MINISTÉRIO PÚBLICO FEDERAL
CÂMARA CRIMINAL DA PGR

NOTA TÉCNICA DO GRUPO DE APOIO SOBRE CRIMINALIDADE CIBERNÉTICA SOBRE A CONVENÇÃO DO CIBERCRIME (CONVENÇÃO DE BUDAPESTE)

O Ministério Público Federal se fez representar na 11ª Conferência Octopus sobre Crime Cibernético, de 11 a 13 de julho de 2018, em Estrasburgo, França, dado o crescente aumento na criminalidade cometida pelos meios digitais, internet e outros sistemas informáticos, bem como a atual necessidade de obtenção de provas digitais para a elucidação de praticamente todos os delitos.

Há vários anos o Ministério Público Federal vem se deparando com os desafios da criminalidade cibernética, tanto que já em 2003 foi criado um grupo de atuação especializada em São Paulo, com o respectivo Núcleo Técnico, com o objetivo de aprimorar o conhecimento especializado necessário para investigar e processar os delitos cometidos via web e outros sistemas informáticos, iniciativa seguida pela Procuradoria da República no Rio de Janeiro e pela criação do Grupo de Trabalho Nacional sobre criminalidade cibernética, transformado em Grupo de Apoio e que efetivamente vem prestando auxílio tanto às unidades do MPF nos estados quanto aos Ministérios Públicos Estaduais do País.

Nos quinze anos de atividade dos grupos, verificou-se um aumento exponencial na quantidade e sofisticação no cometimento dos delitos cibernéticos, com a migração de delitos comuns como fraudes, estelionatos, ameaças e extorsões (ramsonware) para o meio digital que não têm encontrado nem capacitação para o seu combate, nem ferramentas jurídicas aptas a permitir a persecução penal efetiva, aumentando a insegurança da vida diária e dificultando a prevenção.

Da mesma forma, a necessidade de obtenção de provas digitais para a comprovação da autoria e materialidade dos mais variados delitos, como homicídios, corrupção, crimes financeiros etc, cuja elucidação pode depender de e-mails, interceptações telemáticas, arquivos armazenados na "nuvem", tornou-se uma constante para os operadores do direito.

A aprovação do Marco Civil da Internet em 2014 criou um importante arcabouço legislativo para a persecução penal ao estabelecer regras de preservação de dados e sua utilização para fins cíveis e criminais, assim como as regras para obtenção dessas informações digitais, sejam elas dados cadastrais, informações de conexão à internet, de acesso a aplicações de internet ou conteúdo de comunicações. As disposições seguem a tradição do direito brasileiro, nos termos da Lei de Introdução às Normas Brasileiras, e asseguram a soberania nacional ao estabelecer, grosso modo, que as operações de coleta e tratamento de dados a partir do território nacional por empresas que prestem seus serviços aqui, possuindo sede, filial ou representante do mesmo grupo econômico, ou que, pelo menos, ofertem o serviço ao público brasileiro, mesmo que não tenham representante em território nacional, estão sujeitas à lei nacional e devem se submeter à jurisdição brasileira.

No entanto, os meios digitais não respeitam fronteiras, havendo inúmeros serviços prestados na web ou via web que, apesar de não oferecidos ao público brasileiro, estão disponíveis e são alcançáveis por quem deles queira se utilizar, e quando utilizados para a prática de delitos, impõem desafios aos agentes de segurança e investigação.

Nesses casos, existe a necessidade de obter cooperação dos países onde a prova pode ser obtida. Essa cooperação internacional precisa ser ágil e eficiente, notadamente tratando-se de provas digitais, extremamente voláteis, a fim de não se perderem e também com o fito de interromper as condutas criminosas, as quais, praticadas pelos meios digitais passam a ter um alcance com consequências antes inimagináveis. Como exemplo recente, tem-se o ataque do vírus Wannacry, ocorrido em maio de 2017, que afetou mais de 200.000 computadores em 150 países, inclusive no Brasil. Nesse ataque cibernético, que se acredita ter-se originado na Coreia do Norte, os computadores atingidos tinham seus dados criptografados e eram alvo de extorsão, já que se prometia que tais dados somente seriam liberados mediante o pagamento de resgate em criptomoedas, no caso, o Bitcoin. Estima-se que o prejuízo resultante do ataque variou de 100mil a bilhões de dólares.

Atualmente, qualquer ataque cibernético que tenha por objetivo interferir em sistemas vitais da infraestrutura nacional pode em instantes, por exemplo, deixar o país sem energia ou comunicação, afetando diretamente a economia e segurança nacionais.

Nesse cenário, a Convenção do Cibercrime, que data de 2001 e já conta com mais de 60 países aderentes, apresenta-se como um instrumento eficaz de cooperação internacional para a obtenção de provas digitais, além de inserir o Brasil no mapa do combate ao crime cibernético.

Note-se que, apesar de datar de 2001 e ser um tratado com origem no Conselho da Europa, isto é, aparentemente regional, a Convenção é um instrumento vivo, com constantes reuniões de trabalho para treinamento e aprimoramentos em sua interpretação.

Ao par de trazer um arcabouço básico que estatui requisitos mínimos e indispensáveis a serem cumpridos pelos países para possibilitar a cooperação, já que a harmonização da legislação, consequência da adesão à Convenção do Cibercrime, traz tranquilidade aos países-membros no que toca ao respeito por direitos e salvaguardas mínimos e padronizados, a Convenção possui comissões, formadas por todos os países aderentes, que discutem as inovações e interpretações que podem ser dadas aos artigos da Convenção a fim de acompanhar a evolução tecnológica e as necessidades jurídicas atuais.

Esses grupos de discussão, derivados do T-CY ou Comitê da Convenção do Cibercrime, permitem que todos os países membros da Convenção tratem da interpretação das normas da Convenção e do seu alcance. Como exemplo, citem-se o Comitê para o acesso transfronteiriço a provas, o Comitê para o acesso da prova digital na nuvem, o Comitê para o artigo 13 que trata das sanções, dentre outros.

Demonstração clara da constante evolução da convenção é a discussão atual sobre um Protocolo Adicional com o objetivo de tornar mais rápida a obtenção das provas digitais mediante a simplificação dos procedimentos de cooperação internacional via MLAs (*multilateral assistance agreements*). Logo, um país aderente à Convenção neste estágio, está apto a participar das discussões das comissões e influir no resultado dos novos acordos.

Elencamos abaixo os principais ganhos que identificamos para a investigação criminal e a segurança do nosso País com a adesão à Convenção do Cibercrime, analisando também a inexistência de óbices à adesão:

1. **Melhoria do arcabouço legal**. Assinar a Convenção cria a obrigação para o Congresso em aprovar os tipos penais específicos, preenchendo importantes lacunas na legislação brasileira que têm prejudicado a efetiva persecução de crimes cibernéticos;

2. **Harmonização.** A criação de novos tipos penais também harmonizará a legislação brasileira com a legislação de outros países, o que facilitará a cooperação internacional em investigações, a obtenção de provas e a extradição de envolvidos;

3. **A Convenção já existe**. Apesar de a Convenção de Budapeste ter sido uma iniciativa do Conselho da Europa, atualmente ela abarca mais de 60 países ao redor do mundo, incluindo diversos países da América Latina, como Argentina (ratificou, em 05/06/2018), Chile (ratificou, em 20/04/2017), Costa Rica (ratificou, em 22/09/2017), República Dominicana (ratificou, em 07/02/2013), Panamá (ratificou, em 05/03/2014), Paraguai (ratificou, em 30/07/1018), e Colômbia (aprovou o projeto de lei para aderir à Convenção do Cibercrime), e são países observadores da Convenção México e Peru, de forma que a adesão do Brasil também é importante para facilitar o combate ao crime na nossa região;

4. **Convenção da ONU**. A eventual adesão à Convenção do Cibercrime não exclui a continuidade das tratativas para a elaboração de uma Convenção no âmbito da ONU; inclusive países integrantes do BRICS, como Rússia e África do Sul, são países observadores;

5. **Provas Digitais**. A Convenção do Cibercrime é útil não somente para a persecução de crimes cibernéticos, mas principalmente para a obtenção das provas digitais que estão presentes em quase todos os delitos, de fraudes financeiras a tráfico internacional de drogas, obtenção esta que depende de cooperação internacional quando não atendidos os requisitos do Marco Civil da Internet;

6. **Ampliação da rede 24/7**. No âmbito da Organização dos Estados Americanos-OEA existe a rede 24/7 dos pontos de contato (vinte e quatro horas, sete dias por semana). A Convenção do Cibercrime abarca pontos de contato entre todos os signatários, havendo a possibilidade de indicar tanto um órgão para o processamento dos pedidos de cooperação quanto indicar um ponto de contato que atenda diretamente a autoridade judicial ou o ministério público para esclarecer dúvidas ou mesmo acelerar a obtenção da prova eletrônica nos casos emergenciais;

7. **Ampliação das hipóteses de cooperação**. A Convenção do Cibercrime possibilita a cooperação com todos os países signatários, mesmo com aqueles com os quais o Brasil não possui acordo bilateral de cooperação em matéria penal, o que incrementa e acelera a obtenção de provas que dependem da cooperação desses países;

8. **Capacitação e aprimoramento.** O país membro da Convenção tem acesso aos programas de capacitação e treinamento para investigação e processamento de Crimes Cibernéticos, bem como para obtenção de Provas Digitais mediante a cooperação internacional. Os inúmeros projetos já em andamento são implementados através do escritório C-Proc, do Conselho da Europa, com orçamento específico para as diversas regiões do planeta, inclusive América Latina, o que permitiria capacitar as polícias, os Ministérios Públicos e os Juízes no Brasil todo,

contando com alcance e apoio inéditos em nosso País. É preciso ressaltar as dificuldades enfrentadas principalmente pelos Ministérios Públicos Estaduais e Polícias Civis que diariamente confrontam o crime organizado, dentro e fora das unidades prisionais, e que necessitam urgentemente de apoio para esse enfrentamento, seja em conhecimentos tecnológicos e técnicas de investigação, seja em instrumentos jurídicos que precisam ser aperfeiçoados. Note-se ainda a noticiada expansão do crime organizado, notadamente no tráfico de drogas, o Primeiro Comando da Capital, que alcança diversos países vizinhos do Brasil com organização e sofisticação tecnológicas invejáveis aos agentes do Law Enforcement, sendo as provas digitais e a tecnologia a ser compartilhada, essenciais na persecução desses delitos;

9. **Acesso direto a provas eletrônicas em harmonia com a legislação brasileira.** A Convenção do Cibercrime possui previsão de acesso transfronteiriço a provas no seu Artigo 32, o que por vezes gera desconfiança em relação a ele.

Entretanto, é preciso dizer que o Marco Civil da Internet, após ampla discussão com todos os setores da sociedade, trouxe arcabouço legislativo mais ousado, deixando claro em seu Artigo 11 que a jurisdição brasileira é aplicável aos dados coletados em território nacional não importando o local do planeta onde eles estejam armazenados, desde que o serviço atrelado a esses dados esteja sendo ofertado ao público brasileiro. Assim, o acesso a dados armazenados em serviços de nuvem, por exemplo, é quotidianamente feito com ordem judicial fundamentada embasada no Artigo 240 do Código de Processo Penal e no Artigo 11 do MCI.

10. **A Convenção reconhece a soberania local no acesso direto a provas digitais.** Como exposto, o Artigo 11 do Marco Civil explicita que os dados coletados em território nacional por empresas com filiais em território nacional ou pertencentes a grupo econômico com uma sede ou filial em território nacional devem ser fornecidos às autoridades judiciais brasileiras mesmo que tais dados estejam sendo mantidos armazenados fora do País. Tal dispositivo, que apenas reflete questões básicas de soberania (dados coletados no Brasil devem ser acessíveis a autoridades brasileiras diretamente desde que respeitados os ditames do devido processo legal previstos na legislação pátria) tem sido alvo constante de investidas de corporações estrangeiras que desejam ver aplicada no Brasil legislação estrangeira que em nada se assemelha ao quanto defendido pela sociedade brasileira (vide, a esse respeito, a ADC 51, atualmente em trâmite no Supremo Tribunal Federal).

A Convenção, em seu Artigo 18, traz dispositivo semelhante ao citado Artigo 11.

> **Artigo 18º - *Injunção***
>
> 1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes para ordenar:
>
> a) A uma pessoa que se encontre no seu território que comunique os dados informáticos específicos, na sua posse ou sob o seu controlo e armazenados num sistema informático ou num outro suporte de armazenamento de dados informáticos; e
>
> b) A um fornecedor de serviços que preste serviços no território da Parte, que comunique os dados na sua posse ou sob o seu controlo, relativos aos assinantes e respeitantes a esses serviços

Assim, a adesão do Brasil à Convenção dará à legislação local respaldo do direito internacional público, permitindo que seja preservada a soberania nacional quanto aos dados aqui colhidos, e tornando mais

difíceis as recusas de corporações estrangeiras que aqui atuam e aqui possuem filial em cumprir a legislação pátria.

Ao aderir à Convenção de Cibercrime, nossa legislação ganha o reforço de uma Convenção Internacional.

11. **Propriedade intelectual e Direito do Autor.** O Artigo 10 da Convenção do Cibercrime estabelece que devem ser previstas como infrações penais do direito interno do país aderente a violação do direito do autor e dos direitos conexos, para a proteção dos direitos estabelecidos na Convenção Universal sobre o Direito de Autor, de Paris; na Convenção de Berna para a Proteção das Obras Literárias e Artísticas; do Acordo sobre os Aspectos dos Direitos de Propriedade Intelectual relacionados com o Comércio; Convenção Internacional para a Proteção dos Artistas Intérpretes ou Executantes, dos Produtores de Fonogramas e dos Organismos de Radiodifusão (Convenção de Roma); do Tratado da OMPI sobre o Direito do Autor e Tratado da OMPI sobre Interpretações, Execuções e Fonogramas. De todos esses documentos citados, o Brasil somente não é signatário dos dois últimos tratados da OMPI, que datam de 1996 e referem-se a esses direitos no âmbito da tecnologia, protegendo, por exemplo, programas de computador como obras literárias, nos termos da Convenção de Berna, e visando à proteção dos direitos do autor e conexos no âmbito da internet.

Embora o Brasil não tenha ratificado esses dois últimos tratados, a legislação penal atual possui dispositivo que atende ao quanto determinado pela Convenção de Budapeste e é aplicável à proteção dos direitos do autor e conexos na sua difusão pela internet. O Artigo 184 do Código Penal criminaliza a violação do direito do autor e conexos por qualquer meio, o que inclui a internet:

> **Art. 184. Violar direitos de autor e os que lhe são conexos**
> Pena - detenção, de 3 (três) meses a 1 (um) ano, ou multa.
> § 1º Se a violação consistir em reprodução total ou parcial, com intuito de lucro direto ou indireto, por qualquer meio ou processo, de obra intelectual, interpretação, execução ou fonograma, sem autorização expressa do autor, do artista intérprete ou executante, do produtor, conforme o caso, ou de quem os represente

Logo, não há qualquer impedimento à adesão à Convenção do Cibercrime por falta de adesão aos Tratados da OMPI. Nada impedindo também que nossa legislação seja alterada para que fique mais específica, sem que haja a necessidade de se aderir aos Tratados mencionados, caso não seja essa a intenção do País.

12. **Proteção de dados.** Com a promulgação da Lei de Proteção de Dados, espelhada no GDPR-General Data Protection da União Europeia, a adesão à Convenção do Cibercrime completará a introdução do Brasil no cenário mundial da era digital, garantindo que as trocas financeiras e comerciais estarão dentro do padrão internacional também do ponto de vista da segurança, permitindo um melhor combate aos delitos.

O Ministério Público Federal espera ter debelado qualquer dúvida que eventualmente existisse sobre os benefícios da adesão do Brasil à Convenção do Cibercrime e se coloca à disposição para qualquer informação complementar.

NEIDE CARDOSO DE OLIVEIRA **FERNANDA TEIXEIRA DOMINGOS**

Coordenadoras do Grupo de Apoio sobre Criminalidade Cibernética da 2ª CCR

MINISTÉRIO PÚBLICO FEDERAL

Assinatura/Certificação do documento **PR-SP-00095455/2018 NOTA TÉCNICA**

Signatário(a): **FERNANDA TEIXEIRA SOUZA DOMINGOS**
Data e Hora: **28/08/2018 12:39:32**
Assinado com login e senha

Signatário(a): **NEIDE MARA CAVALCANTI CARDOSO DE OLIVEIRA**
Data e Hora: **28/08/2018 12:41:15**
Assinado com login e senha