

PARECER PROFERIDO EM PLENÁRIO AO PL Nº 4.554, DE 2020

PROJETO DE LEI Nº 4.554, DE 2020 (Apensados PL's 2638/2020 e 3363/2020)

Altera o Código Penal, para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Código de Processo Penal, para prever a competência dos crimes cometidos pela internet ou de forma eletrônica pelo lugar de domicílio ou residência da vítima.

Autoria: SENADO FEDERAL

Relatoria: Deputado Vinícius Carvalho

I – RELATÓRIO

O Projeto de Lei nº 4.554 de 2020, de autoria do Senador Izalci Lucas (PSDB-DF), foi apresentado para criar meios mais rigorosos para punir de maneira mais severa fraudes, furtos e estelionatos cometidos de forma eletrônica ou pela internet. Segundo o autor da proposta, “o volume de fraudes já começa a afetar a economia do país, gerando perda do poder aquisitivo e também perdas emocionais por parte das vítimas”. Em 25 de novembro de 2020 a matéria foi aprovada pelo Senado Federal, na forma do Substitutivo.

No dia 07 de dezembro de 2020, o projeto de lei chegou à Câmara dos Deputados para ser analisado. Em 25 de fevereiro de 2021 a proposição foi despachada à Comissão de Constituição e Justiça e de Cidadania (Mérito e Art. 54, RICD), sujeita à apreciação do Plenário. No dia 03 de março de 2021, o Plenário desta Casa aprovou requerimento de urgência de minha autoria.

Tramitam conjuntamente ao Projeto as seguintes proposições que compartilham da preocupação com a proliferação desse tipo de crime no país:

- Projeto de Lei nº 2.638, de 2020, de autoria do ilustre Deputado Marcelo Ramos, estimado 1º Vice-Presidente desta Casa, que “dispõe sobre a tipificação criminal de furto mediante fraude eletrônica; e altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal”.

- Projeto de Lei nº 3663, de 2020, do nobre Deputado Alexandre Frota, “altera o artigo 155 do Decreto Lei 2848 de 7 de dezembro de 1940, para inserir o § 8º ao texto original”.

É o relatório.



II – VOTO DO RELATOR

Preliminarmente, manifestamos nosso entendimento de que as propostas são importantes e necessárias. Os dados e registros de casos relativos a fraudes eletrônicas no Brasil são contundentes e reforçam que precisamos endurecer o combate contra essas condutas perniciosas que afetam a economia, o funcionamento de nossas instituições e o bem-estar social de nosso povo.

II.1 – CONSTITUCIONALIDADE, JURIDICIDADE E TÉCNICA LEGISLATIVA

No que tange à iniciativa **constitucional** das matérias, não existem reparos a serem feitos no texto já deliberado pelo Senado, bem como nas propostas que tramitam apensadas, uma vez que se verifica plena conformidade aos requisitos constitucionais formais, o respeito à competência da União para legislar sobre o tema, consoante dispõe o art. 22, I, da Constituição Federal, e a iniciativa parlamentar legítima, fundada no que dispõe o art. 61, da Carta Magna de 1988, eis que **não incidem**, nas espécies, quaisquer reservas à sua iniciativa. No tocante à constitucionalidade material, **não se vislumbram** também quaisquer discrepâncias entre ela e a Constituição Federal.

Em relação à **juridicidade**, nada há a ser corrigido, já que o texto da proposta principal inova no ordenamento jurídico e alinha-se aos princípios gerais do direito, o mesmo se aplicando às apensadas.

Quanto à **técnica legislativa** utilizada nesta proposição legislativa verificamos que está integralmente de acordo com os ditames da Lei Complementar nº 95, de 26 de fevereiro de 1998, com as alterações introduzidas pela Lei Complementar nº 107, de 26 de abril de 2001. **Não há, portanto, ressalvas** quanto ao projeto principal e seus apensados.

II.2 – EXAME DE MÉRITO

Chamo a atenção dos nobres pares para um problema que fugiu ao controle em nosso país: o número de fraudes praticadas todos os dias transformou o Brasil no paraíso dos cibercriminosos.

Os números confirmam isso.

Golpes Frequentes no Brasil

Só em 2019, foram registradas 24 bilhões de tentativas de ataques cibernéticos no Brasil. Os cibercriminosos estão se adaptando a esta nova era de trabalho remoto com ameaças mais sofisticadas e novas maneiras de executar atividades maliciosas nos sistemas para aumentar seus índices de sucesso.

De acordo com o Centro de Denúncias de Crimes Cibernéticos do FBI, durante a pandemia que ainda assola todo o planeta, houve um aumento de 300% de ataques cibernéticos nas principais economias.



A cada 24 horas, em média 12 mil contas de whatsapp são clonadas. Quem aqui não conhece alguém ou até mesmo já foi vítima da clonagem de whatsapp?

Estamos próximos a semana do consumidor e precisamos protegê-los contra essas fraudes tornando mais rigorosa a nossa legislação. São mais de 12 milhões de consumidores prejudicados pelos criminosos. E a ausência de uma legislação mais dura fará com que esse número aumente a cada dia.

Segundo a Karpesrky, o Brasil é líder mundial em golpes na modalidade phishing. Uma cada cinco brasileiros foi alvo deste golpe em 2020. Esse golpe ocorre quando um criminoso cria página falsa para simular um site verdadeiro para roubar dados e desviar recursos da vítima. Só em fevereiro de 2020, houve um aumento de 120% nesta modalidade de golpe, se comparados os dados do mesmo mês no ano anterior.

Auxílio Emergencial

Os prejuízos são notórios para toda a sociedade. Para termos uma ideia, já foram identificados pelo menos 3,8 milhões de pedidos fraudulentos de auxílio emergencial. Neste período houve um aumento de 60% de tentativas de golpe a idosos e aposentados.

Fraudes Previdenciárias

Só entre 2019 e 2021, a Polícia Federal com o apoio de outros órgãos realizou operações no Ceará, no Piauí, Paraíba no Maranhão, no Rio Grande do Sul, na Bahia, em Pernambuco, no Amapá e em outros estados para cobater fraudes previdenciárias nas mais diversas modalidades.

De acordo com a Ouvidoria do Ministério da Economia, recorrentemente são recebidas denúncias de fraudes na Previdência. Uso de dados falsos nos sistemas do governo, e-mails que são usados para capturar informações sobre os segurados, entre outras fraudes podem ter gerado um prejuízo de pelo menos R\$ 5,5 bilhões entre 2003 e 2019.

Fraudes contra consumidores de serviços financeiros

Os investimentos de bancos com tecnologia aumentaram 48% em 2020. O orçamento total do setor chegou a R\$ 24,6 bilhões no último ano, segundo a Pesquisa Febraban de Tecnologia Bancária; canais digitais foram responsáveis por 63% das transações no ano passado. Cada vez mais, os clientes também pagam suas contas e fazem transferências de valores pelos canais digitais.

Um levantamento realizado pela empresa de segurança da informação Kaspersky mostrou que o Brasil foi o país mais atingido por tentativas de roubo de dados pessoais ou financeiros na internet, prática denominada em inglês de phishing. De acordo com a companhia, entre fevereiro e março do ano passado, o número de ataques cresceu 120% no País.

O estudo também mostra que em 2020 cerca de 19,9% de internautas brasileiros tentaram abrir pelo menos uma vez links enviados para roubar dados. Em segundo lugar no ranking de países vem Portugal (19,7%),



seguido por França (17,9%), Tunísia (17,6%), Camarões (17,3%) e Venezuela (16,8%).

Ataques às Instituições Brasileiras

Os riscos para o Estado também são enormes. Em fevereiro deste ano o Supremo Tribunal Federal (STF) foi alvo de nova tentativa de ataque de hackers que desejavam roubar senhas de servidores. Em novembro do ano passado o Superior Tribunal de Justiça (STJ) sofre ataque que prejudicou os trabalhos do tribunal. Em outubro de 2020, durante as eleições, o Tribunal Superior Eleitoral (TSE) também foi alvo de hackers. Vários outros órgãos e instituições de nosso país têm sido assolados por esses ataques criminosos.

Aspectos Internacionais

Especialistas em segurança cibernética afirmam que o fato de o Brasil não ser signatário da Convenção Internacional para o Combate aos Crimes Cibernéticos, pode estimular que criminosos dessa natureza operem no país. Outro fator é a inexistência de legislação específica que disponha sobre este crime em nosso país. No Brasil é necessário que o criminoso seja enquadrado em crimes análogos que possuem penas brandas. Outras potências mundiais, como EUA, China, Coreia do Sul e Alemanha, possuem Leis rígidas que chegam a penalizar o criminoso de 3 a 10 anos de prisão.

Pedofilia e Pornografia Infantil

Segundo o Ministério de Direitos Humanos, a violência sexual contra crianças e adolescentes é um fenômeno multifacetado e multicausal que se reveste de uma complexidade e gravidade devastadoras.

Entre 2011 e 2019 o Ministério recebeu mais de 200 mil denúncias de violência contra crianças e adolescentes nas suas mais variadas formas. A pornografia infantil e o compartilhamento de conteúdo de pedofilia tem sido combatidas em nosso país, cooperando inclusive para desbaratar quadrilhas internacionais. Todavia, ainda há muito a ser feito.

Infelizmente muitas vezes não é possível identificar as vítimas que estão nesses conteúdos perniciosos, muito menos o domicílios delas. Assim, proporemos mais adiante a supressão de um dispositivo no substitutivo aprovado pelo Senado no PL 4554 de 2020, para garantir que as autoridades competentes não encontrem dificuldades legais no combate a esses e outros crimes praticados no ambiente virtual.

Dados pessoais

A Polícia Federal ressaltou que a aprovação desta lei que reforça a punição para crimes cibernéticos é uma evolução importante para o Brasil, conforme o parlamento brasileiro já sinalizou compreender. Com esta lei que aprovaremos, poderemos confiar que operações como a Deepwater ocorrida na sexta-feira, dia 19 de março de 2021, na qual foram cumpridos cinco mandados de busca e apreensão e um mandado de prisão preventiva nos municípios de Petrolina (PE) e Uberlândia (MG), em investigação sobre fatos criminosos relacionados à obtenção, divulgação e comercialização de dados pessoais de brasileiros, dentre esses diversas autoridades públicas, terão tratamento mais adequado, severo e alinhado com as melhores práticas internacionais. Esses hackers são suspeitos de vazarem mais de 200 milhões de dados.



Supressão de Dispositivo: Preservação de Competências da Polícia Federal

Para atendimento de solicitação da Polícia Federal, após reunião virtual com os delegados, coordenador geral de Polícia Fazendária e a chefe da divisão de repressão aos crimes cibernéticos, realizarei em meu parecer a supressão completa do artigo 2º do texto do Senado. Recomendo aos nobres pares, na condição de relator desta matéria, a retirada completa desse dispositivo, pois na avaliação da Polícia Federal, que ouvi durante os estudos para formulação deste parecer, a definição do domicílio da vítima como fator definidor da competência, poderia gerar questionamentos de ordem processual que atrasariam trabalhos de repressão aos crimes cibernéticos, cujo o desdobramento poderia causar, dentre outros problemas, a prescrição do crime.

Hoje em dia o criminoso avalia os pontos positivos e negativos de sua conduta. Quando alguém comete um crime, ele não sabe a qual pena será condenado, mas sabe qual é a pena máxima e qual é a pena mínima possível para aquele crime. É assim que a mancha da criminalidade se move, onde encontra facilidade – Brasil paraíso dos cibercriminosos, e menos risco para sua conduta – penas brandas aliadas a procedimento processual penal ultrapassado.

Muitas vezes os crimes por meio da internet ocorrem simultaneamente ou continuamente de forma a atingirem pessoas de diferentes estados e até mesmo de diferentes países. Nesse sentido, estou convencido de que a Polícia Federal está bem balizada neste pedido de supressão que me apresentou para suprimirmos o artigo 2º, para garantir a continuidade dos trabalhos de repressão a crimes cibernéticos muito bem conduzidos pela referida instituição.

Alteração no Código de Processo Penal - definição de competência em algumas modalidades de estelionato

Acatamos também sugestões de delegados para solucionarmos uma controvérsia acerca da fixação de regra de competência para determinadas modalidades de crimes de estelionato, com vistas a prestigiar a regra do local de domicílio da vítima em detrimento da regra firmada jurisprudencialmente do local do proveito do ilícito. Essa proposta originária do Projeto de Lei 4.620, de 2020 do Senador Fabiano Contarato, foi adicionada ao substitutivo a pedido de representantes da categoria, com vistas a agilizar o trâmite do assunto de extrema relevância.

Propostas que tramitam apensadas ao texto do Senado

A aprovação de uma lei para combater estes problemas é necessária e vem em boa hora. A atuação do parlamento fará com que o nosso país deixe para trás, de uma vez por todas, o título de paraíso para os cibercriminosos.

Por tudo o que expomos neste parecer, está claro que esta proposta já aprovada pelo Senado é meritória e merece o apoio total desta Casa, considerada a necessidade de excluirmos o artigo segundo.



Igualmente meritórios são os objetivos das proposições apensadas, os quais já encontram-se contemplados na proposição principal em estágio mais avançado de tramitação.

Tanto o texto de autoria do nosso ilustre Vice-Presidente, Deputado Marcelo Ramos (PL-AM), como a proposta apresentada pelo ilustre Deputado Alexandre Frota (PSDB-SP) estão em plena harmonia com os objetivos da proposta oriunda do Senado.

Ocorre que na minha avaliação, a proposta principal já contempla totalmente os objetivos dos nobres parlamentares aqui citados, aos quais cumprimento e agradeço pelas iniciativas e os acolho na forma do substitutivo que ora apresento.

Agradecimentos e encaminhamento à conclusão

Quanto ao mérito, senhor Presidente e nobres colegas deputados federais, eram essas as nossas contribuições.

Registro neste meu voto meus cumprimentos e agradecimentos aos autores das propostas pela Câmara dos Deputados, os Deputados Marcelo Ramos e Alexandre Frota, pois suas propostas muito contribuíram com as reflexões e pesquisas para formulação deste parecer.

Passemos, portanto, à conclusão.

III – CONCLUSÃO DO VOTO

Ante o exposto, pela Comissão de Constituição e Justiça e de Cidadania, somos pela constitucionalidade, juridicidade e adequada técnica legislativa do Projeto de Lei nº 4.554, de 2020, do Projeto de Lei nº 2.638, de 2020, e do Projeto de Lei nº 3.363, de 2020, e, no mérito, pela APROVAÇÃO do Projeto de Lei nº 4.554, de 2020, do Projeto de Lei nº 2.638, de 2020, e do Projeto de Lei nº 3.363, de 2020, nos termos do Substitutivo ora apresentado.

Sala das Sessões, em de de 2021.

Deputado VINICIUS CARVALHO
Relator



SUBSTITUTIVO AO PROJETO DE LEI Nº 4.554, DE 2020

Altera o Código Penal para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet e o Código de Processo Penal para definir a competência de modalidades de estelionato

O Congresso Nacional decreta:

Art. 1º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), passa a vigorar com as seguintes alterações:

“Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:

Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.

§ 2º Aumenta-se a pena de um terço a dois terços se da invasão resulta prejuízo econômico.

§ 3º



Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa.
.” (NR)

“Art.
155.

.....
§ 4º-B. A pena é de reclusão de 4 (quatro) a 8 (oito) anos e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo.

§ 4º-C. A pena prevista no § 4º-B deste artigo, considerando a relevância do resultado gravoso:

I – aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional;

II – aumenta-se de 1/3 (um terço) ao dobro, se o crime é praticado contra idoso ou vulnerável.

.....” (NR)

“Art. 171.....

Fraude eletrônica

§ 2º-A. A pena é de reclusão de 4 (quatro) a 8 (oito) anos e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos



telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo.

§ 2º-B. A pena prevista no § 2º-A deste artigo, considerando a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional.

.....

Estelionato contra idoso ou vulnerável

§ 4º A pena será aumentada de 1/3 (um terço) ao dobro, se o crime for cometido contra idoso ou vulnerável, considerando a relevância do resultado gravoso.

.....” (NR)

Art. 2º O Decreto-Lei nº 3.689, de 3 de outubro de 1941 - Código de Processo Penal passa a vigorar acrescido do parágrafo 4º em seu art. 70:

“Art. 70.

.....

§ 4º Nos crimes previstos no art. 171 do Código Penal, quando praticados mediante depósito, mediante emissão de cheques sem suficiente previsão de fundos em poder do sacado ou frustrando o seu pagamento ou mediante transferência de valores, a competência será definida pelo local do domicílio da vítima, e, em caso de pluralidade de vítimas, a competência firmar-se-á pela prevenção. (NR)”



Art. 3º Esta lei entra em vigor na data da sua publicação.

Sala das Sessões, em de de 2021.

Deputado VINICIUS CARVALHO
Relator

