



SENADO FEDERAL

EMENDA Nº
(ao PL 2/2026)

Modifique-se o §2º e o caput do art. 17 do Projeto de Lei nº 2, de 2026, nos seguintes termos:

“Art. 17. Fica autorizada a implementação e manutenção do Cadastro Nacional de Bloqueio de Conteúdos Violentos contra a Mulher (CNBCV), repositório digital de impressões criptográficas (hashes) de arquivos de conteúdo ilícito.

.....

§ 2º Os provedores de aplicações de internet **poderão sincronizar periodicamente** o CNBCV para aprimorar seus sistemas de detecção, nos termos de regulamento.” (NR)

JUSTIFICAÇÃO

A presente emenda ao art. 17 do Projeto de Lei nº 2/2026 tem por finalidade aperfeiçoar o modelo de funcionamento do Cadastro Nacional de Bloqueio de Conteúdos Violentos contra a Mulher (CNBCV), garantindo que a cooperação entre o Poder Público e os provedores de aplicações de internet ocorra de forma tecnicamente eficiente e juridicamente segura.

A redação original, ao impor que os provedores "deverão consultar" o cadastro, estabelece uma obrigação de fazer que interfere diretamente na arquitetura técnica e nos fluxos de processamento de dados (*pipelines* de upload) das plataformas. Tal imposição configura uma ingerência regulatória



desproporcional sobre a engenharia dos sistemas privados, o que pode gerar gargalos operacionais e riscos à estabilidade das redes.

De acordo com o art. 3º, inciso VIII, do Marco Civil da Internet (Lei nº 12.965/2014), a disciplina do uso da internet no Brasil tem como princípio a liberdade dos modelos de negócios promovidos na rede, desde que não conflitem com os demais princípios estabelecidos na lei. A obrigatoriedade de consulta a um banco de dados governamental externo para cada upload realizado viola a autonomia de engenharia e a liberdade de gestão técnica dos provedores.

A substituição do dever de "consultar" pela possibilidade de "sincronizar" hashes permite que os provedores incorporem os dados de interesse público em seus próprios sistemas de detecção automatizada de forma assíncrona. Isso garante maior celeridade no bloqueio de conteúdos ilícitos — como cenas de feminicídio e exposição não consentida — sem comprometer a performance das aplicações.

Ao evitar um "ponto único de governança" obrigatório sobre decisões de remoção em escala, a emenda previne que falhas técnicas ou indisponibilidades no sistema estatal paralise os mecanismos de segurança das plataformas privadas. O modelo de sincronização facultativa promove uma colaboração mais resiliente e menos suscetível a riscos sistêmicos de censura ou falhas de integração.

A gestão de repositórios de impressões criptográficas (*hashes*) deve observar os princípios da finalidade e necessidade previstos na Lei Geral de Proteção de Dados Pessoais (LGPD - Lei nº 13.709/2018). O modelo colaborativo aqui proposto assegura que a troca de informações técnicas ocorra de modo a proteger a integridade dos dados e a privacidade dos utilizadores, sem criar vínculos de dependência técnica excessiva entre Estado e entes privados.

Em suma, a alteração proposta transforma uma obrigação de difícil execução técnica em um mecanismo de cooperação inteligente, elevando a eficácia do combate à violência contra a mulher no ambiente digital sem ferir os marcos regulatórios da internet brasileira.



Sala das sessões, 17 de março de 2026.

Senador Jorge Kajuru
(PSB - GO)

