José Ricardo Simões Rodrigues

É Especialista em Administração de Redes Linux pela Universidade Federal de Lavras, Minas Gerais (2004), Especialista em Direito para a Carreira da Magistratura (2013) e em Metodologia do Ensino Superior e da Pesquisa (2016), ambas pela Escola da Magistratura do Estado de Rondônia - EMERON. Possui graduação em Matemática (2000) e bacharelado em Direito pela Universidade Federal de Rondônia (2009). Atua no Tribunal de Tribunal de Justiça do Estado de Rondônia desde 1999, onde foi Escrivão pro tempore de 2005 a 2011 e Diretor de Cartório de 2011 a 2013. De 2013 a 2015 foi Chefe do Centro Judiciário de Solução de Conflitos e Cidadania da Comarca de Rolim de Moura. Desde julho de 2015 é Assessor de Juiz de Direito na 1ª Vara Cível de Rolim de Moura. É pesquisador do Centro de Pesquisa e Publicações Acadêmicas (CEPEP) da Escola da Magistratura do Estado de Rondônia.

A COLETA, A MANIPULAÇÃO E A PRESERVAÇÃO DA EVIDÊNCIA DIGITAL PARA O PROCESSO PENAL

José Ricardo Simões Rodrigues

Resumo

Com a democratização do acesso aos computadores e a redes de alcance mundial, os crimes cometidos por meio de computador ou contra sistemas de informação passaram a ser cada dia mais comuns. Tais crimes podem se consumar em meio eletrônico ou no mundo tangível. Os vestígios deixados por essas atividades ilícitas estão muitas vezes exclusivamente em meio digital, o que, em razão de dificuldades técnicas e falta de padronização das ações dos técnicos responsáveis por sua coleta e manipulação, pode render uma evidência imprestável para uso em juízo. Busca-se aqui discutir os procedimentos já padronizados para a coleta desse tipo de evidência bem como para a formação de sua cadeia de custódia, de modo a chegar intocada, autêntica e admissível para o processo penal.

Palavras-chave: Evidência digital. Cena do crime. Coleta. Cadeia de custódia. Processo penal.

Introdução

A Forense Computacional é uma área de pesquisa e atuação relativamente recente e são poucos os trabalhos sobre este assunto no Brasil. Entretanto, é crescente a necessidade de desenvol- vimento de estudos nesse sentido, vez que a utilização de computadores em atividades ilegais é cada vez mais comum.

Da mesma maneira que ocorre com outras ciências forenses, os profissionais da lei estão reconhecendo que a Perícia Forense pode prover evidência extremamente importante para solucio- nar um

crime e, em juízo, fundamentar uma decisão de mérito. Tem sido valorizada a evidência digital, inclusive com o reconhecimento da validade jurídica de documentos assinados digitalmente, se tornará crescentemente crítico que a evidência seja controlada e examinada corretamente.

Perícia Forense em Sistemas Computacionais é o processo de coleta, recuperação, análise e correlacionamento de dados que visa, dentro do possível, reconstruir o curso das ações do infrator e recriar cenários completos de maneira fidedigna.

Atualmente essa disciplina encontra-se num estágio de esforços de padronização de rotinas e criação de um conjunto de melhores práticas. A importância de tal esforço reside na necessidade de se garantir a integridade das evidências apresentadas em juízo, dado que, uma vez padronizados os procedimentos, torna-se mais difícil conseguir levantar teses juridicamente viáveis para o questionamento dos fatos apresentados tomando como tese a metodologia utilizada na manipulação das provas, desde que toda essa técnica tenha sido apli- cada corretamente.

A carência e escassez de metodologias amplamente difundidas e adotadas para o manuseio da evidência digital pode ser explicada pelo fato de existirem inúmeras mídias de armazenamento, plataformas, sistemas operacionais e protocolos, além de diversas mudanças de versão. Todos esses fatores tornam difícil a definição de padrões e metodologias, pelo menos da mesma forma como acontece com as outras disciplinas forenses.

Já existem padrões internacionais definidos e sendo aplicados de forma experimental. Eles foram desenvolvidos pelo Scientific Working Group on Digital Evidence[1] (SWGDE), que é o representante norte-americano na International Organization on Computer Evidence[2] (IOCE). O documento mais atualizado é o SWGDE Best Practices for Computer Forensics Version 3.1[3] de julho de 2014. Algumas das recomendações apresentadas aqui são baseadas nessa coleção de melhores práticas do SWGDE.

1 Grupo Científico de Trabalho em Evidência Digital.

2 Organização Internacional sobre Evidência Computacional.

3 Melhores Práticas para Forense Computacional do SWGDE, versão 3.1.

Segundo Oliveira, Guimarães e Geus (2001, p. 84), todas as organizações que, em seu dia a dia trabalham com a evidência digital e investigação forense deveriam alcançar um nível de qualidade tal que se assegurasse extrema confiabilidade e grande precisão às evidên- cias. Para o atingimento desse nível de qualidade, é necessária padronização mediante elaboração e colocação em prática de Standard Operating Procedures5[4] (SOPs). Esses procedimentos padrão devem abarcar todo tipo de análises, técnicas e materiais de uso difundidos cientificamente.

Esse preconizado nível de qualidade tem sido buscado por países como os Estados Unidos da América, onde existem cartilhas criadas para auxiliar a policiais e investigadores na preservação de cenas de crimes eletrônicos (U. S. DEPARTMENT OF JUSTICE, 2008).

Nacionalmente, não há padronização em curso (OLIVEIRA, GUIMARÃES e GEUS: 2002, p. 129).

Procurar-se-á, aqui, fazer um breve levantamento acerca das novas formas de criminalidade sendo cometidas por meio de computador e contra sistemas de informática, dos vestígios deixados por esses ilícitos e das formas de sua coleta e transformação em evidências e indícios para serem usados no processo penal.

O crime na era digital

Segundo informações disponíveis em Internet Crime Complaint Center (2018, p. 17), o número de reclamações referentes crimes perpetrados via internet[5], nos Estados Unidos, mantém uma média de 284.000 reclamações por ano. O prejuízo apontado pelo relatório é de aproximadamente US$ 1,42 bilhão em 2017. No Brasil, os números disponíveis no sítio eletrônico do Grupo de Resposta a Incidentes de Segurança para a Internet brasileira, mantido pelo Comitê Gestor da Internet no Brasil, demonstram que em 2010 foram reportados

4 Procedimentos Operacionais Padrão.

5 Grafou-se na extensão deste trabalho o termo internet em letras minúsculas por entendermos, como em Uchôa e Alves (2002, p. 7), ser atualmente um meio de comunicação tão popular como rádio ou televisão.

142.844 incidentes de segurança envolvendo redes de computadores, ao passo que em 2017 esse número foi de 833.775 (CERT.BR, 2018).

Esses números evidenciam um crescimento considerável no número de ilícitos envolvendo informática, também chamados de crimes informáticos.

Quanto à classificação desses crimes, em Ferreira (1992, p. 214-215) distinguem-se duas categorias:

1. Os crimes cometidos contra um sistema de informática, seja qual for a motivação do agente;
2. Os crimes cometidos contra outros bens jurídicos, por meio de um sistema de informática.

O delito de informática, *strictu sensu*, é o primeiro, ou seja, aquele em que o computador ou sistemas de computadores, redes, etc, são atacados mediante uso de outros computadores (o computador é a ferramenta e alvo). No segundo caso, o crime é comum e o computador é apenas uma ferramenta utilizada para o atingimento do fim desejado pelo agente, sendo mais comuns nesta espécie as práticas ilícitas de natureza patrimonial, crimes contra a honra, as que atentam contra a liberdade individual e contra o direito de autor.

Outros autores, como por exemplo Vianna (2003, p. 13-26), classificam os crimes informáticos como puros (próprios) ou impuros (impróprios).

Essa classificação leva em conta o também a ferramenta utilizada, o ambiente de consumação e o bem jurídico protegido. Nos crimes de computador puros ou próprios as condutas são praticadas por meio de computador e se realizem ou se consumem também em meio eletrônico. O bem jurídico protegido é a própria segurança dos sistemas, a titularidade das informações e integridade dos dados, do equipamento e seus periféricos.

Quando o bem jurídico a ser protegido tratar-se de bens não computacionais e o computador for apenas o meio utilizado para lesar ou pôr em risco esses bens, produzindo um resultado que ofenda o mundo físico ou real, estaremos diante dos crimes eletrônicos impuros ou impróprios.

Assim, os crimes informáticos dividem-se em crimes contra o

computador e crimes por meio do computador, em que este serve de instrumento para atingir uma meta.

Os crimes de computador, segundo informação de Aras (2001), em geral, são definidos na doutrina norte-americana como *special opportunity crimes*, pois são cometidos por pessoas cuja ocupação profissional implica o uso cotidiano de microcomputadores, não estan do excluída, evidentemente, a possibilidade de serem cometidos por curiosos.

Vive-se, dessa maneira, uma época de proliferação dos crimes dessa índole, sejam, cometidos contra sistemas de computador ou contra bens tradicionalmente protegidos pela norma penal e ofendidos por meio de computadores ou dispositivos assemelhados.

Os vestígios deixados por essas condutas podem estar disponíveis exclusivamente em meio digital, e nesse meio devem ser colhidos e transformados em evidências para uso no processo penal, seja para conseguir uma condenação ou para provar a inocência do acusado.

A evidência digital

Trata-se a evidência criminal de quaisquer provas, sejam documentais, testemunhais ou periciais, que se destinem a firmar a convicção do juiz sobre a veracidade dos fatos alegados pelas partes no Processo Penal. Durante o curso de uma investigação criminal, a coleta dessas evidências visa determinar a existência do ato ilícito, suas circunstâncias bem como seu autor.

Já a evidência digital é aquela que se encontra em algum formato ou meio utilizado em processamento eletrônico digital. Podem ser uma representação digital de dados em estado bruto ou processados, sons, imagens estáticas ou em movimento e textos para processamento por sistemas computacionais.

Segundo Brezinski e Killalea (2002), a evidência digital deve ser:

> Admissible: It must conform to certain legal rules before it can be put before a court. Authentic: It must be possible to positively tie evidentiary material to the incident. Complete: It must tell the whole

> story and not just a particular perspective.Reliable: There must be nothing about how the evidence was collected and subsequently handled that casts doubt about its authenticity and veracity. Believable: It must be readily believable and understandable by a court[6].

Esses requisitos para a evidência digital estão bem próximos daqueles exigidos para a produção da prova conforme aceito pela doutrina brasileira. Para Feitoza (2008, p. 686), por exemplo:

> Os pressupostos ou "requisitos" para a coleta e produção de prova são:
>
> a) admissibilidade ou legalidade: a prova é prevista ou não vedada por lei ou pela Constituição
>
> b) adequação, idoneidade, pertinência, ou aptidão: a prova contribui para a obtenção de fim da persecução criminal ou processo penal concretamente considerados, como demonstrar a existência ou inexistência da infração penal e sua autoria, formar a convicção da entidade decisora (...)
>
> c) necessidade: a prova tem a mesma aptidão que outras para obter os fins da persecução criminal concreta (...)

É da natureza da evidência digital ser menos tangível que as demais evidências. Um corpo, uma arma branca ensanguentada, uma cápsula de munição deflagrada, um projétil ou mesmo uma impressão digital são mais tangíveis que um arquivo eletrônico armazenado em um frágil disco magnético ou em um endereço de memória volátil.

A evidência digital, no atual estágio de desenvolvimento tecnológico de armazenamento e processamento de dados será quase sempre composta por campos magnéticos ou óticos gravados em discos, fitas ou outros dispositivos como circuitos integrados de memória não

6 Admissível: necessita estar em conformidade com certas normas antes de ser posta perante um tribunal. Autêntica: deve ser possível estabelecer um liame entre o material das evidências e o incidente. Completa: deve refletir todos os fatos e não apenas uma perspectiva particular. Confiável: nada deve haver acerca do modo como a evidência foi coletada e subsequentemente manipulada que lance alguma dúvida quanto sua autenticidade e veracidade. Crível: deve ser imediatamente crível e de fácil entendimento pelo julgador. Tradução do autor.

volátil[7] ou por pulsos eletrônicos armazenados temporariamente em memória volátil[8] ou sendo transmitidos por uma rede como a internet ou redes locais. Assim, devem ser considerados como possível fonte de evidências digitais:

- Dispositivos de armazenamento em computadores ou dispositivos capazes de processamento eletrônico digital[9] (registradores e caches);
- Memória de periféricos (modems, pagers, aparelhos de fax, impressoras, monitor de vídeo);
- Dispositivos de rede como roteadores (switches), concentradores de conexão (hubs), modems externos ou aparelhos de telefonia sobre Internet Protocol (IP);
- Dispositivos de armazenamento secundário, como unidades de disco ótico, magnético, de fita ou de estado sólido[10], cartões de memória, pendrives;
- Estado do sistema operacional ou de dispositivos de rede, como os arquivos de configuração e de registro e de *logs*[11].
- Espaços de armazenamento remoto (computação na nuvem ou *cloud computing*, por exemplo).

Apesar dessa volatilidade, as evidências digitais serão passíveis de coleta e análise desde que sejam utilizadas as ferramentas e técnicas apropriadas. Essa extrema volatilidade, ao lado da possibilidade de

7 Um exemplo seriam as memórias do tipo ***Read Only Memory*** (ROM, memória apenas para leitura) e os populares ***pendrives***.

8 ***Ramdon Access Memory*** (RAM, memória de acesso aleatório).

9 Atualmente existe toda uma gama de dispositivos que possuem capacidade de processamento, entre eles, telefones celulares inteligentes, computadores portáteis (notebooks e tablets), aparelhos de televisão e reprodutores de multimídia.

10 SSD, sigla para ***Solid state drives*** ou Dispositivos de estado sólido. Os disco óticos ou magnéticos oferecem armazenamento massivo e a custos baixos. Como ponto negativo, são relativamente lentos para os padrões atuais, ocupam mais espaço e representam soluções energeticamente caras e apresentam partes mecânicas propensas a falhas. Os SSD, apesar do custo mais elevado, solucionam parte desses problemas.

11 ***Logs*** são uma espécie de registro de atividades, seja do usuário, seja do próprio sistema operacional e demais programas. Sobre as normas brasileiras acerca da obrigatoriedade e guarda desses registros por provedores de acesso e de aplicações, ver artigos 10 e seguintes da Lei 12.965/2014 (BRASIL, 2014).

fácil duplicação, são as principais características próprias da evidência digital.

A evidência digital, então, em seus requisitos para coleta e apresentação em juízo, não se distancia em muito daquelas evidências comumente aceitas em juízo nos demais crimes. Os procedimentos devem ser diferentes e especializados em razão dessa volatilidade, das inúmeras formas de armazenamento possíveis e de seu aspecto técnico.

Coleta e preservação

Um dos princípios fundamentais da ciência forense é o Princípio de Locard. Edmond Locard enunciou que qualquer pessoa ou qualquer objeto que adentre numa cena de crime levará consigo algo e deixará para trás alguma coisa (COUTO, 2010). Por isso tal princípio também é conhecido como Princípio da Troca de Locard, ante a permuta de traços entre esses sistemas.

Para a evidência digital, esse princípio também poderá ser considerado válido, pois uma vez que o perito tiver acesso à cena do crime e aos objetos que entraram em contato com ela poderá, apesar da extrema dificuldade e da necessidade de cenários favoráveis, encontrar as evidências dessa troca.

Dado esse princípio, a atividade pericial é sensível a provocar interferências também nos cenários do crime eletrônico, de modo a possivelmente tornar imprestável a evidência adquirida, pois ela falhará em, pelo menos, dois de seus requisitos essenciais que são a autenticidade e a confiabilidade.

Como tal evidência será submetida ao crivo do contraditório em Juízo, as partes certamente questionarão a legitimidade dessa evidência, principalmente ao argumento de que elas foram alteradas, substituídas ou mesmo plantadas.

Portanto, segundo Farmer e Venema (2006) e Scientific Working Group on Digital Evidence (2014), necessárias algumas atitudes do perito antes mesmo da coleta propriamente dita atitudes tendentes a

manter intacta a cena do crime. São elas, principalmente:

- Verificar a autorização legal para a busca da evidência, garantindo que eventuais restrições se aplicarão. Se no curso do processo de coleta de evidências autorizações adicionais forem necessárias estas deverão ser solicitadas e deferidas antes do pross guimento.
- Utilizar mídias novas (virgens) ou completamente limpas (formatadas e sem arquivos) e em boas condições
- Certificar-se de que as ferramentas (programas de computador) estão licenciadas e configuradas para utilização.
- Certificar-se de que os equipamentos forenses (estação de trabalho, por exemplo) e mídias estão prontos e disponíveis para utilização.
- Na cena do crime, providenciar o isolamento não permitindo alterações acidentais ou subtração de possíveis evidências.
- Documentar em vídeo e/ou fotografias o ambiente, os equipamentos (configurações, modelo, série etc), suas conexões e disposição
- Manter a cadeia de custódia estritamente intacta.

Em Dias Filho (2009, p. 447) encontramos uma definição que explicita e conceitua cadeia de custódia:

> Uma sucessão de eventos concatenados, em que cada um proporciona a viabilidade ao desenvolvimento do seguinte, de forma a proteger a integridade de um vestígio do local de crime ao seu reconhecimento como prova material até o trânsito em julgado do mérito processual; eventos estes descritos em um registro documental pormenorizado, validando a evidência e permitindo sua rastreabilidade, sendo seu objetivo-fim garantir que a evidência apresentada na corte se revista das mesmas propriedades probatórias que o vestígio coletado no local de crime.

Mister se faz reforçar a necessidade da manutenção de uma cadeia de custódia hígida e bem documentada. É essa cadeia de custódia que documenta na posse de quem certa evidência estava em um dado

momento no tempo. Quem era, portanto, o responsável por sua conservação. Em caso de comprometimento da evidência ao longo do processo, a cadeia de custódia permitirá mapear as responsabilidades individuais no processo.

Esse protocolo assegura a idoneidade de todo o processo de coleta de provas, pois documenta todas as fases percorridas.

Segundo Chasin (2001, p. 41), a cadeia de custódia se subdivide em externa e interna. A primeira compreende o período entre o transporte do local de coleta da evidência até a chegada às instalações forenses enquanto que a segunda refere-se ao procedimento interno no laboratório, até o possível descarte das amostras.

Obviamente a ação do investigador ou perito deve se pautar dentro da estrita legalidade, em nada se diferindo da atuação para recolhimento das demais evidências. A exemplo disso, a Lei 9.296 de 24 de julho de 1996, que trata das interceptações telefônicas e de tráfego de dados, regulamentando o inciso XII, parte final, do art. 5° da Constituição Federal, estipula que:

> Art. 1º. A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça.
>
> Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática.

Assim sendo, qualquer procedimento pericial que importe em violação da garantia fundamental expressa no inciso XII do artigo 5º da Constituição Federal, deve ter como suporte autorização judicial para sua execução, que circunscreverá os limites dessa atuação.

Para o processo de coleta propriamente dita das evidências consubstanciadas em informações digitais, o perito deverá passar por um processo de três etapas descritas em Pereira *et al* (2007, p. 17-18). São elas:

1. Estabelecimento de uma ordem de prioridade na qual os dados devem ser coletados. Deverão ser considerados fatores como volatilidade da informação, esforço necessário para sua

extração e valor estimado da informação a ser obtida.
2. Processo de cópia dos dados, com o uso de ferramentas apropriadas e confiáveis de modo a garantir a integridade e a segurança da evidência bem como em formato que possibilite sua posterior duplicação e análise.
3. Preservação da integridade dos dados, preferencialmente utilizando-se de aplicações para geração de *hashes*[12] ou assinatura digital com chaves públicas[13].

Adicionalmente, no processo de cópia dos dados, segundo Scientific Working Group on Digital Evidence (2014), os seguintes cuidados deverão ser tomados pelo profissional:

- Cuidados devem ser tomados para prevenir que a evidência não venha ser contaminada fisicamente com substâncias perigosas.
- Deverão ser utilizados bloqueios, sejam via *softwares*[14], sejam via *hardwares*[15] de modo a evitar modificações da evidência original.
- Utilizar métodos conhecidos e verificáveis para a coleta da evidência. Aqui o respeito aos padrões internacionalmente aceitos é muito importante.
- As cópias devem ser feitas utilizando-se de ferramentas que permitam a captura bit-a- bit (*bit stream*) da mídia original.

É importante salientar que, conforme dito anteriormente, muitas vezes as evidências estão trafegando na rede, inclusive o ato ilícito

12 Um hash é uma sequência que se garante ser única para uma cadeia de caracteres ou para um arquivo digital. Deve-se gerar o hash do arquivo original e da cópia, de modo que se possa averiguar, posteriormente, que a cópia extraída é uma reprodução fiel da evidência encontrada. Os algoritimos de hash mais utilizados e em ordem de segurança proporcionada são o MD4, MD5 e o SHA1, cujas implementações são amplamente disponíveis para as mais diversas plataformas computacionais.

13 Trata-se a assinatura de chaves púbicas de uma das técnicas disponíveis para gerar documentos digitais com validade legal. No Brasil, a Medida provisória 2.200-2, que instituiu a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), determina que qualquer documento digital tem validade legal se for certificado pela ICP-Brasil.

14 Sistemas de arquivos, por exemplo, podem ser montados em modo de somente leitura.

15 Alguns tipos de unidades de disco ou de cartões de memória possuem uma trava que, uma vez acionada, não permitirá nenhuma alteração nos arquivos.

pode estar em pleno curso, como no caso de uma invasão de um sistema computacional conectado a uma rede. Nesses casos, pode ser necessária a aquisição de dados adicionais como os mencionados em Scientific Working Group on Digital Evidence (2014):

- Processos e programas sendo executados no momento;
- Serviços providos, portas de conexão ativas e informações de IP;
- Arquivos temporários criados pelo sistema ou ainda não salvos em disco;
- Informações de dispositivos acessados pela rede e respectivas permissões;
- Usuários conectados pela rede que podem ter acesso aos mesmos dados sendo analisa- dos.

Uma vez que os dados coletados estejam em mídias apropriadas, prontas para a análise posterior em laboratório, é de extrema importância a adoção das melhores práticas para a preservação dessas informações. Essas práticas incluem a duplicação da informação armazenada, processo conhecido como cópia de segurança, gerando uma redundância que será útil para recuperação em casos de acidentes no processamento ou falhas nessas mídias de armazenamento. Tais práticas recomendam, inclusive, que o armazenamento das cópias seja feito em lugares distintos, evitando que desastres naturais ou a intervenção humana provo quem sua perda.

Então, quanto ao processo de coleta e preservação das evidências digitais, valem as já conhecidas regras da ciência forense, principalmente aquelas relativas à necessidade de preservação da cena do crime e da produção de uma evidência imaculada de agentes externos.

O respeito aos direitos constitucionais em jogo, principalmente aqueles atinentes à privacidade do investigado deve ser permanente, assim como a busca de melhores práticas aceitas internacionalmente nessa área de atuação.

A evidência digital e o processo penal

Prescreve o Código de Processo Penal Brasileiro (BRASIL, 1941) em seu artigo 158 que "quando a infração deixar vestígios, será indispensável o exame de corpo de delito, direto ou indireto, não podendo supri-lo a confissão do acusado." Resta imprecisa na lei a definição do que seria vestígio.

No conceito de Dias Filho (2009, p. 441),

> (...) vestígio mantém a característica abrangente do vocábulo que lhe deu origem, podendo ser definido como todo e qualquer sinal, marca, objeto, situação fática ou ente concreto sensível, potencialmente relacionado a uma pessoa ou a um evento de relevância penal, e/ou presente em um local de crime, seja este último mediato ou imediato, interno ou externo, direta ou indiretamente relacionado ao fato delituoso.

Assim, ao encontrar um vestígio deixado por um agente ou um evento, ele passará a ser importante para a resolução do caso se for possível estabelecer a ligação entre esse vestígio e o delito sob investigação. Ocorrendo a comprovação objetiva dessa relação de causalidade, o vestígio passará a ser denominado evidência.

Dias Filho (2009, p. 441) arremata então dizendo que "evidência é o vestígio que, após avaliações de cunho objetivo, mostrou vinculação direta e inequívoca com o evento delituoso. Processualmente, a evidência também pode ser denominada prova material."

Interessante notar que, como bem observado por Dias Filho (2009), ao contrário da evidência, o Código de Processo Penal (BRASIL, 1941) delimita bem o conceito de indício em seu artigo 239 ao precisar que "considera-se indício a circunstância conhecida e provada, que, tendo relação com o fato, autorize, por indução, concluir-se a existência de outra ou trascircunstâncias."

Logo, por operações lógicas do sujeito que aprecia o indício, é possível concluir, a partir de um indício, pela existência de outros indícios também circunstanciais. Esse segundo tipo de indício carrega, então, um componente de subjetividade. Ao contrário, um indício que

decorre diretamente de uma evidência é objetivo.

Quanto ao relacionamento entre vestígio, evidência e indício, Dias Filho (2009, p. 442-443) assim conclui:

> (...) podemos deduzir que a evidência é o vestígio que, mediante pormenorizados exames, análises e interpretações pertinentes, se enquadra inequívoca e objetivamente na circunscrição do fato delituoso. Ao mesmo tempo, infere-se que toda evidência é um indício, porém o contrário nem sempre é verdadeiro, pois o segundo incorpora, além do primeiro, elementos outros de ordem subjetiva.

Não existe legislação específica sobre forense computacional no Brasil. Aplicam-se a essa modalidade as regras gerais prescritas para as perícias em geral.

O Código de Processo Penal (BRASIL, 1941) possui as seguintes prescrições atinentes aos exames periciais e que são aplicáveis no trato com a evidência digital:

> Art. 170. Nas perícias de laboratório, os peritos guardarão material suficiente para a eventualidade de nova perícia. Sempre que conveniente, os laudos serão ilustrados com provas fotográficas, ou microfotográficas, desenhos ou esquemas.

Nesse dispositivo, na primeira parte, fica evidenciada a importância jurídica da cadeia de custódia e do correto armazenamento das evidências. É a observância dessas práticas que permitirá a reprodução da evidência coletada e a eventual feitura de novo exame pericial durante o contraditório do processo penal.

Com referência ao laudo pericial, também o Código de Processo Penal (BRASIL, 1941) prescreve:

> Art. 171. Nos crimes cometidos com destruição ou rompimento de obstáculo a subtração da coisa, ou por meio de escalada, os peritos, além de descrever os vestígios, indicarão com que instrumentos, por que meios e em que época presumem ter sido o fato praticado.

Aqui o legislador prevê um requisito essencial para o laudo a ser emitido pelo perito quando o crime sendo apurado envolver,

por exemplo, uma invasão de sistemas de computador. Esse laudo, referindo-se a evidências em meio digital, obrigatoriamente, deverá descrever quais ferramentas (sejam de *software*, sejam de *hardware*) e metodologias foram utilizadas durante o processo de coleta e processamento da evidência. Durante a análise dos arquivos, por exemplo, o perito deverá documentar as informações referentes ao tempo do acesso a esses arquivos pelo agente[16]. Com a correta extração dessas informações será possível reconstruir todos os passos executados pelo infrator.

Normalmente os exames periciais são realizados por uma equipe de profissionais, até porque pode trata-se de um estudo multidisciplinar. A Jurisprudência do Supremo Tribunal Federal determina que:

> Súmula 361
>
> No processo penal, é nulo o exame realizado por um só perito, considerando-se impedido o que tiver funcionado, anteriormente, na diligência de apreensão.

A interpretação posterior do próprio Supremo Tribunal Federal deu conta de que essa Súmula refere-se a peritos não oficiais, ou seja, aqueles que não fazem parte dos quadros da Polícia Judiciária e são nomeados conforme permissão do Código de Processo Penal (BRA- SIL, 1941), por exemplo ante ausência ou impedimento dos peritos oficiais. O próprio Código de Processo Penal foi modificado posteriormente pela Lei 11.690/2008 passando a ter a seguinte redação:

16 O perito chegará a essa informação utilizando-se de ferramentas para extração dos *MAC times*. Tratam-se de informações (metadados) gravadas no sistema de arquivos que registram datas em que ocorreram certos eventos relacionados ao arquivo pela última vez, como, criação, acesso e edição.

> Art. 159. O exame de corpo de delito e outras perícias serão realizados por perito oficial, portador de diploma de curso superior.
>
> § 1º Na falta de perito oficial, o exame será realizado por 2 (duas) pessoas idôneas, portadoras de diploma de curso superior preferencialmente na área específica, dentre as que tiverem habilitação técnica relacionada com a natureza do exame.

No sentido dessa interpretação é o seguinte julgado do Supremo Tribunal Federal (BRASIL, 1996):

> EMENTA: DIREITO PENAL E PROCESSUAL PENAL. FALTA DE DEFESA. LAUDO PERICIAL (ART. 159 DO CÓDIGO DE PROCESSO PENAL). INTERROGATÓRIO. PENA: FUNDAMENTAÇÃO. REGIME DE CUMPRIMENTO. "HABEAS CORPUS". 1. É de repelir a alegação de falta de defesa, se esta não fica evidenciada com a impetração e as informações do Tribunal prolator do acórdão esclarecem que o réu teve Defensora dativa, que ofereceu defesa prévia, participou das audiências de instrução - inclusive com reperguntas - e apresentou alegações finais e razões de apelação. 2. O laudo pericial, segundo o acórdão, foi elaborado por dois peritos oficiais, ainda que, por inadvertência, assinado apenas por um. 3. De resto, a perícia, no caso, foi realizada antes da vigência da Lei nº 8.862, de 28.3.1994, que deu nova redação ao art. 159 do Código de Processo Penal. 4. Enquanto vigorou com sua redação originária o art. 159 do Código de Processo Penal, a Súmula 361 do S.T.F. somente se referiu aos peritos não-oficiais, pois sua jurisprudência posterior considerou válido o laudo assinado por um só perito oficial. 5. O interrogatório do réu foi realizado regularmente e até por ele assinado. 6. O regime fechado de cumprimento de pena era o cabível, no caso, em face do disposto no § 1º do art. 2º da Lei nº 8.072, de 26.07.1990, já que o atentado violento ao pudor ocorreu posteriormente. 7. A pena, no acórdão, foi corretamente fixada, e a impetração não lhe impugna a fundamentação, mas, sim, apenas a da sentença, que, no ponto, não subsistiu. 8. "H.C." indeferido.
>
> (HC 74521, Relator(a): Min. SYDNEY SANCHES, Primeira Turma, julgado em 10/12/1996, DJ 04-04-1997 PP-10522 EMENT VOL-01863-02 PP-00445)

Importante salientar que o mencionado artigo 159 do Código de Processo Penal também impõe outros requisitos para nomeação do perito, quais sejam, idoneidade das pessoas nomeadas, preferência por aqueles que detenham curso de nível superior e habilitação técnica relacionada à natureza do exame.

Nesta seção foram destacadas alguns aspectos da evidência eletrônica com relação ao processo penal. Dentre eles, a imprescindibilidade dos exames periciais para a apuração dessa modalidade criminosa.

Verificou-se que a prova indiciária, assim conhecido como aquele indício que decorre diretamente de uma evidência pericial, possui cunho objetivo, sem avaliação subjetiva, portanto. Desse indício poder-se-á decorrer logicamente outros indícios, conforme autorização da lei processual penal.

Essa mesma legislação processual penal estatui alguns requisitos para o laudo pericial bem como para a nomeação de peritos oficiais e não oficiais para atuação em juízo.

Considerações finais

Procurou-se neste trabalho levar a cabo um rápido levantamento acerca das novas formas de criminalidade que vem sendo cometidas por meio de equipamentos de informática e contra sistemas de computadores, dos vestígios deixados por esses ilícitos e das formas de sua coleta e transformação em evidências e indícios para serem usados no processo penal.

O estudo concluiu que há uma crescente proliferação de crimes dessa espécie, tanto os perpetrados contra sistemas de computador quanto aqueles cometidos contra bens tradicio- nalmente protegidos pela norma penal, como o patrimônio e a honra subjetiva.

Como os demais crimes, essa nova modalidade também deixa vestígios e, dada a for- ma como são praticados, esses vestígios podem estar em meio digital, exigindo que aí sejam coletados e transformados em evidências para uso no processo penal, seja para

conseguir uma condenação ou para provar a inocência do acusado.

Esse tipo de evidência reveste-se de grande volatilidade, exigindo que sejam utiliza- das as ferramentas e técnicas de eficácia comprovada cientificamente.

Do estudo comparado da doutrina e da literatura técnica sobre o tema, conclui-se que a evidência digital, em seus requisitos para coleta e apresentação em juízo, não se distancia em muito daquelas evidências comumente aceitas em juízo nos demais crimes. Os procedimentos devem ser diferentes e especializados em razão de sua volatilidade, das inúmeras formas de armazenamento possíveis e de seu aspecto técnico diferenciado.

Dadas essas semelhanças com os demais tipos de evidências, conclui-se que, quanto ao processo de coleta e preservação das evidências digitais, valem as já conhecidas regras da ciência forense, principalmente aquelas relativas à necessidade de preservação da cena do crime e da produção de uma evidência imaculada de agentes externos. O respeito aos direitos constitucionais em jogo, principalmente aqueles atinentes à privacidade do investigado deve ser permanente, assim como a busca de melhores práticas aceitas internacionalmente nessa área de atuação.

Da legislação processual penal, foram destacadas alguns aspectos relativos à evidência eletrônica, como a imprescindibilidade dos exames periciais para a apuração dessa modalidade criminosa, principalmente por constituir o indício que decorre diretamente da evidência pericial de prova indiciária de cunho objetivo, sem avaliação subjetiva, portanto.

Essa mesma legislação processual penal estatui alguns requisitos para o laudo pericial bem como para a nomeação de peritos oficiais e não oficiais para atuação em juízo.

Por se tratar de uma área de atuação em desenvolvimento e em fase de padronização, é importante manter-se atualizado com as melhores práticas reunidas e recomendadas por or- ganismos nacionais e internacionais.

Referências

ARAS, V. Crimes de informática. Uma nova criminalidade. Jus Navigandi, Teresina, ano 6, n. 51, 1 out. 2001. Disponível em: <http://jus.com.br/revista/texto/2250>. Acesso em: 13 set. 2018.

BRASIL. Decreto-Lei n. 3.689 de 3 de outubro de 1941. Código de Processo Penal. Disponível em <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689Compilado.htm> Acesso em: 13 set. 2018.

BRASIL. Lei n. 12.965 de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689Compilado.htm> Acesso em: 13 set. 2018.

BRASIL. Supremo Tribunal Federal. Habeas-corpus 74521. Primeira Turma. Relator Ministro Sydney Sanches. Julgamento em 10/12/1996. Diário da Justiça de 04/04/1997, p. 10522. Ementário v. 01863-02, p. 445.

BREZINSKI, D. e KILLALEA, T. RFC 3227: Guidelines for Evidence Collection and Archiving. The Internet Society: 2002. Disponível em <http://www.ietf.org/rfc/rfc3227.txt>. Acesso em: 13 set. 2018.

CERT.BR. Estatísticas dos Incidentes Reportados ao CERT.br. Disponível em <http://www.cert.br/stats/incidentes/> Acesso em: 13 set. 2018.

CHASIN, A. A. da M. Parâmetros de confiança analítica e irrefutabilidade do laudo pericial em toxicologia Forense. Revista Brasileira de Toxicologia, v. 14, n. 1, p. 40-46, 2001.

COUTO, S. P. Manual da Investigação Forense. São Paulo: Ideia e Ação, 2010.

DIAS FILHO, Claudemir Rodrigues. Cadeia de custódia: do local de

crime ao trânsito em julgado; do vestígio à evidência. Revista dos Tribunais, São Paulo: RT, v.98, n.882, p. 436- 451, maio 2009.

FARMER, D; VENEMA, W. Perícia forense computacional: Teoria e prática aplicada. Prentice Hall: São Paulo, 2006.

FEITOZA, D.. Direito processual penal: Teoria, crítica e práxis. 5. ed. Impetus: Niterói, 2008.

FERREIRA, I. S. Estudos jurídicos em homenagem a Manoel Pedro Pimentel. In: . São Paulo: Revista dos Tribunais, 1992. cap. Os crimes de informática, p. 139– 162.

INTERNET CRIME COMPLAINT CENTER. 2017 Internet Crime Report. 2018. Disponível em <https://pdf.ic3.gov/2017_IC3Report.pdf> Acesso em: 13 set. 2018.

OLIVEIRA, F. de S.; GUIMARÃES, C. C.; GEUS, P. L. de. Forense Computacional: Aspectos legais e padronização. In: I Workshop sobre Segurança em Sistemas Computacionais, 2001, Curitiba, PR. Anais do WSeg'01 (SCTF'01), 2001. p. 80-85.

OLIVEIRA, F. de S.; GUIMARÃES, C. C.; GEUS, P. L. de. Resposta a incidentes para ambientes corporativos baseados em Windows. In: II Workshop sobre Segurança em Sistemas Computacionais, 2002, Búzios, RJ. Anais do WSeg'02 (SBRC'02), 2002. p. 129- 136.

PEREIRA, E.; FAGUNDES, L.; NEUKAMP, P.; LUDWIG, G.; KONRATH, M. Forense Computacional: fundamentos, tecnologias e desafios atuais. In: VII Simpósio brasileiro em segurança da informação e de sistemas computacionais. Rio de Janeiro: VII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, 2007.

SCIENTIFIC WORKING GROUP ON DIGITAL EVIDENCE. Best practices for computer forensics version 3.1. Set. 2014. Disponível em <https://

www.swgde.org/documents/Current%20Documents/SWGDE%20Best%20Practices%20for%20Computer%20Forensics> Acesso em: 13 set. 2018.

SCIENTIFIC WORKING GROUP ON DIGITAL EVIDENCE. Capture of live systems v 2.0. Set. 2014. Disponível em <https://www.swgde.org/documents/Current%20Documents/SWGDE%20Capture%20of%20Live%20Systems> Acesso em: 13 set. 2018.

UCHÔA, K. C. A.; ALVES, R. M. Introdução à Cibercultura. Lavras: UFLA/FAEPE, 2002. Curso de Pós-Graduação Lato Sensu (Especialização) em Administração de Redes Linux.

U. S. DEPARTMENT OF JUSTICE. Electronic crime scene investigation: A guide for first responders. 2. ed. Washington: 2008. Disponível em <https://www.ncjrs.gov/pdffiles1/nij/219941.pdf> Acesso em: 13 set. 2018.

VIANNA, T. L. Fundamentos de Direito Penal Informático. Rio de Janeiro: Forense, 2003.