

Opinião: Crimes cibernéticos e a Convenção de Budapeste

07/03/2022

A escalada dos crimes cibernéticos, expressa pelos vazamentos de dados de milhões usuários, sequestros de dados e por uma miríade de golpes por meio da internet e redes sociais, catalisa a revisitação da legislação penal sobre o tema, especialmente após a recente formalização da adesão do Brasil à Convenção de Budapeste, instrumento internacional que busca promover a cooperação entre os países signatários no combate aos crimes praticados por meio da internet e com o uso de dispositivos eletrônicos.



São duas as modalidades práticas de crimes

cibernéticos, as próprias e impróprias. Na primeira, há violação dos dados, informações ou sistemas propriamente ditos, abrangendo desde a alteração e a destruição de dados, até o acesso não autorizado desses e de sistemas. A segunda ocorre quando a informática é instrumento para a execução do crime, como nas fraudes eletrônicas.

Dentre as condutas cuja tipificação é recomendada pela Convenção de Budapeste, as que mais impactam a atividade empresarial são: 1) violações à confidencialidade, integridade e disponibilidade de dados e sistemas informáticos, incluindo acesso, interceptações, interferência e utilização, sempre de forma ilícita; 2) falsidade informática e o estelionato eletrônico; e 3) violações de direitos de autorais e conexos.

No Brasil, a legislação é fragmentária, não existindo um diploma único que tipifique os delitos cometidos no ciberespaço ou por meio dele.

O artigo 154-A do Código Penal, incluído pela Lei nº 12.737/2012 (Lei Carolina Dieckmann) e recentemente alterado pela Lei nº 14.155/2021, tipifica a invasão de dispositivo informático, consistente na obtenção de vantagem ilícita pelo acesso a dispositivo informático de uso alheio, quando realizado sem autorização de seu titular, com o fim de obter, adulterar ou destruir dados ou informações ou de instalar vulnerabilidades. Com a Lei nº 14.155/2021, houve uma considerável exacerbação da pena, reclusão de um a quatro anos e multa, tornando-o passível

de interceptação telefônica e captação ambiental, conforme os artigos 2º, III, e 8º-A, II, da Lei nº 9.296/1996.

O §1º do artigo 154-A criminaliza quem "*produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput*", sendo que agora há a causa de aumento de pena do §2º se a invasão resultar em prejuízo econômico. Contudo, sua redação é limitada em relação a alguns outros métodos comuns de controle de acesso, como os por meio da cessão ou comercialização de senhas e nomes de acesso, não previstas no tipo penal.

No §3º há a qualificação da conduta caso da invasão decorra a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas ou o controle remoto não autorizado do dispositivo invadido. Havendo divulgação, comercialização ou transmissão dos dados ou informações obtidos a terceiro, essa pena será aumentada de um a dois terços, nos termos do §4º.

Todavia, a Convenção de Budapeste é ainda mais abrangente. Exemplificando, "sistema informático" nela adotado, é um conceito mais amplo que "dispositivo informático" por aqui adotado, coibindo não apenas a invasão a um dispositivo informático, mas sistemas que realizem tratamento de dados. Ainda, a legislação brasileira não tipifica a interceptação ilícita de dados e a interferência em sistemas informáticos que, por ocasião da adesão à Convenção de Budapeste, devem ser considerados.

A Lei nº 14.155/2021 também incluiu o §2º-A e B, no artigo 171 do Código Penal, prevendo uma reprimenda bem mais severa para as fraudes eletrônicas cometidas por meio de redes sociais, contatos telefônicos e envio de correio eletrônico fraudulento e outros meios análogos, o dito estelionato eletrônico. Ela também incluiu o §4º-B e C no artigo 155 do Código Penal, prevendo a figura do furto mediante fraude cometido por meio de dispositivo eletrônico ou informático, com pena mínima maior que a da modalidade qualificada tradicional.

Muito embora o legislador nacional tenha tipificado o estelionato eletrônico, a Convenção ainda prevê a incorporação do delito de "falsidade informática", que consiste na conduta dolosa de introduzir, alterar, eliminar ou suprimir dados, com a intenção de que sejam considerados ou utilizados para fins legais como se autênticos fossem.

Em relação às violações dos direitos de autorais e conexos, embora a legislação brasileira seja compatível com os tratados internacionais sobre o tema, ainda não prevê qualificadoras ou causas de aumento para a prática desses delitos no ciberespaço.

Mesmo diante das recentes alterações legislativas, a adesão à Convenção de Budapeste implica a revisão de dispositivos penais à luz do já inveterado texto convencional, desde que compatíveis com o direito nacional, sem prejuízo da rediscussão face ao recorrente avanço tecnológico e das melhores práticas.

Considerando o seu caráter transfronteiriço, testemunha-se uma uniformização para a prevenção e o enfrentamento da criminalidade no ciberespaço. Embora com atraso, ao Brasil é oportunizada a possibilidade de otimização de sua legislação sobre crimes cibernéticos, tendo como norte padrões internacionais.



Fonte: <https://conjur.jumps.com.br/2022-mar-07/opinioao-crimes-ciberneticos-convencao-budapeste/>