CÂMARA DOS DEPUTADOS
Gabinete do Deputado Federal Marcos Pollon

PROJETO DE LEI Nº , DE 2025.

(DO SR. MARCOS POLLON)

Dispõe sobre a concessão de porte de arma de fogo, aos profissionais da área de segurança digital e segurança da informação, e dá outras providências.

O CONGRESSO NACIONAL decreta:

Art. 1º Fica assegurado o porte de arma de fogo de porte de uso permitido, para defesa pessoal, aos profissionais que atuem nas áreas de segurança digital, segurança da informação, cibersegurança, engenharia de cibersegurança e atividades correlatas.

Art. 2º Para fins de cumprimento desta Lei, considera-se profissional de segurança digital aquele que exerça funções relacionadas à proteção de sistemas, infraestrutura digital, dados sensíveis, prevenção de ataques cibernéticos ou investigação de incidentes de segurança em ambiente digital, abrangendo, entre outros:

I – analista de segurança digital;

II – analista de segurança da informação;

III – analista de cibersegurança;

IV – engenheiro de cibersegurança;

V – consultor de segurança digital;

VI – especialista em resposta a incidentes cibernéticos (CSIRT);

VII – pentester ou testador de invasão autorizado;

VIII – administrador de segurança de redes.

Art. 3º Poderão requerer o porte de arma de fogo os profissionais que:

I – comprovem exercício profissional, mediante contrato de trabalho, contrato de prestação de serviços ou registro profissional equivalente;

II - apresentação de certidões negativas criminais das Justiças Federal, Estadual, Militar e Eleitoral;

III – comprovação de aptidão psicológica, mediante laudo emitido por psicólogo credenciado pela Polícia Federal;

IV – comprovação de capacidade técnica para o uso seguro da arma de fogo, mediante curso ministrado por instrutor credenciado pela Polícia Federal – comprovação de residência fixa.

Art. 4º O porte de arma de fogo previsto nesta Lei será concedido pela Polícia Federal, com abrangência e validade em todo território nacional e prazo de 5 (cinco) anos, renovável mediante nova comprovação dos requisitos previstos nesta Lei.

Art. 5º O porte de arma de fogo concedido nos termos desta Lei terá caráter pessoal e intransferível, abrangendo qualquer arma de porte de uso permitido devidamente registradas em nome do interessado, independente do sistema de controle.

Art. 6º A autorização de porte de arma de fogo perderá automaticamente sua eficácia caso o portador seja detido ou abordado em estado de embriaguez, sob efeito de substâncias químicas ou alucinógenas, ou pratique conduta incompatível com o exercício responsável do porte.

Art. 7º O Poder Executivo regulamentará esta Lei no prazo de 90 (noventa) dias, contados de sua publicação.

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

JUSTIFICATIVA

A atuação dos profissionais de segurança digital envolve a análise, contenção e neutralização de ataques cibernéticos que frequentemente atingem interesses ilícitos de grande relevância financeira. Esse enfrentamento, ainda que realizado em ambiente virtual, gera riscos reais, pois grupos criminosos organizados podem reagir de forma violenta quando seus esquemas são identificados e interrompidos.

Em diversas situações relatadas por especialistas do setor, é comum que profissionais responsáveis por bloqueios de invasões sofram intimidações como mensagens, tentativas de rastreamento e vigilância suspeita. Tais exemplos demonstram que a atividade possui risco crescente, decorrente da exposição a organizações maliciosas com ampla capacidade operacional.

Imagine um analista que impede um ataque direcionado a fraudar pagamentos eletrônicos. Ao rastrear o esquema, identifica conexões com grupos criminosos já envolvidos em delitos violentos. Esse cenário demonstra risco concreto de retaliação física contra profissionais que frustram ações que poderiam render ganhos ilícitos milionários aos responsáveis.

Outro exemplo ilustrativo ocorre quando técnicos de cibersegurança participam de investigações internas que detectam funcionários infiltrados a serviço de grupos externos. A identificação desse colaborador pode resultar em ameaças, coerção e risco de retaliação direta. É evidente que a atividade estabelece confronto com agentes dispostos a adotar violência para preservar seus interesses.

Em situações envolvendo operações de resposta a incidentes, equipes de segurança digital podem descobrir a origem territorial de ataques, vinculada a criminosos locais. Ao perceberem que foram expostos, tais indivíduos poderiam intimidar o profissional responsável, aumentando a necessidade de mecanismos legais que reforcem sua capacidade de proteção pessoal.

Há casos relatados por entidades de tecnologia, em que profissionais sofrem tentativas de invasão de residências, motivadas por represália após atuação bem-sucedida em barrar intrusões.

Esses cenários, demonstram um padrão preocupante: o crime cibernético deixou de ser um fenômeno isolado e tornou-se um desdobramento de redes criminosas que atuam também no mundo físico. Isso significa que ameaças virtuais podem evoluir para violência real contra os profissionais envolvidos.

A legislação atual não reconhece essa dinâmica híbrida entre o cibercrime e as ações violentas associadas, deixando esses profissionais em situação de vulnerabilidade. A proposta de porte de arma busca corrigir essa omissão, garantindo que indivíduos expostos a riscos crescentes tenham meios proporcionais de proteção, conforme autorizado pela legislação federal.

O avanço tecnológico ampliou a sofisticação das quadrilhas digitais, que utilizam técnicas avançadas de anonimização e criptografia. Ao serem desmascaradas por equipes especializadas, podem recorrer a métodos violentos para identificar, intimidar ou neutralizar tais profissionais. Isso justifica plenamente o porte como instrumento de defesa e prevenção.

Em investigações analistas de cibersegurança que rastreiam padrões de ataque podem inadvertidamente identificar vínculos entre fraudadores digitais e criminosos comuns. Ao perceberem que foram monitorados, esses grupos podem reagir com violência física. Assim, a atividade digital, embora técnica, aproxima-se cada vez mais do enfrentamento direto à criminalidade.

A proposta reconhece que, embora os profissionais de segurança digital não atuem armados no exercício direto da função, sua exposição decorre da interrupção de atividades ilícitas de alto valor. Quando frustram esquemas criminosos lucrativos, tornam-se alvos, gerando necessidade maior de proteção contra represálias.

Não é incomum, em relatos do setor, que profissionais recebam ligações suspeitas, mensagens coercitivas ou sinais de perseguição. O porte de arma surge como ferramenta adicional de autoproteção.

A presente proposição não incentiva o confronto, mas garante que profissionais em risco possam exercer o direito à legítima defesa. A arma, devidamente registrada e portada com responsabilidade, é instrumento de preservação da vida, especialmente em situações extremas decorrentes de atividades que irritam criminosos sofisticados e agressivos.

Em investigações internas de vazamento de dados, equipes de cibersegurança frequentemente lidam com suspeitos que têm conexões com organizações criminosas. Caso tais indivíduos percebam que estão prestes a ser denunciados, podem reagir de forma imprevisível. O porte legal oferece ao profissional a capacidade de enfrentar emergências com segurança.

Outra perspectiva envolve profissionais que atuam na recuperação de sistemas atacados por grupos internacionais. Caso identifiquem a origem do ataque ou bloqueiem pagamentos ilícitos relacionados a extorsões digitais, podem se tornar alvos de criminosos que não hesitam em usar violência para impedir que suas ações sejam desmanteladas.

Esses exemplos demonstram que a atividade de segurança digital não se limita a computadores. Ela envolve disputa direta com criminosos reais, com potencial violento. Negar a esses profissionais o direito ao porte é ignorar a realidade moderna da segurança, caracterizada por riscos concretos e crescentes no ambiente físico.

A concessão do porte também contribuirá para reduzir evasão de talentos, já que muitos profissionais da área relatam sensação de vulnerabilidade. Garantir meios legais de autodefesa reforça a valorização da categoria e estimula a permanência de especialistas qualificados, essenciais à proteção da infraestrutura digital nacional.

A criminalidade digital evoluiu rapidamente, enquanto a proteção pessoal desses profissionais permaneceu estagnada. O projeto visa equilibrar essa equação, oferecendo

condições equivalentes às enfrentadas por outros profissionais de áreas sensíveis, cujas atividades também expõem sua integridade física e justificam tratamento jurídico especial.

Em atividades de prevenção a fraudes financeiras, os profissionais frequentemente bloqueiam transações ilícitas que envolvem altos valores. Esse cenário evidencia a possibilidade de reação violenta por parte de criminosos interessados em recuperar ganhos ilícitos frustrados pela atuação da segurança digital.

A proposta busca ainda reforçar a proteção da família desses profissionais. Se criminosos tentam intimidá-los, podem tentar ampliar ameaças a parentes próximos. Garantir o porte aumenta a capacidade de resposta e preserva o equilíbrio psicológico necessário para desempenhar atividades críticas no combate ao cibercrime.

Em muitos casos, os criminosos tentam identificar o responsável por sua detecção, utilizando técnicas de engenharia social. Ao perceberem a exposição, podem avançar para ações violentas. Sem proteção adequada, esses profissionais ficam vulneráveis a agressões que poderiam ser evitadas por meio que instrumentalize a legítima defesa da vida.

Ademais, o porte não substitui políticas de segurança pública, mas complementa instrumentos de defesa pessoal garantidos pela legislação federal. Sua concessão objetiva assegurar que profissionais ameaçados possam preservar suas vidas, sem depender exclusivamente do tempo de resposta das autoridades em situações críticas.

Ao conceder porte de arma a profissionais de segurança digital, o Estado reconhece que a defesa da infraestrutura tecnológica nacional começa pela segurança de quem a protege. O risco enfrentado por esses especialistas é proporcional à relevância estratégica de suas atividades, e exige proteção compatível.

O projeto também fortalece a segurança institucional das empresas e órgãos públicos que dependem da atuação desses profissionais. Quanto mais protegidos estiverem, maior será a capacidade de desempenhar suas funções sem medo, garantindo continuidade do trabalho essencial contra-ataques cibernéticos e fraudes complexas.

A proposta não concede porte irrestrito, mas condicionado a critérios rigorosos de idoneidade, capacidade técnica e avaliação psicológica. Assim, garante equilíbrio entre direito individual e responsabilidade jurídica, evitando abusos e assegurando que apenas profissionais aptos e qualificados tenham acesso ao benefício.

O reconhecimento da presunção legal de risco, aqui proposto, é instrumento legislativo legítimo e utilizado em diversas áreas sensíveis. Considerando a natureza crescente das ameaças híbridas, o legislador deve agir preventivamente, assegurando proteção adequada a quem está na linha de frente do combate ao crime digital.

Como os cenários apresentados demonstraram, a violência física pode ser consequência direta de ações realizadas no ambiente virtual. Profissionais que identificam redes criminosas, bloqueiam ataques e frustram operações ilegais podem ser alvo de retaliação. Negar a eles instrumentos de autodefesa é desproporcional à realidade vivida.

Este projeto preenche lacuna jurídica e reforça os valores constitucionais da vida, liberdade e propriedade. Reconhece que a legítima defesa é direito fundamental e que deve ser assegurado a indivíduos cuja atividade profissional possui risco inerente, ainda que exercida predominantemente em ambiente digital.

Diante do exposto, e considerando os cenários plausíveis de ameaça física decorrentes da atuação contra o cibercrime, o presente Projeto de Lei é medida necessária, atual e compatível com a proteção dos profissionais que defendem diariamente empresas, cidadãos e instituições. Assim, conclamo os nobres pares à aprovação integral da matéria. Solicita-se, assim, o apoio dos nobres Parlamentares para sua aprovação.

Sala das Sessões, 25 de novembro 2025.

Deputado Federal Marcos Pollon

PL-MS