CÂMARA DOS DEPUTADOS

PROJETO DE LEI N.º 3.751-A, 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; tendo parecer da Comissão de Ciência, Tecnologia e Inovação, pela aprovação (relator: DEP. CORONEL MEIRA).

DESPACHO:
ÀS COMISSÕES DE
CIÊNCIA, TECNOLOGIA E INOVAÇÃO;
SEGURANÇA PÚBLICA E COMBATE AO CRIME ORGANIZADO;
FINANÇAS E TRIBUTAÇÃO (MÉRITO E ART. 54, RICD) E
CONSTITUIÇÃO E JUSTIÇA E DE CIDADANIA (ART. 54 RICD)

APRECIAÇÃO:
Proposição Sujeita à Apreciação Conclusiva pelas Comissões - Art. 24 II

S U M Á R I O

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;

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 desmantelar organizações criminosas que operam no ambiente digital.

Art. 6º Os recursos para o cumprimento desta Lei serão inclusos 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

COMISSÃO DE CIÊNCIA, TECNICOLOGIA E INOVAÇÃO

PROJETO DE LEI Nº 3.751, DE 2025

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.

Autor: Deputado DUDA RAMOS

Relator: Deputado CORONEL MEIRA

I - RELATÓRIO

O Projeto de Lei nº 3.571, de 2025, de autoria do Deputado Duda Ramos, dispõe sobre o estabelecimento de prioridade, pelo Estado, da 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.

Os recursos, segundo a proposição, serão utilizados na aquisição de tecnologias especializadas, bem como no desenvolvimento de competências nas áreas de cibersegurança, inteligência digital e análise de dados, com a prioridade de destinação determinada pela taxa de incidência e pela complexidade dos crimes virtuais.

Congresso Nacional – Anexo III, gabinete 885 | CEP 70160-900
Contato: (61) 3215-5885 | E-mail: dep.coronelmeira@camara.leg.br

A justificação do projeto destaca a priorização de recursos para inteligência digital, tecnologia de ponta e capacitação de profissionais, com o fim de proporcionar um ambiente mais seguro e protegido contra os crimes financeiros virtuais.

A proposição foi distribuída às Comissões de Ciência, Tecnologia e Inovação; Segurança e Combate ao Crime Organizado; Finanças e Tributação (mérito e art. 54, RICD) e Constituição e Justiça e de Cidadania (art. 54 RICD), estando sujeita à apreciação Conclusiva pelas Comissões (art. 24, II, RICD) e tramitação no regime ordinário (art. 151, III, RICD).

Decorrido o prazo regimental, nesta Comissão não foram apresentadas emendas.

II - VOTO DO RELATOR

A proposição em análise objetiva assegurar o investimento, por meio da priorização na destinação de recursos públicos, em tecnologias avançadas e adequadas ao combate aos crimes financeiros virtuais, com ênfase no estelionato digital, phishing, roubo de identidade, fraudes financeiras online e outros crimes cibernéticos.

Em um contexto de crescente informatização dos serviços financeiros, é mais que urgente a criação de mecanismos efetivos para proteção patrimonial em ambiente virtual, diante do aumento acentuado dos casos de fraudes e estelionatos digitais.

Segundo pesquisa encomendada pelo Fórum Brasileiro de Segurança Pública, divulgada pelo Datafolha em agosto de 2025[1], 56 milhões de brasileiros (uma a cada três pessoas) foram vítimas de golpe virtuais com

[1] Disponível em: https://www.infomoney.com.br/brasil/datafolha-golpes-virtuais-atingem-1-3-dos-brasileiros-e-envolvem-r-112-bi-em-1-ano/

Congresso Nacional – Anexo III, gabinete 885 | CEP 70160-900
Contato: (61) 3215-5885 | E-mail: dep.coronelmeira@camara.leg.br

prejuízo financeiro nos últimos 12 meses. Os crimes, que envolvem fraudes no Pix, boletos falsos, compras online não entregues e clonagem de cartões, causaram nesse período o impacto estimado de R$ 111,9 bilhões.

Além disso, o estudo apontou os golpes virtuais como nova fonte de receita de organizações criminosas, com estrutura operacional que ultrapassam as ligações feitas a partir dos presídios.

Outra pesquisa corrobora com a gravidade do tema, dessa vez realizada pela empresa de inteligência antifraude Silverguard[2], que constatou o prejuízo médio das vítimas de golpes digitais em R$ 2.540 em 2025, um aumento de 21% em relação ao ano anterior.

O levantamento, divulgado em 27 de outubro de 2025, mostra que idosos são os mais afetados, correspondendo a 30,8% dos casos. Essa população perde, em média, R$ 4.820 em golpes virtuais, enquanto jovens de 18 a 24 anos têm prejuízo médio de R$ 964, ou seja, valor cinco vezes menor em relação aos idosos.

Nesse sentido, fica evidente a necessidade de formulação de estratégias de proteção patrimonial digital, principalmente quando a vítima é pessoa com maior vulnerabilidade no ambiente virtual. Ressalte-se o comprometimento dos membros da Comissão de Segurança Pública e Combate ao Crime Organizado e da Comissão de Defesa dos Direitos da Pessoa Idosa nesse debate, cujo tema será objeto de audiência pública conjunta nesse ano.

Por isso, o estabelecimento de prioridade na destinação de recursos para ações de informação e inteligência no combate aos crimes financeiros virtuais é meritório, principalmente porque as políticas públicas atuais não têm

[2] Disponível em: https://www1.folha.uol.com.br/tec/2025/10/vitimas-de-golpes-virtuais-perdem-em-media-r-2540-idosos-sao-os-que-mais-tem-prejuizo.shtml

Congresso Nacional – Anexo III, gabinete 885 | CEP 70160-900
Contato: (61) 3215-5885 | E-mail: dep.coronelmeira@camara.leg.br

sido suficientes para garantir desenvolvimento eficaz de competências nas áreas de cibersegurança e inteligência digital.

Ademais, a previsão de articulação interinstitucional entre o Poder Público e a Polícia Federal, bancos, agências reguladoras e empresas de tecnologia, no sentido de desenvolver estratégias integradas no combate aos crimes virtuais, com o compartilhamento de informações e a coordenação de ações para desmantelar organizações criminosas que operam no ambiente digital, contribui substancialmente para o objetivo da proposição.

Diante do exposto, entendendo que a proposição é relevante para o combate aos crimes financeiros virtuais, para um ambiente digital mais seguro e para o desenvolvimento tecnológico na área de cibersegurança, **somos, no mérito, pela aprovação do Projeto de Lei nº 3.751, de 2025.**

Sala da Comissão, em de abril de 2026.

CORONEL MEIRA

Deputado Federal (PL/PE)

Relator

Congresso Nacional – Anexo III, gabinete 885 | CEP 70160-900
Contato: (61) 3215-5885 | E-mail: dep.coronelmeira@camara.leg.br

Câmara dos Deputados

COMISSÃO DE CIÊNCIA, TECNOLOGIA E INOVAÇÃO

PROJETO DE LEI Nº 3.751, DE 2025

III - PARECER DA COMISSÃO

A Comissão de Ciência, Tecnologia e Inovação, em reunião extraordinária realizada hoje, mediante votação ocorrida por processo simbólico, concluiu pela aprovação do Projeto de Lei nº 3.751/2025, nos termos do Parecer do Relator, Deputado Coronel Meira.

Registraram presença à reunião os seguintes membros:

Átila Lira - Presidente, David Soares, Fabio Reis, Jeferson Rodrigues, Jefferson Campos, Julio Cesar Ribeiro, Luisa Canziani, Márcio Marinho, Ricardo Barros, Rodrigo Rollemberg, Rui Falcão, Vitor Lippi, Afonso Hamm, Amaro Neto, Amom Mandel, André Figueiredo, Arnaldo Jardim, Bebeto, Bibo Nunes, Carlos Henrique Gaguim, Coronel Meira, Daiana Santos, Daniel Freitas, Dr Flávio, Dr. Zacharias Calil, Giovani Cherini, Heitor Schuch, Jandira Feghali, Jorge Goetten, Josenildo, Lucas Ramos, Pedro Uczai, Professora Luciene Cavalcante, Raimundo Santos e Rodrigo da Zaeli.

Sala da Comissão, em 15 de abril de 2026.

Deputado ÁTILA LIRA
Presidente