como indicativo de comportamento ilícito e pode abrir precedente regulatório para o levantamento de **suspeitas sobre quem utiliza ferramentas de privacidade** em sentido amplo, dando margem para insegurança jurídica;

4) Reconhecer que o **anonimato**, longe de ser por definição um indicativo de comportamento suspeito, pode ser fundamental para o exercício da liberdade de expressão em situações de risco, a exemplo de direitos fundamentais como o sigilo da fonte, a privacidade e o sigilo das informações, garantidos pelo artigo 5º da Constituição Federal, respectivamente nos incisos XIV, X e XII;

5) Salientar que o uso de tais ferramentas **não** adiciona maior potencial de danos às vítimas, divergindo, portanto, de modelos de responsabilização que atribuem agravantes penais para o uso de tecnologias em comportamentos ilícitos em proporcionalidade aos maiores danos às vítimas;

6) Sublinhar que, uma vez que o aumento de pena só será aplicado quando a investigação já tiver identificado o agente e o nexo causal, a resposta penal vem *a posteriori* e não melhora a capacidade técnica das autoridades para rastrear tais crimes, tendo **pouca eficácia prática**;

7) Destacar que **a premissa** de que o aumento de pena pode desincentivar o recurso à anonimização e produzir um efeito dissuasório sobre as práticas criminais abrangidas pela lei **carece de evidências**;

8) Recomendar **o veto presidencial ao artigo 226-A**, proposto pelo PL 3066/2025 para modificar a Lei nº 8.069/1990 (Estatuto da Criança e do Adolescente);

9) Reafirmar, finalmente, a disposição do CGI.br em contribuir tecnicamente para o debate sobre segurança e responsabilidade no ambiente digital, bem como a proteção a crianças e adolescentes, em diálogo com a comunidade científica e tecnológica, o setor empresarial, a sociedade civil e o governo, de forma a ajudar a construir regulações sólidas em termos técnicos e compatíveis com os princípios para a governança e o uso da Internet no Brasil.

[1] COMITÊ GESTOR DA INTERNET NO BRASIL (CGI.br). **Nota pública sobre a proteção de crianças e adolescentes no ambiente digital.** 2025. Disponível em: https://cgi.br/esclarecimento/nota-publica-sobre-a-protecao-de-criancas-e-adolescentes-no-ambiente-digital/. Acesso em: 20 jul. 2026.

[2] COMITÊ GESTOR DA INTERNET NO BRASIL (CGI.br). **Nota pública sobre exploração sexual por uso indevido de inteligência artificial generativa.** [2025].

Disponível em: https://cgi.br/esclarecimento/nota-publica-sobre-exploracao-sexual-por-uso-indevido-de-inteligencia-artificial-generativa/. Acesso em: 20 jul. 2026.

[3] O CERT.br é um Time de Resposta a Incidentes de Segurança (CSIRT) de Responsabilidade Nacional de último recurso, mantido pelo NIC.br. O centro presta serviços da área de Gestão de Incidentes de Segurança da Informação para qualquer rede que utilize recursos administrados pelo NIC.br. Para mais informações: https://www.cgi.br/publicacao/cartilha-de-seguranca-para-internet/

[4] ICANN (Internet Corporation for Assigned Names and Numbers). **DNS blocking revisited**. Los Angeles: ICANN, 2025. Disponível em: https://itp.cdn.icann.org/en/files/security-and-stability-advisory-committee-ssac-reports/sac127-dns-blocking-revisited-16-05-2025-en.pdf. Acesso em: 21 jul. 2026.