Os Crimes Cibernéticos

Aula 3 – Marco Civil da *Internet* – provas digitais e cooperação jurídica internacional

Em âmbito nacional, até recentemente não havia qualquer legislação específica no tocante à regulação dos crimes cibernéticos. Sendo o Código Penal Brasileiro de 1940, para que a legislação se tornasse compatível com as novas tecnologias, alguns tipos penais tipicamente cibernéticos foram sendo criados e incorporados ao Código Penal ou às leis esparsas ou modificados para que passassem a prever a forma virtual de cometimento.

O Código de Processo Penal sofreu algumas modificações em relação às novas tecnologias pela incorporação da videoconferência, por exemplo, para os atos processuais nos termos da Lei 11.900/2009.

A Lei 11.419/2006 veio dispor sobre a informatização do processo judicial dando lastro aos documentos e evidências digitais, que na verdade já eram aceitos como documentos com base na legislação já existente (Código Civil art. 225 e Código de Processo Civil art. 332/ art. 369 do NCPC)

As alterações da Lei nº 9.613/1998 (Lei da lavagem de dinheiro) introduzidas pela Lei nº 12.683/2012 trouxeram no artigo 17-B a possibilidade de que a autoridade policial e o Ministério Público Federal tivessem acesso aos dados cadastrais do investigado independentemente de autorização judicial mantidos pela Justiça Eleitoral, pelas empresas telefônicas, pelas instituições financeiras, pelos provedores de *internet* e pelas administradoras de cartão de crédito, fazendo menção, portanto, aos dados mantidos pelos provedores de *internet*.

Porém, a grande inovação veio com a promulgação do Marco Civil da *Internet*, Lei nº. 12.965/2014, que estabeleceu princípios, garantias, direitos e deveres para o uso da *Internet* no Brasil e em seu bojo regulou as questões processuais criminais referentes à preservação das provas digitais pelos provedores, disciplinando o acesso a elas.

Assim, o artigo 11 do Marco Civil[1] estabelece que será aplicada a legislação brasileira sempre que alguma das condutas referentes ao manuseio de dados ou comunicações por provedores de conexão e de aplicações de *internet* ocorrer em território nacional. O § 2º desse artigo esclarece que o *caput* se aplica mesmo que as atividades descritas sejam realizadas por pessoa jurídica sediada no exterior quando o serviço for ofertado ao público brasileiro ou ao menos uma integrante do mesmo grupo econômico possuir estabelecimento no Brasil.

O artigo 13 do Marco Civil trata da guarda e retenção ~~preservação~~ dos registros de conexão à *internet*, que devem ser mantidos em sigilo e em ambiente controlado e de segurança pelo prazo de um ano, podendo o Ministério Público ou as autoridades policial e administrativa requererem cautelarmente que a guarda e preservação se dê por período superior a um ano, cabendo à autoridade requerente providenciar a autorização judicial para acesso aos dados dentro de 60 dias.

[1]Lei 12.695/2014. art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.
(…) § 2º O disposto no caput aplica-se mesmo que as atividades seja realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.

O artigo 15 do Marco Civil estabelece o dever de guarda e retenção ~~preservação~~ dos registros de acesso a aplicações de *internet*, sob sigilo e em ambiente controlado e de segurança pelo prazo de seis meses, também sendo facultado ao Ministério Público e às autoridades policial e administrativa requerer cautelarmente a preservação dos registros de acesso a aplicações por prazo superior, desde que providenciem o ingresso do pedido de autorização judicial para o acesso aos dados no mesmo prazo de 60 dias.

A importância do Marco Civil na questão das provas digitais está em ser a primeira lei a prever prazos de retenção e possibilidade de preservação de registros de conexão e de aplicação à *internet*, que são, ao mesmo tempo, meios investigativos para se buscar a identificação da autoria dos delitos virtuais e também elementos probatórios para embasar a conclusão da individualização pessoal da conduta.

Conceitos

Assim, importa ressaltar que o Marco Civil da *Internet* traz em seu artigo 5º, conceitos básicos como a definição de **endereço de protocolo de internet (endereço IP)**: código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais (inciso III); definição do que é **registro de conexão**: conjunto de informações referentes à data e hora de início e término de uma conexão à *internet*, mediante a atribuição ou autenticação de um endereço IP (inciso VI); definição do que é **registro de acesso a aplicações de *internet*:** o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de *internet* a partir de um determinado endereço IP (inciso VIII).

O artigo 10, §1º estabelece que as informações dos provedores de conexão e de aplicação somente poderão ser obtidas por ordem judicial. Mas para autoridades, o acesso a dados cadastrais dispensa a ordem judicial.

Neste ponto é de se destacar que o regulamento do Marco Civil da *Internet*, Decreto nº 8.771, de 11 de maio de 2016, define **dados cadastrais** como filiação, endereço e qualificação pessoal (nome, prenome, estado civil e profissão). Embora as informações financeiras não constem desse rol, é pacífica a jurisprudência no sentido de que os dados de pagamento de um serviço, seja ele por meio de conta bancária ou cartão de crédito, ou outro meio, não são protegidos pelo sigilo, de forma que os provedores tanto de conexão, quanto de aplicação devem informá-los às autoridades requerentes (polícia, Ministério Público e autoridade administrativa) independentemente de ordem judicial. Aliás, como já previsto no artigo 17-B da Lei nº 9.613/1998 (Lei da lavagem de dinheiro) com as alterações introduzidas pela lei nº 12.683/2012.

Note-se, ainda, que no art. 13, §2º, I e II do regulamento há a obrigação de exclusão dos dados pessoais, comunicações privadas e registros de conexão e de acesso a aplicações após atingida a finalidade de seu uso ou o prazo legal se não houver solicitação de preservação por prazo superior (um ano para provedores de conexão, seis meses para provedores de aplicação).

Prazos de Retenção e de Preservação

Quanto aos prazos estabelecidos nos artigos 13 e 15 do Marco Civil da *Internet*, deve-se atentar que foram previstos prazos de retenção para os registros de conexão pelo período de um ano (art. 13) e de retenção pelo período de seis meses, havendo a possibilidade de pedido de preservação por período superior a ser feito pela polícia, Ministério Público ou autoridade administrativa.

Atente-se também que não há obrigação de guarda/retenção de conteúdo, mas este pode ser objeto de pedido de preservação enquanto se obtém a ordem judicial para o seu fornecimento. Ressaltando-se que bastará a ordem judicial para afastar o sigilo e obter o conteúdo armazenado nos termos do art.

7º, inciso III do MCI, mas para o conteúdo *online*, isto é, para interceptação de conteúdo em tempo real, a ordem judicial deve ser na forma da lei, nos termos do art. 7º, inciso II do MCI e compreende-se que é a Lei nº 9296/96, Lei das Interceptações Telefônicas e Telemáticas, devendo, portanto, obedecer aos requisitos nela previstos.

Jurisdição

Como já explicado acima, o artigo 11 do MCI deixa claro que se aplica a legislação brasileira para qualquer operação de tratamento de dados realizada em território nacional, devendo ser respeitados os direitos à privacidade, proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros quando pelo menos um dos terminais está localizado no Brasil. Ou seja, a coleta de dados se deu a partir de uma conexão feita no território nacional, não importando que a sede da pessoa jurídica esteja no exterior, desde que o serviço esteja sendo ofertado ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.

Esse dispositivo vem para assegurar que os dados do público brasileiro terão asseguradas as garantias de privacidade e segurança estipulados na lei nacional. Assim, da mesma forma para o afastamento do sigilo desses dados deve ser observada a lei brasileira, emprestando segurança quanto ao regime de proteção desses dados.

Note-se que a hipótese de oferta de serviços ao público brasileiro sem que haja sede ou filial da empresa em território nacional também determina a jurisdição brasileira, embora possa haver problemas para dar eficácia às decisões direcionadas a essas empresas.

Para se determinar se a oferta de serviços é direcionada ao público brasileiro, aplica-se o *targeting test* da doutrina americana, verificando-se se os serviços são oferecidos na língua portuguesa, se é possível adquirir produtos e serviços na moeda local, se os dados recolhidos no país são utilizados para fazer publicidade direcionada a esse mesmo público.

Sanções: art. 12 MCI pelo descumprimento dos artigos 10 e 11

As sanções estipuladas para o descumprimento dos artigos 10 e 11 do MCI, sem prejuízo das demais sanções cíveis, criminais ou administrativas cabíveis, são:

I – advertência, com indicação de prazo para adoção de medidas corretivas;
II – multa de até 10% do faturamento do grupo econômico no Brasil, observando-se a condição econômica do infrator e avaliando-se a proporcionalidade entre a gravidade da fala e a intensidade da sanção;
III – suspensão temporária das atividades que envolvam os atos previstos no artigo 11;
IV – interrupção das atividades que envolvam os atos previstos no art. 11

Logo, há o dever legal da empresa de prestar informações requisitadas por ordem judicial (brasileira), notando-se que a multa cominatória (art. 12, parágrafo único): estabelece a solidariedade da empresa estrangeira pelo pagamento da multa cominada a sua filial, sucursal ou escritório ou estabelecimento situado no país.

Atualmente, há dois entendimentos quanto à natureza da multa cominada. Enquanto há decisão no TRF da 1ª Região (MS Criminal nº0042962-14.2016.4.01.0000/AM) entendendo ser necessário um procedimento administrativo fiscal com inscrição na dívida ativa da União, onde haja contraditório

fiscal, para cobrança dessa multa. Tanto o TRF da 4ª Região (AgrMS nº5039203-70.2016.4.04.0000/SC), quanto o da 2ª Região possuem acórdãos no sentido de que deve ser determinada a penhora dos valores por meio da ferramenta BACENJUD, sob pena de ineficácia da multa que visa ao cumprimento da obrigação.

Retirada de conteúdo

A retirada de conteúdo da *internet* somente pode ocorrer por ordem judicial que analisará a natureza do conteúdo, reputando-o ilícito ou não, de forma que os provedores de aplicações de *internet* não serão responsabilizados pelo conteúdo gerado por terceiros ao qual dão suporte sem que haja ordem judicial específica determinando a remoção desse conteúdo, nos termos do art. 19 do MCI.

A própria plataforma de serviços de aplicações também pode retirar conteúdo que viole expressamente seus Termos de Serviço, desde que esses estejam em conformidade com a lei vigente.

No entanto, o Marco Civil da *Internet* trouxe em seu artigo 21, uma hipótese de responsabilização civil subsidiária do provedor de aplicações por violação da intimidade decorrente de divulgação sem autorização de conteúdo íntimo gerado por terceiros, se, após notificação do seu participante ou representante legal, não retirar o conteúdo.

Nesses casos, a remoção é obrigatória, referindo-se a cenas de nudez ou de atos sexuais de caráter privado.

Note-se que caso as imagens retratem menores de 18 anos, surgirá responsabilidade penal para o responsável legal da empresa que não as remover, mas somente após notificação oficial para tanto, nos termos do artigo 241-A §§ 1º e 2º do Estatuto da Criança e do Adolescente.

Comentado [Fabiula G1]: Pessoas, jovens, indivíduos? Verificar qual é o termo mais adequado neste caso.

Das provas digitais

Pode-se dizer, na verdade, que as inovações tecnológicas tornaram essencial a preocupação com as provas digitais, pois não somente os crimes tipicamente digitais, mas todos os delitos podem ter deixado pistas digitais e precisar dessas provas para sua elucidação.

Qualquer crime comum, como o homicídio, por exemplo, pode vir a ser solucionado com o auxílio de provas digitais. *E-mails* recebidos e enviados, pesquisas de busca sobre determinados temas na *internet*, documentos, ora armazenados em meio digital, podem vir a ser pistas e provas acerca do cometimento de delitos.

No que pertine aos crimes tipicamente digitais, que somente podem ser cometidos no meio virtual ou em sistemas ou dispositivos informáticos, a importância da prova digital, obtida por meio da perícia, é absoluta, já que esses delitos deixam rastro.

Características

As provas digitais apresentam características intrínsecas que as tornam aptas à verificação. Elas deixam marcas, ou seja, são o próprio rastro dos crimes cibernéticos, pois no mundo virtual, toda atividade deixa rastro. Pode ser verificada. Uma vez que uma informação é registrada na *internet* ou em algum dispositivo informático, essa informação pode ser recuperada dentro de um certo período, mesmo que seja apagada. Assim, a perícia forense tem condição de analisar as provas digitais para verificar sua autenticidade e integridade, podendo assim determinar seu grau de confiabilidade.

Como esclarecido em estudo específico sobre o assunto[2], as provas digitais possuem requisitos específicos de validade que precisam ser observados em qualquer transferência de informações, seja ela interna ou transnacional. Deve ser primeiramente admissível, isto é, como qualquer outra prova sua aquisição deve ser correta para que possa ser admissível. O segundo requisito, desta vez, específico à sua natureza, é que sua coleta e preservação devem ser realizadas observando-se os princípios da ciência computacional a fim de garantir sua **autenticidade** e **integridade**. Estas características podem ser verificadas na ~~pela~~ análise das provas digitais pela perícia forense que poderá determinar então o seu grau de **confiabilidade**. Dessa forma, a prova somente será convincente em juízo se bem esclarecido no laudo pericial o grau de confiabilidade dessa prova, pois na maior parte das vezes, é a prova determinante para a indicação de autoria do delito.

A perícia forense terá papel fundamental, portanto, na análise dessas provas, sendo indispensável que o perito, ou agente apto, acompanhe as ações de busca e apreensão para garantir a correta coleta das provas digitais a fim de que nenhuma informação seja perdida ou corrompida. Tal padrão no procedimento pericial para garantir a integridade dos dados é necessário para dar credibilidade também a dados obtidos de outros países, como, inclusive, indicado na Convenção de Budapeste sobre o cibercrime no seu Artigo 19.

Outro aspecto fundamental a ser observado é o tempo na obtenção dessas evidências, já que a prova digital é também extremamente volátil. Eis o porquê da importância de mecanismos ágeis de cooperação entre os países quando deles depender a comunicação das informações.

Da importância da prova pericial nos delitos cibernéticos

No dizer de Araújo Cintra, Ada Pelegrini e Cândido Dinamarco, *a prova constitui, pois, o instrumento por meio do qual se forma a convicção do juiz a respeito da ocorrência ou inocorrência dos fatos controvertidos no processo.*[3]

Dentre os meios de prova tradicionais – exame de corpo de delito e perícias em geral, interrogatório, confissão, depoimento do ofendido, prova testemunhal, reconhecimento de pessoas e coisas, acareação, prova documental, prova indiciária e busca e apreensão – podemos dizer que praticamente todos eles sofreram alguma modificação ou influência em virtude das novas tecnologias.

Embora o Código de Processo Penal não pudesse e não possa prever todas as inovações que viriam evenham a integrar as necessidades modernas de colheita e produção de prova, essas inovações são perfeitamente compatíveis com o estatuto legal.

Assim, embora o interrogatório por videoconferência, por exemplo, seja aceito em situações específicas previstas na Lei 11.900/2009, a prova testemunhal é colhida por esse método correntemente, nos termos do §3º do artigo 222 da mesma Lei, sendo atualmente, tanto o interrogatório e as oitivas de testemunhas, presenciais, gravados e registrados em meio digital, inclusive, para garantir a fidedignidade da prova.

---

[2] DOMINGOS, Fernanda Teixeira Souza. *As provas digitais nos delitos de pornografia infantil na internet.* IN *A Prova no enfrentamento à Macrocriminalidade*, organização DANIEL DE RESENDE SALGADO e RONALDO PINHEIRO DE QUEIROZ. Ed. JusPodivm. 2015.

[3] CINTRA, Antonio Carlos de Araujo. *Teoria Geral do Processo*. Antônio Carlos de Araújo Cintra, Ada Pellegrini Grinover, Cândido R. Dinamarco. Editora Revista dos Tribunais. 8ªedição, revista e ampliada. 1991.

No entanto, percebemos que, com a migração dos delitos para o meio virtual, os meios de provas que passaram a merecer especial atenção dadas as peculiaridades da tecnologia digital são a prova documental, a prova pericial e também a busca e apreensão.

Quando falamos em crimes cibernéticos, necessariamente serão examinados registros, os quais, para nós, são considerados documentos. E mesmo para os crimes em geral, como já pontuado, as evidências digitais se fazem presentes no dia a dia, pois os documentos assumiram a forma digitalizada.

Documento é *toda base materialmente disposta a concentrar e expressar um pensamento, uma ideia ou qualquer manifestação de vontade do ser humano, que sirva para expressar e provar um fato ou acontecimento juridicamente relevante. São documentos: escritos, fotos, fitas de vídeo e som, desenhos, esquemas, gravura, disquetes, CDs, DVDs, pen drives, e-mails, entre outros. Trata-se de uma visão moderna e evolutiva do tradicional conceito de documento – simples escrito em papel – tendo em vista o avanço da tecnologia.*[4]

A Lei nº 11.419/2006, que regula os processos eletrônicos ao dispor sobre a informatização do processo judicial, prevê no seu artigo 11 que *os documentos produzidos eletronicamente e juntados aos processos eletrônicos com garantia de origem e de seu signatário, na forma estabelecida nesta Lei, serão considerados originais para todos os efeitos legais.*

Essa disposição legal demonstra a assertiva de Nucci de que o conceito de documento não se restringe mais ao papel, tendo sido estendido aos registros digitais.

E, da mesma forma que cabe questionamento sobre a autenticidade e validade de um documento real, em papel, que é feito através do incidente de falsidade documental – nos termos dos artigos 145 a 148 do Código de Processo Penal – esse questionamento pode ser feito em relação aos documentos digitais. E com muita razão.

Veja-se que as provas digitais possuem alto grau de volatilidade, sendo facilmente manipuláveis. Elas podem sofrer alteração pelo criminoso ao tentar, este, apagar os rastros digitais do delito que cometeu. O próprio investigador pode, inadvertidamente, alterar as evidências digitais pela manipulação inadequada destas durante as etapas de aquisição e análise.

A partir dessa assertiva, temos que a perícia pode ser necessária para comprovar a autenticidade do documento digital que pode ser evidência de crime cibernético, praticado por meio dos sistemas informatizados ou *internet*, ou evidência relativa ao crime comum, mas que possui associado a si evidências com registro digital.

No que toca aos delitos cibernéticos, é preciso ressaltar a necessidade da prova pericial para a constatação do crime.

Tomemos como exemplo o tipo penal do artigo 241-A do Estatuto da Criança e do Adolescente que descreve as seguintes condutas:

Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente. ***Pena – reclusão, de 3(três) a 6 (seis) anos e multa.***

[4]NUCCI, Guilherme de Souza. *Provas no processo penal*. São Paulo: Editora Revista dos Tribunais, 2009.

As condutas descritas nesse tipo penal, quando cometidas por meio de sistema de informática ou telemático, dependem necessariamente da prova pericial que irá examinar os registros digitais deixados no computador ou outros dispositivos eletrônicos do autor do delito.

Nos termos do artigo 158 do Código de Processo Penal Brasileiro: *quando a infração deixar vestígios, será indispensável o exame de corpo de delito, direto ou indireto, não podendo supri-lo a confissão do acusado.*

Assim, conforme Nucci[5], "Impõe-se a produção da prova pericial como forma *indispensável* para a prova da existência da infração penal, nos casos em que esta deixe vestígios materiais". Ora, todos os delitos cometidos por intermédio de sistemas ou dispositivos informatizados deixam vestígios.

Os computadores e a *internet* dependem de combinações numéricas e equações matemáticas que transformam *bits* e *bytes* equivalendo-os a *sites* e conteúdos visualizados de forma amigável para os usuários. Operações bancárias ou transmissão de vídeos e fotos de qualquer natureza no mundo virtual dependem de protocolos previamente estabelecidos, deixando o seu registro nos sistemas. Logo, todas as movimentações no meio virtual deixam rastro, de forma que crimes dessa natureza sempre dependerão da produção da prova pericial para que seja provada a sua existência.

Preservação

As provas digitais possuem determinadas características que devem ser observadas no seu tratamento em geral. A alta volatilidade já mencionada, que possibilita fácil alteração da prova, recomenda atenção e verificação da autenticidade por meio das técnicas periciais. Por isso, as provas que se encontram em poder dos provedores de aplicação devem ser objeto de preservação imediata, tão logo os investigadores dela tenham conhecimento, pois mesmo que obedecidos os prazos de retenção, este pode estar findando. Logo, a primeira coisa a se fazer é pedir a preservação da prova para que esteja íntegra quando for obtida a necessária ordem judicial para sua entrega.

Já quando são encontradas diretamente, sem a intermediação dos provedores, todo cuidado deve ser tomado para que a integridade e autenticidade sejam asseguradas.

O fato de poderem ser duplicadas sem maiores problemas vem como uma vantagem para a coleta e análise das provas digitais, pois dessa forma, pode-se preservar a prova original, analisando-se a "cópia", não se correndo o risco de, na própria análise ocorrer algum tipo de adulteração acidental. A facilidade de duplicação também vem a ser característica relevante, na medida em que facilita aos peritos a coleta de grande quantidade de material a ser analisado. Numa apreensão de grande quantidade de equipamentos ou em havendo equipamentos de dimensões muito grandes, não é necessário removê-los do local, bastando fazer o espelhamento do *hardware* para que se proceda à análise do conteúdo.

Outro fator que aponta vantagem aos investigadores do delito digital é a intangibilidade da evidência digital, tornando a sua destruição mais difícil.

Não raro, os criminosos que possuem fotografias de pornografia infantil armazenadas em seus computadores, que foram objeto de compartilhamento ou não, ao serem surpreendidos por uma ação policial para busca e apreensão de seus equipamentos informáticos, tentam destruir a evidência digital mediante o apagamento da mesma. No entanto, devido à característica inerente dos equipamentos informáticos, é possível, por meio da prova pericial, recuperar os dados apagados e demonstrar a

[5]NUCCI, Guilherme de Souza. *Provas no processo penal*. São Paulo: Editora Revista dos Tribunais, 2009.

ocorrência dos delitos de posse, armazenamento e/ou compartilhamento, mesmo em datas posteriores ao evento delituoso.

A manipulação da prova digital deve ser adequada também visando a obtenção de metadados, pois estes a permeiam, sendo facilmente coletados na perícia e devendo ser fornecidos também pelos provedores de aplicações. Devido à abundância de informações que é possível obter-se numa perícia de evidências digitais, o perito deve ser capaz de reduzir a quantidade de informações a fim de que estas possam ser organizadas para que seja exposto somente aquilo que é relevante para a investigação.

Procedimentos

Assim que chega ao conhecimento da autoridade a notícia de crime cuja materialidade e autoria dependa de provas digitais, é preciso fazer a coleta da prova ou pedir sua preservação ao provedor de aplicações onde ela está publicada ou armazenada.

Para os provedores de aplicações que prestam serviços no País e aqui mantêém escritório, basta enviar um ofício requerendo a preservação da página ou do perfil investigado. É importante a correta identificação através do endereço na *web*, a url, a fim de que a preservação seja feita corretamente, tanto do conteúdo quanto dos dados cadastrais e dados associados a essa página ou perfil, os chamados metadados.

Os metadados são os dados sobre dados. Informações que, se corretamente analisadas e associadas, podem trazer informações relevantes acerca da autoria do delito e auxiliar na localização de vítimas.

Alguns provedores de aplicações mantêm canais específicos para pedidos de preservação e para envio de ordens judiciais através de endereços de *e-mail* destinados às equipes montadas para responder às autoridades ou através de portais na própria *internet* criados especialmente para responder as autoridades.
Muitas vezes, o conteúdo criminoso ainda está disponível na *web*, podendo ser coletado por um técnico em informática ou agente treinado para tal que pode certificar a coleta da prova, devendo ser um agente público.

Como explicado acima, é muito importante que a cadeia de custódia da prova não seja quebrada, de forma que sua integridade se mantenha, garantindo sua autenticidade.

Na hipótese de ser necessário contatar um provedor de aplicações que não presta serviços no país, quando esteja hospedando o conteúdo investigado, já que nessas situações é comum que a vítima esteja no Brasil e também o criminoso, apenas se valendo este da *internet* para esconder-se, pode-se contatar diretamente o provedor da aplicação através de *e-mail* em geral disponibilizado e também fazer uso da rede 24x7 da Organização dos Estados Americanos - OEA. Nessa rede, pontos de contato estão 24 horas nos 7 dias da semana disponíveis para requerer a preservação de dados e conteúdo que deverão ser obtidos depois por meio da cooperação internacional. Para tanto, utilizar o *e-mail* cybercrime_brazil24x7@dpf.gov.br, já que o contato da rede 24x7 da OEA no Brasil é a Polícia Federal. Para demais países deve-se utilizar a Interpol.

De acordo com o que estudamos ~~na Aula 2~~ sobre Marco Civil da *Internet*, os provedores de aplicações que prestam serviços no Brasil devem reter os dados por seis meses. Porém, quando recebemos a notícia de um crime, não sabemos exatamente quanto tempo de retenção resta, de forma que sempre deve ser pedida a preservação dos dados e do conteúdo pretendido até que se obtenha a ordem judicial para sua obtenção.

Somente com a informação recebida sobre o *Internet Protocol* – IP, é que será possível identificar o provedor de conexão que alocou aquele IP.

Antes do MCI, era feito o pedido de preservação de dados também aos provedores de conexão até que se obtivesse a ordem judicial afastando o sigilo, pois embora houvesse decisões do STJ assegurando ser desnecessária ordem judicial para obtenção de dados cadastrais, sempre se pedia para evitar qualquer futura alegação de nulidade.

Com a redação trazida pelo MCI, esses dados podem ser obtidos diretamente pelas autoridades policiais, Ministério Público e autoridades administrativas.

Com a identificação do endereço de onde partiram as imagens ou mensagens criminosas, deve ser feita a busca e apreensão no local para confirmação da materialidade e individualização da autoria. Saliente-se que o mandado de busca e apreensão deve ser específico, elencando um rol amplo de possibilidades para a apreensão, a fim de se evitar dúvidas que possam vir a gerar nulidades.

Quanto aos aparelhos celulares, que são hoje muito mais que meros telefones, mas sim computadores pessoais que armazenam milhares de dados, a jurisprudência mudou. Em 2007, decisão do STF dizia bastar um mandado genérico para se ter acesso a todo o conteúdo de um celular apreendido. Em 2016, o STJ, no HC 51.531, decidiu ser necessária autorização específica para que os agentes de investigação tivessem acesso ao conteúdo do aparelho celular apreendido em uma prisão em flagrante. Recentemente, foi reconhecida a Repercussão Geral pelo Supremo Tribunal Federal ao Agravo em Recurso Extraordinário ARE nº 1.042.075 em que se discute exatamente essa questão: de que para acesso ao aparelho celular apreendido com conhecimento do registro das chamadas e da agenda de telefones, bem como das demais informações, é necessária prévia autorização judicial.

Interceptação de fluxo telemático de e-mails - Lei federal nº 9.296/96

Para a interceptação do fluxo de dados telemáticos, é necessária ordem judicial nos termos da Lei de interceptações nº 9.296/96, ou seja, somente será utilizada quando houver indícios razoáveis da autoria ou participação em infração penal, quando a prova não puder ser feita por outros meios disponíveis e quando o fato investigado não constituir infração penal punida, no máximo, com pena de detenção.

O meio de efetivar essa interceptação é a criação de uma conta espelho, com a colaboração do provedor desse serviço, de forma que os agentes de investigação teriam acesso em tempo real a todo o fluxo de *e-mails* recebidos e enviados pelo investigado.

Na prática, o provedor de serviços de *e-mail* grava em meio eletrônico o conteúdo da caixa postal investigada e o disponibiliza ao agente investigador.

Cooperação Jurídica Internacional nos Crimes Cibernéticos

Tendo em vista que a rede mundial de computadores permite a criação de páginas na *internet* a partir de um determinado país, as quais, porém, podem estar hospedados em outro, e que também é possível a partir de conexão estabelecida em um país navegar por sítios estabelecidos sob a soberania de outro, podendo-se fazer, inclusive, postagens, percebemos que a rede mundial de computadores é um espaço

virtual sem fronteiras, onde de alguma forma, procura-se estabelecer normas semelhantes às divisões territoriais de soberania existentes em nosso mundo real.

Dessa maneira, ao ser necessário obter registros de acesso a aplicações de *internet*, bem como comunicações telemáticas e conteúdo cujo suporte é dado por provedores estrangeiros sem representação no país, mas dentro das hipóteses do artigo 11 do Marco Civil da *Internet*, o contato com tais provedores dependerá dos mecanismos de cooperação internacional.

Note-se que essa regra é a mesma, inclusive, para os provedores de *internet* que oferecem os serviços de armazenamento de *cloud computing* e para os provedores de outros serviços, como os de segurança da *Internet* e serviços de servidor de nome de domínio distribuído, localizados entre o visitante e o provedor de *host* do usuário que agem como um *proxy* reverso para *sites.*

O armazenamento e gerenciamento de dados na nuvem gera confusão a respeito de onde estariam esses dados. De fato, ao serem transferidos para a "nuvem" esses dados podem ser acessados remotamente e também compartilhados a partir do espaço que ocupam nos servidores do provedor desse serviço, podendo tais servidores estarem localizados em qualquer outro país diferente de onde se encontra o usuário.

No entanto, encontrando-se tal provedor na situação descrita no artigo 11 do Marco Civil da Internet, isto é, mesmo sediado no exterior, ofereça o serviço ao público brasileiro ou mantenha um integrante do mesmo grupo econômico no país, sujeita-se às leis e jurisdição brasileira de forma que mesmo quanto aos dados mantidos na "nuvem" têm obrigação de fornecê-los mediante ordem judicial brasileira

Assim, a cooperação internacional em matéria de provedores de aplicações de *internet*, somente será necessária quando o provedor não tiver sede, filial ou subsidiária no Brasil, já que para estes, a regra geral do artigo 12 da LINDB – Lei de Introdução ao Direito Brasileiro, ~~que~~ diz que para operar no Brasil a empresa precisa estar constituída sob as leis brasileiras. Portanto, devem-se sujeitar à jurisdição nacional, combinando-se com o artigo 21 do Novo Código de Processo Civil que diz competir à autoridade judiciária brasileira processar e julgar as ações quando no Brasil tiver que ser cumprida a obrigação e o fundamento seja fato ocorrido ou ato praticado no Brasil. E a regra especial para empresas de tecnologia está insculpida no artigo 11 do MCI que diz bastar que um dos terminais esteja no Brasil, ou seja, que haja uma conexão a partir do território nacional e que a empresa esteja aqui coletando os dados ou tenha a filial no território nacional a qual reputa-se parte do mesmo grupo econômico.

Para as empresas de tecnologia que não possuem escritório, sede ou filial no território nacional, será necessária a cooperação jurídica internacional para dar eficácia às decisões judiciais como forma de obtenção de dados e conteúdos publicados ou armazenados na *web*.