Crimes cibernéticos e a proposta de adesão do Brasil à Convenção de Budapeste

CMG (T) Fabio Bittencourt Quirino *1
Angela Dias Mendes *2

Na sociedade atual, as inovações digitais não encontram barreiras para concretizar o desenvolvimento tecnológico. As inúmeras ferramentas domesticadas pelo mercado ampliam-se continuamente e, com elas, as habilidades pessoais para o uso desses recursos, fatos significativos para alimentar as preferências e desejos de navegar nesse mundo quase mágico. Além disso, governos e organizações civis expandem os investimentos em tecnologias inovadoras com vistas à maior eficiência na prestação de serviços e no aprimoramento da cadeia produtiva.

A transformação digital favoreceu o desenvolvimento econômico, permitiu novas práticas educacionais e comerciais, criou profissões, trouxe avanços nas áreas da Saúde e da Segurança Pública, entre outras. Com a crise sanitária mundial da COVID-19, essa transformação recebeu um forte impulso, o que aumentou significativamente o índice de crimes cibernéticos. Além disso, a cada dia surgem novas modalidades de crimes ou são aperfeiçoados seus métodos de ataques. Desta forma, Estados, organizações privadas e a sociedade em geral precisam adotar medidas mais apropriadas para conter a incidência desses delitos, identificar e punir os autores e minimizar os danos deles decorrentes.

Para o bem ou para o mal, as novas tecnologias existem! Sendo assim, é vital fomentar reflexões acerca dos desafios desse que, atualmente, é um dos temas mais relevantes da sociedade mundial. Portanto, no presente

texto abordaremos brevemente a proposta de adesão do Brasil à Convenção de Budapeste e os crimes cibernéticos. O objetivo principal, nas breves linhas que nos cabem, não é fazer um estudo aprofundado, mas informar e suscitar reflexões necessárias e úteis para os assuntos de Estado, como é o caso da referida proposta.

O termo convenção[1] é atribuído ao instrumento internacional utilizado por Estados, quando se reúnem para dispor sobre soluções conjuntas de problemas cuja relevância ultrapassa as fronteiras nacionais, assim como os crimes de natureza cibernética. A convenção para ser aprovada deve harmonizar-se com a ordem constitucional de cada Estado, pressuposto da soberania interna dos países. Por isso, há uma longa discussão sobre os benefícios e riscos da adesão, a fim de lapidar a opção desejada pelo Estado-parte.

Recentemente, no Brasil, foi indicado o Projeto de Decreto Legislativo (PDL) nº 255/21[2] para aprovação da Convenção de Budapeste. O governo brasileiro recebeu o convite de adesão do Conselho Europeu em 2019, através do Ministério das Relações Exteriores, e tem o prazo de três anos para apresentar a resposta. A Convenção foi discutida no âmbito da Comissão de Relações Exteriores e Defesa Nacional da Câmara, convertendo-se em seguida, pela Câmara dos Deputados, no PDL nº 255/21. Após transitar regularmente nesse Poder, se aprovada, ela seguirá para o chefe do Poder Executivo a quem compete editar o Decreto, conforme art. 84, V, da Constituição da República.[3]

Entre os objetivos da Convenção ressaltamos três: facilitar a cooperação internacional, com vistas ao combate dos delitos praticados por cibercriminosos; alcançar uma política criminal comum que proteja a sociedade dos crimes cibernéticos e permitir celeridade na troca de dados informáticos entre as partes.

Vale acrescentar que o instrumento prevê a essencialidade do direito à proteção de dados pessoais e à privacidade. Esta é uma exigência da comunidade internacional que, diga-se, o Brasil vem acompanhando através da adoção de medidas legislativas e administrativas para efetivar internamente o sistema de proteção no País. A promulgação da Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e a criação da Autoridade Nacional de Proteção de Dados (MP nº 869/2018) indicam o nível de maturidade jurídica nesse cenário.

A pavimentação de políticas estratégicas que reestruturem uma nova governança na área de segurança cibernética requer tempo. Podemos destacar o marco temporal em 2012 com a tipificação dos delitos informáticos pela Lei n º 12.737. Mais recentemente o Decreto nº 10.222/2020 instituiu a Estratégia Nacional de Segurança Cibernética e a Lei nº 4.554/20 ampliou as penas para o crime de furto e estelionato com o uso de dispositivos eletrônicos. Como vemos, o País caminha no sentido de consolidar uma política robusta de segurança nesse novo ambiente.

1. As palavras Convenção e Tratado podem ser consideradas sinônimas "ambas significando um acordo bilateral ou multilateral de vontades manifestadas por Estados Soberanos ou organismos internacionais, regularmente representados por órgãos competentes, destinando-se a produzir efeitos jurídicos" (Ricardo Alexandre, 2009, p. 199)

2. Projeto de Decreto Legislativo de Acordos, tratados ou atos internacionais – PDL. Link de acesso ao PDL 255/21: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2287513, acesso em 18 ago. 2021.

3. Disponível em Agência Câmara de Notícias. https://www.camara.leg.br/noticias/779447-projeto-aprova-adesao-do-brasil-a-convencao-europeia-sobre-crime-cibernetico/ , acesso em 18 ago. 2021.

Entretanto, quando se trata de crimes cibernéticos é vital compreender que não há barreiras físicas, temporais e legais para eles, pois características específicas de tais crimes os permitem ultrapassar os limites jurisdicionais das nações. Por esta razão, hoje, exige-se que os instrumentos legais favoreçam uma rede unívoca, sólida e eficaz para combatê-los. Nesse campo, a segurança jurídica será alcançada à medida que o lastro normativo acompanhar o lastro das ações de contenção.

Os crimes cibernéticos têm natureza complexa, o que exige uma análise mais detida de seus elementos, formas e busca pela autoria. As inúmeras técnicas de despistamento, cada dia mais sofisticadas, e as falhas na identificação efetiva do usuário são exemplos dos desafios para detecção de sua origem, pois ela poderia advir de qualquer computador conectado à internet, seja de forma direta, via *proxy*, ou na pior situação, por meio de uma rede wi-fi aberta ou em uma *lan house*. Dois países podem estar a milhares de quilômetros de distância, mas uma comunicação entre computadores, neles localizados, é realizada em alguns segundos, tempo suficiente para que evidências eletrônicas sejam eliminadas com facilidade. Por isso, o recurso da cooperação internacional visando recuperar dados apagados pode ser crucial nesses casos. Daí a importância desse instrumento legal que oportuniza a troca de experiências e facilita o intercâmbio de informações. Um típico exemplo são os crimes relacionados com pornografia infantil, quando os arquivos são armazenados em um servidor em um país diferente daquele onde se pratica o delito. Caso não sejam signatários da mesma convenção, haverá maior dificuldade na obtenção de provas e na identificação dos culpados.

Para termos uma ideia ainda mais clara da mag-

nitude do tema, recentemente o Fórum Econômico Mundial anunciou a criação do Centro Global de Segurança Cibernética[4], cujo principal objetivo é o fortalecimento da cooperação internacional. O Centro visa estabelecer uma plataforma global onde governos, empresas, agências reguladoras e especialistas possam contribuir para vencer os desafios da segurança cibernética. Entre os *stakeholders*[5] comprometidos estão a *International Telecommunications Union (ITU),* a INTERPOL, a Organização dos Estados Americanos (OEA), a Universidade de Oxford e o Centro Nacional de Segurança Cibernética do Reino Unido.

O Brasil conta hoje com uma Estratégia Nacional de Defesa Cibernética (E-Ciber), que prevê a possibilidade de ampliação da cooperação internacional nessa área, além do estímulo à participação do País em iniciativas de estruturação normativa externa. Este é um assunto de alta relevância para a Defesa Nacional tendo em vista o número expressivo de crimes de espionagem e ações de células terroristas que se comunicam no ciberespaço, disseminando o medo e a instabilidade econômica e social. Em Audiência Pública na Câmara dos Deputados, o Comando de Defesa Cibernética do Exército se mostrou favorável à proposta e preocupado com os "prejuízos causados pelos crimes cibernéticos no mundo, onde 86% dos ataques cibernéticos têm motivação financeira e 10%, atos de espionagem...". O Brasil possui cerca de 70 milhões de vítimas, segundo fontes oficiais.[6]

Evidentemente, se o Brasil aderir à Convenção de Budapeste, ainda precisará definir e realizar ações políticas, jurídicas e administrativas internamente para ajustar-se às exigências prescritas na Convenção, além de outras medidas legislativas necessárias para regulamentar e efetivar a cooperação.

No ambiente cibernético há perceptíveis conexões de ações delituosas que exigem uma força contrária, também conectada, para impedir a disseminação das ações criminosas e romper a cadeia complexa de delitos. Assim será possível somar esforços comuns e trocar experiências, conferindo maior uniformidade e celeridade nas estratégias internacionais conforme preconiza a Convenção de Budapeste. ■

1 Especialista em Cibersegurança, membro do CTEMI do Clube Naval

2 Doutora em Direito, membro do CTEMI do Clube Naval

4. Disponível em: https://www.weforum.org/ , acesso em 01 set. 2021.

5. Partes envolvidas

6. Exposição do Chefe do Comando de Defesa Cibernética do Exército, General Heber Garcia Portella. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-permanentes/credn/noticias/em-audiencia-publica-expositores-sao-favoraveis-a-adesao-do-brasil-a-convencao-de-budapeste-sobre-crimes-ciberneticos , acesso em 03 set. 2021.