



CÂMARA DOS DEPUTADOS
Gabinete do Deputado Federal **Duda Ramos** - MDB/RR

Apresentação: 06/08/2025 10:42:02.380 - Mesa

PL n.3751/2025

PROJETO DE LEI Nº , DE 2025

(Do Sr. DUDA RAMOS)

Estabelece a prioridade na destinação de recursos para ações de informação e inteligência no combate aos crimes financeiros virtuais, com ênfase no estelionato digital, *phishing*, roubo de identidade, fraudes financeiras *online* e outros crimes cibernéticos, além de implementar a capacitação de profissionais, a utilização de tecnologias avançadas e a criação de um ambiente mais seguro no espaço digital.

O Congresso Nacional decreta:

Art. 1º Fica estabelecido que o Estado deve priorizar a destinação de recursos financeiros para ações de informação e inteligência no combate aos crimes financeiros virtuais, especialmente o estelionato digital, *phishing*, roubo de identidade e outros tipos de fraudes cibernéticas.

§1º Os recursos deverão ser utilizados para a aquisição de tecnologias especializadas e para o desenvolvimento de competências nas áreas de cibersegurança, inteligência digital e análise de dados.

§2º A alocação de recursos será vinculada à implementação de estratégias para melhorar a prevenção, detecção e repressão desses crimes, com a integração de esforços entre órgãos de segurança pública, instituições financeiras e empresas de tecnologia.

Art. 2º A destinação dos recursos será aplicada nas seguintes áreas de ação prioritária:

I - Aquisição e implementação de tecnologias avançadas, como inteligência artificial, *machine learning*, *blockchain*, e análise preditiva, para a detecção de padrões de fraudes e transações suspeitas em tempo real;



* C D 2 5 3 2 1 3 7 8 7 4 0 0 *

II - Criação de unidades especializadas em inteligência digital dentro das forças de segurança pública, com o objetivo de atuar na investigação e desmantelamento de redes criminosas que operam no espaço virtual;

III - Capacitação e treinamento contínuo de profissionais da segurança pública e agentes envolvidos na luta contra crimes virtuais, com ênfase na formação em cibersegurança, análise de dados e investigações digitais;

IV - Parcerias entre órgãos de segurança pública, bancos, empresas de tecnologia e instituições financeiras para o monitoramento contínuo, o compartilhamento de dados e a prevenção de crimes virtuais.

Art. 3º A prioridade na destinação de recursos será determinada pela taxa de incidência e pela complexidade dos crimes virtuais no Estado, com o objetivo de adaptar os recursos às necessidades específicas de cada área, como estelionato digital, fraudes bancárias online, roubo de identidade, entre outros.

§1º A alocação dos recursos será ajustada anualmente, de acordo com a evolução das tecnologias utilizadas pelos criminosos virtuais e a efetividade das ações já realizadas.

§2º A execução das políticas de informação e inteligência será monitorada através de relatórios anuais, disponibilizados publicamente, contendo a avaliação das ações implementadas e os resultados alcançados, como a redução de fraudes e a desarticulação de redes criminosas.

Art. 4º A transparência e rastreabilidade de transações financeiras online devem ser promovidas por meio da implantação de plataformas de monitoramento e pela cooperação entre órgãos reguladores e empresas privadas, a fim de garantir a segurança das informações financeiras e prevenir o estelionato virtual.

§1º As plataformas de monitoramento serão dotadas de ferramentas para rastrear transações suspeitas, identificar padrões de comportamento criminoso e alertar as autoridades de segurança pública e as instituições financeiras em tempo real.



§2º As ações de monitoramento também devem focar na identificação e bloqueio de sites fraudulentos, aplicativos falsos e e-mails de *phishing*, com o intuito de proteger os cidadãos contra os golpes virtuais.

Art. 5º O Governo Estadual deverá realizar a articulação interinstitucional com a Polícia Federal, bancos, agências reguladoras e empresas de tecnologia para desenvolver estratégias integradas no combate aos crimes virtuais, incluindo o compartilhamento de informações e a coordenação de ações para dismantelar organizações criminosas que operam no ambiente digital.

Art. 6º Os recursos para o cumprimento desta Lei serão incluídos anualmente na Lei de Diretrizes Orçamentárias (LDO), com prioridade nas áreas de cibersegurança, inteligência digital e capacitação de profissionais.

§1º A destinação de recursos será progressiva, com o aumento anual de no mínimo 5%, de forma que os valores sejam compatíveis com o crescimento da complexidade das fraudes digitais e as necessidades de infraestrutura e tecnologia.

Art. 7º O Governo Estadual deve promover campanhas educativas para a população, visando à conscientização sobre os riscos do estelionato digital, como fraudes bancárias e golpes online, e as melhores práticas para evitar cair em fraudes virtuais.

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

JUSTIFICAÇÃO

A crescente digitalização das atividades cotidianas e a rápida evolução da tecnologia têm gerado um aumento alarmante de crimes financeiros virtuais. O estelionato digital é um exemplo claro de como criminosos têm explorado as vulnerabilidades do ambiente digital para enganar cidadãos e roubar informações financeiras. O *phishing*, o roubo de identidade, as fraudes bancárias online e outros crimes cibernéticos têm gerado prejuízos bilionários à sociedade, prejudicando tanto indivíduos quanto empresas.



De acordo com o Instituto Brasileiro de Defesa do Consumidor (IDEC), em 2022, o Brasil registrou um aumento de 40% no número de fraudes financeiras virtuais em comparação ao ano anterior. R\$ 9 bilhões foram estimados como prejuízos causados por golpes online em 2022, o que representa uma alta de 20% em relação ao ano de 2021. Além disso, o Relatório Anual da Polícia Federal (2023) destacou que os crimes cibernéticos foram responsáveis por mais de 30% do total de fraudes registradas no país, evidenciando o crescente impacto dessas práticas criminosas na economia nacional.

O estelionato digital ocorre principalmente através de fraudes como falsas ofertas de produtos e serviços, clonagem de sites, e-mails de *phishing* e fraudes bancárias, onde os criminosos se passam por instituições financeiras ou comerciantes, enganando as vítimas e roubando dados bancários e valores financeiros. Esse tipo de crime compromete a confiança nas transações digitais e coloca em risco o comércio eletrônico, a inclusão digital e a inovação tecnológica.

O combate eficaz a esses crimes exige ações coordenadas e especializadas. Tecnologias avançadas como inteligência artificial, *machine learning*, *blockchain* e análise de dados são ferramentas fundamentais para a detecção de fraudes em tempo real, a identificação de padrões de comportamento criminoso e a prevenção de ataques cibernéticos. No entanto, para que essas tecnologias sejam implementadas de forma eficiente, é essencial que os órgãos de segurança pública recebam recursos adequados, incluindo capacitação de seus profissionais e a criação de unidades especializadas.

Além disso, a cooperação interinstitucional é um ponto crucial para enfrentar o estelionato digital, pois os criminosos frequentemente operam em redes transnacionais, exigindo a colaboração entre bancos, empresas de tecnologia, agências reguladoras e órgãos de segurança pública.

Este projeto de lei visa, portanto, a priorização de recursos para inteligência digital, tecnologia de ponta e capacitação de profissionais, criando um ambiente mais seguro e protegido contra os crimes financeiros



virtuais. A implementação dessas ações não só reduzirá os impactos sociais e financeiros desses crimes, mas também restaurará a confiança das pessoas e empresas nas transações digitais, fortalecendo a economia digital e a inclusão tecnológica.

Diante disso, solicito o apoio dos nobres parlamentares para a aprovação deste Projeto de Lei.

Sala das Sessões, em 05 de agosto de 2025.

Deputado DUDA RAMOS

