



CÂMARA DOS DEPUTADOS

PROJETO DE LEI Nº , DE 2025.
(Sr. Domingos Neto)

Altera as Leis nº 12.850, de 2 de agosto de 2013, nº 9.613, de 3 de março de 1998, e nº 12.965, de 23 de abril de 2014, para aprimorar a tipificação, as penas e as medidas contra organizações criminosas digitais.

O Congresso Nacional decreta:

Art. 1º Inclua-se o seguinte dispositivo na Lei nº 12.850, de 2 de agosto de 2013:

“Art. 1º-A. Considera-se organização criminosa digital a associação de 3 (três) ou mais pessoas, estruturalmente ordenada e caracterizada pela divisão de tarefas, ainda que informalmente, que se valha, prioritária e habitualmente, de meios cibernéticos ou tecnológicos para a prática de crimes cujas penas máximas sejam superiores a 4 (quatro) anos, ou que sejam de caráter transnacional.

§ 1º As ações praticadas por essas organizações incluem, mas não se limitam a:

I – fraudes bancárias eletrônicas;

II – ransomware e sequestro de dados;

III – clonagem de cartões e dispositivos de pagamento;

IV – manipulação de sistemas informatizados;

V – ocultação ou dissimulação de bens, direitos ou valores por meio de criptoativos ou plataformas digitais.”

§ 2º A pena para quem integrar, organizar, chefiar ou financiar organização criminosa digital será de 4 (quatro) a 8 (oito) anos de reclusão, além da pena correspondente ao crime praticado.





CÂMARA DOS DEPUTADOS

§ 3º As penas serão aumentadas de $\frac{1}{3}$ (um terço) a $\frac{2}{3}$ (dois terços) se:

I – houver uso de ferramentas de anonimização avançada para dificultar a investigação; e

II – houver ataque a instituições financeiras, serviços públicos essenciais ou infraestrutura crítica.

§ 4º As empresas de tecnologia, provedores de internet, bancos, bancos digitais e corretoras de criptoativos deverão colaborar com autoridades policiais e judiciais na identificação de usuários suspeitos, sob pena de multa.” (NR)

Art. 2º Inclua-se o seguinte dispositivo na Lei nº 9.613, de 3 de março de 1998 (Lei de Lavagem de Dinheiro):

“Art. 1º.....

§ 2º-A A prática de lavagem de dinheiro ou ocultação de bens, direitos e valores por meio de criptoativos ou plataformas digitais, quando comprovada a habitualidade e a finalidade de dissimular a origem, a localização, a movimentação ou a propriedade de ativos, será considerada crime antecedente para os fins desta Lei, com pena aumentada de $\frac{1}{3}$ (um terço) a $\frac{2}{3}$ (dois terços) se a operação for realizada por organização criminosa digital.” (NR)

Art. 3º Inclua-se o seguinte dispositivo na Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet):

“Art. 10

§ 3º O provedor de aplicações de internet será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço, tornar indisponível o conteúdo apontado como infringente, ressalvadas as hipóteses de colaboração obrigatória com a investigação de crimes cibernéticos, especialmente os cometidos por organizações criminosas digitais, nas quais deverá fornecer dados de conexão, dados cadastrais e registros de acesso, nos termos da lei e de ordem judicial, sob pena de multa diária.” (NR)





Art. 4º Esta Lei entra em vigor na data de sua publicação.

JUSTIFICATIVA

A criminalidade contemporânea tem migrado, de forma acelerada, para o ambiente digital, onde atua com sofisticação, anonimato e alcance global. A presente proposição de lei visa enfrentar esse desafio ao criar um marco jurídico específico para combater as organizações criminosas digitais, uma ameaça crescente à segurança pública, à economia e à privacidade dos cidadãos.

A inclusão do Art. 1º-A na Lei nº 12.850 de 2013 busca adaptar o conceito de organização criminosa à realidade cibernética. A criminalidade digital não se resume a atos isolados; ela é perpetrada por estruturas complexas, com divisão de tarefas, que exploram vulnerabilidades tecnológicas e fragilidades institucionais. A tipificação desses grupos permitirá às autoridades utilizar instrumentos de investigação e persecução penal já previstos em lei, como a colaboração premiada, a infiltração de agentes e a interceptação de comunicações, de forma mais efetiva contra esses criminosos.

Além disso, a proposta reconhece que a cibersegurança não é apenas uma questão de repressão, mas também de prevenção. A cooperação com o setor privado é um pilar fundamental. Ao estabelecer uma obrigação clara para provedores de internet e plataformas digitais de cooperar com as autoridades, a lei supera um dos maiores entraves das investigações: a dificuldade em obter dados e registros.

Outro avanço significativo reside na atualização da Lei de Lavagem de Dinheiro, Lei nº 9.613, de 3 de março de 1998. A menção explícita a criptoativos e plataformas digitais é um reconhecimento da nova economia do crime. Moedas virtuais, como o Bitcoin, e plataformas de pagamento anônimas são amplamente utilizadas para ocultar a origem ilícita de ativos e dificultar o rastreamento financeiro. A proposição de lei, ao criminalizar o uso desses instrumentos para a lavagem de dinheiro, fecha uma das principais brechas que as organizações criminosas digitais exploram para converter seus ganhos ilegais em ativos "limpos".

A proposta também reconhece que o crime cibernético não é apenas uma questão de segurança, mas também de soberania nacional. Ataques cibernéticos a





CÂMARA DOS DEPUTADOS

infraestruturas críticas, como redes de energia, sistemas de transporte e instituições financeiras, podem paralisar um país.

Além dos aspectos de segurança pública e soberania nacional, esta proposição de lei carrega um forte pilar de proteção social, fundamental para a justiça e equidade. A criminalidade digital, ao explorar vulnerabilidades humanas e tecnológicas, atinge de forma desproporcional as populações mais suscetíveis, como idosos, pessoas de baixa escolaridade e indivíduos com menor letramento digital.

Esses grupos são frequentemente alvos de fraudes bancárias eletrônicas, golpes de *phishing* e sequestros de dados, que se valem de engenharia social e da falta de familiaridade com o ambiente digital. O dano causado por esses crimes vai além da perda financeira; ele abala a confiança nas instituições, causa prejuízos emocionais e, muitas vezes, compromete o sustento e o patrimônio de uma vida inteira.

Ao classificar essas ações como parte de organizações criminosas digitais, a lei permite que as autoridades atuem com maior rigor e coordenação. A tipificação não apenas aumenta as penas, mas também facilita o uso de ferramentas de investigação sofisticadas para dismantelar as redes criminosas por trás desses golpes. A obrigação de colaboração imposta a empresas de tecnologia e instituições financeiras, por sua vez, agiliza a identificação e a responsabilização dos criminosos, garantindo uma resposta mais rápida e efetiva.

Assim, esta lei se estabelece como um instrumento de inclusão e proteção, assegurando que o avanço tecnológico não se torne uma nova fronteira para a exploração de vulnerabilidades. Ela fortalece o Estado em seu papel de garantir a segurança de todos os cidadãos, independentemente de sua idade ou conhecimento técnico, reafirmando que a segurança no mundo digital é um direito fundamental.

Sala das Sessões, de setembro de 2025.

Deputado DOMINGOS NETO
PSD/CE

