

# COMISSÃO DE SEGURANÇA PÚBLICA E COMBATE AO CRIME ORGANIZADO

## PROJETO DE LEI Nº 6.697, DE 2025

Regulamenta o uso de tecnologias de monitoramento e alerta para mulheres ameaçadas por violência psicológica digital, como perseguição eletrônica, vigilância não consentida e invasão de dispositivos, e dá outras providências.

**Autor:** Deputado AMOM MANDEL

**Relatora:** Deputada DUDA SALABERT

### I - RELATÓRIO

O Projeto de Lei (PL) nº 6.697, de 2025, de autoria do ilustre Amom Mandel, visa regulamentar o uso de tecnologias de monitoramento e alerta para mulheres ameaçadas por violência psicológica digital, como perseguição eletrônica, vigilância não consentida e invasão de dispositivos, e dá outras providências.

A norma define “violência psicológica digital” como qualquer ação praticada via tecnologia que objetive intimidar, controlar, vigiar, manipular, constranger ou ameaçar a mulher, afetando sua integridade emocional, liberdade ou privacidade (art. 2º). O texto prevê a disponibilização às vítimas, mediante avaliação de risco, de ferramentas como sistemas de alerta emergencial conectados à polícia, aplicativos de detecção de monitoramento indevido, ferramentas contra invasão ou clonagem, e dispositivos de registro seguro de incidentes (art. 3º).

Adicionalmente, o projeto estabelece: a elaboração pelo Poder Executivo, com o apoio de órgãos de segurança pública, de protocolo nacional



de verificação de risco digital (art. 4º); a oferta, às vítimas, de suporte técnico para higienização de aparelhos, análise de invasões e orientações sobre denúncias e preservação de provas (art. 5º); e o dever de sigilo com relação às informações obtidas, em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD) (art. 6º).

Na justificação que acompanha a matéria, o Autor ressalta que o avanço tecnológico facilitou novas formas de violência de gênero, muitas vezes invisíveis mas extremamente danosas, que limitam a liberdade de movimento da mulher e dificultam o pedido de ajuda. Argumenta que as políticas públicas atuais são insuficientes para lidar com o abuso digital, tornando urgente a padronização de protocolos de proteção e suporte técnico pelo Estado.

O PL está sujeito à apreciação conclusiva pelas Comissões (art. 24, II, do RICD), sob o regime de tramitação ordinário (art. 151, III, do RICD), e foi distribuído à Comissão de Segurança Pública e Combate ao Crime Organizado; à Comissão de Defesa dos Direitos da Mulher; à Comissão de Finanças e Tributação (art. 54 do RICD); e à Comissão de Constituição e Justiça e de Cidadania (art. 54 do RICD).

A proposição foi apresentada em 22 de dezembro de 2025 e recebida nesta Comissão no dia 12 de fevereiro de 2026. Em 4 de março deste ano, foi aberto o prazo de cinco sessões para emendamento. Encerrado esse lapso temporal no dia 17 do mesmo mês, não foram apresentadas emendas.

A proposta legislativa não possui apensos.

É o relatório.

## II - VOTO DA RELATORA

Compete a esta Comissão Permanente manifestar-se sobre o mérito de Projetos de Lei (PLs) que, como o ora examinado, versem sobre proteção a testemunhas e vítimas de crime, e suas famílias, além de matérias e políticas de segurança pública, consoante o disposto nas alíneas “c”, “d” e “g”



do inciso XVI do art. 32 do Regimento Interno da Câmara dos Deputados. A apreciação cingir-se-á à ótica da segurança pública.

A proposição mostra-se oportuna e necessária. A violência doméstica e de gênero contemporânea não se restringe mais ao ambiente físico, migrando velozmente para o espaço cibernético. A utilização de *spywares*, o rastreamento ilegal de geolocalização e o acesso indevido a dados privados são métodos atuais de controle e intimidação que precedem, com frequência, agressões físicas graves.

Nesse sentido, dados do *Anuário Brasileiro de Segurança Pública 2025* corroboram a urgência da matéria ao registrar um aumento de 18,2% nos casos de perseguição (*stalking*) e de 6,3% nas ocorrências de violência psicológica em relação ao ano anterior<sup>1</sup>. Tais métodos de controle virtual retroalimentam o que a literatura e os dados de saúde pública chamam de “ciclo da violência”. Conforme aponta o *Atlas da Violência 2025*, os homicídios femininos não são eventos isolados, mas o resultado trágico de trajetórias de abusos que englobam a violência psicológica<sup>2</sup>.

O uso de tecnologias de rastreamento facilita o *modus operandi* do agressor de isolar a mulher e exercer controle excessivo sobre sua vida, impedindo-a de buscar ajuda<sup>3</sup>. A urgência de frear esse controle em sua fase cibernética e psicológica é atestada pelos números do Ministério da Saúde: apenas em 2023, foram notificados 17.501 casos de violência psicológica contra mulheres, com uma taxa de repetição assustadora, em que mais de 55% das vítimas já haviam sofrido abusos anteriores<sup>4</sup>. Quando o Estado falha em coibir esse rastreio e intimidação prévios, o desfecho costuma ser letal: no mesmo ano, 35% dos assassinatos de mulheres (1.370 mortes) ocorreram dentro de suas próprias casas, provando que o controle que muitas vezes se inicia nos aparelhos celulares termina de forma fatal no ambiente doméstico<sup>5</sup>.

<sup>1</sup> Disponível em: <<https://forumseguranca.org.br/wp-content/uploads/2025/07/anuario-2025.pdf>>. Acesso em: 1º abr. 2026. p. 18.

<sup>2</sup> Disponível em: <<https://forumseguranca.org.br/wp-content/uploads/2025/05/atlas-violencia-2025.pdf>>. Acesso em: 1º abr. 2026. p. 49.

<sup>3</sup> *Ibid.*, p. 72.

<sup>4</sup> *Ibid.*, p. 66 e 71.

<sup>5</sup> *Ibid.*, p. 56.



Ao prever o fornecimento de ferramentas de detecção e alerta, o projeto fortalece a capacidade de resposta imediata das forças de segurança, permitindo uma intervenção preventiva antes que a ameaça digital se materialize em violência física. O protocolo nacional de verificação de risco previsto no PL é medida administrativa de inteligência essencial para que o Estado compreenda a letalidade de cada situação.

Não obstante o inegável mérito da matéria, visando conferir-lhe maior densidade jurídica e operacional, optamos por apresentar Substitutivo que promova ajustes entendidos como necessários.

Primeiramente, estabelecemos uma integração conceitual sistêmica, ao definir a violência psicológica digital por remissão expressa à Lei Maria da Penha (Lei nº 11.340/2006) (art. 2º do Substitutivo). Essa medida garante a unidade do ordenamento, assegurando que condutas já reconhecidas no mundo físico sejam transponíveis para o ambiente virtual. Ademais, a vinculação, meramente exemplificativa, a tipos penais específicos do Código Penal (parágrafo único do art. 2º) – como perseguição, invasão de dispositivo informático e violência psicológica contra a mulher – confere a segurança jurídica necessária para a lavratura de boletins de ocorrência e fundamentação de medidas protetivas.

O Substitutivo mantém a faculdade do poder público de disponibilizar ferramentas que identifiquem e neutralizem atividades que configurem violência psicológica digital, mas a complementa com uma obrigação de desenvolver esses sistemas (nova redação ao art. 3º). Ademais, cogitou-se da conexão entre mecanismos de alerta utilizados pelas mulheres, de um lado, e a rede de proteção concebida pela Lei Maria da Penha, de outro, composta, por exemplo, por centros de atendimento, defensorias públicas e prestadores de serviços de saúde (inciso I do § 1º do art. 3º do Substitutivo). Também se passou a exigir que *softwares* voltados para registro de incidentes cibernéticos observem as normas sobre cadeia de custódia inscritas no Código de Processo Penal, de modo a garantir a validade das provas em juízo (inciso IV do § 1º do art. 3º).



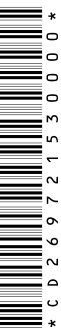
Inovamos, ainda, ao fixar critérios mínimos para um protocolo nacional de avaliação de risco (art. 4º do Substitutivo), como o histórico do agressor e sua perícia tecnológica, permitindo contramedidas proporcionais à sofisticação da ameaça. Por fim, a ampliação do suporte multidisciplinar à vítima (inciso IV do art. 5º do Substitutivo) e a harmonização com a Lei de Proteção a Vítimas e Testemunhas (Lei nº 9.807/1999), citada expressamente em parágrafo único ao art. 6º, blindam o sistema contra brechas que poderiam expor o paradeiro da mulher ameaçada. Trata-se, portanto, de um texto mais robusto, técnico e efetivo para a interrupção do ciclo de violência no século XXI.

Ante o exposto, votamos, no MÉRITO, pela APROVAÇÃO do Projeto de Lei nº 6.697, de 2025, na forma do Substitutivo anexo.

Sala da Comissão, em 28 de abril de 2026.

Deputada DUDA SALABERT  
Relatora

2026-3677



# COMISSÃO DE SEGURANÇA PÚBLICA E COMBATE AO CRIME ORGANIZADO

## SUBSTITUTIVO AO PROJETO DE LEI Nº 6.697, DE 2025

Dispõe sobre o desenvolvimento, a disponibilização e o uso de tecnologias de monitoramento, detecção e alerta destinadas à proteção de mulheres ameaçadas por violência psicológica digital.

O Congresso Nacional decreta:

Art. 1º Esta Lei dispõe sobre o desenvolvimento, a disponibilização e o uso de tecnologias de monitoramento, detecção e alerta destinadas à proteção de mulheres ameaçadas por violência psicológica digital, visando à interrupção de ciclos de abuso e à preservação da integridade emocional, liberdade e privacidade das vítimas.

Art. 2º Para os fins desta Lei, considera-se violência psicológica digital qualquer conduta, definida de acordo com o inciso II do *caput* do art. 7º da Lei nº 11.340, de 7 de agosto de 2006, praticada mediante tecnologia de informação e comunicação.

Parágrafo único. O conceito previsto no *caput* deste artigo abrange, entre outras, condutas que podem configurar os seguintes crimes previstos no Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal):

- I – ameaça (art. 147);
- II – perseguição (art. 147-A);
- III – violência psicológica contra a mulher (art. 147-B);
- IV – invasão de dispositivo informático (art. 154-A);
- V – extorsão (art. 158);
- VI – fraude eletrônica (art. 171, § 2º-A).



Art. 3º O poder público desenvolverá tecnologias de proteção e poderá, mediante avaliação de risco baseada no protocolo a que se refere o art. 4º desta Lei, disponibilizá-las às vítimas.

§ 1º As tecnologias de que trata o *caput* poderão incluir:

I – sistemas de alerta emergencial diretamente conectados a órgão policial e à rede de proteção formada pelos serviços mencionados nos incisos I a III do *caput* do art. 35 da Lei nº 11.340, de 7 de agosto de 2006;

II – aplicativos para detecção de *malwares*, acessos remotos não autorizados ou clonagem de dispositivos;

III – ferramentas de criptografia e segurança contra invasões;

IV – dispositivos portáteis ou aplicativos que permitam o registro seguro de incidentes cibernéticos, com preservação da cadeia de custódia, nos termos do Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal).

§ 2º Para os fins desta Lei, considera-se *malware* qualquer programa de computador, código ou *software* malicioso projetado para infiltrar-se, danificar, monitorar indevidamente ou causar prejuízo a sistemas informáticos ou dispositivos eletrônicos sem o consentimento do usuário.

§ 3º O desenvolvimento, o aprimoramento e a manutenção das tecnologias previstas no § 1º deste artigo poderão ser realizados:

I – diretamente pelo poder público, inclusive mediante parceria com empresas de tecnologia, universidades e organizações especializadas da sociedade civil; ou

II – por terceiros contratados nos termos da Lei nº 14.133, de 1º de abril de 2021.

Art. 4º O Poder Executivo elaborará, em regulamento, protocolo de avaliação de risco, que adotará, no mínimo, os seguintes parâmetros para aferir o nível de probabilidade e severidade de exposição da mulher à violência psicológica digital:



I – histórico de violência doméstica ou familiar do potencial agressor;

II – seu nível de perícia tecnológica e grau de acesso a dados sensíveis da vítima;

III – frequência e intensidade das interações digitais não consentidas; e

IV – natureza, gravidade e constância das ameaças e outros abusos cometidos em ambiente virtual.

Art. 5º A mulher atendida com fundamento nesta Lei poderá receber suporte técnico especializado, consistente em:

I – análise de aparelhos suspeitos de terem sofrido invasão;

II – higienização e revisão de dispositivos;

III – instruções de segurança digital e preservação de provas;

IV – orientações sobre:

a) registro de ocorrência;

b) requerimento à autoridade policial;

c) representação ao Ministério Público;

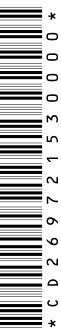
d) solicitação de medida protetiva;

e) encaminhamento a outros serviços especializados, previstos na Lei nº 11.340, de 7 de agosto de 2006.

Art. 6º As informações obtidas pelas tecnologias de que trata o § 1º do art. 3º desta Lei serão tratadas em consonância com o disposto na Lei nº 13.709, de 14 de agosto de 2018.

Parágrafo único. O uso das tecnologias de que trata o § 1º do art. 3º desta Lei observará e complementarará os programas de proteção a vítimas ameaçadas, instituídos com base na Lei nº 9.807, de 13 de julho de 1999.

Art. 7º O Poder Executivo regulamentará esta Lei no prazo de 120 dias, contados de sua entrada em vigor.



Art. 8º Esta Lei entra em vigor na data de sua publicação.

Sala da Comissão, em 28 de abril de 2026.

Deputada DUDA SALABERT  
Relatora

2026-3677

