INVESTIGAÇÃO FORENSE JUDICIAL

Luísa Emiko MOMII[1]
Sérgio Tibiriçá AMARAL[2]

.

RESUMO: A investigação forense judicial visa, por intermédio dos instrumentos e procedimentos previstos na legislação vigente no País, propiciar provas para o convencimento da existência do delito e sua autoria. O art. 158 do Código de Processo Penal norteia sobre os crimes que deixam vestígios e a necessidade do exame do corpo de delito direto ou indireto, a fim de comprovar a conduta delituosa. Nos casos de invasão de sites de Internet, muitas vezes estes invasores experientes não deixam rastros de sua ação impossibilitando a verificação dos modos de operação desses ataques, que podem alterar uma informação em sites de Internet ou deixar um serviço fora do ar ou obter informações indevidas. Se houver vestígios desses crimes deixados em arquivos de logs nos equipamentos invadidos é possível iniciar uma investigação a fim de comprovar o fato delituoso e sua possível autoria. A perícia é um dos meios de prova regulados de modo expresso pela lei sendo necessário observar o que declara a Constituição Federal de 1988 no art.5º, LVI: "inadmissíveis, no processo, as provas obtidas por meio ilícitos". As ferramentas utilizadas pela perícia computacional deverão estar devidamente licenciadas, pois caso isso não ocorra, a utilização das mesmas será considerada como prova obtida por meio ilícito.Algumas provas somente serão possíveis de serem realizadas mediante mandado judicial, pois verificarão arquivos de outras empresas para reproduzir o percurso utilizado pelo invasor.

Palavras-chave: Invasão de sites de Internet, Investigação Forense, Direito Eletrônico

---

[1] Discente do curso de Direito das Faculdades Integradas "Antônio Eufrásio de Toledo" de Presidente Prudente.
[2] Orientador e coordenador do Grupo de Estudo e Pesquisa Estado e Sociedade

1 INTRODUÇÃO

Os progressos tecnológicos e facilidades decorrentes na área da Informática, assim como todas as descobertas científicas, podem ser utilizadas para o benefício da sociedade promovendo a divulgação de informações e conhecimentos de forma mais rápida. Esses progressos, no entanto, podem também ser usados de forma ilegal e maléfica. Essa nova tecnologia pode servir para divulgação de idéias preconceituosas, invasão de privacidade e até mesmo para a efetivação de fraudes.

A Internet tem sido um grande instrumento de divulgação de conhecimentos sobre vários assuntos. É igualmente importante para a democratização e divulgação das mais variadas mensagens relativas à manifestação do pensamento, bem como para a ampliação de serviços, interligando as pessoas em todo o mundo. Ao mesmo tempo, a "rede" tem sido uma das ferramentas utilizadas pelos "hackers"[3] para invasão de sites, a fim de obter informações sigilosas e promover quebra de sigilo para fraudar serviços bancários ou empresariais.

Algumas vezes, a invasão não tem o objetivo causar prejuízo financeiro ou moral, mas é feita por diversão com o intuito de mostrar a habilidade do "hacker" dentro da comunidade ou de ganhar notoriedade entre o seu grupo social.

Nos casos de invasão de sites de Internet, tanto por fraudes, como sem outros motivos há uma grande dificuldade para obter provas concretas sobre a consumação do fato, que configura o crime. Analisaremos, inicialmente os vestígios e os indícios destas invasões. Posteriormente, a realização da prova pericial, que poderá servir de subsídio à conclusão da ocorrência do delito.

As invasões dos sites de Internet podem ser executadas por intermédio de ataques a aplicações Web como os sistemas de compra e venda, validações de cartão de crédito, páginas de empresas, noticiário e ocorrem na autenticação de um

[3] Vasconcelos,2000, p.55.

usuário, ataques criptográficos, ataques de sessão, envio de códigos maliciosos não esperados, estouro de memória, etc.

O ataque de autenticação de um usuário é aquele realizado com uma injeção de SQL[4] que pode modificar desde o conteúdo da página até a mudança de dados no banco de dados da empresa. O ataque de sessão ocorre quando um hacker entra no sistema e acessa o estado de sessão de outra pessoa e se comporta como se fosse a outra pessoa, se esta sessão possuir dados pessoais como o cartão de crédito, é possível imaginar os estragos que poderão ser realizados. O tipo mais comum de estouro de memória é o buffer overflow. Ocorre quando o buffer passa a armazenar uma quantidade maior de dados do que sua capacidade permite, possibilitando executar programas indesejáveis na área de memória que foi ultrapassada. Se um usuário mal-intencionado conseguir explorar uma vulnerabilidade de buffer overflow de modo eficiente, poderá executar, mesmo a distância, qualquer tarefa de sua escolha e tomar controle total do computador afetado. Não serão considerados neste artigo a utilização de e-mails que tentam induzir a vítima a clicar em links falsos para captura de dados como login e senha ou envio de códigos maliciosos como os “cavalos de tróia” que ficam observando a máquina da vítima e enviando as informações ao invasor, uma vez que não são ataques diretos ao site de Internet e sim uma forma de obtenção de dados de terceiros que possibilitam acessar informações com a identificação verdadeira do usuário atacado impossibilitando a detecção de qualquer anormalidade do ponto de vista tecnológico.

2 VESTÍGIOS E EVIDÊNCIAS

Segundo o art.158 CPP, “Quando um crime deixar vestígios é indispensável o exame de corpo de delito direto, ou indireto, não podendo suprí-lo a confissão do acusado”, sendo o exame de corpo de delito elaborado por peritos para se comprovar a materialidade do crime, sob pena de nulidade durante o processo crime. O exame destina-se à comprovação por perícia dos elementos objetivos do

[4] Structured Query language – linguagem padrão utilizada para manipular dados de um banco de dados.

tipo, principalmente ao evento produzido pela conduta delituosa[5]. Busca encontrar provas atinentes a outros aspectos, como a materialidade do fato.

O termo vestígio significa um sinal que homem ou animal deixa com os pés no lugar por onde passa; rastro, rasto, pegada, pista. A existência desses vestígios pode tornar-se uma evidência de que houve o delito.

Vestígio é todo objeto ou material bruto constatado e/ou recolhido em um local de crime para análise posterior. Já a evidência é o vestígio depois de feitas as análises, onde se constata técnica e cientificamente a sua relação com o crime.

Nos casos de invasão de sites de Internet a busca de vestígios começa por uma análise nos arquivos de registro (logs) do equipamento afetado pelo crime. Por intermédio de uma checagem ou varredura desses arquivos é possível verificar os passos adotados pelo hacker. Importante salientar também que após a invasão, os autores tentam alterar estes arquivos para “esconder seus vestígios”. Uma das formas de verificar se o arquivo foi alterado é o checksum[6], que é uma soma de verificação gerado por um algoritmo matemático devendo ser executado após a instalação inicial dos softwares necessários em um equipamento. Isto permite que se determine se dois arquivos são idênticos em momentos distintos, ou seja, se houve modificação no arquivo. O ideal é armazenar em outra máquina as somas de verificação dos arquivos do modo que se encontravam no sistema antes da invasão, mantendo assim uma possibilidade de assegurar que mesmo com a modificação ou exclusão dos arquivos originais seja possível confrontá-los com os do outro equipamento.

Um outro elemento principal na determinação da integridade do arquivo são suas permissões. Quando criamos um arquivo ou um programa executável é necessário para sua utilização que o usuário privilegiado dê permissões para outros usuários a fim de que estes possam utilizar estes recursos. Deste modo se estas permissões estiverem alteradas podem indicar uma alteração na integridade do arquivo.

Hackers experientes removerão as linhas individuais dos arquivos de registro que mostrem seu acesso indevido, enquanto um iniciante tentará excluir

[5] Mirabete, 2002, p.478.
[6] Hatch, 2002, p.42.

todos os registros. Esses recursos só estarão disponíveis através de um ataque a sua máquina como usuário privilegiado que possui permissões de modificar os arquivos existentes em sua instalação.[7]Uma das formas de evitar a destruição destes vestígios é propagar estes arquivos de registro em outros equipamentos.

A análise desses registros pode levar ao indício do responsável pelo delito. Em contrapartida a inexistência desses vestígios impossibilita qualquer comprovação da invasão de sites de Internet.

3 INDÍCIOS

O indício é aquele argumento probatório indireto que deduz o desconhecido do conhecido por meio da relação de causalidade. Os indícios podem ser de duas espécies: os necessários, que revelam uma determinada causa; e os contingentes de probabilidade, que apresentam maior convergência de motivos para crer que para não crer no fato. Portanto, quando há um nascimento de uma criança supõe-se que houve um parto anterior a este considerado como indício necessário.

Os indícios contingentes verificam todas as probabilidades por meio de um raciocínio lógico. Um fato que pode indicar uma causa, só pode provar seu efeito de modo mais ou menos provável, pois no campo das coisas contingentes, causas que devam produzir necessariamente um determinado efeito não existem. Como as manchas de sangue encontradas nas vestes de uma pessoa após a ocorrência de um homicídio serão um indício contingente da culpabilidade desta pessoa.

O indício é uma expressão, utilizada no meio jurídico, que significa cada uma das informações (periciais ou não) relacionadas com o crime.

A existência de um indício não é causa probatória do delito. É necessário considerar que estes indícios podem ser modificados a fim de incriminar o outro para proveito próprio ou alheio, bem como para prejudicar outrem ou por mera brincadeira.

---

[7] Hatch,2002,p.277 e segs.

Mesmo que as análises dos caminhos percorridos pelo invasor indiquem um determinado indivíduo isto não é o bastante para afirmar sua autoria do delito, pois alguns hackers mais experientes podem utilizar a técnica de “IP Spoof“[8] ou de “man-in-the-middle”[9] que mascaram o verdadeiro invasor do equipamento. A comunicação entre os equipamentos ocorre com a transmissão de dados, via um protocolo de comunicação (TCP/IP, IPX/SPX), que envia dados de um endereço (IP) de origem (remetente) a um endereço (IP) de destino (destinatário). Quando o destinatário (IP) resolve a solicitação encaminha para o remetente (IP), invertendo seu cabeçalho, ou seja, o destinatário passa a ser origem e o remetente passa a ser destinatário. Essas comunicações com seus endereços e solicitações, normalmente são registrados em um arquivo de log. O IP spoofing é uma técnica de subversão de sistemas informáticos que consiste em mascarar (*spoof*) pacotes IP (Internet Protocol) com endereços remetentes falsificados, ou seja, o verdadeiro remetente tem endereço diverso do que consta no pacote enviado. Já o “man-in-the-middle“ ocorre quando uma máquina se coloca entre os dois equipamentos que se comunicam, sem interromper o protocolo de comunicação, mas capturando todos estes pacotes de comunicação. Este equipamento simula ser outro, ou seja, se configura com o endereço MAC (Media Access Control) de outro e passa a receber todos os pacotes transmitidos para este e reencaminha ao IP verdadeiro para que este não perceba que está sendo interceptado. Esta simulação é possível, pois para a transmissão dos dados o TCP necessita do ARP para descobrir qual é o endereço MAC de destino, transmitindo assim a solicitação. Estas trocas de informações não são registrados em arquivos de log, sendo somente possíveis de verificar através de softwares que analisem o comportamento destes pacotes na rede.

Estas técnicas podem conduzir a autoria dos ataques a equipamentos que foram forjados ocultando o verdadeiro autor do delito que modifica o endereço de seu equipamento (IP) para outro, ou simula ser outro equipamento.

[8] http://pt.wikipedia.org/wiki/IP_spoofing
[9] Hatch, 2002, p. 199.

4 PROVA

A prova é o instrumento por meio do qual se forma a convicção do Juiz a respeito da ocorrência ou inocorrência dos fatos controvertidos no transcorrer de um processo.[10] É com base nas provas, que o magistrado deve deferir o direito no caso concreto. O Código de Processo Penal implicitamente adota o princípio da liberdade dos meios de prova (Art.155 CPP) e o Código de Processo Civil estabelece que todos os meios legais, desde que moralmente legítimos são hábeis para provar a verdade dos fatos (Art. 332 CPC).

Os meios de prova regulados de modo expresso pela lei são: prova documental, testemunhal, pericial, inspeção judicial, etc. É importante lembrar que a Constituição de 1988, declara “inadmissíveis, no processo, as provas obtidas por meio ilícito” (art.5º, LVI).

Para que um crime seja atribuído como fato certo a um imputado, é preciso provar que se deu o fato criminoso e que este evento foi causado pela ação do imputado ou outros sobre os quais exerceu influência à vontade do imputado, ou seja que houve subjetividade exterior criminosa e que esta ação ou influência sobre a ação foi animada de intenção criminosa.

A prova pericial, portanto, tem gênese quando diante de fatos complexos, onde o juiz não possui conhecimentos técnicos e científicos suficientes ao esclarecimento do fato. Realiza-se a perícia através de exames, vistorias e avaliações, sejam estas judiciais, extrajudiciais ou informais, por intermédio de um especialista no ramo do saber técnico ou científico em questão. Assim, é de cabal importância a produção probatória por meio pericial para a solução das mais diversas lides que tramitam nos foros estaduais e federais, como ocorre nos casos de invasão de sites de Internet.

Há diversas formas utilizadas para averiguar o caminho utilizado pelo hacker na invasão de sites da Internet, como análise de logs dos servidores de Web atacados e firewalls a fim de obter o endereço IP e horário de origem e a partir daí realizar pesquisas em sites como Registro.br ou outros que regulam os endereços

[10] Cintra, 2004, p. 349.

de Internet. Há também a possibilidade de utilizar softwares chamados de IDS (Intrusion Detection System)[11], que analisam comportamentos fora do padrão da rede e também registram informações a respeito das mesmas.

Estas ferramentas deverão estar devidamente licenciadas caso contrário serão consideradas provas obtidas por meio ilícito. Algumas provas somente serão possíveis de serem realizadas mediante mandado judicial, pois verificarão arquivos de outras empresas para reproduzir o percurso utilizado pelo invasor.

Para provar a autoria do delito é necessário verificar os possíveis meios utilizados pelo invasor. Algumas vezes é preciso periciar outro computador pessoal a fim de averiguar se este equipamento foi invadido pelo hacker utilizando este para o ataque principal.

Estes caminhos percorridos pelo invasor podem estar contidos em equipamentos de outros países, necessitando da colaboração de organismos internacionais.

Toda invasão de sites de Internet com a intenção de modificar ou obter informações indevidas pode ser considerada de intenção criminosa.

Há várias ferramentas que possibilitam recuperar os dados mesmo que estes sejam apagados do Hard Disk, salientando que somente é possível esta recuperação desde que a área apagada não seja sobrescrita por outros dados.

5 A PERÍCIA E O PERITO

O Código de Processo Penal no art.159 estabelece as regras para realização das perícias nos casos admissíveis de tais provas. A perícia pode ser judicial que é realizada em processo judicial, e extrajudicial que não é realizada em processo judicial. O Art.420 do CPC define que a prova pericial consiste em exame, vistoria ou avaliação que poderá ser indeferida quando a prova do fato não depender do conhecimento especial de técnico; for desnecessária em vista de outras provas

[11] McClure,2003, p.177-178,513,546.

produzidas; a verificação for impraticável. O exame é a inspeção feita por perito sobre pessoas e coisas móveis e semoventes, inclusive documentos e escritas comerciais, a vistoria é a verificação que o perito faz sobre imóveis e a avaliação é o exame pericial designado a verificar o valor do objeto, de alguma coisa ou obrigação, estimado em valor.

A perícia, por via de regra, importa sempre em exame que precisa ser realizado por técnicos, isto é, por perito ou pessoas hábeis e conhecedoras da matéria, que se refere.

A perícia, segundo princípio da lei processual, é, portanto, a medida que vem mostrar o fato, quando não exista meio de prova documental para mostrá-lo, ou quando se quer esclarecer circunstâncias, a respeito dele, que não sejam perfeitamente definidas.

O perito é um apreciador técnico que auxilia o juiz com o fim de fornecer dados instrutórios de ordem técnica e proceder à verificação e formação do corpo de delito. São considerados “auxiliares da justiça”, sujeitando-os à “disciplina judiciária” e à “suspeição” dos Juízes[12]. (Art.275,280 CPP). Em regra os exames periciais devem ser realizados por peritos oficiais, que desempenham suas funções independentemente de nomeação da autoridade policial ou juiz, pois são cargos providos pela lei. Na ausência de peritos oficiais, o exame deve ser realizado por pessoas idôneas portadoras de diploma de curso superior que possuam habilitação técnica à natureza do exame. Estes devem prestar o compromisso de bem e fielmente desempenhar o encargo, embora a ausência deste compromisso constitua mera irregularidade.

Com a redação dada no caput do art. 159 CPP é obrigatório que o laudo seja elaborado por dois peritos oficiais e, na ausência destes, dois peritos não oficiais.

O Código de Processo Civil no art.145 estabelece que quando necessários os peritos serão escolhidos entre profissionais de nível universitário, inscritos no órgão de classe competente, sendo esta a comprovação de sua

[12] Situação, expressa em lei, que impede os juízes, representantes do Ministério Público, advogados, serventuários ou qualquer outro auxiliar da Justiça de, em certos casos, funcionarem no processo em que ela ocorra, em face da dúvida de que não possam exercer suas funções com a imparcialidade ou independência que lhes competem. Os peritos estão sujeitos a impedimentos e suspeições como parentesco,consangüinidade, amizade íntima ou inimizade capital, herdeiro presuntivo, donatário ou empregador, ser o periciante seu cliente.

especialidade na matéria a ser examinada. Na ausência destas condições, a indicação desses peritos será de livre escolha do juiz.

O perito na invasão de sistemas computacionais necessita possuir conhecimentos específicos em Arquitetura de Computadores, Redes de Computadores, Sistemas Operacionais e Segurança da Informação. Nem sempre um profissional da área de Informática possui os conhecimentos técnicos necessários para realizar tal perícia, pois além dos conhecimentos gerais de sua formação, há a necessidade de conhecimentos específicos e especializados que podem não ser tratados nas formações superiores da área de Informática. Estes também não possuem um órgão de classe competente, pois a profissão não está legalmente regulamentada.

Segundo o art.5º, XIII, CF/88 “é livre o exercício de qualquer trabalho, ofício ou profissão atendidas as qualificações profissionais que a lei estabelecer”. Algumas profissões possuem regulamentação como os advogados, engenheiros, médicos, etc. Estas leis regulam a forma de atuação de um profissional numa área de conhecimento, a instrução necessária, a necessidade de inscrição em um órgão de classe competente para o exercício da profissão.

O órgão que vem discutindo a regulamentação da profissão na área de Informática é a Sociedade Brasileira de Computação (SBC) desde 1978. A SBC consolidou sua posição institucional em relação a esta questão pela formulação dos seguintes princípios, que deveriam ser observados em uma eventual regulamentação da profissão: Exercício da profissão de Informática deve ser livre e independer de diploma ou comprovação de educação formal; nenhum conselho de profissão pode criar qualquer impedimento ou restrição ao princípio acima; a área deve ser Auto-Regulada. Outros órgãos de classe tentaram incluir os profissionais de Informática em sua área, como os administradores, engenheiros, mas a SBC interviu e isto não foi aprovado.

6 DO EXAME DO CORPO DE DELITO E DAS PERÍCIAS EM GERAL

Corpo de delito significa aquilo que representa a exteriorização material e a aparição física do delito ligados a consumação do próprio crime[13].Como o cadáver no crime de homicídio, os ferimentos nas lesões corporais, a moeda e a cédula falsa no crime de falsificação de moeda, o escrito injurioso no libelo difamatório. A figura física do delito pode ser representada em fatos permanentes ou transitórios.Os fatos transitórios são aqueles que não deixam vestígios permanentes, necessitando da recordação das testemunhas sobre o fato ocorrido, como ocorre nos casos de injúria verbal. Neste caso com o avanço da tecnologia torna-se possível gravar a voz do agente, evidenciando-se assim a materialidade do crime. Ao contrário os fatos permanentes são os que deixam vestígios permanentes. Por isso a ciência e a prática cogitam o corpo de delito nos fatos permanentes.

O exame do corpo de delito, portanto é a perícia realizada sobre o corpo de delito. Segundo o art.158 CPP, existem dois tipos de exame do corpo de delito. O exame de corpo de delito direto é aquele realizado sobre o próprio corpo de delito, como a necropsia sobre o cadáver.O exame de corpo de delito indireto, conforme dispõe o art.167 CPP, será realizado quando os vestígios desaparecerem podendo a prova testemunhal suprir-lhes a falta. Estes vestígios são aqueles que nunca existiram nos autos do processo ou aqueles que embora pudessem ser apurados na época oportuna não o foram. A prova testemunhal descreverá com exatidão a ocorrência do delito, sendo quando possível suficientemente esclarecedor e preciso a respeito da prova material do crime.

O art.158 CPP, tornando indispensável o exame de corpo de delito nas infrações penais que deixam vestígios, não podendo suprí-lo, sequer a confissão do acusado, afastou-se do princípio de livre convicção motivada vigente em nossa lei processual. A lei nº 9099 de 26 de setembro de 1995 estabelece em seu art.77 § 1º que o Ministério Público para o oferecimento da denúncia não dependerá do exame de corpo de delito quando a materialidade do delito estiver aferida por boletim de socorro médico ou prova equivalente.

---

[13] Malatesta, 1996, p.604

A perícia deve ser determinada por autoridade policial logo que tiver conhecimento da prática da infração penal (art.6, VII CPP) ou até a conclusão do inquérito, bem como pelo juiz, durante a instrução, ou mesmo a requerimento das partes na denúncia ou queixa ou no prazo da defesa prévia, ou ainda no final da instrução[14].

O laudo pericial será elaborado pelos próprios peritos, composto de um preâmbulo com nome dos peritos, títulos, objeto da perícia, de uma exposição contento a narração minuciosa do que foi observado, de uma discussão com a análise ou crítica do observado, com argumentação do parecer e de uma conclusão com respostas aos quesitos formulados segundo o art.160 CPP.

O local onde houver sido praticado o crime deve ser preservado (art.169 CPP) e deverá ser guardado material para necessidade de novas perícias (art.170 CPP).

O exame de corpo de delito nos casos de invasão de sites de internet deve ser executado em réplicas dos arquivos de log originais e em equipamentos distintos dos periciados com o propósito de não alterar os dados através de uma investigação não-intrusiva, pois o ato de ligar ou desligar um equipamento altera vários arquivos do sistema operacional modificando as informações contidas nos mesmos. A verificação dos setores livres do Hard-Disk serão úteis para a comprovação da ação delituosa uma vez que alguns dados modificados ou excluídos ainda poderão estar gravados nestes setores. Método este, utilizado na perícia da “Análise do Sistema de Votação Eletrônica do Senado Federal (SVE-SF)”, conhecido como “Painel do Senado”. A perícia deverá verificar as possibilidades de violação do equipamento examinado a fim de comprovar se não há possibilidades de modificação destes dados por meio externo. Deve também assegurar que estes arquivos analisados são compatíveis com os originais, através de vários métodos existentes como o checksum, hash e outros. Vários sites na Internet divulgam os procedimentos necessários para a perícia computacional forense.[15]

[14] Mirabete, 2002, p.479
[15] www.guiatecnico.com.br/PericiaForense; www.codigoseguro.com.br/CodigoSeguro.

7 DO VESTÍGIO Á PROVA

O objetivo do exame de corpo de delito e das perícias em geral é extrair conclusões concretas sobre as circunstâncias e os fatos que perfazem o corpo de delito, a fim de servirem de fundamentação das decisões judiciais.

O exame ou diligência ou qualquer medida realizada num computador que não tenha como finalidade a descoberta de um fato, que dependa de habilidade técnica, não constitui perícia. A perícia quer sempre estabelecer um vestígio ou uma prova.

Adotou a lei o princípio do livre convencimento motivado ou persuasão racional, segundo o qual o juiz forma sua convicção pela livre apreciação da prova. Sequer o laudo pericial vincula a decisão do juiz, mas sua sentença tem por obrigatoriedade a fundamentação, sob pena de nulidade (art.93, IX, CF/88). Embora fundado no “livre convencimento” impõe-se que sua convicção seja demonstrada mediante a análise da prova constante dos autos.

No caso da invasão de sites de Internet a perícia computacional é necessária para estabelecer que existe a materialidade do crime, quais foram os caminhos percorridos pelo invasor tentando demonstrar a autoria do crime. Os softwares utilizados pelo invasor, códigos maliciosos, registros, dispositivos de busca de vulnerabilidades devem ser considerados. A análise dos arquivos de log visam determinar fatos; início e término do acesso, quais urls foram acessadas, como foi o login na rede, de onde foi efetuado o acesso, etc. Algumas precauções devem ser executadas, como: se o computador estiver desligado, não ligue, ou ao contrário, se estiver ligado não desligue; tire fotos visíveis de boa qualidade (monitor, computador (frente e atrás) e do local físico onde o computador ficava; capture dados voláteis (memória) se necessário. [16]

Apesar do alto nível de precisão da computação forense, a coleta de vestígios de forma errônea pode tornar ilícita esta prova, sendo possível que esta

[16] www.patriciapeck.com.br

contamine as demais (teoria dos frutos da árvore envenenada)[17] eliminando todas as chances no litígio judicial. Cabe ao perito, através de um laudo pericial claro, retirar o caráter dúbio desta prova.

Nos casos de invasão de sites não é possível a prova testemunhal, pois é difícil provar a autoria deste tipo de crime através desta prova. Muitas vezes, as empresas que sofrem este tipo de invasão permitem que o invasor continue agindo com a finalidade de pegá-lo praticando o crime.

8 FALSA PERÍCIA

A palavra perícia é de origem latina e tem como significado habilidade e saber. Na linguagem jurídica designa especialmente, em sentido lato, a diligência realizada ou executada por peritos, a fim de que se esclareçam ou se evidenciem certos fatos[18]. No caso, a pesquisa ou exame vai verificar acerca da verdade ou realidade de determinados fatos, por pessoas que tenham reconhecida habilidade ou experiência em computadores.

A perícia nos casos de invasão de sites procura nos vestígios comprovar a ocorrência do delito e também a autoria do mesmo. Através das análises dos logs ou recuperação de informações excluídas para recompor o trajeto do invasor, resguardando os dados originais a fim de não comprometer os vestígios iniciais.

O sujeito ativo do delito de falsa perícia é qualquer pessoa que como perito realize ação descrita no art. 342 do CP que consiste em fazer afirmação falsa, negar ou calar a verdade em processo judicial, policial ou administrativo. O perito que, em seu laudo, distorce a verdade, com o objetivo preciso de favorecer alguém a influir sobre a decisão judicial, mesmo que não atinja o fim desejado, pratica o crime de falsa perícia. O delito pode se praticado de forma comissiva quando o perito faz

[17] Teoria americana “fruits of posonous tree” que defende a tese de que havendo prova ilícita no processo, e se as demais provas somente foram possíveis a partir dela, a sua ilicitude contamina todas as demais. Embora os alemães Klaus Roxin e os espanhóis Cerezo Mir Puig, já falem no peso das provas. Em julgamento da Corte Alemã ao abordar a prisão de pedófilos com base em escuta clandestina estes acabam sendo condenados mesmo com uma prova ilícita, pois haviam raptado e matado crianças depois de abusar delas.

[18] De Plácido e Silva, Vocabulário Jurídico, p. 603.

afirmação falsa apresentando como verdade o que não é e de forma omissiva quando o agente cala ou oculta a verdade. O elemento subjetivo da conduta é o dolo enquanto vontade de realizar a perícia em desacordo com o que o agente tem ciência ou verificou em seu exame pericial. A conduta deixa de ser punível se antes da sentença o agente se retrata ou declara a verdade (art.342 § 2º CP).

A falsa perícia em invasão de sites pode ocorrer quando a perícia não confirma a ocorrência do delito quando este ocorreu, através de uma análise superficial dos dados. Também quando afirma a autoria do delito a um indivíduo não considerando que este na realidade pode ser vítima do verdadeiro autor, não verificando as vulnerabilidades do equipamento da vítima a ataques externos. Ainda pode ocorrer na falta de habilidade técnica para a realização adequada da perícia manipulando inadequadamente o equipamento contaminando a prova. Isto pode ser observado no Anexo I, como exemplo de uma falsa perícia, embora o caso envolvido seja de urna eletrônica violada. Há também neste anexo, o exemplo de uma perícia realizada no caso “Painel do Senado”, esta bem sucedida.

9 INQUÉRITO POLICIAL

O Inquérito Policial é o procedimento administrativo destinado a fornecer ao órgão da acusação o mínimo de elementos necessários a propositura da ação (art.4º CPP). Por ser procedimento administrativo não se aplicam ao inquérito policial os princípios processuais, mas é dever o controle de sua legalidade, impondo-se as garantias constitucionais específicos (art. 5º, LXIII a LXVII, CF/88).

Cabe a polícia judiciária, exercida pelas autoridades policiais a atividade de apuração das infrações penais e da autoria por meio do inquérito policial, preliminar ou preparatório da ação penal.O destinatário imediato do inquérito é o Ministério Público quando esta for uma ação penal pública ou o ofendido na ação privada para proposição da denúncia ou da queixa. É dever da autoridade policial conservar os elementos deixados pelo delito (art. 6º, I, CPP), recolher os objetos e provas que servirem para o esclarecimento do fato e suas circunstâncias (art. 6º, II e

III, CPP), determinar que se proceda o exame de corpo de delito e outras perícias que julgar necessário conforme o art. 158 a 184 CPP.

No caso em análise, a polícia judiciária irá apurar a invasão, determinando perícias se necessário para elucidar a autoria, a busca e apreensão de equipamentos, pesquisas a sites como Registro.Br ou outros que regulam os endereços de Internet, mandados judiciais para verificação em arquivos de log de empresas, para reconstituírem o caminho utilizado pelo invasor.

Segundo Plínio Sales,delegado da 4ª Delegacia da DIG (Delitos nos Meios Eletrônicos) do Departamento de Investigação sobre o Crime Organizado (DEIC), a investigação desse tipo de crime difere muito pouco daquela feita tradicionalmente. “Nós utilizamos a parte técnica para descobrir o IP de quem cometeu o delito. Depois, a investigação segue normalmente, como qualquer outra”. O problema é que essas informações nem sempre ficam registradas nos servidores e provedores que gerenciam o acesso à Internet. “Por lei, esses servidores não são obrigados a guardar essas informações. Além disso, eles também alegam problemas técnicos. Isso prejudica em muito o nosso trabalho, pois o criminoso pode permanecer anônimo”, alerta Onias Tavares de Aguiar, diretor do núcleo de Perícias de Informática do IC. Para a realização da perícia, de acordo com Onias, o núcleo de Perícias de Informática atende São Paulo inteiro e também alguns casos do interior. "Procuramos as provas – diretas ou indiretas – nos equipamentos de informática, como HDs (hard drive – a ‘memória’ do computador), cds, dvds e também servidores", esclarece. "Se o criminoso deixou alguma prova neles, nós iremos encontrar". O perito, que já está há cinco anos na direção do núcleo, diz que o IC conta com ótimos softwares para analisar os equipamentos. "Mesmo que o sujeito seja hacker, nós encontraremos as provas. Em 95% dos casos nós achamos alguma evidência",afirma.[19]

10 BUSCA E APREENSÃO

A autoridade policial deve apreender os instrumentos e todos os objetos que tem relação de causalidade com o delito, afim de que não desapareçam

[19] http://www.ssp.sp.gov.br/home/noticia.aspx?cod_noticia=8701

as provas do crime (art.6º, II, CPP). Os objetos e pessoas que podem ser objeto da busca e apreensão estão relacionados no art.240 do CPP, que será efetuado tanto pela autoridade policial como pelo juiz.Quando efetuada pela autoridade policial deverá ser realizada por mandado judicial na forma do art.243 CPP, no período diurno, salvo se o morador consentir que se realize a noite (art.245 CPP). Se efetuado pessoalmente pelo juiz não será necessária uma ordem judicial expressa. A busca e apreensão domiciliar visa a apreensão de objetos achados ou obtidos por meios delituosos, como o computador pessoal utilizado para cometer fraudes pela internet,material furtado, etc. A busca e apreensão pessoal é realizada em relação a própria pessoa, geralmente nos casos de crimes de porte de arma, quando o agente tem consigo (junto a seu corpo) arma de fogo.

A busca e apreensão pode ocorrer anteriormente a qualquer procedimento policial ou judicial pela autoridade que tem conhecimento da infração penal (art.6º, II, CPP) ou na hipótese de crime contra a propriedade imaterial, durante o inquérito policial, na fase de instrução criminal e durante a execução.

Há referências de diligência de busca e apreensão nos crimes contra a propriedade intelectual de programas de computador e sua comercialização (art.13 Lei nº 9609/98).

Nestes dias tem havido muitas discussões com relação a inviolabilidade do advogado, do seu local de trabalho e de seus instrumentos de trabalho como arquivos, pastas, computador, correspondências, etc., que estariam protegido pelo sigilo profissional, constantes no art. 133 da CF/88.

Segundo Luiz Flávio Gomes, em seu artigo “Limites à Inviolabilidade do Advogado e do Seu Escritório” [20] , em duas situações (pelo menos) o escritório do advogado pode ser objeto de busca e apreensão: (a) quando o advogado é o investigado (nesse caso, claro, ele não está no exercício da profissão); (b) quando nele se ingressa para apreender documento que constitua "elemento do corpo de delito" (CPP, art. 243, § 2º), delito esse praticado pelo advogado ou por qualquer outra pessoa (que seja seu cliente).Todo mandado de busca de apreensão, conseqüentemente, para que não seja expressão de abuso, facilmente reconduzível ao patamar da prova ilegítima, não está sujeito só aos limites formais atinentes à

[20] www.lfg.com.br/public_html/article.php?story=20050815152740883

competência para sua expedição, à atribuição para seu cumprimento etc.. O mandado de busca e apreensão, ademais, está ainda adstrito a duas individualizações absolutamente necessárias: (a) a subjetiva (quem é a pessoa ou pessoas investigadas) e (b) a objetiva (qual é o fato objeto da investigação).

A busca e apreensão do computador pessoal utilizado para cometer fraudes é necessário a fim de fazer uma perícia nos arquivos existentes no equipamento. Normalmente estes arquivos de log são do tipo texto que são facilmente modificáveis com a manipulação de editores de texto. Em um computador há dois tipos de memória, a volátil que deixa de existir quando o equipamento é desligado e a outra permanente que são os dados gravados no Hard Disk. Um cuidado essencial na busca e apreensão do equipamento é copiar a memória volátil (RAM) e os arquivos temporários se o equipamento estiver ligado, pois alguns dados somente estarão neste tipo de memória e não nos Hard Disk.

11 CONCLUSÕES

A investigação forense judicial visando comprovar a ocorrência do delito e sua possível autoria inicia pela busca de vestígios deixados no local do crime e que depois de verificados tecnicamente poderão constatar sua relação com o crime. Todos os vestígios encontrados serão indícios da ocorrência do crime que deverão ser analisados a fim de comprovar a relação de causalidade do delito e sua autoria. Nem sempre estes indícios indicarão o verdadeiro autor do delito, assim o exame de corpo de delito visa produzir provas do crime a fim de que o julgador possa deferir o direito com fundamentação nestas provas.

Nos casos de invasão de sites o exame de corpo de delito, deve ser realizado com a técnica não intrusiva para preservar os dados originais e não causar modificações que poderão alterar dados importantes dos arquivos periciados. Este exame será realizado por peritos tecnicamente habilitados que ao final elaborarão um laudo pericial com suas análises do que foi observado e respostas aos quesitos formulados. Já a falsa perícia não observa todas as possibilidades ou circunstâncias

da ocorrência do delito, ou o faz de maneira indevida contaminando a prova tornando a ilícita.

A dificuldade de comprovação da autoria do crime, conforme disse Onias Tavares de Aguiar, diretor do núcleo de Perícias de Informática do IC, pela falta de legislação que obriga os servidores e provedores de Internet a manterem as informações dos arquivos de log podem deixar impunes os autores dos delitos na área de Informática, promovendo assim um crescimento deste tipo de delito. Aliado a isto temos desenvolvedores de sites de Internet que por falta de informação técnica permitem falhas que possibilitam o ataque de hackers. É importante salientar que com o avanço da tecnologia a cada dia novas formas de invasão são criadas e efetuadas às vezes sem o conhecimento da vítima. Portanto, é necessária uma legislação que contemple estas mudanças que ocorrem com o uso da Internet, lembrando que isto envolve os princípios de territorialidade e extraterritorialidade, uma vez que estes delitos podem utilizar computadores no mundo todo.

No entanto o avanço da Informática nos vários setores da sociedade é indispensável para o desenvolvimento e as facilidades advindas da tecnologia. A economia de tempo, de recursos financeiros e a facilidade de comunicação são fatores que nos tempos atuais não podem ser desconsiderados como observamos nos casos de audiência dos presos por teleconferência, atos processuais que podem ser obtidos pela Internet, pagamento de contas pela Internet, etc. Não podemos deixar de utilizar uma tecnologia com o temor do risco nele envolvidos, mas temos que prevenir os riscos possíveis de serem antecipados.

11 REFERÊNCIAS BIBLIOGRÁFICAS

Bustamante, Ricardo; Sodré, Paulo César. **Ensaios Jurídicos**. Vol.3 – Rio de Janeiro: Instituto Brasileiro de Atualização Jurídica IBAJ, 1996.

Cintra, Antônio Carlos de Araújo; Grinover, Ada Pellegrini; Dinamarco, Candido Rangel. **Teoria Geral do Processo**. 20. ed.rev. e atual – São Paulo: Ed. Malheiros, 2004.

Guelfi, Airton; Bernal, Volnys Borges. **Investigação Forense Judicial** – Artigo

Hatch, Brian; Lee, James; Kurtz, George. **Hackers Expostos** – Linux. São Paulo: MAKRON Books, 2002.

Malatesta, Nicola Framarino Dei. **A Lógica das Provas em Matéria Criminal**. 3ª ed. – Campinas: Ed. Bookseller, 1996.

McClure, Stuart; Scambrav, Joel; Kurtz, George. **Hackers expostos**: segredos e soluções para a segurança de redes. 4.ed – Rio de Janeiro : Ed. Campus , 2003.

Mirabete, Julio Fabrini. **Código de Processo Penal Interpretado**. 9ª ed. – São Paulo: Ed. Atlas, 2002.

Prado, Luiz Regis. **Falso Testemunho e Falsa Perícia**. 2ª ed.rev.e atual – São Paulo : Ed. Revista dos Tribunais, 1994.

Vasconcelos, Márcio José Accioli de. **A Internet e os Hackers** : Ataques e Defesas / M@RCIO. 5. ed.rev. e atual – São Paulo: Ed. Chantal, 2000.

Rosa, Marcos Valls Feu. **Perícia Judicial**: Teoria e Prática. Porto Alegre: Ed. Sergio Antonio Fabris, 1999.