PARECER Nº , DE 2023

Da COMISSÃO DE COMUNICAÇÃO E DIREITO DIGITAL, sobre o Projeto de Lei nº 613, de 2021, do Senador Marcos do Val, que *altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, para tipificar como crime condutas indevidas praticadas contra sistemas e dados informáticos*.

Relator: Senador **ASTRONAUTA MARCOS PONTES**

I – RELATÓRIO

Vem a esta Comissão de Comunicação e Direito Digital (CCDD) o Projeto de Lei (PL) nº 613, de 2021, de autoria do Senador Marcos do Val, que *altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, para tipificar como crime condutas indevidas praticadas contra sistemas e dados informáticos*.

O art. 1º da proposição altera a redação do atual art. 154-A do Código Penal para tipificar o crime de *acesso ilegítimo a sistema informático*, consistente em *acessar, de qualquer forma, sem autorização legal ou do seu titular, sistema informático, com ou sem violação de mecanismo de segurança, ou instalar vulnerabilidades para obter vantagem ilícita*. Para esse crime, é cominada a pena de detenção, de um a três anos, e multa.

De acordo com o § 1º do referido dispositivo, na mesma pena incorre quem *produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta* prevista no **caput**.

Nos termos do § 3º do mesmo artigo 154-A, a pena passa a reclusão, de dois a quatro anos, e multa, caso não constitua crime mais grave, se *do acesso resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas* [...] *ou o*

controle remoto não autorizado do dispositivo invadido. Essa pena pode ser ainda aumentada de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro das informações obtidas indevidamente.

Já nos termos do § 5º, a pena é aumentada de um terço à metade se o crime for cometido contra os chefes do Poder Executivo da União, dos estados, do Distrito Federal e dos municípios; os presidentes da Câmara dos Deputados, do Senado Federal, das assembleias legislativas dos estados, da Câmara Legislativa do Distrito Federal e das câmaras municipais; o presidente do Supremo Tribunal Federal; ou ainda contra *dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal*.

O art. 2º projeto, por seu turno, acrescenta os arts. 154-C a 154-J ao Código Penal.

O art. 154-C trata do crime de *interferência em dados de sistema informático*, consistente em *obter, adulterar ou destruir, intencional e indevidamente, sem autorização legal ou do titular, dados informações de sistema informático*. A essa conduta é cominada a pena de reclusão, de dois a cinco anos, e multa.

O art. 154-D, por sua vez, tipifica a conduta de *interferência em sistema informático*, descrita como *interferir, intencional e indevidamente, sem autorização legal ou do titular, no funcionamento de sistema informático, por meio da introdução, transmissão, eliminação, deterioração, modificação ou supressão de dados informáticos*. A pena prevista para esse crime é de reclusão, de dois a cinco anos, e multa.

Já o art. 154-E introduz o crime de *burla informática*, caracterizado como a obtenção de vantagem ilícita mediante *introdução, alteração, eliminação ou supressão indevida de dados ou informações em sistema informático* ou *qualquer intervenção indevida no funcionamento de sistema informático*. Para esse crime, é prevista a pena de reclusão, de dois a cinco anos, e multa, se o fato não constituir crime mais grave.

No art. 154-F é descrita a conduta de *falsidade informática*, configurada por *introduzir, alterar, eliminar ou suprimir dados, indevidamente ou mediante fraude, em sistema informático, produzindo dados não autênticos, com o fim de que sejam considerados ou utilizados para fins legais como*

autênticos. O dispositivo comina para este crime a pena de reclusão, de três a seis anos, acrescida de multa, se o fato não constituir crime mais grave.

O último tipo a ser inserido no catálogo do Código Penal é o de *uso abusivo de dispositivo ou dado informático*, a ser tratado no art. 154-G. O crime consiste em *produzir, vender, obter, possuir, importar ou distribuir, para a prática de quaisquer dos crimes previstos nos arts. 154-C a 154-F, dispositivo ou programa informático* ou *senha, código de acesso ou qualquer outro dado informático que permita acessar o todo ou parte de sistema informático*. Para essa conduta, a pena cominada é de reclusão, de um a três anos, e multa.

Nos termos do art. 154-H, as penas dos crimes descritos nos arts. 154-A e 154-C a 154-F serão aumentadas de um a dois terços quando forem praticados contra a administração pública direta ou indireta de qualquer nível de governo, contra empresas concessionárias de serviços públicos ou quando resultarem em prejuízo econômico.

O art. 154-I esclarece as definições de sistema informático e dado informático que devem ser utilizadas para a aplicação do disposto nos arts. 154-A e 154-C a 154-G.

Por fim, o art. 154-J estabelece que, para a caracterização dos crimes previstos nos arts. 154-A e 154-C a 154-F, é indiferente se o sistema informático está ou não conectado à internet. Além disso, o dispositivo especifica que os referidos crimes somente se processam mediante representação, salvo quando cometidos contra a administração pública direta ou indireta de qualquer nível de governo ou contra concessionárias de serviços públicos.

O art. 3º da proposição revoga o § 2º do atual art. 154-A e o art. 154-B, ambos do Código Penal. No primeiro caso, o conteúdo do dispositivo revogado foi incorporado ao inciso II do novo art. 154-H. Já para o segundo caso, prescrição equivalente encontra-se prevista no inciso II do art. 154-J.

Ao justificar a proposição, seu autor cita casos emblemáticos como os ataques aos sistemas do Superior Tribunal de Justiça e do Tribunal Superior Eleitoral para ressaltar a necessidade de atualização do ordenamento jurídico brasileiro no que diz respeito aos crimes cibernéticos. Acrescenta ainda que o aperfeiçoamento da legislação em relação a esse tema também decorre

de exigência da Convenção de Budapeste sobre o Crime Cibernético, atualmente em análise no Congresso Nacional.

O projeto foi inicialmente distribuído para a então Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática e, na sequência, para a Comissão de Constituição, Justiça e Cidadania (CCJ) para decisão terminativa. Com o advento da Resolução nº 14, de 7 de junho de 2023, novo despacho determinou a apreciação da matéria por esta CCDD e pela CCJ, cabendo a esta última a decisão terminativa.

Não foram apresentadas emendas ao projeto.

II – ANÁLISE

Nos termos do art. 104-G do Regimento Interno do Senado Federal, compete a este colegiado manifestar-se sobre temas afetos a direito digital, internet e outros temas correlatos.

O projeto em análise tem o objetivo de atualizar e aperfeiçoar a legislação brasileira sobre crimes cibernéticos. Nesse esforço, desdobra as condutas hoje descritas no art. 154-A do Código Penal, que trata do crime de *invasão de dispositivo informático*, dando-lhes maior detalhamento e especificidade, e introduz novos tipos penais. Além disso, promove escalonamento de penas, com aumento daquelas aplicáveis a condutas mais graves.

Trata-se, portanto, de contribuição positiva para o aprimoramento da legislação referente ao tema, especialmente diante de um quadro em que as ameaças cibernéticas apresentam incremento não apenas quantitativo, mas também qualitativo.

De acordo com levantamento divulgado pela empresa FortiGuard Labs, houve 103,16 bilhões de tentativas de ataques cibernéticos no Brasil em 2022. Esse número representa um aumento de 16% em relação ao ano anterior, em que foram registradas 88,5 bilhões de casos. Na América Latina, foram identificadas ao todo 360 bilhões de tentativas em 2022. O Brasil ficou em segundo lugar entre os países da região em número de casos, atrás apenas do México, que registrou 187 bilhões de tentativas de ataques cibernéticos.

Ainda de acordo com o mesmo relatório, 73,9% dos crimes cibernéticos em todo o mundo são motivados pela busca de ganhos financeiros. O segundo motivo com maior representatividade é a espionagem, presente em 13% dos casos. Entre os crimes com motivação financeira, destaca-se o emprego do *ransomware*, modalidade em que o invasor usa criptografia para impedir que a vítima tenha acesso a seus dados ou sistemas e exige um "resgate" para que o acesso seja restabelecido.

O relatório destaca ainda o uso repetido de códigos ou infraestruturas já empregados em ataques anteriores, continuamente aperfeiçoados, como forma de otimizar os recursos despendidos em sua aquisição ou desenvolvimento. No entanto, não se pode descartar a possibilidade de utilização de novas tecnologias para a criação de subterfúgios ainda mais sofisticados. Com efeito, a disponibilização de ferramentas de inteligência artificial pode não apenas facilitar o desenvolvimento de mecanismos mais elaborados para invasão de sistemas, como também permitir que um número maior de criminosos potenciais possa ter acesso a essas possibilidades.

Diante desse contexto, é necessário dotar os órgãos públicos responsáveis pela investigação e pela persecução penal dos instrumentos jurídicos adequados para lidar com esse tipo de crime. Nesse sentido, a proposição em exame promove pertinente e necessária atualização da legislação penal no sentido de dar uma descrição mais precisa às condutas e de prever penas mais adequadas para enfrentar o vertiginoso crescimento das estatísticas relativas aos crimes cibernéticos.

Por essa razão, propõe-se que esta Comissão se manifeste de forma favorável à aprovação do projeto.

III – VOTO

Diante do exposto, o voto é pela **aprovação** do Projeto de Lei nº 613, de 2021.

Sala da Comissão,

, Presidente

, Relator