VERA KAISER SANCHES KERR

A DISCIPLINA, PELA LEGISLAÇÃO PROCESSUAL PENAL BRASILEIRA, DA PROVA PERICIAL RELACIONADA AO CRIME INFORMÁTICO PRATICADO POR MEIO DA INTERNET

São Paulo
2011

VERA KAISER SANCHES KERR

A DISCIPLINA, PELA LEGISLAÇÃO PROCESSUAL PENAL BRASILEIRA, DA PROVA PERICIAL RELACIONADA AO CRIME INFORMÁTICO PRATICADO POR MEIO DA INTERNET

Dissertação apresentada à Escola Politécnica da Universidade de São Paulo para obtenção do título de Mestre em Engenharia

Área de Concentração:
Engenharia Elétrica–Sistemas Eletrônicos

Orientador: Prof. Livre-Docente
Pedro Luis Prospero Sanchez

São Paulo
2011

Este exemplar foi revisado e alterado em relação à versão original, sob responsabilidade única do autor e com a anuência de seu orientador.

São Paulo, 05 de setembro de 2011.

Assinatura do autor _____

Assinatura do orientador _____

FICHA CATALOGRÁFICA

Kerr, Vera Kaiser Sanches
A disciplina, pela legislação processual penal brasileira, da prova pericial relacionada ao crime informático praticado por meio da internet / Vera Kaiser Sanches Kerr. -- ed. rev. -- São Paulo, 2011.
135 p.

Dissertação (Mestrado) – Escola Politécnica da Universidade de São Paulo. Departamento de Engenharia de Sistemas Eletrônicos.

1. Crime por computador. 2. Engenharia Elétrica. 3. Pericias (Processo penal). I. Universidade de São Paulo. Escola Politécnica. Departamento de Engenharia Elétrica Sistemas Eletrônicos. II. t.

DEDICATÓRIA

Dedico este trabalho a Jesus, Senhor da minha vida e luz do meu caminho;
aos meus pais, Oswaldo (em memória) e Maria do Carmo, por investirem em mim;
ao Davi pelo amor incondicional e à Sofia, tesouro da minha vida.

AGRADECIMENTOS

Aos professores Volnys Bernal e Edson Satoshi Gomi pela orientação tão necessária.

Ao Professor Sidnei Colombo Martini, pelo apoio efetivo.

Aos amigos Juliana e Renato, pela generosidade em compartilhar conhecimento e informação.

Ora, a fé é a certeza de coisas que se esperam,
a convicção de fatos que se não vêem.
(Hebreus 11:1, Bíblia Sagrada)

RESUMO

Com o advento e o desenvolvimento da tecnologia da informação e principalmente da Internet, as infrações penais ganharam novo ambiente para sua prática. A vertente inovadora referente a esses ilícitos é o meio digital, também denominado meio eletrônico. Ocorre que, o crime informático praticado por meio da Internet é do tipo que deixa vestígio, sendo obrigatório, para se estabelecer a autoria e materialidade do ato delitivo, o exame do corpo de delito, exame este realizado por meio de perícia em meios computacionais. Embora a prova pericial seja regrada pelo Código de Processo Penal brasileiro, uma vez que se trata de meio de produção de prova típico, este regramento é extremamente genérico, não prevendo, portanto, regramento específico quanto à prova pericial em meios computacionais relacionada ao crime informático praticado por meio da Internet. Desta forma, o presente trabalho objetiva analisar a prova pericial em meios computacionais relacionada ao crime informático praticado por meio da Internet, como meio de produção de prova típico, em função do avanço tecnológico, e discutir a viabilidade de sua disciplina, de forma específica, pela legislação processual penal brasileira. A importância de se ter instrumentos legais que regulem a matéria, justifica-se não somente quanto às investigações em âmbito nacional mas também, em âmbito internacional, o que facilitará a adesão do Brasil a Tratados e Convenções Internacionais que regulam investigações conjuntas entre Estados soberanos, visto que o crime informático praticado por meio da Internet, na maioria dos casos, tem caráter transnacional.

Palavras-chave: Crime informático. Internet. Perícia em meios computacionais. Legislação Processual Penal brasileira.

ABSTRACT

With the advent and development of information technology and especially of the Internet, criminal offenses have gained a new practice environment. The innovative aspect related to such illicits is the digital media, also called electronic media. As it happens, computer crime committed through the Internet is the type that leaves evidence, being that it is mandatory, to establish the authorship and materiality of the criminal act, the examination of the corpus delicti. This examination is performed by experts in computational forensics. Although the expert examination is ruled by the Brazilian Code of Criminal Procedure, since it is a typical means of generating evidence, this procedure is extremely generic and does not foresee, therefore, specific procedures about expert examination in computer crime committed through the Internet. Thus, the present work aims to examine the expert evidence on computer media, computer-crime crime committed through the Internet as a means of typical evidence, as a function of technological progress, and discuss the viability of its discipline, specifically, by the Brazilian criminal procedure law. The importance of having legal instruments governing the subject is justified not only when investigations run at national level but also internationally, what will facilitate the adherence of Brazil to international treaties and conventions governing joint investigations between sovereign states, considering that computer crime committed through the Internet, in most cases, has a transnational nature.

Keywords: Computer crime. Internet. Computational Forensics. Brazilian Criminal Procedure Law.

SUMÁRIO

1. INTRODUÇÃO

Atualmente, no Brasil, a colheita[1] e custódia dos elementos de prova até o momento da realização da perícia em meios computacionais relacionadas ao crime informático praticado por meio da Internet, bem como a própria execução do exame pericial, tanto na fase do inquérito policial bem como na fase judicial, não raro, processam-se segundo critérios fixados pelo agente policial, no caso da colheita e custódia, ou pelo próprio perito, não atentando, muitas vezes, aos direitos e garantias constitucionais do acusado. Sem contar que o exame dos vestígios digitais[2], na maioria das vezes, é processado na mídia original, não observando qualquer metodologia relacionada à colheita e custódia da prova, bem como à realização do exame pericial propriamente dito, colocando em risco a integridade dos elementos de prova bem como a possibilidade de reprodução do exame pericial caso seja necessário.

> Como alguns exames podem alterar metadados de arquivos como data de acesso, data de modificação, etc., principalmente quando não temos todas as ferramentas necessárias ao exame, é extremamente recomendável que façamos mais de uma cópia da mídia de provas. Esse procedimento é particularmente útil no caso dos discos rígidos e possibilita exames com maior grau de liberdade e segurança. (COSTA, 2003, p.26).

Tais fatos ocorrem, entre outros motivos, em virtude das normas técnicas que veiculam boas práticas relacionadas à matéria serem normas infra-legais que, ao contrário das leis, estão na esfera da recomendação não sendo, portanto, auto-impositivas. Ademais, as normas legais vigentes e, portanto, de natureza cogente, expressam-se por meio de regramento genérico e ultrapassado, veiculado pelo

---

1 "O processo referente à Computação Forense consiste na Preparação, Aquisição, Preservação, Exame e Análise, e Comunicação. Entre essas etapas, a etapa de aquisição é um processo no qual os investigadores coletam evidências digitais e garantem a integridade das provas recolhidas no local do crime. Assim, a etapa de aquisição é o passo mais significativo para uma investigação eficiente." (LEE; KIM; LEE; LIM, 2005, p. 1, tradução nossa)

2 "A noção de vestígio digital significa "quaisquer dados digitais relevantes o suficiente para provar um crime em suporte informático e de rede. É um tipo de evidência física, incluindo os padrões de texto, foto, voz e imagem. Em outras palavras, suporte informático ou armazenamento eletromagnético na rede pode ser usado como prova de crime". (COSIC; BACA, 2010, p. 429, tradução nossa).

diploma processual penal pátrio, não tendo incorporado as mudanças na produção da prova relacionadas ao avanço tecnológico.

Importante registrar que, embora o Código de Processo Penal brasileiro tenha entrado em vigor em 1941, espelhando o regime autoritário no qual estava inserido, carecendo, portanto, de reforma estrutural compatível com o regime democrático, inaugurado com a Constituição de 1988, por questão de política legislativa, vem sofrendo, ao longo dos anos, mudanças pontuais. Recentemente, foram aprovados importantes projetos de lei, já em vigor, que trouxeram nova disciplina à prova e, por conseguinte , merecem ser analisados.

Ademais, estamos diante de um código que passou a viger muito antes da revolução tecnológica das últimas décadas, sendo imperativo alinhá-lo às mudanças tecnológicas que muito tem influenciado os meios de obtenção e de produção de prova, notadamente relacionados à tecnologia da informação e à Internet.

Além disso, no tratamento dispensado à matéria, parte da dificuldade encontrada pelos especialistas reside na imprecisão da terminologia utilizada, bem como numa não uniformização do conceito técnico-processual da prova, resultando em enunciados equivocados quanto aos textos legais e doutrinários e quanto à linguagem empregada na prática judiciária penal, refletindo diretamente na redação utilizada na elaboração de laudos periciais.

Outrossim, considerando que o ilícito informático praticado por meio da Internet, em muitos casos, é transnacional, exigindo investigação que envolve mais de um Estado soberano, há que se ter regras mínimas capazes de permitir colheita, preservação e armazenamento da prova, de forma conjunta, entre mais de um país[3].

1.1 Motivação

[3] "[...] como foi reconhecido já em 1989 pelo Conselho da Europa, o cibercrime é transnacional por natureza [...] O crime comum é visivelmente diferente do crime cibernético como um fenômeno. Sua natureza intangível e abstrata resulta em desafios significativos para o investigador forense. Enquanto um investigador forense experiente reconheceria as melhores práticas de conduta dentro de uma cena de crime tradicional, poucos reconhecem como estabelecer limites e selecionar o que é relevante nesse ambiente cibernético tão abstrato e intangível. Isso não é apenas um problema técnico, mas um importante problema sócio-cultural e de colaboração, que se torna ainda mais complexo devido à sua natureza transnacional." (BEDNAR; KATOS; HENNEL, p. 5, tradução nossa).

Como prova da pertinência e atualidade do tema em questão, constatam-se importantes iniciativas internacionais tais como: a Convenção de Budapeste, tratado internacional sobre crime cibernético, firmado em Budapeste, na Hungria, a 23 de novembro de 2001, que tem como objetivo a harmonização das legislações nacionais dos Estados membros da União Europeia em matéria de criminalidade cometida por estes meios, bem como facilitar a cooperação internacional e as investigações de natureza criminal, contando com mais de quarenta países signatários.

Há também a iniciativa da Organização das Nações Unidas (ONU), expressa em seu XII Congresso sobre Prevenção ao Crime e Justiça Criminal, ocorrido no período entre 12 a 19 de abril de 2.010 que, por meio da Declaração de Salvador[4], reafirmou seu compromisso em promover ações para auxiliar na normatização, não só em âmbito nacional, bem como em âmbito internacional, das questões relacionadas ao crime informático e sua investigação.

Em nível nacional, pode-se apontar o Projeto de Lei Substitutivo do senador Eduardo Azeredo, Projeto de Lei Susbtitutivo ao Projeto de Lei da Câmara nº 89 de 2003, Projeto de Lei do Senado nº 137 de 2000 e nº 76 de 2000, todos referentes a crimes informáticos e sua investigação, bem como o projeto de reforma do Código de Processo Penal – PLS 156/2009. Contudo, nenhum deles trata da disciplina da prova pericial em meios computacionais, nos termos propostos por este presente trabalho.

Por fim, importante registrar a iniciativa da ABNT (Associação Brasileira de Normas Técnicas) por meio da comissão intitulada “Comissão de Estudos Especiais de Ciências Forenses”, em andamento, que objetiva fixar normas de boas práticas referentes à prova pericial.

1.2 Objetivo

[4] Minuta da Declaração de Salvador sobre Estratégias Amplas para Desafios Globais: Sistemas de Prevenção ao Crime e Justiça Criminal e seus Desenvolvimentos em um Mundo em Transformação.

Dessa forma, em face do crescente avanço tecnológico e das novas demandas geradas pela criminalidade informática, a presente pesquisa objetiva analisar a prova pericial em meios computacionais relacionada ao crime informático praticado por meio da Internet, como meio de produção de prova típico, em função do avanço tecnológico e discutir a viabilidade de sua disciplina, de forma específica, pela legislação processual penal brasileira por meio da fixação de critérios mínimos de admissibilidade, em juízo, desse meio de produção de prova.

Busca-se, portanto, proporcionar maior segurança às partes no pleno exercício do contraditório e, ao magistrado, parâmetros válidos para sua decisão, visto que o resultado da prova pericial em meios computacionais relacionada ao crime praticado por meio da Internet, na maioria dos casos, tem sido elemento único na fundamentação de sentenças judiciais.

1.3 Escopo

Não se trata, no entanto, de se analisar a realização do exame pericial propriamente, sob a ótica do método técnico-científico, pois entre as habilidades esperadas do perito, inclui-se a capacidade de escolher a metodologia adequada a ser utilizada para a realização da perícia, com a devida fundamentação. Ademais, o método técnico-científico não está sujeito à regramento legal visto que se funda no conhecimento científico da época, passível de ser revisto, de tempos em tempos, dependendo da “última verdade” descoberta. Regrá-lo significa “engessar” a tecnologia.

O que se pretende é analisar a possibilidade de se disciplinar a colheita, preservação e armazenamento dos equipamentos e vestígios digitais a serem periciados e não o método técnico-científico adotado para a realização do exame pericial e analisar a possibilidade de se exigir que o laudo pericial seja fundamentado, apontando quais seriam os critérios norteadores da referida fundamentação.

1.4 Metodologia

Para o procedimento metodológico adotou-se a revisão bibliográfica, analisando-se juristas nacionais considerando tratar-se de pesquisa relacionada ao ordenamento jurídico pátrio, bem como a análise de artigos científicos internacionais relacionados à prova pericial, visto ser este meio de produção de prova essencialmente técnico sendo que sua análise extrapola os limites nacionais e, a título de ilustração, com o fim de fundamentar pontos conclusivos do trabalho, analisou-se três casos de crimes informáticos praticados por meio da Internet, respectivos laudos periciais e parecer técnico.

1.5 Organização do trabalho

Por fim, a presente dissertação compõe-se de dez capítulos. No capítulo um ocorre a introdução do tema contextualizando-o, delimitando seus objetivos, escopo, metodologia e a forma como o trabalho foi organizado. No capítulo dois examina-se os crimes informáticos em função de sua estreita relação com a perícia em meios computacionais. No capítulo três relata-se a evolução da processualística sobre a busca da verdade à luz das garantias constitucionais do acusado. No capítulo quatro aborda-se os aspectos gerais sobre a disciplina da prova no processo penal brasileiro, contextualizando-a ao tipo de sistema processual ao qual está inserida, apontando seus reflexos à luz das recentes mudanças legislativas ocorridas. No capítulo cinco trata-se dos conceitos fundamentais e da terminologia da prova, preponderantemente no discurso técnico-jurídico, apontando as classificações mais importantes. No capítulo seis analisa-se os meios de prova típicos, especialmente a prova pericial e sua disciplina pelo Código de Processo Penal brasileiro. No capítulo sete investiga-se a perícia em meios computacionais. No capítulo oito comenta-se alguns casos envolvendo crimes informáticos praticados por meio da Internet e respectivos exames periciais tecendo algumas considerações sobre os mesmos. No capítulo nove discute-se alternativas para a disciplina, pela legislação processual penal brasileira, da prova pericial em meios computacionais relacionada aos crimes cometidos por meio da Internet e, no capítulo dez aponta-se as conclusões, as contribuições, as dificuldades encontradas e os possíveis trabalhos futuros.

2. CRIMES RELACIONADOS À INFORMÁTICA

Embora o tema central desse trabalho consista na análise da prova pericial em meios computacionais, instituto de natureza essencialmente processual, inicialmente, tratar-se-á da criminalidade informática, em função da estreita relação que há entre os dois temas e, principalmente porque seu entendimento é pré-requisito para a compreensão da referida prova técnica.

O desenvolvimento da tecnologia da informação e, principalmente, o surgimento da Internet, ocorridos nas últimas décadas, têm propiciado um crescente movimento de informatização de dados relacionados aos mais diversos ramos de atividades no seio da sociedade. Por esse motivo, muitos atos e fatos jurídicos que, anteriormente, ocorriam no meio físico, passaram a se concretizar no ambiente virtual, também denominado de espaço virtual.[5]

Com efeito, da mesma forma que ocorre no meio físico, muitos destes atos, agora praticados também no meio virtual, apresentam natureza delituosa, adaptando-se a essa nova era, como consequência previsível do avanço da tecnologia da informação. Isto porque, o aparato tecnológico disponível e de fácil acesso, aliado ao ambiente "aparentemente" anônimo e impune que a Internet, equivocadamente, ainda representa, têm estimulado o aumento tanto quantitativo como qualitativo dos mais variados ilícitos, possibilitando o surgimento e incremento de uma espécie de criminalidade, denominada pelos especialistas de criminalidade informática, que tem aumentado exponencialmente.

Segundo Bednar; Katos e Hennel (2008), o anonimato assegurado através da Internet estimula crimes que envolvem o uso de sistemas de computador, uma vez que os criminosos acreditam que há uma pequena chance de serem processados e uma change menor ainda de serem apanhados por seus atos. Esse comportamento

---

[5] Segundo Boiteux (2004, p.47): "O conceito de ciberespaço (cyberspace), ou espaço virtual alcançado pela rede mundial de computadores, a Internet, que reduziu as distâncias e aproximou as pessoas, foi concebido como uma nova dimensão espacial que transcende fronteiras, e permite a todos aqueles conectados à rede imediato contato com qualquer lugar do mundo em segundos, independentemente de fronteiras ou meios de transporte."

é reforçado porque, pela primeira vez, os criminosos podem atravessar as fronteiras internacionais sem o uso de passaportes ou documentos oficiais.

Ainda seguindo esse mesmo raciocínio, pondera Govil e Govil (2007) que o cibercrime é difícil de se detectar, proporcionando aos agressores abundância de tempo para fugir do local onde o crime foi praticado. Assim, os criminosos podem estar em outro país, longe da cena do crime, no momento em que o mesmo for detectado. Crimes cibernéticos diferem da maioria dos crimes comuns sob quatro aspectos: é fácil de aprender como executá-los; exigem poucos recursos em comparação ao dano que podem causar; podem ser cometidos em uma jurisdição sem estar fisicamente presente na mesma e, muitas vezes, não são claramente ilegais.

Em resposta a este novo cenário que retrata não somente uma realidade brasileira pois trata-se de uma questão global, o legislador pátrio vem posicionando-se por meio de algumas leis relativas à questão informática, bem como uma série de projetos de lei ainda em trâmite no Congresso Nacional, com o intuito de suprir a omissão legislativa quanto à matéria em questão, especialmente no campo penal e processual penal, visto que o avanço tecnológico caminha em uma velocidade consideravelmente maior que o processo legislativo.

2.1 Aspectos conceituais

Segundo Ferreira (2005), ao se tratar da criminalidade relacionada ao campo informático, deve-se entendê-lo em sentido amplo, englobando a tecnologia da informação, bem como o processamento e transmissão de dados. Deve-se entender também que, em função do país ou do doutrinador, embora exista uma diversidade de classificações e denominações, há um aspecto comum entre as condutas ilícitas, qual seja, seu objeto ou os meios de atuação.

Em 1960 foram notificados os primeiros casos referentes a ilícitos praticados por meio do computador tais como a manipulação de dados, espionagem, sabotagem. Segundo Costa (2003, p.7):

> “A computação vem sendo empregada em grandes empresas e corporações desde a década de 60 e, desde aquela época, os crimes já aconteciam. Em Crime by Computer Minnesota, o autor Donn B. Parker cita o primeiro caso de que se teve notícia nos EUA, mas precisamente no estado de Minnesota, noticiado no Minneapolis Tribune do dia 18 de outubro de 1.966, sob o título 'Perito em computador acusado de falsificar seu saldo bancário”. Naquela época já se utilizavam os computadores para cometer crimes, mas a quantidade e a frequência com que aconteciam era pequena, pois o uso de computadores era restrito devido a seu alto custo, e somente grandes corporações, como bancos e governos, podiam adquiri-los.”

Esses eventos continuaram raros ao longo dos anos 70, quando surgiram alguns estudos empíricos sobre o tema, revelando que a maioria dos ilícitos não eram detectados por falhas nas investigações ou em função do resultado das mesmas não ser divulgado.

Assevera ainda Ferreira (2005) que com o desenvolvimento de novas tecnologias, nos anos 80, ocorreu um aperfeiçoamento e expansão das condutas delitivas na área informática, atingindo caixas eletrônicos por meio de fraudes, programas de computador através de pirataria bem como a exploração dos sistemas de telecomunicações. Essa nova realidade gerou a ampliação do conceito inicial do crime informático, que passou a englobar condutas até então consideradas crimes de natureza econômica, contra a intimidade e a vida privada, contra a propriedade intelectual, entre outros. Sendo que, atualmente, com a popularização da Internet, constata-se um novo aumento no campo da criminalidade informática em função do surgimento de novas figuras delituosas, de natureza transnacional, tais como a transferência eletrônica de fundos (Internet banking), intromissão abusiva em sistemas (hacking), disseminação de “vírus” em computadores, revelando a vulnerabilidade do sistema, apontando para a necessidade da prevenção e repressão dessas novas figuras delituosas.

Isto porque, condutas dessa natureza, em função da rapidez e do alcance proporcionados pela Internet, por si só já representam um agravamento na sua potencialidade lesiva, aliada à dificuldade na investigação que implica em perícias cada vez mais complexas e caras.

No âmbito internacional, ganhou força a discussão sobre a questão da segurança da informação e a necessidade de se reprimir ilícitos dessa natureza,

resultando na tipificação, pela legislação penal de alguns países, de certas condutas classificadas como crimes informáticos.

Este processo de criminalização teve início, conforme relatado por Boiteux (2004) em meados da década de 80, nos Estados Unidos, com a edição do *Crime Control Act,* de 1984, seguido pelo *Computer Fraud and Abuse Act*, de 1986. Por sua vez, a Alemanha em 15.05.1986 editou a lei conhecida por *Computer Kriminalität,* seguida pela França por meio da Lei *Godfrain,* de 05.01.1988, posteriormente incorporada ao Código Penal Francês, bem como pela Itália por meio da Lei 548 de 23.12.1993 que modificou seu Código Penal à luz dessa nova criminalidade informática, sendo que a Espanha incluiu delitos informáticos na reforma do Código Penal de 1995. Diante desse cenário, surgem as primeiras comissões europeias para o estudo da delinquência informática, destacando-se a atuação da Associação Internacional de Direito Penal (AIDP), precursora na reunião de especialistas para estudo do tema, mencionando-se o colóquio preparatório realizado na Alemanha em 1992, cujos anais foram publicados em 1993.

No Brasil, a matéria foi tratada pela doutrina, inicialmente, como uma questão de direito econômico, tutelando o programa de computador como direito autoral por meio da Lei 7.646, de 18.12.1987 e, posteriormente, por meio das Leis 9.609/98 e 9610/98. Num segundo momento, ampliou-se o rol dos ilícitos informáticos prevendo-se crimes contra a ordem tributária (Lei 8.137/1997), crimes eleitorais (Lei 9.100/95), crimes próprios praticados por funcionários públicos, alterando alguns artigos do Código Penal brasileiro (Lei 9.983/2000),

Atualmente, nota-se um avanço da delinquência informática relacionada à pornografia infantil, ao jogo ilegal, ao terrorismo, entre outros, que se utilizam da tecnologia da informação e comunicação, notadamente da Internet, para incrementar suas ações. No Brasil, há uma tendência à criminalização de condutas envolvendo os sistemas informáticos veiculada por uma série de projetos de lei ainda em trâmite. São exemplos desses instrumentos legislativos: projetos de lei 137/1989; 152/1991; 597/1991; 22/1996; 1713/1996; 3.943/1997; 6.210/2002; 76/2000.

2.2 A transnacionalidade da criminalidade informática

Ao se tratar da criminalidade informática não é possível articular soluções apenas em âmbito nacional uma vez que se trata de fenômeno nitidamente marcado pela globalização, em função da rede mundial de computadores, a Internet. A ampla mobilidade de dados e sua livre circulação por meio dos sistemas informáticos e das redes de telecomunicações, permite que o ilícito desta natureza seja praticado à distância. O delito informático é caracterizado pela interdependência de ações, visto que, em muitos casos, os atos executórios são praticados em um dado país e os resultados, produzidos em outro, sujeito a diferentes ordenamentos jurídicos, ultrapassando assim as fronteiras nacionais.

Segundo Bednar, Katos e Hennel (2008), a natureza global dos cibercrimes, intensificou a necessidade de investigadores para se engajarem na complexa comunicação inter-grupos em uma base multinacional, pois eles e também os criminosos tiraram proveito destas tecnologias interligadas. Além disso, a necessidade de navegar entre diferentes sistemas judiciais em todo o mundo cria um ambiente desafiador para os investigadores da cena do crime.

Em face da transnacionalidade do crime informático, é imperativo que se articule a cooperação internacional por meio de tratados e convenções internacional com o intuito de promover a harmonização da legislação tanto penal como processual penal. Isto porque, entre outros motivos, conforme Boiteux (2004, p.167):

> "diante da complexidade da questão e da característica global dos delitos informáticos, a existência de leis nacionais diversas com o objetivo de previnir delitos poderia levar à criação de paraísos criminais (chamados *data heavens* ou *computer crime heavens).* Paraísos criminais seriam locais nos quais provedores se instalariam e seriam beneficiados por legislações mais brandas, que não punissem crimes informáticos, em alusão aos conhecidos paraísos fiscais de taxas e impostos que atraem as companhias internacionais interessadas em reduzir seus custos."

Em resposta à necessidade de uniformização das legislações nacionais e de instrumentos internacionais de assistência mútua é que em 2001 surgiu o primeiro tratado internacional sobre crimes informáticos praticados por meio da Internet, a Convenção Europeia sobre Crimes Cibernéticos, popularmente conhecida como

Convenção de Budapeste, elaborada pelo Conselho da Europa, vinculante aos países signatários. Importante registrar que, embora seja um tratado europeu, está aberto à adesão de outros países que não fazem parte da Comunidade Europeia.

Instrumento internacional mais abrangente e atual sobre a matéria, a Convenção de Budapeste tem como prioridade uniformizar a legislação europeia por meio de uma política criminal comum, recomendando aos Estados signatários a adequação de sua legislação às diretivas da Convenção para facilitar e agilizar a cooperação internacional, tipificando novas condutas e procedimentos penais padrões.

2.3 O direito penal e o crime informático

Segundo a moderna criminalística, crime informático é toda a ação típica, antijurídica e culpável, praticada contra ou através da transmissão, processamento e armazenamento automático de dados.

Analisando a definição acima apontada, o termo “ação” trata-se de comportamento humano, que pode ser comissivo ou omissivo, típico, ou seja, que se enquadre ao modelo descrito na lei penal como crime, seguido da penalidade correspondente, respeitando o princípio da legalidade previsto tanto no Código Penal, artigo primeiro bem como no texto constitucional, em seu artigo 5º, inciso XXXIX, que estatui: “Não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal”.

A conduta típica poderá ocorrer de duas maneiras diversas: contra um sistema informático ou por meio da utilização de um sistema informático. No primeiro caso, o sistema informático é o bem contra o qual se pratica a conduta delituosa e, no segundo caso, passa a ser o instrumento da ação delituosa.

Há autores que advogam a tese de que é necessária uma nova doutrina para o direito penal da informática com a elaboração de uma teoria geral que tutele a informação e os meios intangíveis que compõem os sistemas informáticos. Isto porque, em virtude da inaplicabilidade da analogia em matéria penal, não há como

preencher as lacunas legais existentes, em função de um código penal que não contempla os novos tipos penais relacionados à matéria.

O mesmo ocorre quanto à questão processual, visto que não há previsão legal satisfatória, de natureza processual, que discipline a produção e análise da prova em meios computacionais, em função desta nova realidade que se nos apresenta, fruto do desenvolvimento tecnológico.

Relativamente ao crime informático, por vezes, trata-se apenas de uma nova forma de executar delitos que já estão previstos no diploma penal, tais como a fraude, o furto, a apropriação indébita, o estelionato, o vandalismo, os crimes contra a honra, contra a liberdade individual, a violação de direito autoral, a violação da propriedade industrial ou da proteção das marcas de indústria e comércio, entre outros. Outras vezes, apresentam características peculiares, não previstas na descrição do tipo penal veiculado pela legislação penal existente, tais como delitos praticados diretamente contra o funcionamento do ambiente operacional do computador, como é o caso da disseminação de “vírus de computador” que destrói programas e arquivos dos usuários e cujos resultados em função da Internet, extrapolam os limites nacionais, tornando-se uma questão global, indo além do tipo penal descrito pelo crime de dano.

2.4 Classificação dos crimes informáticos

Várias são as classificações apresentadas pela doutrina com o intuito de ordenar sistematicamente o assunto, entre elas a que estabelece a diferença entre crimes tradicionais disciplinados pela legislação penal, comum ou especial, tendo a informática como meio ou instrumento para a prática delituosa e, as outras hipóteses, relacionadas ao uso indevido da informática, específicas da área, nomeadas como crimes da informática ou crimes informáticos.

Outra classificação muito adotada, mencionada por Ferreira (2005, p.244), fazendo referência à Hervé Croze e Yves Bismuth, a qual parece a mais adequada, é a que distingue duas categorias de crime:“i) os atos dirigidos contra um sistema de

informática, por qualquer motivo;ii) os atos que atentam contra outros valores sociais ou outros bens jurídicos, cometidos através de um sistema de informática."

Assevera ainda Ferreira (2004) que, relativamente à primeira classe, identifica-se o verdadeiro núcleo da criminalidade informática, segundo Crose e Bismuth, onde situam-se as várias condutas que atentam contra o próprio material informático, quer seja contra os suportes lógicos, quer seja contra os dados do computador. Quanto à segunda classe, pode-se afirmar que são incluídas todas as espécies de infrações previstas nas leis penais, pois a informatização da sociedade gera a informatização da delinquência. Nesta categoria, os ilícitos mais comuns são os crimes de natureza patrimonial ou econômica, crimes contra a liberdade individual, violação de direito autoral e da propriedade industrial.

Neste sentido é o posicionamento de Daoun (2008,176):

> "Podemos afirmar que condutas praticadas por meios eletrônicos, não constituem, via de regra, nova modalidade de crimes. Majoritariamente, já há tipificação em leis vigentes – Código Penal e Legislação Penal Especial, tratam-se de bens jurídicos já tutelados no nosso ordenamento, praticados por meios eletrônicos. A inovação restringe-se ao *modus operandi*. Assim, não há que se admitir a criação de novos dispositivos legais para o que já está tutelado em matéria penal. É o que se entende por crimes informáticos de natureza mista ou imprópria. São raras as situações em que verificamos o dado, a informação e o sistema informatizado como alvo de conduta praticada pelo agente e, portanto, objeto carecedor de guarida. Para tais hipóteses, ainda que mínimas, podemos admitir o firmamento de um bem jurídico a ser tutelado expressamente por lei penal específica, definindo-se como crimes informáticos de natureza pura."

2.4.1 Condutas praticadas contra um sistema informático

Considerando a classificação anteriormente apontada, os atos praticados contra um sistema informático, tendo como critério o objeto material visado pela conduta, exteriorizam-se de duas formas: atos dirigidos contra o próprio equipamento, ou seja, contra o computador, seus componentes e acessórios ou atos dirigidos contra os dados e informações nele contidos.

2.4.1.1 Condutas praticadas contra o computador, seus componentes e acessórios

Esta modalidade engloba os crimes de furto do equipamento e de seus componentes, bem como a apropriação indébita, o crime de dano. Nesta categoria inclui-se, inclusive, os atos praticados contra os acessórios do computador entendidos estes como os suportes materiais da informação tais como os disquetes, as fitas magnéticas, entre outros. Tais ilícitos enquadram-se perfeitamente nos tipos penais previstos pelo código, sendo que há doutrinadores que argumentam que tais condutas sequer deveriam ser classificados como crimes informáticos visto que o computador, seus componentes e acessórios tratam-se de bens comuns, como qualquer outro bem juridicamente tutelado. Há também a figura do furto de uso, não previsto pelo código mas objeto de construção jurisprudencial.

2.4.1.2 Condutas praticadas contra os dados ou programas de computador

Os atos praticados contra os dados armazenados ou fornecido pelo computador podem equivaler-se à cópia, sem autorização, das informações contidas no sistema, sua adulteração ou ainda, na destruição total ou parcial dos dados pelo apagamento do conteúdo dos suportes.

Quanto à cópia de programas de computador, popularmente conhecida como pirataria, esta não se confunde com o crime de furto ou mesmo com a apropriação indébita, uma vez que se trata de bem de natureza imaterial, bem como não ocorre a subtração visto que seu proprietário permanece com a posse sobre o mesmo. Não há que se falar também em estelionato visto que inexiste o emprego do meio fraudulento. O que ocorre é a violação da propriedade intelectual, especificamente, a violação de direito autoral disciplinado pela lei de software (Lei 9.609/98) e, subsidiariamente pela lei de direito autoral (Lei 6.9010/98).

Há também a modificação, não autorizada, dos programas de computador, que altera sua programação original, possibilitando o acesso a banco de dados, registros e códigos. Uma das técnicas mais difundidas de alteração do programa de computador, sem autorização, é a utilização do denominado Cavalo de Tróia. Trata-se de um vírus que, ao infectar a máquina, dissemina instruções diferentes das originais, ou mesmo, instala outro programa que passa a atuar juntamente com o programa original, modificando seus comandos.

Há casos, ainda, em que ocorre a destruição total ou parcial do programa de computador através do apagamento ou supressão do conteúdo dos suportes decorrentes da atuação de vírus que contaminam a máquina. Segundo Ferreira (2005, p.244):

> "o vírus eletrônico nada mais é que um programa introduzido no computador, ou transmitido via Internet, que se reproduz sem autorização do usuário e interfere nos procedimentos normais da máquina, após ser ativado pelo próprio funcionamento do computador."

O problema tem sido agravado, multiplicando-se em escala global, principalmente com o advento e popularização do uso da Internet. Isto porque, embora um único computador possa ser infectado mediante a introdução de um suporte contendo vírus ou por meio de um comando disparado pelo mero toque do teclado, este cenário ganha proporções incontroláveis, quando a transmissão do vírus ocorre através de redes de computadores como é o caso da Internet.

Essas alterações nos programas de computador ou mesmo o apagamento ou supressão de dados, não autorizados, necessitam de previsão legal adequada. A lei de software bem como a lei de direito autoral juntamente com o código penal, notadamente por meio da figura típica do crime de dano comum, têm se mostrado insuficientes para coibir e reprimir tais condutas. Não têm o alcance necessário diante da amplitude do problema, quando se trata da proteção a direitos intelectuais.

Isto porque, para ser considerada crime, a conduta deve estar tipificada pelo diploma legal, o que não acontece nestes casos, pois a evolução legislativa não ocorre na mesma velocidade que o avanço tecnológico.

2.4.2 Condutas praticadas por meio de um sistema informático

Com o crescente movimento de informatização de dados, grande parte das condutas delituosas já tipificadas, ou seja, já previstas nas leis penais, passaram a se utilizar da informática para facilitar, agilizar ou mesmos potencializar o resultado almejado.

Tais condutas não são classificadas como crimes de informática mas como crimes comuns ou especiais, já tipificados, cujo sistema informático é apenas o meio ou o instrumento utilizado pelo agente para a sua prática. Há doutrinadores que os denominam crimes de informática impróprios em contraposição aos crimes de informática próprios, cujo sistema de informática é o bem jurídico visado pela conduta ilícita, como visto anteriormente.

Apesar de haver uma gama enorme e crescente de possibilidades relacionadas a ilícitos praticados por meio de sistemas informáticos, a casuística revela que tais condutas concentram-se no âmbito dos crimes contra o patrimônio, contra a liberdade individual, contra a propriedade imaterial, bem como outros crimes de natureza econômica.

3. A BUSCA DA VERDADE E AS GARANTIAS CONSTITUCIONAIS DO ACUSADO

A disciplina da prova é um dos temas mais relevantes para o direito processual, uma vez que a decisão judicial é motivada a partir das pretensões das partes fundadas nas provas produzidas ao longo do processo. Sentenças justas pressupõem provas capazes de refletir a realidade mais próxima ao fato, ou seja, a verdade possível sobre o ocorrido, resultado de um processo que não busca a verdade a qualquer preço, na medida em que respeita as garantias do acusado e as regras do devido processo.

A importância da disciplina da prova na teoria geral do processo é ainda mais acentuada no processo penal, pois, conforme Gomes Filho (2005, p.303): “só a prova cabal do fato criminoso é capaz de superar a presunção de inocência do acusado, que representa a maior garantia do cidadão contra o uso arbitrário do poder punitivo”.

O tema torna-se pertinente pois, há bem pouco tempo, era defendida a tese de que vigorava, notadamente, no processo penal o princípio da verdade material, uma vez que se acreditava que era possível, por meio da prova, reproduzir, com exatidão, o fato ocorrido em todos os seus contornos.

A pesquisa da verdade, portanto, possuía um caráter praticamente ilimitado, transformando-se em verdadeira obsessão do inquisidor que, não raro, era alguém totalmente parcial, comprometido, desde o início da investigação, com a tese da culpabilidade, que tanto procurava demonstrar. A investigação, em muitos casos, era apenas um meio para a confirmação de uma verdade preestabelecida.

Contudo, hodiernamente, entende-se que a verdade material é inalcançável, pois o que deve ser buscado é a verdade possível de ser atingida, a verdade processual. Esta visível alteração de posicionamento, principalmente no sistema processual penal brasileiro, deve-se aos novos paradigmas introduzidos em nossa processualística pela Constituição de 1988 e pela Convenção Americana sobre Direitos Humanos, recentemente incorporada ao nosso ordenamento. Ambos os

diplomas refletem concepção garantista, com o fim de promover a efetiva participação dos interessados na formação do convencimento do juiz.

Este também tem sido o entendimento jurisprudencial do Tribunal de Justiça do Estado de São Paulo, conforme abaixo transcrito:

> Apelação Criminal, No. 892571.3/7-0000-000, da Comarca de Votorantim, em que é(são) APELANTE(s) MARCOS PAULO DE MORAES, sendo APELADO(s) MINISTÉRIO PÚBLICO.
> Mesmo a busca da verdade real não se faz a qualquer preço, ao contrário, tem seus limites nos princípios constitucionais e nos direitos e garantias individuais. A verdade processual deve ser alcançada através do sistema de provas e contraprovas, assegurado o direito às partes de participar de todos os atos processuais em igualdade de condições, de forma a permitir que o julgador chegue a uma verdade processual equilibrada .
> Nesse sentido preleciona Marco António Marques da Silva:"...a busca da verdade no processo penal deve ser feita com cautela, pois não se admite qualquer meio de prova, mas somente aqueles processualmente admitidos, ainda que desta limitação resulte um sacrifício à verdade material. Estes os princípios que orientam o direito penal e o processo penal, no Estado Democrático de Direito." (Marco António Marques da SILVA. Acesso à justiça penal e estado democrático de direito. São Paulo: Juarez de Oliveira, 2001, p. 35).

Ainda nesse mesmo sentido é o entendimento do Tribunal de Justiça de Santa Catariana:

> Tipo: Apelação criminal Número: 28.510 Des. Relator: Des. Ernani Ribeiro. Data da Decisão: 19/04/1993 LESÕES CORPORAIS E INVASÃO DE DOMICÍLIO. ABSOLVIÇÃO EM FACE DA DÚVIDA. RECURSO DO MINISTÉRIO PÚBLICO. CRIMES PROVADOS E CARACTERIZADOS. RECURSO PROVIDO.
> [...]
> “Mesmo que se tenha presente que a verdade absoluta jamais será alcançada pelo juiz porque ela pertence exclusivamente a Deus, sabe o magistrado que a sua meta é alcançar a verdade processual que é, apenas, uma verdade relativa, como afirma Roberto Lira. Esta é alcançada no sopesamento sereno dos "fatores de convergência" da acusação com os "fatores de divergência" da defesa. É através, pois, da perquirição da verdade no processo que se chega à "certeza judicial" para punir os culpados e absolver os inocentes.”
> [...]
> "não se acredita mais hoje que o juiz, ao proferir as suas decisões, tenha certeza absoluta de como os fatos, dos quais surgiu uma pretensão deduzida, uma pretensão resistida ou uma pretensão insatisfeita, ocorreram, principalmente em se tratando de prova testemunhal. Por que a certeza, a que antes a doutrina se referia, na verdade não passa de razão de probabilidade, em alguns casos mais acentuada a sua manifestação e em outros menos. Nem mesmo com a extraordinária evolução da ciência, é possível o Juiz decidir com certeza absoluta.”

Segundo Ferrajoli (2006), sabe-se que a realidade está fora do processo, visto que a verdade, resultante da prova produzida no interior do feito, trata-se de uma verdade aproximativa, aquela que deriva do que é possível saber sobre ela, a verdade processual. Em parte, devido às restrições impostas à produção da prova em observância aos procedimentos e às garantias da defesa, tais como o princípio da presunção da inocência, o princípio do contraditório, o princípio da inadmissibilidade de provas obtidas por meios ilícitos, entre outros. Afasta-se, portanto, a superada noção da verdade material, por meio da qual justificava-se o uso de quaisquer meios, mesmo os violadores de garantias do acusado, para se descobrir a verdade.

Nesse sentido, assevera ainda o mesmo autor que:

> "esta verdade não pretende ser a verdade; não é obtida mediante indagações inquisitivas alheias ao objeto pessoal; está condicionada em si mesma pelo respeito aos procedimentos e às garantias da defesa. É, em suma, uma verdade mais controlada quanto ao método de aquisição, porém mais reduzida quanto ao conteúdo informativo do que qualquer hipotética 'verdade substancial', no quádruplo sentido de que se circunscreve às teses acusatórias formuladas de acordo com as leis, de que deve estar corroborada por provas recolhidas por meio de técnicas normativamente preestabelecidas, de que é sempre uma verdade apenas provável e opinativa, e de que na dúvida, ou na falta de acusação ou de provas ritualmente formadas, prevalece a presunção de não culpabilidade, ou seja, da falsidade formal ou processual das hipóteses acusatórias" **(FERRAJOLI, 2006, p.48).**

Diante dessa perspectiva, o processo só será eficiente quando se desenvolver:

> "de modo a permitir às partes, de forma contraditória, evidenciar a veracidade de suas afirmações e, ao juiz, sem perda de sua imparcialidade, esclarecer dúvidas relevantes para o seu julgamento, com respeito às regras do devido processo" **(SCARANCE, 2009, p. 571).**

A processualística moderna concebe a verdade material como sendo inalcançável, uma vez que a verdade, resultante da prova produzida no interior do feito, trata-se de uma verdade aproximativa, aquela que deriva do que é possível saber sobre ela, a verdade processual. Esta mudança de concepção da verdade, sobretudo no sistema processual penal brasileiro é o resultado dos novos

paradigmas por ele incorporados sob a influência da Constituição de 1988 e da Convenção Americana sobre Direitos Humanos.

A partir desta análise é importante registrar a noção técnico-processual da prova como sendo o resultado da atividade instrutória, realizada dentro do processo, na presença de juiz imparcial e das partes, com pleno exercício do contraditório.

4. O SISTEMA PROCESSUAL PENAL BRASILEIRO

4.1 O Código de Processo Penal brasileiro

O Código de Processo Penal, introduzido no ordenamento jurídico brasileiro pelo Decreto-lei 3.689, de 3 de outubro de 1941, entrou em vigor em 1.º de janeiro de 1942. Quando de sua edição, durante o Estado Novo, regime ditatorial inaugurado por Getúlio Vargas, vigorava a Constituição de 1937, outorgada, conhecida como “Polaca” por ter sido inspirada na Constituição da Polônia, de tendência fascista. Por se tratar de uma Constituição de natureza autoritária e policialesca, tais características refletiram-se em todo o ordenamento jurídico vigente à época, notadamente no Código de Processo Penal.

Desde sua promulgação, passou-se por três Constituições: 1946, 1967 e 1969 até à Constituição de 1988. Diversos artigos do Código foram revogados tanto pelas Constituições como também por leis infraconstitucionais, em virtude do crescente processo de redemocratização.

O Código de Processo Penal era considerado, por parcela significativa da doutrina, como instrumento legislativo ultrapassado e carecedor de reformas sistêmicas urgentes, mormente para alinhá-lo ao texto constitucional vigente, visto que este privilegiou os direitos e as garantias individuais. Embora tenha sofrido alterações importantes ao longo dos seus sessenta e nove anos de vigência, a contar de sua promulgação, até recentemente, conservava as características iniciais, de conteúdo marcadamente inquisitivo, apresentando diversas falhas e incoerências na sistemática processual penal quanto ao sistema acusatório, às garantias do acusado, ao apego ao formalismo, embora com ligeira feição garantista.

Diante desse contexto, com o intuito de modernizar a legislação processual penal, o então Ministro da Justiça, José Carlos Dias, por meio da Portaria 61/2000, constituiu uma comissão para o trabalho de reforma. Fruto dessa iniciativa governamental, a referida comissão apresentou sete anteprojetos que, posteriormente, foram convertidos em projetos de lei, sendo que:

- Projeto de Lei 4.204/2001 foi abrangido pela Lei 10.792/2003, referente ao interrogatório do acusado.
- Projeto de Lei 4.203/2001 foi aprovado pela Lei 11.689, de 9 de junho de 2008, referente ao júri.
- Projeto de Lei 4.205/2001 foi aprovado pela Lei 11.690, de 9 de junho de 2008, referente às provas.
- Projeto de Lei 4.207/2001 foi aprovado pela Lei 11.719, de 20 de junho de 2008, referente a procedimentos.

Por uma questão de política legislativa, optou-se por reformas pontuais para viabilizar sua tramitação pelo legislativo. Acredita-se que, em futuro próximo, serão ainda aprovados o Projeto de Lei 4.206/2001, que dá nova sistemática aos recursos e ações de impugnação, o Projeto de Lei 4.208/2001, que modifica a prisão e as medidas cautelares e o Projeto de Lei 4.209, referente à investigação criminal. A respeito do objetivo da reforma, conforme Mendonça (2008, p.11):

> "pode-se afirmar que a idéia central da reforma foi modernizar o processo penal, à luz dos seguintes fundamentos: a) fortalecimento do sistema acusatório; b) reforço às garantias do acusado; c) celeridade; d) efetividade na busca da prestação jurisdicional; e) revalorização do papel da vítima no processo penal".

Especificamente quanto à temática da prova, a Lei 11.690, de 9 de junho de 2008, trouxe significativas modificações ao diploma processual. Isso porque, a disciplina da prova era a que mais evidenciava a influência do regime autoritário durante o qual fora concebido o Código de Processo Penal. É certo que mudanças ocorreram ao longo dos anos, fruto do posicionamento jurisprudencial, sem, contudo, dispensar a necessária reforma legislativa.

Sobre as alterações em relação à disciplina da prova, nos dizeres de Gomes Filho (2008, p.247):

> "são características salientes no novo texto: a delimitação do alcance do princípio do livre convencimento do juiz; a consagração do contraditório como elemento essencial do próprio conceito de prova; a regulamentação legal da proibição das provas ilícitas; e ainda, uma nova disciplina dos meios de prova pericial e testemunhal, mais adequada ao contraditório como método de formação das provas".

Importante registrar que recentemente foi aprovado no Senado Federal o projeto de lei referente ao Novo Código de Processo Penal - PLS 156/2009, que representa uma reforma integral e sistêmica do diploma legal processual e que incorpora as reformas pontuais referentes à prova acima expostas.

4.2 Sistema acusatório

Segundo o entendimento majoritário da doutrina, a Constituição Federal assegura o sistema processual acusatório, cujas particularidades são apontadas por Nucci (2006, p. 77):

> "nítida separação entre o órgão acusador e o julgador; há liberdade de acusação, reconhecido o direito ao ofendido e a qualquer cidadão; predomina a liberdade de defesa e a isonomia entre as partes no processo; vigora a publicidade do procedimento; o contraditório está presente; existe a possibilidade de recusa do julgador; há livre sistema de produção de provas; predomina maior participação popular na justiça penal e a liberdade do réu é a regra".

Contudo, há doutrinadores que entendem que o sistema processual pátrio é o sistema misto, fruto da união dos sistemas inquisitivo e acusatório, cujas peculiaridades são resumidamente elencadas pelo mesmo autor já anteriormente citado:

> "O sistema misto, surgido após a Revolução Francesa, uniu as virtudes dos dois anteriores, caracterizando-se pela divisão do processo em duas grandes fases: a instrução preliminar, com os elementos do sistema inquisitivo, e a fase de julgamento, com a predominância do sistema acusatório. Num primeiro estágio, há procedimento secreto, escrito e sem contraditório, enquanto, no segundo, presentes se fazem a oralidade, a publicidade, o contraditório, a concentração dos atos processuais, a intervenção de juízes populares e a livre apreciação das provas" (NUCCI, 2006, p.77-78).

Embora não se desconheça o posicionamento contrário, com a nova ordem constitucional instaurada em 1988, evidenciou-se a adoção do sistema acusatório no

direito brasileiro. Mesmo na primeira fase da persecução penal, asseguram-se direitos e garantias processuais ao investigado, que é tido por sujeito de direitos.

A propósito, cumpre registrar que, com a recente reforma do Código de Processo Penal, quanto à disciplina da prova, veiculada pela Lei 11.690, de 9 de junho de 2008, dando nova redação ao art. 155 do CPP[6], ficou claro que há diversidade conceitual entre o que constitui prova – ou seja, dado resultante de instrução realizada com imediação e pleno contraditório das partes – e elemento de convicção, obtido por meio do inquérito policial.

Da previsão normativa que estabelece a necessidade de apreciação da prova produzida em contraditório judicial, extrai-se que só é possível utilizar informações obtidas na investigação ocorrida na fase do inquérito policial desde que existam também, para corroborá-las, provas produzidas em contraditório judicial. Nesse sentido, assevera Gomes Filho (2008, p. 251):

> "Isso significa que, para se ter como provada – no sentido de demonstrada, verificada – uma afirmação sobre um fato, com base nos dados de conhecimento existentes no processo, é possível utilizar informações obtidas na investigação, mas sob a condição de que existam também – para confirmá-las – provas (elementos de prova) produzidas em contraditório judicial".

Observa-se, portanto, que a alteração da redação do art. 155 do CPP apontada, também veio mitigar as feições inquisitivas do sistema processual penal, como de fato o fez a recente reforma como um todo.

4.3 Sistema de legislação processual penal uniforme

Quanto à unidade, duplicidade ou pluralidade de ordens de regência ou legislações processuais, o Brasil é dotado de sistema de legislação processual penal uniforme para todo o território nacional, ou seja, o processo penal é disciplinado em

---

[6] Código de Processo Penal, artigo 155: "Art.155. O juiz formará sua convicção pela livre apreciação da prova produzida em contraditório judicial, não podendo fundamentar sua decisão exclusivamente nos elementos informativos colhidos na investigação, ressalvadas as provas cautelares, não repetíveis e antecipadas."

todo o território nacional pelo Código de Processo Penal, conforme dispõe o art. 1.º do referido diploma legal[7].

[7] Código de Processo Penal, Art. 1° O processo penal reger-se-á, em todo o território brasileiro, por este Código, ressalvados:

I - os tratados, as convenções e regras de direito internacional;

II - as prerrogativas constitucionais do Presidente da República, dos ministros de Estado, nos crimes conexos com os do Presidente da República, e dos ministros do Supremo Tribunal Federal, nos crimes de responsabilidade (Constituição, arts. 86, 89, §2°, e 100);

III - os processos da competência da Justiça Militar;

IV - os processos da competência do tribunal especial (Constituição, art. 122, n° 17);

V - os processos por crimes de imprensa.

Parágrafo único. Aplicar-se-á, entretanto, este Código aos processos referidos nos n°s. IV e V, quando as leis especiais que os regulam não dispuserem de modo diverso."

5. ASPECTOS GERAIS SOBRE A TERMINOLOGIA DA PROVA

Uma das dificuldades, anteriormente referida, quanto ao estudo da prova, reside no fato de se tratar de expressão com várias acepções, tanto na linguagem comum quanto na linguagem científica, nela inserido o discurso técnico-jurídico. Essa imprecisão quanto à linguagem representa obstáculo à comunicação, gerando confusão e entendimento equivocado pela falta de clareza da terminologia empregada, contaminando a atividade probatória no âmbito do processo judicial.

Diante dessa constatação, em face da necessidade de se atingir maior uniformidade e precisão possíveis quanto à terminologia a ser utilizada no âmbito da ciência do processo, com o fim de se estabelecer linha de raciocínio coerente ao longo deste trabalho, optamos por ter como referência a terminologia e conceituação adotadas por Antonio Magalhães Gomes Filho, em trabalho intitulado Notas sobre a terminologia da prova, reflexos no processo penal, e pelo mesmo autor e por Gustavo Henrique Righi Ivahy Badaró, em trabalho intitulado Prova e sucedâneo da prova no processo penal brasileiro, salvo pontuais adaptações ou mesmo circunstanciais considerações de outros autores, ambas referendadas.

5.1 Os diversos significados do termo prova na ciência do processo

A verificação dos sentidos do termo prova no âmbito da linguagem comum tem a função apenas de evidenciar a complexidade da matéria. No contexto da ciência processual, essa linguagem se mostra insuficiente e superficial. É fruto dessa percepção a preocupação da doutrina em definir e estabelecer distinções quanto ao termo prova inserido no âmbito da atividade probatória.

5.1.1 Elemento de prova e resultado da prova

Dessa forma, na terminologia processual, denomina-se elemento de prova (*evidence*), quando o vocábulo “prova” referir-se aos “dados objetivos que confirmam ou negam uma asserção sobre determinado fato que interessa à decisão da causa” (GOMES FILHO, 2005, p.307). Apresentam-se os seguintes exemplos de elemento de prova: a declaração de uma testemunha quanto ao fato ocorrido, a opinião de um perito sobre a matéria de sua especialidade, o conteúdo de um documento (GOMES FILHO, 2005). São também considerados como elemento de prova os vestígios digitais resultado do ilícito praticado por meio da Internet.

Com fundamento nesse sentido do vocábulo prova, esclarecem-se os termos da garantia processual prevista no art. 5.º, inc. LVI, da Constituição brasileira: são “inadmissíveis os elementos de prova resultantes de atos de obtenção praticados com violação a direitos” (GOMES FILHO, 2005, p.307).

É ligado a elemento de prova o que se denomina resultado de prova. A palavra “prova” pode significar a própria conclusão que se extrai dos diversos elementos de prova existentes, a propósito de um determinado fato: é resultado da prova (*proof*), que é obtido não apenas pela soma dos elementos de prova, mas sobretudo por meio de um exercício intelectual feito pelo juiz, que permite estabelecer se a afirmação ou negação do fato é verdadeira ou não (GOMES FILHO, 2005).

5.1.2 Fonte de prova, meios de prova e meios de investigação da prova

A terminologia processual estabelece ainda as diferenças entre fonte de prova, meios de prova e meios de investigação de prova.

Entende-se como fonte de prova pessoas ou coisas por intermédio das quais é possível obter os elementos de prova, classificando-se, portanto, em fontes

pessoais: testemunhas, vítimas, acusado, peritos; e fontes reais: documentos, em sentido amplo (GOMES FILHO, 2005, p.308).

Os meios de prova, também chamados de meios de produção de prova, são “os instrumentos ou atividades por meio dos quais os dados probatórios (elementos de prova) são introduzidos e fixados no processo (produção da prova). São, em síntese, os canais de informação de que se serve o juiz” (GOMES FILHO, 2005, p.308). Dessa forma, ao se referir à prova testemunhal, prova documental, prova pericial, deve-se entender que a representação do fato foi obtida a partir do testemunho, do documento ou da perícia. No direito processual brasileiro, são exemplos de meios de prova a prova testemunhal, a prova documental e a prova pericial, todos disciplinados pelo Código.

Já os meios de pesquisa, de investigação ou meios de obtenção de prova são “certos procedimentos (em geral, extraprocessuais), regulados por lei, com o objetivo de conseguir provas materiais, e que podem ser realizados por outros funcionários (policiais, por exemplo)” (GOMES FILHO, 2005, p.308). São exemplos de meio de pesquisa de prova as interceptações telefônicas feitas por policiais com ordem judicial.

Ainda em relação aos meios de prova, mister se faz estabelecer as diferenças entre estes e os denominados meios de pesquisa ou de investigação da prova.

a) “Os meios de prova ou meios de produção de prova referem-se a uma atividade endoprocessual, que se desenvolve perante o juiz, com o conhecimento e participação das partes, visando a introdução e a fixação de dados probatórios no processo. Os meios de pesquisa ou de investigação dizem respeito a certos procedimentos (em geral, extraprocessuais), regulados pela lei com o objetivo de se obter provas materiais” (GOMES FILHO, 2005, p.308).

b) Os meios de pesquisa, de investigação ou de obtenção de prova apresentam o fator “surpresa, sem o qual seria inviável a obtenção das fontes de prova, ao passo que nos meios de prova é rigorosa a obediência ao contraditório” (GOMES FILHO, 2005, p.308).

c) Por fim, uma última distinção a ser registrada é que quando presentes irregularidades quanto aos meios de prova, a consequência em razão do vício será a nulidade da prova, ao passo que presentes irregularidades quanto aos meios de

pesquisa ou investigação, a consequência em razão do vício é a inadmissibilidade da prova no processo.

5.1.3 Objeto de prova

O objeto de prova (*thema probandum*) “é determinado pelas proposições representativas do fato juridicamente relevantes, e colocadas pelas partes como base da acusação e da defesa, ou mesmo como fundamento de eventual pesquisa judicial” (GOMES FILHO, 2005, p.317).

Portanto, segundo o conceito anterior, objeto de prova refere-se a proposições representativas do fato e não ao próprio fato, ou seja, é equivocado afirmar que a prova destina-se a obter conhecimento sobre um fato, pois “o que se apura no processo é a verdade ou a falsidade de uma afirmação sobre um fato” (GOMES FILHO, 2005, p.308).

5.1.4 Prova típica e prova atípica

Não há na doutrina consenso quanto à noção de tipicidade e atipicidade, fato que tem gerado inúmeros equívocos terminológicos. Extrai-se da doutrina que são típicas as provas catalogadas e reguladas em lei, ou seja, para as quais é previsto um procedimento probatório específico e, atípicas, sob a perspectiva de uma “posição ampliativa”, “em duas situações: 1) quando ela seja prevista no ordenamento, mas não o seja seu procedimento probatório; 2) quando nem ela nem seu procedimento probatório sejam previstos em lei” (DEZEM, 2008, p.147).

A relevância de se estabelecer os conceitos de prova típica e prova atípica percebe-se na medida em que permite verificar quais os requisitos de admissibilidade de determinado meio de prova, trazendo maior segurança às partes no processo.

Nesse sentido, necessário se faz conceituar e estabelecer as diferenças entre prova atípica, prova anômala, prova irritual e prova inominada, não em função de um preciosismo linguístico sem sentido mas em face das consequências práticas que equívocos terminológicos geram à atividade probatória.

5.1.5 Prova atípica, prova anômala, prova irritual e prova nominada

A doutrina adjetiva anômala a prova se, embora o meio de prova seja expressamente previsto, para a sua colheita, vale-se de outro meio de prova. Exemplifica-se com o procedimento adotado pelo Ministério Público, muito utilizado na prática judiciária diária, consistente na oitiva, pelo órgão da acusação, de testemunha, em seu gabinete com a pretensão de introduzir essa oitiva no processo como prova documental. Não se trata de prova atípica, mas sim de estratégia adotada para se superar eventual óbice quanto à oitiva da testemunha em juízo por meio da oitiva exclusivamente pela acusação, violando-se os princípios da ampla defesa e do contraditório (DEZEM, 2008).

Com relação ao tema, é importante destacar manifestação de Fernandes (2007, p.223):

> "A substituição da prova testemunhal por documento é feita no Brasil para escapar da necessidade de que o depoimento fosse colhido pelo juiz em audiência com a participação das partes e para superar os limites de admissibilidade da prova testemunhal, pois o documento pode ser juntado a qualquer momento do processo, enquanto a prova testemunhal deve ser requerida no início da fase postulatória e deve ser produzida em momentos determinados".

Ainda sobre a questão, assevera Badaró (2005, p. 341):

> "por se tratar da supressão do contraditório em um meio de prova de característica essencialmente dialética, como é a prova testemunhal, a prova produzida unilateralmente, no gabinete do Ministério Público, não pode ser admitida como prova, devendo ser desentranhada dos autos".

Outra importante distinção é a que deve ser feita entre prova atípica e prova irritual, isto é, a prova típica colhida sem a observância do modelo previsto em leil.

Assevera Dezem (2008) a semelhança e a diferença entre a prova anômala e a prova irritual. Ambas se aproximam por gerarem nulidade ou ilicitude, se utilizadas no processo. A diferença decorre da constatação de que:

> "na prova anômala segue-se procedimento previsto em lei, mas não o procedimento previsto para aquele meio de prova. Na prova irritual, segue-se procedimento previsto para o meio de prova, mas sem a observância dos elementos típicos previstos em lei" (DEZEM, 2008, p.155).

Por fim, não há que se confundir prova típica, cujo conceito foi apresentado anteriormente, com prova nominada, pois a prova nominada é aquela prevista em lei, com ou sem procedimento previsto, como no caso da reconstituição, que está disciplinada no art. 7.º do Código de Processo Penal, mas não há previsão quanto ao seu procedimento. Trata-se de prova nominada e atípica (DEZEM, 155).

6. OS MEIOS DE PRODUÇÃO DE PROVA TÍPICOS

Conforme mencionado anteriormente, no direito processual brasileiro, são exemplos de meios de produção de prova típicos a prova testemunhal, a prova documental e a prova pericial, todos disciplinados pelo Código de Processo Penal. Embora igualmente importantes para a elucidação do fato delituoso, no âmbito deste trabalho apenas será analisada a prova pericial como meio de produção de prova.

6.1 A prova pericial

A prova pericial é um meio de produção de prova típico consistente no exame de coisa ou pessoa realizado por técnicos ou especialistas em determinada área do conhecimento, cabendo fazer afirmações ou extrair conclusões relevantes ao processo.

É disciplinado pelos arts. 158 a 184, do Título VII do Código de Processo Penal (Capítulo II – O exame do corpo de delito e as perícias em geral), que, conforme visto anteriormente, sofreu alterações quanto a alguns pontos relacionados à matéria probatória. Especificamente em relação à prova pericial, houve alterações quanto ao número e qualificação dos peritos e a introdução da figura do assistente técnico.

Segundo Mendonça (2008) duas foram as finalidades das alterações referentes à prova pericial: simplificar a realização das perícias e melhor assegurar às partes a garantia do contraditório.

O Código de Processo Penal brasileiro disciplina a prova pericial de forma genérica e não sistemática. Enumera algumas perícias específicas. São elas: exame de corpo de delito (art. 158); autópsia (art. 162); exumação (art. 163); exame de lesões corporais (art.168); exame do local do crime (art. 169); exames de laboratório (art. 170); exame sobre destruição ou rompimento de obstáculos à subtração da coisa ou por meio de escalada (art. 171); perícia no crime de incêndio (art. 173);

exame para o reconhecimento de escritos (art. 174) e exame de instrumentos do crime (art. 175).

Embora o Código apresente elenco das provas periciais, não há previsão legal satisfatória para várias delas quanto ao procedimento probatório e, considerando o avanço tecnológico dos últimos tempos, não há sequer a previsão nominal de muitas perícias já praticadas na atualidade, gerando a problemática quanto à tipicidade desse meio de prova.

Nesse sentido, ao tratar do tema, Fernandes (2007, p. 204) cita ponderações feitas pelos relatores da XX Jornada de Ibero-americana de Direito Processual na transcrita afirmação: “Salientam os relatores que, em todos esses casos, há regras genéricas sobre as perícias, em especial sobre seu objeto, sem que haja, contudo, uma disciplina específica sobre o procedimento a ser adotado”.

Esse autor pondera ainda que a principal questão relacionada à perícia é quanto à tipicidade, pois falta regulamentação do procedimento a ser adotado na sua realização, em função do surgimento de novas técnicas de investigação, fruto do constante avanço tecnológico. Ele cita exemplos dessas modalidades não previstas no Código: “perícia de voz para comprovação da autoria do diálogo objeto de interceptação telefônica; exame de DNA para comprovação de material genético do acusado com material genético encontrado; perícias em discos rígidos nos crimes cometidos pela internet” (Fernandes, 2007, p. 205).

Posição contrária defende Dezem, ao afirmar que:

> “tem havido alguma discussão doutrinária acerca de perícias não previstas em lei. Com efeito, a evolução da ciência acontece com maior rapidez do que a evolução legislativa, daí por que a dificuldade em se regulamentar estas demais perícias. A questão aqui, contudo, não está ligada diretamente à tipicidade do meio de prova, mas ao método investigativo utilizado pelo perito. Não é possível que se reconheça atipicidade nesta situação, pois a perícia existe regulamentada como meio de prova. O que não está regulamentado é o procedimento técnico levado a cabo pelo perito, e, insista-se, tal não precisa estar para que se possa reconhecer a tipicidade do meio de prova. A forma como se dá o trabalho científico não é, via de regra, integrante da tipicidade processual” (DEZEM, 2008, p.114 - 115).

Mesmo em face da ausência de previsão específica, quanto ao procedimento a ser adotado para a realização da perícia, há doutrinadores que entendem que se

deve aplicar as regras gerais do Código de Processo Penal, adaptando-se o procedimento a meios de prova semelhantes. Entretanto, segundo esses doutrinadores, também não está contemplado no Código de Processo Penal qualquer procedimento probatório genérico que possa ser aplicado a todos os casos em que não há disciplina expressa para a realização da prova. Para esses casos, nada impede que sejam aplicados procedimentos probatórios já existentes, por analogia.

Nesse sentido, é a conclusão do relatório da XX Jornada Ibero-americana de Direito Processual apresentada por Fernandes (2007, p. 232):

> "Os problemas de atipicidade da prova pericial derivam do fato de serem realizadas perícias não regulamentadas, ou seja, perícias atípicas, como, por exemplo, a perícia de reconhecimento de voz. Os relatórios informam a existência de normas genéricas sobre a produção das perícias e a previsão de procedimentos específicos para algumas perícias, mas, principalmente ante o desenvolvimento tecnológico e as novas técnicas de investigação, referem-se à necessidade de realização de perícias não reguladas. Seguem-se nesses casos as regras genéricas sobre a prova pericial e, se existente, forma análoga de produção da prova. O problema é muitas vezes mais de ordem técnica, ou seja, sobre a maneira de se realizar a perícia, do que jurídico".

Entretanto, especificamente quanto aos crimes informáticos praticados por meio da internet, tais como ameaça ou crimes contra a honra cometidos por meio de e-mail, pornografia infantil utilizando-se de sites de relacionamento, fraudes bancárias utilizando-se do serviço de internet banking, entre outros, que exigem prova pericial em meios computacionais para se estabelecer a autoria e materialidade do ato delitivo, a problemática da atipicidade da prova não se trata, exclusivamente, de questão de ordem técnica, sobre a maneira de se realizar a perícia, mas também de questão jurídica.

A prova pericial em meios computacionais relacionada ao crime informático praticado por meio da Internet é o instrumento pelo qual se introduz no processo elementos de prova fundados em especiais conhecimentos técnico-científicos, normalmente desconhecidos do juiz e demais operadores do direito. No entanto, tal constatação evidencia o risco de o juiz e as partes serem incapazes de verificar a idoneidade da prova pericial para a reconstrução dos fatos, tornando-se reféns de um conhecimento hermético, decifrável apenas pelos especialistas.

Desse modo, é imperativo introduzir elementos normativos quanto ao procedimento a ser utilizado na colheita, preservação e armazenamento dos equipamentos e vestígios digitais relacionados ao crime informático praticado pela Internet bem como requisitos de admissibilidade do laudo pericial como critério uniformizador do trabalho do perito. Isso porque a casuística revela que tais procedimentos não raro são executados segundo critérios completamente aleatórios, fixados pelo próprio perito e, em muitos casos, em flagrante desrespeito a direitos e garantias constitucionais, tais como a vida privada, a violação da prova, entre outros. Segundo Leigland (2004), em muitos casos, os procedimentos forenses empregados são construídos de maneira informal e por isso, podem impedir a eficácia ou a integridade da investigação. Muitos investigadores forenses desenvolveram procedimentos empíricos para a realização de investigações digitais. A natureza informal desses procedimentos pode impedir a verificação das provas coletadas ou diminuir o valor das mesmas em processos judiciais.

Sob esse prisma, constata-se a indeclinável necessidade da prova pericial ser produzida sob critérios mínimos fixados previamente por lei. Tais critérios devem ser suficientes para permitir que tanto o juiz como as partes sejam capazes de aferir a validade de sua produção e sua admissibilidade como elemento motivador de decisão judicial.

Por fim, consoante à recente reforma, vale mencionar que a Lei 11.690/2008 promoveu importantes modificações no Código de Processo Penal quanto à prova pericial. O art. 159 e seus parágrafos sofreram pontuais alterações, tendo sido incluídos cinco parágrafos novos. As principais delas são apontadas a seguir.

Quanto aos peritos, passou-se a exigir apenas um, e não dois como o era na antiga redação (art. 159, caput). Contudo, tratando-se de perícia complexa, pode ser nomeado mais de um perito oficial (art. 159, § 7.º).

Outra exigência pertinente e que certamente melhorará a qualidade do trabalho técnico é que o perito oficial deverá ter diploma de curso superior (art. 159, caput). “A mesma regra deverá ser aplicada aos peritos não oficiais, sendo que, neste caso, o curso superior deverá ser preferencialmente na área específica” (GOMES FILHO, 2008, p.278).

Quanto aos quesitos e esclarecimentos dos peritos, foi prevista a possibilidade de formulação de quesitos pelos interessados: Ministério Público, assistente de acusação, ofendido, querelante e acusado (art. 159, § 5.º). Em regra, apenas o Ministério Público e o ofendido terão a faculdade de apresentar quesitos na fase de investigação; o querelado, o assistente de acusação e o acusado só poderão fazê-lo nas perícias determinadas em juízo ou em hipótese de requerimento de esclarecimento em perícia, comenta Gomes Filho (2008).

Uma verdadeira inovação relacionada ao contraditório diz respeito à previsão de oitiva dos peritos, a requerimento das partes para esclarecerem a prova ou para responderem a quesitos (art. 159, § 5.º, I).

Quanto aos assistentes técnicos, importante novidade foi a introdução da figura do assistente técnico no processo penal. Sua atuação é permitida somente na fase judicial (art. 159, § 5.º). Deve ser admitido pelo juiz após a elaboração da perícia oficial (art. 159, § 4.º). Além disso, ele poderá ser inquirido em audiência (art. 159, § 5.º, II, segunda parte).

A propósito da prova pericial, confiram-se, também, as palavras de Gomes Filho (2008, 272):

> "O que deve ser buscado, assim, é o indispensável equilíbrio entre a autoridade do saber especializado e a necessidade de apresentar-se à sociedade uma decisão judicial fundada em uma argumentação coerente e compreensível. Daí também a indeclinável necessidade de que a prova pericial, como qualquer outra prova, seja produzida e discutida com a observância da garantia do contraditório, que, como visto, além de ter fundamentos políticos e sociológicos, também constitui o melhor método para se chegar a uma reconstrução mais verdadeira dos fatos".

A nova sistemática de investigação baseada na verdade processual tem influenciado sobretudo as recentes alterações pontuais do Código de Processo Penal brasileiro, notadamente em relação à disciplina da prova pericial. Entretanto, com o avanço tecnológico, mormente com o desenvolvimento da tecnologia da informação e com o advento da Internet, surge uma nova espécie de delinquência, a criminalidade informática e com ela novos meios de prova, influenciando os clássicos meios de produção de prova, notadamente a prova pericial, sem que a legislação processual tenha incorporado essas inovações, comprometendo a investigação do crime informático.

7. A PERÍCIA EM MEIOS COMPUTACIONAIS

O significativo desenvolvimento da ciência e da tecnologia, notadamente da tecnologia da informação, nas últimas décadas, possibilitando o acesso a conhecimentos cada vez mais especializados e precisos, tem influenciado consideravelmente os meios de pesquisa e de obtenção da prova, notadamente a prova pericial, promovendo a reconstrução dos fatos muito mais próxima à realidade.

Contudo, embora esse arsenal técnico-científico permita uma investigação mais precisa e, portanto, mais eficiente na apuração da verdade, também representa maior risco, uma vez que eventuais erros, distorções, alterações ou mesmo violação dos elementos de prova, na maioria das vezes, são imperceptíveis aos sujeitos do processo.

Segundo Beckwith, TG, Marangoni, RD, Lienhard, JH, apud Casey (2002), para serem úteis, as medidas devem ser confiáveis. Ter informações incorretas é potencialmente mais prejudicial do que não ter informação. A situação, naturalmente, suscita a questão da exatidão ou incerteza de uma medição. Arnold O. Beckman, fundador da Beckman Instruments, declarou: “Uma coisa que você aprende na ciência é que não existe uma resposta perfeita, nenhuma medida perfeita.”

Dentro dessa perspectiva, pretende-se examinar a perícia em meios computacionais a partir dos procedimentos relacionado à colheita e custódia dos vestígios digitais deixados pelo crime informático praticados por meio da Internet, tidos como atos preparatórios que antecedem ao exame pericial propriamente dito.

Também, tenciona-se analisar o laudo pericial a fim de apontar critérios norteadores à sua fundamentação.

A perícia em meios computacionais é objeto de estudo da computação forense, ciência que se dedica à análise técnica de situações fáticas em que os sistemas informáticos são o meio para a prática de ilícitos ou o bem visado pela prática do ilícito.

Como todo o meio de produção de prova, a perícia em meios computacionais é um instituto de direito processual e consiste numa manifestação técnico-científica

que se materializa por meio de um laudo que poderá servir como elemento a fundamentar medida cautelar, bem como sentença judicial.

Ainda que não exista previsão legal específica que regule a matéria, parte do que vem disciplinado no Código de Processo Penal, por se tratar de normas genéricas, aplica-se igualmente a este tipo específico de perícia.

Somente deve ser realizada quando, para a apuração da verdade, houver a necessidade de um parecer que exija conhecimentos técnico-científicos especializados, relacionados aos meios computacionais.

Conforme Aranha (1994), a perícia consiste em uma manifestação eminentemente técnica mediante a qual o experto nomeado emite uma declaração de ciência, uma afirmação de um juízo ou então, ambas simultaneamente. Sendo que, a função do perito pode restringir-se ao relato técnico das impressões colhidas, consistindo tão somente numa declaração de ciência. Ao passo que, em uma outra situação poderá ser requisitado a interpretar ou apreciar cientificamente um fato, emitindo um juízo. Por fim, poderá ser solicitado a realizar ambas as ações, ou seja, por primeiro, examinar tecnicamente o fato e, em seguida, emitir um juízo.

De qualquer forma, consistindo numa declaração de ciência ou na emissão de um juízo, o fato é que a manifestação do perito, quando acatada, passa a fazer parte da fundamentação da decisão judicial, sendo muitas vezes, o único meio de prova obtido, o que nos faz questionar sobre sua validade como fundamento exclusivo para embasar sentença judicial visto não haver, nesses casos, a possibilidade de cotejá-lo com outros meios de prova. Segundo Casey (2002), mesmo quando as incertezas são minimizadas, não é possível se ter fontes totalmente confiáveis relacionadas às evidências digitais pois essas, na melhor das hipóteses, são circunstanciais, o que torna mais difícil incriminar um indivíduo apenas por meio de vestígios digitais. Portanto, é necessário mais do que uma evidência digital, é necessário um conjunto probatório formado por confissões, imagens de vigilância por vídeo, ou provas físicas para superar a incerteza inerente ao vestígio digital.

Importante consignar que no sistema processual penal brasileiro o legislador previu o sistema da relativa liberdade ao juiz, pois em regra, não é obrigado a determinar a realização da prova pericial, exceto nos crimes que deixam vestígio, tais como os crimes informáticos, conforme preceitua o artigo 158 do referido código:

“Quando a infração deixar vestígios, será indispensável o exame de corpo de delito, direto ou indireto, não podendo suprí-lo a confissão do acusado.”

Sobre o resultado da perícia, é facultado ao magistrado aceitá-lo ou não, em função do princípio do livre convencimento, confirmando o brocardo latino segundo o qual o Juiz é o perito dos peritos.

No entanto, ainda que o magistrado não esteja vinculado ao resultado da perícia, podendo rejeitar suas conclusões conforme preceitua o artigo 182 do Código de Processo Penal: “O juiz não ficará adstrito ao laudo, podendo aceitá-lo ou rejeitá-lo, no todo ou em parte”.

Segundo Aranha (1994), embora o juiz não esteja vinculado ao resultado do exame pericial, podendo não aceitá-lo (CPP, art. 182), somente poderá rejeitá-lo em duas situações, quais sejam, por erro ou por dolo dos peritos. Considerando que a prova pericial tem como fundamento a nomeação de experto com conhecimentos especializados, os quais as partes e o juiz desconhecem seria incoerente a rejeição de sua conclusão, exceto nos casos de erro ou dolo. Cumpre mencionar que, embora não esteja vinculado ao resultado da perícia, o juiz só poderá rejeitar a perícia nessas hipóteses, pois se fosse capaz de chegar a esse resultado sozinho, o exame pericial seria totalmente desnecessário.

Resta, no entanto, uma terceira hipótese de recusa do laudo pericial pelo juiz, a falta de fundamentação. Não é aceitável que um juízo técnico-científico que poderá constituir-se em elemento fundante de sentença judicial que, por sua vez, decidirá sobre a condenação ou absolvição do acusado, seja desprovido de fundamentação. A questão da fundamentação do laudo pericial será abordada posteriormente.

7.1 Do corpo de delito e dos instrumentos do crime relacionados à perícia em meios computacionais

Ao analisar a prova pericial em meios computacionais é imperativo o entendimento de dois conceitos básicos, pré-requisitos para a compreensão da matéria. São eles o corpo de delito e os instrumentos do crime.

Corpo de delito trata-se de expressão que foi criada para estabelecer a diferença entre a materialidade do crime e as circunstâncias que motivaram o agente à prática do ilícito.

Há certos crimes que deixam vestígios materiais, por outro lado, há os que não deixam os referidos vestígios. Desse modo, o corpo de delito trata-se do conjunto, da somatória de todos os vestígios e sinais deixados pelo delito.

Segundo Mendes, apud Aranha (1994, p. 143): “Corpo de delito é o conjunto de elementos sensíveis do fato criminoso”. Assim, elementos sensíveis trata-se de tudo o que pode afetar os sentidos, ou seja, pode ser captado por nossos órgãos sensoriais tais como pela vista, pelo ouvido, pelo tato, pelo gosto, pelo olfato.

Formar o corpo de delito significa, portanto, recompor, por meio da observação, esses elementos sensíveis que compõem o fato criminoso. Dessa forma, o exame do corpo de delito é a análise técnica desses elementos sensíveis também denominados vestígios.

Por sua vez, instrumentos do crime são todos os objetos materiais utilizados pelo agente para a prática do ilícito. E, consequentemente, o exame dos instrumentos do crime, ainda segundo Aranha (1994, p. 144):

> “Constitui numa análise técnica dos objetos materiais utilizados pelo agente para delinquir e, com base nos quais, serão apreciados a natureza e eficiência, potencialidade danosa, intensidade dolosa e grau de culpa e, por derradeiro, a periculosidade do criminoso.”

Por esta razão, o exame do corpo de delito constitui elemento essencial nos crimes que deixam vestígio, sendo prova fundamental e obrigatória[8], não suprida por

[8] Importante decisão do Superior Tribunal de Justiça que negou trancamento do inquérito policial, recomendando ao juízo monocrático determine a realização imediata da perícia requerida pelo Ministério Público nos autos, sob pena de trancamento da ação penal, merece ser registrada como ilustração quanto à exigência da realização do exame pericial quando o crime deixa vestígio.
Recurso em habeas corpus nº xxxxxx
Recorrido : tribunal regional federal da 3a região
Recurso em *habeas corpus* . Penal. Art. 241. Internet.
Sala de bate papo. Sigilo das comunicações.
Inviabilidade. Trancamento do inquérito policial.
Necessidade de exame aprofundado do conjunto
Probatório. Inadequação da via eleita.
“1. A conversa realizada em "sala de bate papo" da internet, não está amparada pelo sigilo das comunicações, pois o ambiente virtual é de acesso irrestrito e destinado a conversas informais.

qualquer outra prova, mesmo a confissão do acusado. É o que se conclui da redação do artigo 158 do Código de Processo Penal que preceitua: “Quando a infração deixar vestígios, será indispensável o exame de corpo de delito, direto ou indireto, não podendo supri-lo a confissão do acusado.”

Ainda que o artigo acima citado mencione a possibilidade do exame de corpo de delito indireto, tal somente será admitido excepcionalmente. Neste sentido tem sido a jurisprudência dominante, conforme abaixo colacionado:

> “Em se tratando de delito que deixa vestígio o seu reconhecimento somente é possível diante de prova técnica, admitindo-se o exame indireto, apenas quando absolutamente impossível o direto” (Ap.182.963, TACrimSP, Rel. Camargo Aranha; JTACrim, 64:177).
> “Provas. Exame de corpo de delito. O exame pericial direto deve ser feito quando a infração deixa vestígios. A prova testemunhal apresenta-se como expediente meramente supletivo para comprovação do corpo de delito” (JTACrim, 72:282).

O Egrégio Tribunal de Alçada Criminal de São Paulo ao posicionar-se sobre a questão, julgou que a prova pericial indireta somente é admitida quando a direta for inalcançável por impedimento legal absoluto ou fato absolutamente invencível (JTACrim, 38:210 e 46:203). Sendo que a jurisprudência dominante tem entendido que o exame indireto somente é possível, desde que justificado, quando os vestígios desaparecerem e os informes sejam harmônicos quanto à natureza e existência do delito.

Cumpre esclarecer que a prova pericial direta é aquela feita sobre o próprio corpo de delito, sendo que o perito tem acesso à materialidade real do fato criminoso, ao passo que a prova pericial indireta trata-se de raciocínio dedutivo que se infere a partir de determinado fato narrado por testemunhas, ou seja, uma reprodução do ocorrido, na impossibilidade da prova direta.

Desse modo, pode-se concluir que: para os delitos que deixam vestígio a prova pericial é obrigatória, não suprível por qualquer outra, sequer pela confissão do réu, sendo que sua ausência importará na absolvição por falta de provas,

---

2. O trancamento do inquérito policial em sede de recurso em *habeas corpus* é medida excepcional, somente admitida quando constatada, *prima facie*, a atipicidade da conduta ou a negativa de autoria.
3. Recurso que se nega provimento, com a recomendação de que o juízo monocrático determine a realização imediata da perícia requerida pelo *parquet* nos autos, sob pena de trancamento da ação penal.”

conforme o artigo 386, inciso II[9], do Código de Processo Penal e, ainda, em regra, a prova pericial será sempre direta, sendo admitida a prova indireta, em último caso, diante da impossibilidade da primeira, devidamente justificada.

Relativamente aos crimes contra a propriedade imaterial tais como violação de programa de computador (considerado crime informático), como espécie de crime que deixa vestígio, a prova pericial é disciplinada por normas processuais específicas. O exame de corpo de delito, nesses casos constitui prova essencial para o recebimento da queixa ou denúncia, ou seja, trata-se de condição de procedibilidade, conforme depreende-se do artigo 525 do Código de Processo Penal: "No caso de haver o crime deixado vestígio, a queixa ou a denúncia não será recebida se não for instruída com o exame pericial dos objetos que constituam o corpo de delito."

Neste sentido é a decisão do Tribunal de Justiça do Estado de São Paulo, de 17 de agosto de 2.004:

> Recurso Criminal n. 2002.016893-4 Gab. Des. Amaral e Silva.
> PROCESSUAL PENAL - QUEIXA-CRIME - VIOLAÇÃO DE PROGRAMA DE COMPUTADOR - AUSÊNCIA DE PERÍCIA PRÉVIA A CONSUBSTANCIAR O PEDIDO - FALTA DE INTERESSE DE AGIR - REJEIÇÃO - DESPACHO MANTIDO - PRECEDENTES JURISPRUDENCIAIS.
> Nos crimes contra propriedade imaterial que deixam vestígios, a perícia constitui condição de procedibilidade, cuja falta obsta o recebimento da queixa-crime.
> Para o recebimento é imprescindível esteja a queixa revestida de um mínimo de prova capaz de demonstrar o interesse de agir.
> (…)
> É imprescindível, nos casos de violação de programa de computador (Lei n. 9.609/98), que venha a queixa-crime acompanhada de inquérito ou prova pericial que demonstre a probabilidade da existência, em tese, do crime.
> A mera alusão a documentos, como o ofício de fl. 57, onde constaria confissão dos recorridos, não basta para justificar o recebimento da inicial.
> O artigo 525 do Código de Processo Penal é claro ao afirmar que:
> "*No caso de haver o crime deixado vestígio, a queixa ou a denúncia não será recebida se não for instruída com o exame pericial dos objetos que constituam o corpo de delito*.
> E prossegue o mencionado artigo:

[9] Artigo 386 do código de processo penal "O juiz absolverá o réu, mencionando a causa na parte dispositiva, desde que reconheça:
[...]
II-não haver prova da existência do fato;

> *Sem a prova de direito à ação, não será recebida a queixa, nem ordenada qualquer diligência preliminarmente requerida pelo ofendido*.
> Guilherme de Souza Nucci, sobre os crimes contra a propriedade imaterial, explica:
> "O exame de corpo de delito (exame pericial constatando a existência do crime) é condição de procedibilidade para o exercício da ação penal. Sem ele, nem mesmo o recebimento da denúncia ou queixa ocorrerá" (Código de Processo Penal Comentado, 2ª ed. São Paulo: RT, 2003, p. 734/735).
> Neste Tribunal:
> PROPRIEDADE INTELECTUAL. VIOLAÇÃO DE DIREITO DE AUTOR DE PROGRAMA DE COMPUTADOR. QUEIXA-CRIME DESPROVIDA DE PRÉVIA VISTORIA (ART. 13 DA LEI N. 9.609/98). NÃO RECEBIMENTO. DECISÃO MANTIDA
> "Nos crimes contra a propriedade intelectual, como no caso de cópia ilegal de software (Lei n. 9.609/98), o recebimento da queixa-crime fica vinculado à prévia vistoria (art. 13)" (Recurso Criminal n. 98.009039-3, de Brusque, rel. Des. José Roberge).

7.2 Procedimento referente à prova pericial em meios computacionais

À semelhança do ilícito praticado no meio físico, o ilícito informático praticado por meio da Internet também é passível de ser investigado, mormente por tratar-se de crime que deixa vestígio. Ainda que as evidências dessa espécie de crime estejam em grau de complexidade diferente, parte dos procedimentos são semelhantes para ambas as investigações.

No que diz respeito ao procedimento relacionado à prova pericial em meios computacionais, podemos dividi-lo em três momentos, quais sejam: iniciativa, execução e materialização ou exteriorização.

7.2.1 Iniciativa

A iniciativa do exame pericial dependerá diretamente do momento em que se encontra a investigação do fato delituoso. Se estiver na fase do inquérito policial, fase extrajudicial, portanto, a iniciativa é da autoridade policial. Caso já tenha sido proposta ação, ou seja, esteja já na fase judicial, o juiz poderá requerer a perícia de

ofício e de imediato, quando obrigatória, ou mediante provocação, nos demais casos. Contudo, no caso de não ser obrigatória, se requerida pelas partes, poderá ser indeferida pela autoridade policial ou pelo juiz, caso não seja necessária, nos termos do artigo 184 do Código de Processo Penal, que preceitua: “Salvo o caso de exame de corpo de delito, o juiz ou a autoridade policial negará a perícia requerida pelas partes, quando não for necessária ao esclarecimento da verdade.”

Importante frisar que, em função do direito à prova e ampla defesa, toda prova requerida pelas partes, em tese, deve ser deferida, desde que admissível e cujo pedido seja tempestivo.

Aspecto importante a ser mencionado quanto ao momento referente à iniciativa é a questão tanto da nomeação do perito bem como da oportunidade para a realização da perícia.

7.2.1.1 Da Nomeação do perito

Concernente à nomeação, o elemento justificador é o fato de ser o perito detentor de conhecimentos técnico-científicos altamente especializados, que caracterizam a função.

Entretanto, antes de tratar especificamente deste tópico, faz-se necessário tecer algumas considerações quanto à figura do perito.

O perito é considerado um auxiliar da justiça, compromissado, imparcial, sem impedimentos ou incompatibilidades para atuar no processo. É considerado auxiliar da justiça pois trata-se de pessoa física que, não sendo juiz nem exercendo funções judicantes, presta serviços permanentes à justiça, no caso das periciais oficiais ou em função de livre nomeação, tendo sido incluído no Título VIII do Livro I do Código de Processo Penal (Capítulo VI), no tópico relativo aos auxiliares da justiça.

É pessoa legitimamente compromissada uma vez que é exigido do perito que preste compromisso, em função das declarações que emitirá, sendo que as mesmas são capazes de fundamentar a decisão judicial. Os peritos oficiais prestam compromisso uma única vez, ao assumirem o cargo. Ao passo que os peritos não

oficiais, prestarão compromisso caso a caso, segundo o art. 159, §2º, do Código de Processo Penal.

O perito deve ser imparcial, comportando-se como um terceiro equidistante das partes, visto que as causas de suspeição são as mesmas dos juízes, como disciplina o art. 280 do Código de Processo Penal.[10]

Os impedimentos que sujeitam o perito são de três categorias: por indignidade (CPP, art. 279, I), por incompatibilidade (CPP, art. 279, II) e por incapacidade (CPP, art. 279, III)[11].

Como auxiliares da justiça, os peritos estão sujeitos à disciplina judiciária (CPP, art. 275)[12], e aos estatutos funcionais. Para efeitos penais, são considerados funcionários públicos (CP, art.327)[13].

Tem como deveres: não recusar a nomeação (CPP, art. 277); não deixar de acudir à intimação ou ao chamado da autoridade (CPP, art. 277, a); não deixar de comparecer no dia e local designados para o exame (CPP, art. 277, b); não dar laudo ou concorrer para que a perícia não seja feita dentro dos prazos pré-estabelecidos (CPP, art. 277, c)[14].

A infração a tais deveres é a multa, além da condução coercitiva (art.278).[15]

Por fim, há o crime de falsa perícia, tipificado no art. 342 do Código Penal, que pode ser praticado mediante as seguintes condutas: a) fazer afirmações falsas,

---

10 Artigo 280 do Código de Processo Penal: "É extensivo aos peritos, no que lhes for aplicável, o disposto sobre suspeição dos juízes."

11 Artigo 279 do Código de Processo Penal: "Não poderão ser peritos:
I - os que estiverem sujeitos à interdição de direito mencionada nos ns. I e IV do art. 69 do Código Penal;
II - os que tiverem prestado depoimento no processo ou opinado anteriormente sobre o objeto da perícia;
III - os analfabetos e os menores de 21 anos."

12 Artigo 275 do Código de Processo Penal: "O perito, ainda quando não oficial, estará sujeito à disciplina judiciária."

13 Artigo 327 do Código Penal: "Art. 327 - Considera-se funcionário público, para os efeitos penais, quem, embora transitoriamente ou sem remuneração, exerce cargo, emprego ou função pública.

14 Artigo 277 do Código de Processo Penal: "Art.277.O perito nomeado pela autoridade será obrigado a aceitar o encargo, sob pena de multa de cem a quinhentos mil-réis, salvo escusa atendível.
Parágrafo único.Incorrerá na mesma multa o perito que, sem justa causa, provada imediatamente:
a) deixar de acudir à intimação ou ao chamado da autoridade;
b) não comparecer no dia e local designad o exame;
c) não der o laudo, ou concorrer para que a perícia não seja feita, nos prazos estabelecidos.

15 Artigo 278 do Código de Processo Penal: "No caso de não-comparecimento do perito, sem justa causa, a autoridade poderá determinar a sua condução."

por meio de conduta comissiva por meio da qual afirma uma inverdade; b) negar a verdade, na qual o louvado nega o que sabe; e c) calar a verdade, omitindo o que sabe.[16]

Com a reforma do Código de Processo Penal, por meio da lei 11.690/2008, anteriormente mencionada, houve consideráveis alterações relativas à prova pericial, notadamente quanto à nomeação do perito.

Atualmente, a norma exige apenas um perito oficial, portador de diploma de curso superior [17], ressalvando-se os casos de perícia complexa, envolvendo mais de uma área de conhecimento em que poderá ser designado mais de um perito oficial para o caso[18], mantendo-se a adoção, pelo Código, do princípio da perícia oficial.

Com relação aos peritos não oficiais, permanece a exigência de duas pessoas idôneas para a realização da perícia, desde que sejam portadores de diploma de curso superior, preferencialmente na área específica[19].

Entretanto, a grande novidade da lei foi prever a figura do assistente técnico no âmbito do processo penal, antes apenas admitido no processo civil. Da mesma forma que o perito, o assistente técnico é pessoa detentora de conhecimentos técnico-científicos, trazendo ao processo informações especializadas importantes na execução e conclusão da perícia.

Como atua no interesse da parte não tem o assistente técnico o dever de imparcialidade, não estando sujeito, diferentemente do perito, a impedimento e

---

16 Art. 342. Fazer afirmação falsa, ou negar ou calar a verdade como testemunha, perito, contador, tradutor ou intérprete em processo judicial, ou administrativo, inquérito policial, ou em juízo arbitral:

Pena - reclusão, de um a três anos, e multa.

§ 1º - Se o crime é cometido com o fim de obter prova destinada a produzir efeito em processo penal:

Pena - reclusão, de 2 (dois) a 6 (seis) anos, e multa.

§ 2º - As penas aumentam-se de um terço, se o crime é praticado mediante suborno.

§ 3º - O fato deixa de ser punível, se, antes da sentença, o agente se retrata ou declara a verdade.

§ 1° - As penas aumentam-se de um sexto a um terço, se o crime é praticado mediante suborno ou se cometido com o fim de obter prova destinada a produzir efeito em processo penal, ou em processo civil em que for parte entidade da administração pública direta ou indireta.

§ 2° - O fato deixa de ser punível se, antes da sentença no processo em que ocorreu o ilícito, o agente se retrata ou declara a verdade.

17 Artigo 159 do Código de Processo Penal: “O exame de corpo de delito e outras perícias serão realizados por perito oficial, portador de diploma de curso superior.”

18 Artigo 159,

19 Artigo 159, §1°: “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.”

suspeição.[20] A lei não é clara mas, segundo entendimento jurisprudencial já firmado, tudo leva a crer que a atuação do assistente técnico se dá na fase judicial.

7.2.1.2 Da oportunidade para a realização da perícia

A respeito da oportunidade, embora o Código de Processo Penal não discipline especificamente a questão, a regra mais segura e acertada, considerando os crimes que deixam vestígio, é “quanto antes melhor”, implicando em providências ágeis a serem adotadas pela autoridade policial ou, se for o caso, pela autoridade judicial, a fim de se preservar os vestígios, evitando que os mesmos desapareçam.

Atentando à celeridade que se impõe ao cumprimento das diligências para a colheita e preservação dos vestígios, a lei processual prevê a possibilidade da perícia ser realizada a qualquer dia e hora, conforme estatui o artigo 161 do Código de Processo Penal, textualmente:“O exame de corpo de delito poderá ser feito em qualquer dia e a qualquer hora.”

Nesse sentido, a conduta da referida autoridade, que antecede ao exame pericial, é de fundamental importância para a obtenção dos elementos de prova a serem periciados.

Importante mencionar que entre a iniciativa e a execução do exame pericial há um momento intermediário, referente aos atos preparatórios, consistente na coleta e preservação dos vestígios digitais que possibilitarão a realização do referido exame.

Conforme preceitua o artigo 6º do Código de Processo Penal:

---

[20] Artigo 159,

§3º Serão facultadas ao Ministério Público, ao assistente de acusação, ao ofendido, ao querelante e ao acusado a formulação de quesitos e indicação de assistente técnico.

§ 4º O assistente técnico atuará a partir de sua admissão pelo juiz e após a conclusão dos exames e elaboração do laudo pelos peritos oficiais, sendo as partes intimadas desta decisão.

§ 5º Durante o curso do processo judicial, é permitido às partes, quanto à perícia:

[...]

II – indicar assistentes técnicos que poderão apresentar pareceres em prazo a ser fixado pelo juiz ou ser inquiridos em audiência.

> “Logo que tiver conhecimento da prática da infração penal, a autoridade policial deverá:
> I - dirigir-se ao local, providenciando para que não se alterem o estado e conservação das coisas, até a chegada dos peritos criminais;
> II - apreender os objetos que tiverem relação com o fato, após liberados pelos peritos criminais;
> III - colher todas as provas que servirem para o esclarecimento do fato e suas circunstâncias;
> (…)
> VII - determinar, se for o caso, que se proceda a exame de corpo de delito e a quaisquer outras perícias;”

De fato, cabe à autoridade policial zelar pela preservação do local onde ocorreu o suposto ilícito a ser investigado, como também dos equipamentos a serem periciados, até a chegada da equipe técnica.

Qualquer alteração do estado das coisas não somente poderá comprometer a conclusão sobre a materialidade e a autoria do ilícito, como também poderá levar à nulidade de futuro exame pericial em função da violação da prova.

Da mesma forma, cabe à autoridade determinar a realização do exame de corpo de delito e quaisquer outras perícias, principalmente no âmbito do inquérito policial, uma vez que é da competência da referida autoridade a presidência do inquérito.

Entretanto, crítica que se faz ao artigo acima citado relaciona-se aos equipamentos e eventuais vestígios deixados pelo crime informático praticado por meio da Internet, armazenados nesses equipamentos. Trata-se de vestígios digitais, que envolvem conhecimentos técnicos não somente para a sua análise mas igualmente para a sua colheita e preservação, sem falar no manuseio e no transporte dos referidos equipamentos.

Portanto, somente o experto em realizar perícias em meios computacionais tem o conhecimento e a competência adequados para executar pessoalmente a coleta, preservação e análise dos vestígios digitais e respectivos equipamentos responsabilizando-se pelos mesmos, sob pena de expor ao risco de alteração, violação ou até destruição dos elementos de prova relacionados.

Não se pode exigir da autoridade policial, que não tem formação técnica nem tampouco treinamento adequados, seja responsável pela apreensão dos objetos que tiverem relação com o fato após liberados pelos peritos criminais e pela colheita de todas as provas que sirvam para o esclarecimento do fato e suas circunstâncias.

Em se tratando de crimes informáticos praticados por meio da Internet, os objetos referem-se a equipamentos informáticos que devem ser apreendidos e custodiados pelos peritos, diretamente ou sob sua supervisão e responsabilidade uma vez que somente eles saberão sob que condições os mesmos deverão ser apreendidos, transportados e custodiados, fiscalizando o atendimento a essas exigências, visto que não podem ser expostos a temperaturas excessivas, a campos magnéticos, entre outros.

É pertinente lembrar que o exame pericial dos vestígios coletados, em geral, não é realizado no local do crime. Portanto, o material a ser periciado deverá ser transportado ao laboratório do instituto de criminalística correspondente para sua análise. Daí a importância do transporte como parte da cadeia de custódia a ser preservada.

Atualmente, os referidos equipamentos e mídias, depois de periciados, ficam sob a guarda da autoridade policial ou mesmo do instituto de criminalística correspondente. Isto porque, conforme dispões o artigo 11 do Código de Processo Penal, os instrumentos do crime, bem como os objetos que interessarem à prova, acompanharão os autos do inquérito, que, conforme acima mencionado, estão sob a presidência da autoridade policial.

Contudo, ainda que os referidos equipamentos e mídias estejam sob a responsabilidade da polícia ou do instituto de criminalística, tal fato não tem significado garantia da devida custódia. Isto porque, muitos destes materiais são armazenados em locais inadequados sem qualquer cuidado ou controle, sendo expostos a todo tipo de violação. Somente regras rígidas e fiscalização adequada seriam capazes de assegurar a preservação da prova relacionada não somente à coleta mas também a toda a cadeia de custódia do material apreendido.Ainda neste contexto, o artigo 159, §6° do mesmo diploma legal, incluído pela Lei 11.690/08, estatui:

> “Havendo requerimento das partes, o material probatório que serviu de base à perícia será disponibilizado no ambiente do órgão oficial, que manterá sempre sua guarda, e na presença de perito oficial, para exame pelos assistentes, salvo se for impossível a sua conservação.”

Segundo Gomes Filho (2008, 279), com a inovação legal, estabeleceu-se que, havendo requerimento das partes, o material que serviu de base à perícia será disponibilizado no ambiente do órgão oficial, que manterá sempre sua custódia, e na presença de perito oficial, para exame pelos assistentes técnicos, salvo se for impossível a sua conservação. Desta forma, segundo o autor citado, fixou-se uma dupla obrigação para os órgãos oficiais: que conservem sob sua guarda os objetos materiais que forem objeto de perícia e, ainda, que o perito oficial esteja presente na realização de exames pelos assistentes técnicos.

Pondera ainda Gomes Filho (2008) que a expressão “sempre sua guarda” empregada pelo legislador pode ensejar o entendimento de que a conservação desses objetos é indefinida. Mas isso deve ser lido à luz do sistema do Código de Processo Penal, que no art. 118, prevê textualmente: “Antes de transitar em julgado a sentença final, as coisas apreendidas não poderão ser restituídas enquanto interessarem ao processo”. Conclui então o referido doutrinador que, com o trânsito em julgado da sentença final, cessa essa obrigação para o órgão oficial. Mesmo antes disso, será possível que o juiz, depois de ouvir os eventuais interessados na realização de exames pelos assistentes técnicos, verifiquem que a conservação dos referidos objetos é dispensável.

Desta forma, há que se ter instrumento legal que contemple a exigência do respectivo instituto de criminalística ser responsável, pela custódia não só dos equipamentos e mídias relacionados à prática do delito, bem como dos materiais a eles relacionados, até o trânsito em julgado do processo ou durante o período em que o juiz da causa entender pertinente. Pois, pode ser necessária a realização de novo exame pericial por invalidade do primeiro ou mesmo para a verificação de algum ponto obscuro relacionado à conclusão.

Embora, neste momento ainda não ocorra a análise dos vestígios, ou seja, o exame pericial propriamente dito, esta fase é essencial, pois caso os vestígios sejam colhidos e preservados de forma inadequada, poderão inviabilizar a perícia ou mesmo tornar nulo futuro exame pericial.

Contudo, compete ao Estado prover condições mínimas de trabalho e estrutura adequada para que as polícias e os institutos de criminalística possam atender a essas exigências, visto que não são poucos os casos em que não há

peritos suficientes para acompanhar as diligências, ou mesmo ferramentas adequadas para a realização do exame pericial, sem falar nas condições em que estes equipamentos e mídias são transportados e custodiados, entre outras dificuldades.

7.2.2 Coleta e custódia dos vestígios digitais

Conforme já mencionado, a coleta e custódia dos vestígios digitais, a serem periciados, exigem uma série de cuidados até o momento da realização da perícia propriamente dita, pois é necessária a adoção de procedimentos a serem executados metodicamente.

A casuística revela que o tempo gasto para a concessão da medida de busca e apreensão dos equipamentos informáticos e materiais a eles relacionados a ser executada pela autoridade policial e também a forma como se processa sua operacionalização, é determinante para a viabilização do exame pericial em crimes desta natureza. Isto porque, segundo Hosmer (2002), a confiabilidade dos vestígios digitais é uma questão crítica para o perito, pois os mesmos são provenientes de uma multiplicidade de fontes, incluindo: computadores apreendidos, discos rígidos e mídias de backup, mensagens em tempo real de e-mails, salas de bate-papo (chat-rooms), registros do provedor de Internet (ISP), páginas web, tráfego digital de redes, bancos de dados locais e virtuais, diretórios digitais, dispositivos sem fio, cartões de memória e câmeras digitais.

Ainda segundo o mesmo autor, uma vez que a extração dos elementos de prova digital foi realizada, proteger a integridade digital torna-se uma preocupação fundamental para investigadores, Ministério Público e os acusados. A facilidade com que os vestígios digitais podem ser alterados, destruídos ou fabricados de uma maneira convincente, até mesmo por usuários de computador iniciantes, é alarmante. Para piorar as coisas, existe hoje a necessidade de preservar, arquivar e proteger a integridade dos vestígios digitais por longos períodos de tempo, e os métodos utilizados dependem da integridade das pessoas, processos,

procedimentos e da segurança do acesso físico. Estes métodos são caros de implementar, repletos de erros potenciais, vulneráveis à modificação acidental ou mal-intencionada, restringindo a utilização generalizada da prova digital em processos litigiosos cruciais.

Corroborando com Hosmer, segundo Kwan; Ray; Stephens (2008), infelizmente, a prova digital é frequentemente danificada ou destruída durante atividades padrão de contenção, erradicação e de recuperação.

Desta forma, alguns cuidados essenciais devem ser atendidos durante uma busca e apreensão para preservar a integridade física dos computadores e mídias contendo dados.

Seria indispensável que, em cada operação dessa natureza, a lei determinasse como requisito essencial a presença de um perito especializado em computação forense para acompanhar toda a operação e que, inclusive, fosse o responsável pelo desligamento dos equipamentos e sua apreensão bem como efetuasse a busca por mídias e dados.

7.2.2.1 O local do crime

A preservação do local do crime, pela autoridade policial até a chegada dos peritos é fundamental para o êxito da colheita dos elementos de prova, como visto anteriormente. Sendo que cabe ao perito registrar todo o material observado e coletado de forma detalhada e precisa.

Desse modo, ao se dirigir ao local do crime, o perito deve ficar atento na busca de quaisquer evidências materiais ou digitais relacionadas ao delito investigado. Mesmo o que aparentemente seja alheio ao fato criminoso pode ter alguma relação com o delito.

Para tanto, o perito poderá valer-se de esquemas ilustrativos, fotografias, filmes, gráficos, ou qualquer outro recurso que facilite a elucidação do caso. É o que se conclui a partir do artigo 169 do Código de Processo Penal que prevê textualmente:

> “Para o efeito de exame do local onde houver sido praticada a infração, a autoridade providenciará imediatamente para que não se altere o estado das coisas até a chegada dos peritos, que poderão instruir seus laudos com fotografias, desenhos ou esquemas elucidativos.”

Ainda sobre o local do crime, segundo Espíndula e Chisum apud Caricatti (2006, p.69) referindo-se ao princípio de Locard:

> “Ocorre transferência mútua de vestígios quando existe contato entre dois objetos ou pessoas, o que implica que haja provas/vestígios em todos os locais em que são cometidos crimes. Os autores podem deixar ou retirar provas/vestígios no local, bem como aqueles que os recolhem”.

Assim, é fundamental que o perito perceba as alterações ocorridas no mundo exterior provocadas por ações humanas ou causas naturais, registrando-as, a fim de analisar o local do crime, identificando os reais vestígios deixados, segundo prevê o parágrafo único do artigo 169 do Código de Processo Penal: “Os peritos registrarão, no laudo, as alterações do estado das coisas e discutirão, no relatório, as consequências dessas alterações na dinâmica dos fatos”.

Observação importante a ser feita é que cabe à autoridade policial garantir a preservação da cena física referente ao crime sob investigação. Sobre a cena física, o local deverá ser totalmente isolada até o término dos trabalhos. Desse modo, não deve ser permitido o ingresso de pessoas estranhas, nem tampouco a entrada ou retirada de qualquer equipamento sem autorização expressa e registro apropriado.

Com efeito, embora seja da autoridade policial a responsabilidade pela segurança da cena física do crime, cabe ao perito a análise da mesma.

Por sua vez, é da responsabilidade do perito garantir a preservação da cena lógica, conjunto dos vestígios digitais deixados pelo ilícito informático praticado por meio da Internet, uma vez que somente o experto tem o preparo necessário para fazê-lo. A cena lógica pode ser protegida, inicialmente, mediante o bloqueio dos usuários, desconectando o sistema da rede.

Entretanto, antes de assegurar a cena lógica é necessário identificar onde ela se encontra pois as evidências podem estar espalhadas por diferentes localidades e dispositivos.

Quando a ação e o resultado do ato ilícito ocorrem em diferentes lugares, muito comum nos crimes informáticos praticados por meio da Internet, em tese, não há uma regra de prioridade sendo que a hierarquia entre eles é estabelecida caso a caso, conforme seja possível precisar a quantidade e qualidade dos vestígios registrados e o grau de informação que seja possível obter quanto à ação delituosa, os agentes envolvidos, a sequência dos fatos, entre outros.

7.2.2.2 A busca por vestígios em sistemas informáticos

Há pouco tempo atrás, a busca e apreensão das máquinas, contendo vestígios digitais, encontradas nos locais em que o crime informático praticado por meio da Internet ocorria, fazia-se a partir do imediato desligamento dos referidos equipamentos.

Com a prática, constatou-se que, ao desligar o equipamento, perdia-se a memória volátil e respectivos registros e uma série de rotinas eram iniciadas tais como: alteração de áreas do disco rígido, com o conteúdo que estava na memória RAM, alteração de arquivos temporários, entre outros. Sem contar que desligar uma estação ou servidor por meio de interrupção do fornecimento de energia pode gerar sérios danos a ponto de impedir sua inicialização.

Com a evolução dos trabalhos relacionados à perícia forense computacional, percebeu-se que, em se tratando de criminoso experiente, este trabalha preferencialmente com a memória volátil , cuidando para não deixar vestígios em áreas permanentes do computador como é o caso dos arquivos em disco.

Conforme Caricatti (2006)[21], com o fim de aperfeiçoar o trabalho do perito, procurou-se classificar por categorias os elementos, tendo como critério o seu grau de volatilidade. Desta forma, enumerou-se os elementos mais voláteis seguidos pelos que têm maiores chances de permanecer inalterados por maior tempo, conforme segue: 1.registros de processador em memória cache, 2.memória

[21] Caricatti, André Machado. O local do crime no Ciberespaço in BLUM, Renato M.S. Opice; BRUNO, Marcos Gomes da Silva; ABRUSIO, Juliana Canha (Coordenadores) – Manual de Direito Eletrônico e Internet, São Paulo: Aduaneiras, 2006.p.73.

principal, 3.estado das conexões de rede, 4.estado dos processos em execução, 5.conteúdo das mídias não removíveis e 6.conteúdo das mídias removíveis.

Dessa forma, considerando a classificação acima, o perito deve, preferencialmente, iniciar seu trabalho de coleta e preservação dos vestígios a partir dos elementos mais voláteis, pois espera-se que resguarde os elementos que têm maiores chances de se perder.

Segundo Lee; Kim; Lee e Lim (2005), especialmente, quando o sistema está ligado, é preciso coletar informações voláteis o mais rápido possível. E então, a coleta de informações não-voláteis é realizada no sistema desligado. Por isso, há um processo de coleta de evidências digitais diferente para sistema ligado e para sistema desligado.

Ainda segundo Caricatti (2006), da mesma forma que a observação de um fenômeno interfere neste, considerando o princípio de Locard, o processo de análise de sistemas informatizados que estejam em funcionamento produz alterações de estados. Na tentativa de reproduzir conteúdos da memória principal ou de memórias auxiliares, é necessária a execução de comandos, sobrescrevendo áreas daquela.

Por outro lado, ao desligar o equipamento perde-se o conteúdo de suas memórias voláteis. Conforme Meyers e Rogers (2004), por exemplo, quando um computador é desligado, os dados em mídia de armazenamento temporário são, do ponto de vista técnico, praticamente impossíveis de serem reconstruídos. Nos crimes da era pré-digital, a eletricidade não era um fator importante para se executar uma busca e apreensão adequada. Embora não haja casos documentados em tribunal estadual ou federal dos EUA que tenha abordado este problema, é uma possibilidade para o futuro. No Reino Unido, um réu questionou a validade de uma mídia de memória volátil indevidamente apreendida. Aaron Caffrey, o réu, foi preso sob a suspeita de lançar um ataque de negação de serviço contra os sistemas do Porto de Houston em 20 de setembro de 2001. A defesa argumentou que um Trojan (cavalo de Tróia) foi instalado no computador do réu por outros que queriam incriminá-lo pelo ataque. O cavalo de Tróia, a defesa sustentou, lançou o ataque a partir do computador do réu, mas o réu não tinha conhecimento do ataque. A perícia revelou que não havia nenhum sinal de um Trojan, somente ferramentas de ataque no computador, mas não conseguiu eliminar a possibilidade de que um cavalo de

Tróia pudesse ter estado na memória de acesso aleatório (RAM). O júri decidiu por unanimidade que o réu não era culpado.

Desse modo, deve o perito, conforme anteriormente mencionado, iniciar a coleta de vestígios a partir dos elementos mais voláteis e, findo o processo de coleta de dados, aí sim, desligar o equipamento.

Com o fim de manter a coerência ao longo do exame, o perito deve observar cada ato seu, registrando-o e documentando, com detalhes, desde a cena física até a cena lógica do crime. As referidas anotações devem ser registradas também no laudo pericial pois entende-se que as mesmas fazem parte da fundamentação do referido documento, sendo portanto, requisito de validade do mesmo.

Contudo, da mesma forma que o equipamento deve ser desligado por perito habilitado, sua inicialização também deve ser feita pelo mesmo profissional. Isto porque o programa principal, pode conter outro programa embutido que, ao ser inicializado particiona o disco rígido e, portanto, precisa ser desativado sob pena de afetar a integridade do referido disco, inviabilizando a realização da perícia.

Nesse sentido, segundo Cosic e Baca (2010), o processo de coleta de vestígios digitais não é simples e os investigadores e peritos devem saber o que se deve fazer no primeiro contato com a evidência. Isso não é trivial, se soubermos que apenas um passo em falso pode ser fatal. Por exemplo, se os investigadores desligarem o computador "ligado" com o sistema operacional Windows XP, mais de 50 arquivos serão alterados e outros 5 novos arquivos serão criados na próxima inicialização. Isso significa que um momento de descuido é suficiente para perder a prova e violar sua integridade.

Conforme Meyers e Rogers (2004), o perito deve conhecer, em detalhes, os sistemas de arquivos e a teoria por trás da estrutura do sistema de arquivos para adaptar esses princípios a novos sistemas de arquivos. Além disso, a fim de determinar se os dados foram devidamente preservados e analisados, o perito deve conhecer a mecânica de engenharia por trás desses dispositivos.

Assim, o que se espera de um perito é que o mesmo seja capaz de tomar decisões, antevendo e responsabilizando-se por suas implicações a fim de que os vestígios digitais, tão efêmeros, não sejam apagados em função de escolhas equivocadas feitas por quem deveria preservá-los.

Ainda que cada área do conhecimento possua suas próprias regras, o trabalho do perito, deverá alinhar-se às diretrizes do método científico tais como a ação planejada e metódica, rigor na preservação das evidências, anotação de cada ação executada, preocupação com o detalhe e seu registro.

Dessa forma, o trabalho do perito, desde a fase de colheita e preservação dos vestígios deve ser planejado antecipadamente, revelando uma ação metódica por meio de registros não só dos equipamentos e mídias apreendidos bem como de cada ato realizado, evitando as alterações provocadas no sistema informático fruto da coleta e análise dos vestígios, sempre tendo como princípio a não violação da prova.

7.2.2.3 A duplicação da mídia

Especificamente no caso dos vestígios digitais, vimos que sua principal limitação é quanto à sua volatilidade pois são facilmente criados, alterados ou mesmo destruídos e, muitas vezes, sem deixar qualquer evidência. Portanto, constitui-se um dever ao perito computacional preservar a integridade dos vestígios durante a sua coleta, ao longo da cadeia de custódia e durante a realização da prova pericial propriamente dita.

Alguns autores utilizam o termo "cadeia de evidências" em vez de cadeia de custódia. O propósito da cadeia de custódia é certificar que a prova não foi alterada ou modificada em todas as fases, e deve incluir a documentação sobre como a evidência é colhida, como foi transportada, analisada e apresentada. Conhecer a localização atual da evidência original, não é suficiente para o tribunal. Deve haver registros precisos de rastreamento de todas as provas materiais em todo tempo. O acesso aos elementos de prova devem ser controlados e auditados. Para comprovar a cadeia de custódia, é preciso conhecer todos os detalhes de como a prova foi tratada a cada passo do caminho. A velha fórmula utilizada pela polícia, jornalistas e pesquisadores - Quem, O quê, Quando, Onde, Por quê e Como - "Cinco Ws" (e um

H) pode ser aplicada para ajudar na investigação forense digital. (COSIC; BACA, 2010, p.429)[22]

Desse modo, para se evitar qualquer tipo de contestação quanto à integridade do vestígio obtido é imperativo fixar controle rígido em sua coleta, estabelecer o gerenciamento da cadeia de custódia correspondente, incluindo o controle de seu armazenamento.

Outro ponto de fundamental importância na preservação da integridade do vestígio digital é a duplicação da mídia original, também denominada mídia de prova[23], para que o exame dos dados seja realizado na mídia de destino[24], possibilitando exames com maior grau de liberdade e segurança.

Exames feitos diretamente na mídia original podem alterá-la, na medida em que modificam, por exemplo, metadados[25] de arquivos, tais como registro de tempo (hora de criação, última edição, último acesso) implicando na violação da prova.

Atualmente, a computação forense possui meios técnicos suficientes e disponíveis para efetuar a duplicação de mídias sem que se altere seu conteúdo, garantindo a integridade dos dados a serem periciados. Ademais, o exame pericial deve ser realizado sob vestígios inalterados, integralmente preservados, visto que, em caso de futuro questionamento, possa ser refeita a perícia a fim de se confirmar o resultado do exame executado.

Há quem entenda ainda que deve ser feita mais de uma cópia da mídia original, permitindo a realização do exame pericial com mais liberdade pois no caso de uma das mídias de destino ter seus dados danificados, em razão do exame, outras cópias existirão para se trabalhar, preservando assim a prova.

---

[22] Importante mencionar que a referida fórmula, usada tanto para as investigações científicas bem como para as investigações policiais, consiste em um procedimento considerado básico para a obtenção de informações a respeito de determinado fato. Trata-se de fórmula usada para se obter a maior quantidade possível de dados a respeito do fato investigado. A máxima dos cinco Ws (e um H) preconiza que para que um informe seja considerado completo deve responder a uma lista de verificações representadas por seis perguntas, cada uma delas compreendendo um termo em inglês: Who (quem), What (o que), Where (onde), When (quando), Why (por quê) e How (como).

[23] Mídia de provas – o suporte original (disco rígido) que precisa ser investigado, seja o sistema de um suspeito ou a vítima de um ataque. (COSTA, 2003)

[24] Mídia de destino – o suporte no qual a mídia de provas é duplicada. Em outras palavras, a imagem pericial de uma unidade de provas é transferida à mídia de destino. (COSTA, 2003)

[25] Metadados são dados de arquivos. Indicam status dos dados como data de criação, data de acesso, data de modificação, tamanho, atributos, etc. (COSTA, 2003)

Entretanto, o principal motivo de se fazer a duplicação da mídia ou mesmo mais de uma cópia, reside no fato de que, além de se evitar que a perícia seja feita diretamente na mídia original, preserva-se o que em computação forense convencionou-se chamar de linha do tempo que nada mais é do que a cronologia dos eventos registrados, relacionados com a prova a ser produzida, denominados metadados, que mostram o status dos dados incluindo a respectiva data. A linha do tempo é capaz de revelar a evolução integral do caso até o final, sendo extremamente útil ao exame pericial.

A duplicação da mídia requer uma série de cuidados a serem observados e o principal deles é que a ferramenta adotada para a execução do processo, em hipótese alguma altere dados da mídia original que contém os elementos de prova. Isto porque, pode ser solicitado judicialmente, a repetição do processo de duplicação a fim de se comprovar que a metodologia empregada assegurou a não violação da prova. Considerando tratar-se de um trabalho técnico-científico, o método empregado deve ser relatado de forma clara e didática, permitindo sua repetição por outro especialista.

Com o intuito de assegurar a fidelidade na duplicação da mídia, Costa (2003, p.29) traz importante contribuição, ao se referir à soma de verificação, nos seguintes termos:

> "A soma de verificação é uma assinatura digital resultante da utilização de um algoritimo sobre a mídia de prova e sobre a mídia de destino, que resultará numa identificação única e que poderá ser verificada a qualquer momento. Se houver qualquer alteração sobre a mídia de prova, essa assinatura será alterada e não coincidirá com a assinatura original. Logo, se fizermos uma soma de verificações de uma mídia de prova antes e depois de sua duplicação e, mantidos os resultados, poderemos afirmar que não houve alterações de estado na mídia de prova questionada."

7.2.3 Execução

A execução corresponde ao momento em que ocorre a realização do exame pericial, propriamente dito. Ocasião em que o perito fará a análise técnico-científica

dos vestígios deixados pela prática do ilícito, já colhidos e preservados, bem como os vestígios que forem sendo descobertos ao longo do exame.

Para a realização da perícia, os expertos podem utilizar-se de todos os meios admissíveis, inclusive de laboratórios, devendo fazer menção de tais meios. [26]

Pode ser que o perito tenha participado da coleta dos equipamentos e mídias, já tendo identificado cada um deles ou, pode ser que tenha recebido o material coletado por outro perito ou policial. Na segunda hipótese, caso o material não esteja identificado, deverá o perito individualizá-lo, indicando sua origem, a ocorrência policial a qual está vinculado, a autoridade policial ou judicial que determinou o exame, o tipo de equipamento e/ou mídias, data e hora da coleta, a quem pertence, entre outros detalhes capazes de identificar o material. Todas essas informações devem vir etiquetadas no equipamento ou mídias.

Importante também que o perito, na hipótese de ter recebido o material, verifique se os equipamentos e mídias correspondem ao que consta da listagem de recebimento para se certificar que recebeu todo o material indicado.

Ao iniciar o exame, o especialista deverá abrir os equipamentos e checar seu interior fotografando-os. Recomenda-se que seja anotado os componentes dos equipamentos, permitindo completar a individualização dos mesmos. Esses registros são importantes pois saber a configuração do equipamento permitirá relacioná-los aos vestígios encontrados.

Neste momento é fundamental efetuar a duplicação dos discos rígidos e mídias encontrados para que o exame não seja executado na mídia original.

Conforme mencionado anteriormente, o ideal é que se faça mais de uma cópia promovendo maior segurança e liberdade na realização do exame.

É necessário que o perito documente todo o processo desde a coleta dos equipamentos e mídias ou desde o recebimento dos mesmos até à elaboração do laudo pericial de forma a registrar o encadeamento de todas as ações praticadas, a fim de que nenhuma etapa seja esquecida. Assim, será possível verificar eventual erro do especialista ou mesmo repetir o exame a partir de determinado momento.

Ademais, os exames envolvendo perícia em meios computacionais tendem a

---

[26] Código de Processo Penal, 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.”

ser longos e complexos e é esperado que o perito tenha o controle de todo o processo.

Para a realização do exame pericial é essencial que seja definida a metodologia adotada, sendo documentada cada uma das etapas até a conclusão dos trabalhos e sejam relacionados os equipamentos (hardwares) e softwares necessários. Caso seja necessária a realização de novo exame pericial em virtude de determinação judicial, a exposição clara da metodologia, a documentação das ações e a relação de ferramentas utilizadas serão determinantes para a repetição do exame, a fim de que se alcance os mesmos resultados e às mesmas conclusões do exame original.

Desse modo, não basta que o exame pericial tenha sua lógica e seja conclusivo. Ele deverá ser passível de ser refeito, alcançando-se os mesmos resultados e conclusões do primeiro exame.

Importante registrar que toda a documentação referente ao caso, desde a coleta ou recebimento dos equipamentos até a conclusão do laudo pericial, deverá ser arquivada sob a responsabilidade do perito ou do instituto de criminalística correspondente.

Por fim, a execução do exame pericial trata-se de um processo prospectivo, em que o experto, por meio de reflexão chega às próprias conclusões a respeito do fato. Possui natureza subjetiva visto que através do referido processo o perito formula um juízo de valor, um julgamento técnico-científico que poderá servir como fundamento da sentença judicial.

7.2.3.1 Quesitos

Com respeito à execução da perícia, importante papel desempenha a formulação de quesitos, que nada mais são que perguntas a serem respondidas pelo experto, de forma fundamentada, em função da natureza do delito praticado.

A Lei 11.690/2008 previu a possibilidade de formulação de quesitos pelos interessados: Ministério Público, assistente de acusação, ofendido, querelante e

acusado.[27] Contudo, não se trata propriamente de inovação pois o artigo 176 do Código de Processo Penal já determinava que os quesitos poderiam ser formulados pela autoridade e pelas partes até o ato da diligência, ou seja, até o início da realização do exame pericial.[28]

Importante consignar que tal dispositivo aplica-se apenas à fase judicial uma vez que na fase extrajudicial, o poder concentra-se na autoridade policial, que o utiliza de forma discricionária, visto que o inquérito policial possui natureza inquisitorial.

Desse modo, concernente às perícias realizadas durante a fase administrativa do inquérito policial, somente o Ministério Público e o ofendido poderão apresentar quesitos. Por sua vez, o querelante, o assistente de acusação e o acusado só poderão fazê-lo nas perícias determinadas em juízo ou em eventuais esclarecimentos sobre o laudo apresentado pelo perito.

A grande novidade inaugurada pela Lei 11.6902008 foi a previsão de ouvida dos peritos, a requerimento das partes com o fim de prestar esclarecimentos quanto à prova pericial bem como, responder a quesitos[29], conforme pondera Gomes Filho (2008, 277):

> "Uma verdadeira inovação relacionada ao contraditório diz respeito à previsão textual de ouvida dos peritos, a requerimento das partes, para esclarecimento da prova ou para responderem a quesitos, como consta do artigo 159, §5°, introduzido pela Lei 11.690/2008. A disposição foi reforçada, aliás, com a nova redação dada ao artigo 400 do Código de Processo Penal pela Lei 11.719/2008, na qual a inquirição dos peritos é arrolada entre os atos da audiência de instrução e julgamento."

---

[27] Artigo 159,§3º do Código de Processo Penal : "Serão facultadas ao Ministério Público, ao assistente de acusação, ao ofendido, ao querelante e ao acusado a formulação de quesitos e indicação de assistente técnico."

[28] Artigo 176 do Código de Processo Penal: "A autoridade e as partes poderão formular quesitos até o ato da diligência."

[29] Código de Processo Penal, Artigo 159, §5º : "Durante o curso do processo judicial, é permitido às partes, quanto à perícia:
I – requerer a oitiva dos peritos para esclarecerem a prova ou para responderem a quesitos, desde que o mandado de intimação e os quesitos ou questões a serem esclarecidas sejam encaminhados com antecedência mínima de 10 (dez) dias, podendo apresentar as respostas em laudo complementar;

Tal inovação inaugura o contraditório no âmbito da prova pericial, uma vez que objetiva a superação de eventuais dúvidas das partes quanto à fundamentação ou conclusões do laudo pericial.

Por fim, a materialização deste meio de prova ocorre através do laudo pericial a seguir examinado.

7.2.4 O laudo pericial

A prova pericial materializa-se por meio de uma peça escrita, de natureza técnico-científica, denominada laudo pericial, mediante a qual o experto nomeado relata o exame realizado, descreve todo o trabalho executado, consignando suas observações bem como as conclusões resultantes de uma declaração de ciência ou de uma análise valorativa, ou de ambas, a partir dos elementos de prova colhidos.

A descrição do trabalho do perito materializada no laudo pericial deve ser tão precisa, detalhada e documentada a ponto de possibilitar que qualquer outro perito seja capaz de executar o mesmo exame, nos mesmos materiais e vestígios, da forma como foi exposta no referido laudo, chegando-se às mesmas conclusões, ao mesmo resultado.

Embora o laudo pericial seja uma peça de natureza técnico-científica, sua redação deve ser didática, clara, concisa, contendo explicações sobre os termos técnicos, visto que seus destinatários são pessoas leigas que solicitaram o referido exame exatamente para terem suas dúvidas esclarecidas.

Em linhas gerais, o laudo pericial divide-se nas seguintes partes: preâmbulo, descrição, objetivos, metodologia, exames, conclusão e encerramento.[30]

I – O preâmbulo é a parte introdutória da peça, onde vêm registrados os elementos que o particularizam: o nome do perito ou peritos, a autoridade que

---

[30] Os tópicos apresentados que compõem o laudo pericial trata-se de mera orientação para a elaboração do referido documento, baseada em adaptação às ponderações expostas por Adalberto José Q. T. De Camargo Aranha in Aranha, Adalberto José Q. T. de Camargo. Da Prova no Processo Penal. Editora Saraiva. 3. ed.. atual. e ampl. - São Paulo: Saraiva, 1994.p.157 e Marcelo Antônio Sampaio Lemos Costa in Costa, Marcelo Antônio Sampaio Lemos. Computação forense – Campinas, SP: Milennium.2.003.p.157.

determinou a realização da perícia, a justificativa, o local, as circunstâncias em que foi realizada e a natureza da perícia.

II – Na descrição, relata-se o histórico do que foi apresentado, visto ou encontrado. É neste momento que se deve relatar a coleta ou recebimento dos equipamentos e mídias a serem periciados e sua descrição minuciosa.

III – No objetivo deve ser abordado o propósito do exame com base no requerimento da autoridade que o solicitou.

IV – Na metodologia, deve-se detalhar cada etapa do exame pericial, incluindo as ferramentas utilizadas, ou seja, softwares, hardwares, entre outros.

V – Nos exames descreve-se os exames realizados, detalhando todo o trabalho executado com o auxílio da documentação relacionada.

VI – Conclusão é o momento em que o experto relatará o que extraiu do material periciado, respondendo aos quesitos apresentados. Conforme visto anteriormente, sua função poderá restringir-se à retratação técnica das percepções colhidas, consistindo em uma declaração de ciência. Poderá, no entanto, ser requisitado a interpretar ou apreciar tecnicamente um fato mediante um juízo de valor ou, por fim, ambas as hipóteses. Tudo dependerá da solicitação feita pela autoridade que determinou a perícia bem como da natureza dos quesitos apresentados.

Segundo Costa (2003), o perito, na elaboração do laudo pericial, deve ser sincero, fazendo somente afirmações que possam ser provadas e demonstradas técnica e cientificamente. Toda conclusão deverá estar fundada em fatos e dados comprovados e demonstrados e, quando por meio dos exames realizados, por insuficiência de elementos de prova, não for possível obter os dados técnico-científicos que possam fundamentar uma conclusão, quer positiva quer negativa, por seu compromisso com a verdade, deve registrar no laudo quais foram de fato os elementos de prova concretamente obtidos.

IV – O encerramento é a parte autenticatória da peça, contendo a data de sua redação bem como a assinatura do perito responsável.

Embora os itens acima expostos, como partes do laudo pericial, trata-se de mera orientação, um norte para a elaboração da referida peça, o recomendável seria

houvesse regramento legal que fixasse critérios de admissibilidade ao referido documento.

8. ANÁLISE DE ALGUNS CASOS

Com o intuito de verificar a repercussão das possíveis lacunas presentes na legislação processual penal nacional aplicável à perícia em meios computacionais relacionadas ao crime informático praticado por meio da Internet, será traçado um paralelo entre os conceitos e ponderações até então expostos e a realidade do trabalho pericial concernente a essa espécie de crime.

Para tanto, será feita uma breve análise do trabalho dos peritos e assistente técnico a partir de três casos reais sobre crimes informáticos praticados por meio da Internet descritos sucintamente nos anexos A, B e C e os respectivos laudos periciais e parecer técnico apresentados.

Considerando que os casos analisados referem-se a processos de grande repercussão e que ainda tramitam no judiciário, sob segredo de justiça, toda e qualquer informação capaz de identificá-los foi mantida em sigilo, a fim de preservar a privacidade das partes envolvidas e atender aos preceitos legais sobre a matéria.

Desta forma, os laudos periciais e parecer técnico analisados não apresentarão imagens, cópias de páginas da internet, resultados de exames impressos a partir de páginas da internet ou arquivos, tabelas, fotos, entre outros.

8.1 Comentários ao laudo pericial referente ao caso I, a partir dos critérios de admissibilidade fixados no tópico 6.2.4

I. Preâmbulo: segundo o que foi exposto, preâmbulo é a parte introdutória da peça, onde vêm registrados os elementos que o particularizam: o nome do perito ou peritos, a autoridade que determinou a realização da perícia, a justificativa, o local, as circunstâncias em que foi realizada e a natureza da perícia.

Consta do preâmbulo:

a) O nome do Delegado que determinou a realização da perícia pois embora o caso verse sobre Ação Penal Privada, o laudo foi requerido ainda na fase do inquérito policial; o nome dos peritos oficiais nomeados, o número do laudo e do Inquérito Policial; o nome da vítima; não consta o nome do indiciado pois o laudo está sendo requisitado justamente para se fixar a autoria do ilícito; a data e o local de elaboração do laudo;

b) Justificativa: coletar evidências da conduta, em tese, criminosa do requerido – prática de crimes contra a honra;

c) Local: Instituto de Criminalística do Estado de XXXXX, ao qual os peritos nomeados pertencem.

d) Natureza da perícia: não foi possível identificar no laudo qualquer menção à justificativa da perícia.

Observação: Infere-se a partir dos dados constantes do laudo e da Queixa Crime tratar-se de perícia realizada em fase extrajudicial, administrativa, ou seja, em sede de Inquérito Policial, restringindo-se ao relato técnico das constatações colhidas, consistindo tão somente numa declaração de ciência em função dos objetivos fixados pelo delegado de polícia ao requisitar o laudo pericial.

e) Peritos: a perícia foi executada por dois peritos oficiais, ou seja, técnicos concursados pertencentes ao Instituto de Criminalística.

II. Descrição: segundo o que foi exposto, na descrição relata-se o histórico do que foi apresentado, visto ou encontrado. É neste momento que se deve relatar a coleta ou recebimento dos equipamentos e mídias a serem periciados e sua descrição minuciosa.

Consta da descrição:

a) Histórico do caso: o único histórico relatado foi o recebimento das mídias.

b) Equipamentos e mídias recebidos para serem periciados:

Um disco rígido ostentando a marca “XXXX” e apresentado, entre outras características, a inscrição “XXXX” na parte superior.

Dezessete discos ópticos graváveis, por números de IC – 1 a IC – 17.

Neste tópico deve-se relatar o recebimento dos equipamentos e mídias e sua descrição minuciosa. Desse modo, deveria ter sido descrito de forma detalhada, cada um dos materiais recebidos, tais como seu estado de conservação, se os mesmos foram coletados por policiais ou por peritos habilitados para tanto, entre outros.

Infere-se do registro feito no laudo que o material foi recebido, sendo que os peritos não fizeram a coleta do material. Contudo, não se sabe se a coleta foi feita por policial ou por perito.

c) O que foi encontrado pelo perito:

No item RESULTADOS e nos anexos denominados “textos” foi feito um relatório detalhado do que foi examinado e o que foi encontrado por meio do exame, tanto no disco rígido bem como nos dezessete discos ópticos.

Observação: Em função da preservação da privacidade das pessoas envolvidas nesse processo, não foi possível transcrever neste trabalho o que consta dos “anexos” pois trata-se de impressão de páginas da internet e de arquivos encontrados.

III. Objetivos: segundo o que foi exposto, no objetivo deve ser abordado o propósito do exame com base no requerimento da autoridade que o solicitou.

Consta do objetivo:

a) Objetivo do exame fixados pelo Delegado de Polícia:

“Verificar HD e mídias a fim de localizar e imprimir arquivos de mensagens enviadas através das caixas postais eletrônicas XXXXX, imprimindo o que for localizado.”

“Verificar o HD a fim de localizar e imprimir arquivos que contenham os perfis XXXXXXX no site de relacionamentos XXXX .”

“Localizar e imprimir arquivos que tenham relação com o nome XXXXXX”.

“Proceder a procura e recuperação de possíveis arquivos deletados que ensejam o crime de calúnia, injúria e difamação.”

Observação: Percebe-se a partir dos objetivos fixados pelo delegado de polícia, solicitante da perícia, que o referido exame restringiu-se à retratação técnica das percepções colhidas, consistindo em uma declaração de ciência. Não sendo requerido um juízo de valor a partir de uma análise técnica sobre o caso.

IV. Metodologia: segundo o que foi exposto, na metodologia deve-se detalhar cada etapa do exame pericial, incluindo as ferramentas utilizadas, ou seja, softwares, hardwares, entre outros.

Consta da metodologia:

a) Não há qualquer menção à metodologia utilizada.

Observação: neste tópico, espera-se que o perito aponte e detalhe a metodologia utilizada, incluindo as ferramentas usadas na realização da perícia, indicando os softwares, hardwares, entre outros equipamentos. Percebe-se, entretanto, que o perito não mencionou a metodologia utilizada e foi extremamente genérico quanto às ferramentas utilizadas o que certamente dificultará a realização de nova perícia seguindo a mesma metodologia.

Outra questão importante a ser registrada é que a perícia foi realizada na mídia original, sendo que em nenhum momento ficou registrado que houve a duplicação da mídia, correndo-se o risco de violação da prova.

V. Exames: segundo o que foi exposto, nos exames descreve-se os exames realizados, detalhando todo o trabalho executado com o auxílio da documentação relacionada.

Consta dos exames:

a) Descrição dos exames e respectiva documentação:analisou-se o conteúdo do disco rígido e dos discos ópticos recebidos para exame, sendo utilizados softwares apropriados, inclusive, quando fosse o caso, um software para recuperação de arquivos apagados e dados não alocados.Sendo que todos os exames foram descritos e documentados nos textos anexos.

Observação: percebe-se uma certa confusão entre a metodologia utilizada e a descrição dos exames efetuados.

VI. Conclusão: segundo o que foi exposto, na conclusão é o momento em que o experto relatará o que extraiu do material periciado, respondendo aos quesitos apresentados. Conforme visto anteriormente, sua função poderá restringir-se à retratação técnica das percepções colhidas, consistindo em uma declaração de ciência. Poderá, no entanto, ser requisitado a interpretar ou apreciar tecnicamente um fato mediante um juízo de valor ou, por fim, ambas as hipóteses. Tudo dependerá da solicitação feita pela autoridade que determinou a perícia bem como da natureza dos quesitos apresentados.

Consta da conclusão:

a) O presente exame restringiu-se à retratação técnica das percepções colhidas, consistindo em uma declaração de ciência. Não sendo requerido um juízo

de valor a partir de uma análise técnica sobre o caso. Desta forma, a conclusão foi respondida no item referente aos “Resultados”.

8.2 Comentários ao laudo pericial referente ao caso II, a partir dos critérios de admissibilidade fixados no tópico 6.2.4

I. Preâmbulo: segundo o que foi exposto, preâmbulo é a parte introdutória da peça, onde vêm registrados os elementos que o particularizam: o nome do perito ou peritos, a autoridade que determinou a realização da perícia, a justificativa, o local, as circunstâncias em que foi realizada e a natureza da perícia.

Consta do preâmbulo:

a) O Juiz que autorizou a medida e a quem é endereçado o laudo, respectiva comarca e vara; o número dos autos; o nome do requerente; o nome do requerido; a data e o local;

b) Justificativa: coletar evidências da conduta, em tese, criminosa do requerido – prática de crime de concorrência desleal e violação de segredo profissional;

c) Local: Instituto de Criminalística do Estado de XXXXX.

d) Natureza da perícia: trata-se de perícia realizada em fase judicial, ou seja, em sede de Medida Cautelar de Busca e Apreensão, tendo sido proposta, posteriormente, a Ação Penal Privada. A perícia requerida consistiu em um relato técnico das constatações colhidas, traduzindo-se numa declaração de ciência, embora no laudo conste também um juízo de valor emitido pelo perito (vide conclusão).

e) Peritos – a perícia foi executada por dois peritos oficiais, ou seja, técnicos concursados pertencentes ao Instituto de Criminalística.

II. Descrição: segundo o que foi exposto, na descrição relata-se o histórico do que foi apresentado, visto ou encontrado. É neste momento que se deve relatar a coleta ou recebimento dos equipamentos e mídias a serem periciados e sua descrição minuciosa.

Consta da descrição:

a) Histórico do caso: foi elaborado histórico detalhado do cumprimento da Medida Cautelar de Busca e Apreensão. Foram especificados e detalhados o local da diligência , as pessoas que participaram da medida, as pessoas encontradas no local onde foi cumprida a diligência;

b) Equipamentos e mídias apreendidos para serem periciados:muitos foram os equipamentos e mídias apreendidos sendo que a relação e descrição completa e detalhada de cada um deles, inclusive com fotos, consta do item 4 do referido laudo.

c) O que foi visto e encontrado pelo perito: há no laudo uma descrição detalhada do lugar onde foi feita a busca e apreensão bem como uma descrição minuciosa do material apreendido, sendo tudo muito bem documentado por meio de fotos tanto do local onde ocorreu a diligência bem como de cada um dos materiais apreendido. Também foram feitos registros por escrito.

Observação: foi feito um excelente trabalho de coleta de dados e equipamentos pelos peritos e uma excelente documentação, reforçando a tese de que o procedimento de coleta e custódia de equipamentos e dados bem como sua documentação deve ser feito por perito especializado, pois é nítida a diferença entre o trabalho do perito e o trabalho da polícia, em casos como esses.

III. Objetivos: segundo o que foi exposto, no objetivo deve ser abordado o propósito do exame com base no requerimento da autoridade que o solicitou.

Consta dos objetivos:

a) Objetivo do exame fixado pela autoridade judicial: não foi possível identificar o objetivo específico da diligência fixado pela autoridade que o determinou. Contudo, do que se infere a partir da medida de busca e apreensão bem como dos quesitos apresentados, o objetivo foi coletar evidências da conduta, em tese, criminosa do requerido qual seja, prática de crime de concorrência desleal e violação de segredo profissional;

IV. Metodologia: segundo o que foi exposto, na metodologia, deve-se detalhar cada etapa do exame pericial, incluindo as ferramentas utilizadas, ou seja, softwares, hardwares, entre outros.

Consta da metodologia:

a) Foram geradas imagens forenses (cópia *bit* a *bit*) das mídias de armazenamento apreendidas (HD, Pen Drive, etc.), ficando o assistente técnico com uma cópia de cada imagem gerada. Para o respectivo procedimento, foram utilizados os softwares forenses AcessData FTK Imager e bloqueadores de escrita;

b) Para o presente trabalho, foram utilizadas as distribuições LINUX forenses Helix (versão 3) e CAINE (Computer Aided Investigative Environment, versão 0.5) para a análise dos dados armazenados nas imagens geradas.

Observação: neste tópico, espera-se que o perito aponte e detalhe a metodologia utilizada, contudo, isso não ocorreu. Não houve uma descrição técnica dos passos adotados na condução do exame pericial que possa ser repetida por outro técnico caso a perícia seja refeita. Houve sim, o detalhamento das ferramentas utilizadas no exame em questão, contudo, somente o detalhamento das ferramentas utilizadas não é suficiente para determinar a metodologia a ser utilizada na realização de novo exame, caso seja necessário. Importante registrar que no item 2, “d” (referente ao laudo pericial), relatou-se que foram geradas imagens forenses

(cópia *bit* a *bit*) das mídias de armazenamento apreendidas (HD, Pen Drive, etc.), ficando o assistente técnico com uma cópia de cada imagem gerada. Tal procedimento foi realizado em função dos quesitos 6 e 7 abaixo transcritos:

> 6) Queira a Sr. Perito gerar copias fiéis (clones "byte a byte") de todos as discos rígidos existentes no local. A cópia dever ser realizada através da metodologia e ferramentas que reproduzam integralmente o HD, inclusive os dados deletados, as áreas não alocadas, dados remanescentes de eventuais formatações anteriores, os arquivos do sistema operacional e assim por diante, tarefa usualmente realizada através do software "FTK" da ACESSDATA,via CD-ROM"bootaver:
>
> 7) Queira a Sr. Perito copiar, "byte a byte" os dados de interesse pericial eventualmente presentes nos demais dispositivos digitais encontrados, como HDs soltos, memórias, pen drives, disquetes, CD-ROMs, DVDs e demais dispositivos de armazenamento.

Desse modo, fica evidente que a duplicação da mídia foi realizada em função de uma solicitação do requerente para que o assistente técnico pudesse ter acesso ao conteúdo das mídias a serem periciadas. Não foi, portanto, para preservação da mídia original, mesmo porque, em momento algum há referência de que o exame pericial tenha sido realizado na mídia de destino. Conclui-se, portanto que o exame pericial foi executado nas mídias originais, correndo-se o risco de haver a violação da prova.

V. Exames: segundo o que foi exposto, nos exames descreve-se os exames realizados, detalhando todo o trabalho executado com o auxílio da documentação relacionada.

Consta dos exames:

a) Não houve um detalhamento dos exames realizados mas foi feito um detalhamento do que foi constatado a partir dos referidos exames (item 5 – constatações).

VI. Conclusão: segundo o que foi exposto, a conclusão é o momento em que o experto relatará o que extraiu do material periciado, respondendo aos quesitos apresentados. Conforme visto anteriormente, sua função poderá restringir-se à

retratação técnica das percepções colhidas, consistindo em uma declaração de ciência. Poderá, no entanto, ser requisitado a interpretar ou apreciar tecnicamente um fato mediante um juízo de valor ou, por fim, ambas as hipóteses. Tudo dependerá da solicitação feita pela autoridade que determinou a perícia bem como da natureza dos quesitos apresentados.

Consta da conclusão:

a) Os peritos relataram minuciosamente o que extraíram do material periciado, conforme registrado nos itens 5 – Constatações e 6 – Conclusão onde há as respostas aos quesitos apresentados, sendo que as respostas foram motivadas na medida em que foram documentadas com o resultado dos exames realizados. Ocorre que os objetivos da perícia fixados nos quesitos apresentados pela requerente revelam que o trabalho solicitado ao perito consistiu em uma declaração de ciência restringindo-se ao relato técnico das constatações colhidas, ou seja, não foi requerido que o perito interpretasse o fato emitindo um juízo. Entretanto, no item 6 (do laudo pericial), referente à conclusão, o perito, antes de responder aos quesitos, inicia sua conclusão (itens a, b e c) emitindo um juízo, ao fazer uma interpretação técnica dos fatos.

8.3 Comentários ao laudo pericial referente ao caso III, a partir dos critérios de admissibilidade fixados no tópico 6.2.4

1. Preâmbulo: segundo o que foi exposto, preâmbulo é a parte introdutória da peça, onde vêm registrados os elementos que o particularizam: o nome do perito ou peritos, a autoridade que determinou a realização da perícia, a justificativa, o local, as circunstâncias em que foi realizada e a natureza da perícia.

Consta do preâmbulo:

a) O nome do assistente técnico e data .

b) Justificativa – coletar evidências que comprovem acesso indevido a contas bancárias.

Observação: a justificativa não está explícita. Contudo, chegou-se a ela a partir de inferência.

c) Local: Núcleo de Segurança da Instituição Financeira XXXXX.

d) Autoridade que determinou a realização da perícia: o exame técnico foi requerido pela Instituição Financeira que, posteriormente requereu a instauração do Inquérito Policial.

e) Natureza da perícia – trata-se de exame técnico realizado em fase extrajudicial, ou seja, visando coletar provas para instruir pedido de Instauração de Inquérito Policial, restringindo-se ao relato técnico das constatações colhidas, consistindo tão somente numa declaração de ciência, embora a conclusão envolva um juízo de valor (vide conclusão).

Observação: a natureza da perícia também não está explícita. Chegou -se a ela a partir do consta como objetivo do parecer.

f) Peritos: a perícia foi executada por um perito em tecnologia da informação, desempenhando a função de assistente técnico, uma vez que é funcionário do Núcleo de Segurança da Instituição Financeira XXXXX, que figura como requerente no pedido de Instauração do Inquérito Policial.

II. Descrição: segundo o que foi exposto, na descrição, relata-se o histórico do que foi apresentado, visto ou encontrado. É neste momento que se deve relatar a coleta

ou recebimento dos equipamentos e mídias a serem periciados e sua descrição minuciosa.

Consta da descrição:

a) Histórico do caso – o requerente foi noticiado por alguns de seus clientes-correntistas sobre transações bancárias lançadas via Internet Banking por eles não reconhecidas, portanto, supostamente ilícitas. Dessa forma, há um histórico do caso a ser investigado contudo, não há menção nem descrição de qualquer equipamento ou mídias apreendidos.

b) O que foi visto e encontrado pelo perito : foram detectadas transações na conta corrente da cliente XXXX, que não foram reconhecidas pela mesma, titular da conta corrente n° XXXX, agência n° XXXX e, portanto, consideradas indevidas, constituindo-se em transações realizadas através da Internet, utilizando-se chaves de acesso válidas ao sistema Internet Banking Pessoa Física. Mencionadas transações contemplam pagamentos de contas de consumo (água, energia elétrica e telefone), pagamento de impostos, transferências, boletos bancário, conforme discriminação abaixo.

III. Objetivo: segundo o que foi exposto, no objetivo deve ser abordado o propósito do exame com base no requerimento da autoridade que o solicitou.

Consta do objetivo:

a) Descrever as ocorrências acusadas como fraudulentas por clientes da Instituição financeira XXX, para diversas transações realizadas através da Internet.

IV. Metodologia: segundo o que foi exposto, na metodologia, deve-se detalhar cada etapa do exame pericial, incluindo as ferramentas utilizadas, ou seja, softwares, hardwares, entre outros.

Consta da metodologia:

a) Após terem sido detectadas as transações inválidas na conta corrente da cliente XXXX, verificou-se a data e hora de acesso das respectivas transações. Assim, foi possível identificar os endereços IPs correspondentes. Com os endereços IPs foi possível, por meio do Registro.br (órgão responsável por alocações de endereçamento IPs no Brasil), identificar o provedor e operadora de acesso XXXXXX responsáveis pelos endereços Ips.

Observação: Não houve menção ou descrição clara quanto à metodologia nem tampouco a menção à ferramentas utilizadas no exame realizado.

V. Exames: segundo o que foi exposto, nos exames descreve-se os exames realizados, detalhando todo o trabalho executado com o auxílio da documentação relacionada.

Consta dos exames:

a) O detalhamento do que foi realizado está expresso no item acima referente à metodologia, documentado por meio de tabelas cujo conteúdo é sigiloso.

Observação: percebe-se uma certa confusão entre metodologia e os exames realizados e por isso, não há uma descrição clara nem da metodologia nem dos exames realizados.

VI. Conclusão: segundo o que foi exposto, conclusão é o momento em que o experto relatará o que extraiu do material periciado, respondendo aos quesitos apresentados. Conforme visto anteriormente, sua função poderá restringir-se à retratação técnica das percepções colhidas, consistindo em uma declaração de ciência. Poderá, no entanto, ser requisitado a interpretar ou apreciar tecnicamente um fato mediante um juízo de valor ou, por fim, ambas as hipóteses. Tudo

dependerá da solicitação feita pela autoridade que determinou a perícia bem como da natureza dos quesitos apresentados.

Consta da conclusão:

a) O assistente técnico relatou o que foi encontrado atendendo ao que foi solicitado no item “objetivo”. Não houve quesitos a serem respondidos. Constata-se que embora o referido exame tenha se restringido ao relato técnico das constatações colhidas, consistindo tão somente numa declaração de ciência, na conclusão, ao tecer recomendações ao requerente do exame, o assistente técnico, implicitamente emitiu um juízo de valor, revelando sua interpretação técnica a respeitos dos fatos.

Observação: Embora esteja-se diante de um parecer produzido por um assistente técnico e não um laudo pericial produzido por um perito oficial, entende-se que o rigor na produção do parecer deve ser o mesmo exigido para a elaboração do laudo. Isto porque, trata-se de informações técnicas que fundamentarão a instauração de Inquérito policial. Desta forma, entendemos que pareceres como este devem ser elaborados por instituição imparcial, contratada especificamente para essa produção de prova e não por um departamento de segurança da empresa requerente.

8.4 Considerações a respeito dos laudos periciais e parecer técnico analisados

A partir da análise feita dos laudos e parecer técnico constatou-se que:

I. A única descrição detalhada e bem documentada tanto do local do crime bem como dos materiais e mídias coletados, a serem periciados, ocorreu no caso II, referente à uma busca e apreensão acompanhada por dois peritos oficiais. Tal observação reforça a tese de que a análise do local do crime e a coleta dos

equipamentos e mídia contendo vestígios referentes ao crime informático deve ser feita obrigatoriamente por perito especialista em computação forense.

II. Em nenhum dos trabalhos analisados houve uma descrição clara da metodologia empregada, detalhando cada etapa do exame efetuado e, na maioria deles, não houve menção às ferramentas (software e hardwares) utilizadas, o que dificulta a realização de nova perícia seguindo a mesma metodologia do exame inicial, caso seja necessário.

III. Em todos os casos analisados constatou-se que a perícia foi realizada na mídia original, sendo que em nenhum momento ficou registrado que houve a duplicação da mídia, correndo-se o risco de ocorrer a violação da prova.

IV. Em todos os casos analisados não houve uma descrição clara e satisfatório dos exames realizados. Constatou-se uma certa confusão entre descrição da metodologia empregada e descrição dos exames realizados.

V. A conclusão do laudo relaciona-se ao objetivo do exame pericial fixado pelo solicitante, diretamente ou por meio de quesitos. Neste ponto, constatou-se que em todos os casos o que foi requerido ao perito foi uma mera retratação técnica das percepções colhidas, consistindo em uma declaração de ciência, quando se deveria solicitar além da declaração de ciência, um juízo de valor a partir de uma análise técnica sobre o caso. Percebe-se, portanto, um certo despreparo da autoridade solicitante na formulação dos quesitos ou mesmo na fixação dos objetivos do exame a ser realizado.

VI. Quanto se tratar de parecer técnico que instruirá um pedido de instauração de inquérito policial ou mesmo uma ação penal, entende-se que o rigor na produção do parecer deve ser o mesmo exigido para a elaboração do laudo, ou seja, entre outros, deve ser elaborado por instituição imparcial (independente), contratada especificamente para essa produção de prova e não por um departamento de segurança da empresa requerente.

9. ALTERNATIVAS PARA A DISCIPLINA DA PROVA PERICIAL

Conforme analisado, a prova pericial é um meio de produção de prova típico pois é nominada e tem seu procedimento regrado pelo Código de Processo Penal brasileiro. Contudo, este regramento, por ser extremamente genérico e, até certo ponto, ultrapassado, como foi visto, não incorporou a prova pericial em meios computacionais relacionada ao crime informático praticado por meio da internet.

Desta forma, ao se realizar perícias dessa natureza, por não haver disciplina legal quanto aos requisitos de admissibilidade desse meio de prova, fica ao talante, ao arbítrio da autoridade policial e do próprio perito, apreender os equipamentos informáticos e respectivas mídias bem como ao perito, colher os vestígios digitais e realizar o próprio exame pericial sobre os mesmos, segundo critérios aleatórios por eles próprios fixados sem qualquer controle legal. Ademais, as regras de boas práticas que tratam da matéria nem sempre são atendidas por eles, uma vez que não são auto-impositivas.

Assim, quanto aos atos preparatórios referentes ao exame pericial, consistentes na coleta, preservação, transporte e armazenamento de equipamentos informáticos contendo vestígios digitais bem como mídias avulsas, entende-se que não se deve aplicar o artigo 6°, incisos II e III, quais sejam:

> “Logo que tiver conhecimento da prática da infração penal, a autoridade policial deverá:
> [...]
> II - apreender os objetos que tiverem relação com o fato, após liberados pelos peritos criminais;
> III - colher todas as provas que servirem para o esclarecimento do fato e suas circunstâncias;
> [...]
> VII - determinar, se for o caso, que se proceda a exame de corpo de delito e a quaisquer outras perícias;”

Somente o experto em realizar perícias em meios computacionais e o instituto de criminalística correspondente, têm o conhecimento e a competência adequados para executar diretamente as referidas ações, documentando-as e responsabilizando-se pelas mesmas, sob pena de não o fazendo, expor ao risco de alteração, violação ou até destruição dos elementos de prova relacionados, inviabilizando ou invalidando o exame pericial.

Cabe à autoridade policial tão somente garantir: a segurança e preservação do local do crime, a segurança ao longo do percurso por onde o material será transportado, bem como do local onde ficarão armazenados.

Pelas razões apontadas, entende-se que é da responsabilidade do instituto de criminalística correspondente, o armazenamento do material objeto de exame pericial, por todo o tempo que a autoridade judicial achar pertinente, podendo estender-se até o trânsito em julgado da respectiva ação, pois pode ser necessária a realização de novo exame pericial.

Entende-se que em toda busca e apreensão é requisito essencial à validade do ato a presença de um perito especializado em computação forense para acompanhar toda a diligência e realizar os atos que lhe compete, acima descritos.

Para se evitar qualquer tipo de contestação quanto à integridade do vestígio obtido é dever do perito e respectivo instituto de criminalística fixar controle rígido em sua coleta, estabelecer o gerenciamento da cadeia de custódia correspondente, incluindo o controle de seu armazenamento e, quando possível, aplicar métodos de controle de integridade no momento da coleta.

A fim de se preservar a integridade dos vestígios deve ser obrigatória a duplicação da mídia, por meio de processo que não viole a mídia original, bem como garanta a autenticidade do conteúdo da mídia de destino.

Dessa forma, cada uma das considerações acima apontadas, referentes à coleta, preservação e armazenamento dos equipamentos e dos vestígios digitais, devem ser disciplinadas por meio de texto legal, regulamentando os atos preparatórios que antecedem o exame pericial .

Com relação à execução do exame pericial propriamente dito, a liberdade que possui o perito refere-se à metodologia que adotará, desde que justificada, bem como às ferramentas tecnológicas que empregará para colher e analisar os elementos de prova.

É neste momento que se afere o preparo do perito e sua atualização frente às novas tecnologias. Portanto, legislar sobre a metodologia a ser adotada bem como a tecnologia a ser utilizada seria um despropósito, seria tentar controlar o incontrolável pois ambas estão em constante evolução. O que não significa que o trabalho pericial possa ser realizado sem uma metodologia definida e justificada e sem relacionar as

ferramentas utilizadas e as etapas de execução do exame, em nome de uma suposta “ liberdade”.

O laudo pericial deve ser fundamentado e essa fundamentação consiste: na descrição detalhada e documentada dos materiais e vestígios (elementos de prova) coletados, incluindo avaliação quanto ao seu estado de preservação em relação à sua integridade; na exposição da metodologia empregada na coleta e na preservação dos referidos elementos de prova; no registro documentado dos exames realizados e ferramentas utilizadas e respectiva metodologia empregada; na clareza e didática da linguagem usada na explanação técnico-científica; na motivação apresentada não só às respostas aos quesitos propostos como também à conclusão dos trabalhos e, sobretudo, na repetibilidade do exame pericial nele materializado. São esses, portanto, os critérios essenciais para se certificar se de fato o laudo pericial é fundamentado.

Tais critérios nada mais são que os requisitos de admissibilidade do laudo pericial que devem ser fixados por lei para nortear a sua elaboração e servir como parâmetro para a validade do exame pericial nele materializado. O laudo pericial exterioriza um juízo, e o juízo vale pelo rigor da argumentação expressa em sua fundamentação devidamente documentada.

O procedimento adotado pelo perito deverá realizar-se rigorosamente à luz das exigências do método técnico-científico aplicado à matéria à época da execução do exame pericial, utilizando-se da tecnologia disponível, atendendo à sua evolução e sobre este ponto, não se pode abrir mão.

Entende-se ainda que as considerações feitas, anteriormente, aos casos de crimes informáticos e respectivos laudos apenas vêm corroborar as conclusões acima expostas.

10. CONCLUSÃO

Por meio do presente trabalho concluiu-se ser imperativo e viável disciplinar, por meio da legislação processual penal brasileira, a perícia em meios computacionais relacionada ao crime informático praticado por meio da Internet.

É imperativo fixar-lhe requisitos de admissibilidade tendo como princípios norteadores a não violação da prova e a fundamentação de todo o trabalho do perito materializado no laudo pericial, à luz dos novos paradigmas incorporados pela processualística moderna e da inovação tecnológica das últimas décadas.

Esse regramento, além de necessário, de forma alguma significa um controle legal sobre a tecnologia envolvida no exame pericial.

É insuficiente termos apenas normas infra-legais que servem como mera orientação ao trabalho do perito. Há que se ter exigências veiculadas por meio de texto legal que imponham condutas sobre as quais não se pode abrir mão sob pena de se outorgar ao perito um poder ilimitado na condução do exame pericial e na formação do juízo que fará sobre o caso e que servirá como fundamento à sentença judicial. Nem mesmo o juiz, que preside a condução do processo judicial tem o poder de sentenciar discricionariamente, pois além de ser obrigado a motivar sua decisão também está sujeito ao duplo grau de jurisdição como exigências constitucionais.

10.1 Contribuições

A principal contribuição do presente trabalho foi realizar um estudo essencialmente multidisciplinar envolvendo, de um lado, a ciência jurídica, e de outro, a área técnica relacionada aos sistemas digitais, um dos ramos da engenharia elétrica.

Entende-se que não é possível a análise da disciplina da prova pericial em meios computacionais relacionada ao crime cometido por meio da Internet sem que

se estabeleça uma linha de pesquisa nitidamente marcada pela convergência entre o Direito e a Tecnologia, revelando o quão alinhado o tema está à vocação primeira da pós-graduação *stricto sensu*, qual seja, a multidisciplinariedade.

Outra contribuição importante foi mostrar a necessidade e viabilidade da disciplina, por meio da legislação processual penal brasileira, da prova pericial em meios computacionais relacionada ao crime cometido por meio da Internet e apontar alguns caminhos para que, posteriormente, por meio de estudo mais profundo, seja possível a elaboração de projeto de lei que discipline a matéria.

10.2 Dificuldades Encontradas

Por tratar-se de tema essencialmente multidisciplinar, a dificuldade encontrada foi conciliar a metodologia da pesquisa científica aplicada à área jurídica e a metodologia da pesquisa tecnológica aplicada à área técnica.

Outra questão importante a abordar é que há poucos autores nacionais que cuidam do tema da tipicidade da prova pericial bem como da própria pericia em meios computacionais sob a ótica da tipicidade e, considerando que estamos analisando a possibilidade da disciplina desse meio de prova pelo Direito posto, seria importante um estudo mais profundo com autores nacionais, o que não foi possível em função da falta de doutrinadores que explorassem o tema.

10.3 Trabalhos Futuros

Considerando tratar-se de tema multidisciplinar, há a possibilidade de exploração e aprofundamento do tema em questão tanto na Engenharia como no Direito.

Seria fundamental a realização de nova pesquisa por meio da qual fosse feito um estudo de caso com o objetivo de analisar laudos periciais com o fim de, a partir de casos concretos, ser possível confirmar as conclusões extraídas do presente

trabalho como também ampliá-las, fixando princípios norteadores para uma proposta legislativa que discipline perícias dessa natureza.

Com o estudo de caso, seria possível atestar, a partir de casos concretos, não somente a necessidade, bem como a viabilidade de se introduzir elementos normativos quanto ao procedimento a ser utilizado referente aos atos preparatórios para a realização da perícia em meios computacionais (colheita da prova, cadeia de custódia e preservação da mídia original), como também sobre a própria realização do exame pericial considerando a não violação da prova.

Outro ponto que merece um estudo detalhado, com um enfoque mais técnico, é a questão da aplicação do método técnico-científico na realização do exame pericial e a relação entre a metodologia utilizada e a liberdade outorgada ao perito nessa escolha e aplicação. Seria importante esclarecer até onde o perito pode agir com discricionariedade e até onde deve seguir critérios pré-estabelecidos do ponto de vista do método técnico-científico.

REFERÊNCIAS

ARANHA, A.J.Q.T.C. **Da prova no processo penal**. 3. ed. atual. São Paulo: Saraiva, 1994. 221 p.

BADARÓ, G.H.R.I. **Provas atípicas e provas anômalas: inadmissibilidade da substituição da prova testemunhal pela juntada de declarações escritas de quem poderia ser testemunha**. In: YARSHELL, F.L.; MORAES, M.Z. (org.). Estudos em homenagem à professora Ada Pellegrini Grinover. São Paulo: DPJ, 2005. 865 p.

BEDNAR, P.M.; KATOS, V.; HENNEL, C. **Cyber-Crime Investigations: Complex Collaborative Decision Making**. In: Third International Annual Workshop on Digital Forensics and Incident Analysis. WDFIA 2008. Malaga, Spain. 9 p.

BOITEUX, L. **Crimes Informáticos: reflexões sobre política criminal inseridas no contexto internacional atual**. Revista Brasileira de Ciências Criminais, São Paulo, n. 47. RT, 2004.

CASEY, E. **Error, uncertainty, and loss in digital evidence**. In: INTERNATIONAL JOURNAL OF DIGITAL EVIDENCE. Summer 2002, v.1 (2), 2002.

COSIC, J.; BACA, M. **Do we have full control over integrity in digital evidence life cycle?**. In: PROCEEDINGS OF THE ITI 2010. 32ND INT. CONF. ON INFORMATION TECHNOLOGY INTERFACES. ITI 2010. Cavtat, Croatia. p.429-434.

COSTA, M. A. S. L. **Computação forense**. 2. ed. Campinas: Milennium, 2003. 246 p.

DAOUN, A. J. **Crimes informáticos e o papel do direito penal na tecnologia da informação**. In: DE LUCCA, N.; SIMÃO FILHO, A. (coord.) et al. Direito & Internet aspectos jurídicos relevantes. v. II. São Paulo: Quartier Latin, 2008. 718p.

DEZEM, G. M. **Da prova penal: tipo processual, provas típicas e atípicas: (atualizado de acordo com as Leis 11.689/08, 11.690/08 e 11.719/08)**. Campinas: Millenium, 2008. 321 p.

FERNANDES, A. S. **Prova e sucedâneo da prova no processo penal.** Revista Brasileira de Ciências Criminais, São Paulo, n. 66, 2007.

_____. **Efetividade, processo penal e dignidade humana**. In: Miranda, J.; Silva, M. A. M. (Coord.). Tratado luso-brasileiro da dignidade humana. 2. ed. São Paulo: Quartier Latin, 2009. 1359 p.

FERRAJOLI, L. **Direito e razão**. 2. ed. rev. e ampl. Tradução de Ana Paula Zomer, Fauzi Hassan Choukr, Juarez Tavares e Luiz Flávio Gomes. São Paulo: RT, 2006. 925 p.

FERREIRA, I. S. **A criminalidade informática**. In: DE LUCCA, N.; SIMÃO FILHO, A. (coord.) et al. Direito & Internet aspectos jurídicos relevantes. 2. ed. São Paulo: Quartier Latin, 2005. 543 p.

GOMES FILHO, A. M. **Notas sobre a terminologia da prova (reflexos no processo penal brasileiro)**. In: YARSHELL, F. L.; MORAES, M. Z. (org.). Estudos em homenagem à professora Ada Pellegrini Grinover. São Paulo: DPJ, 2005. 865 p.

_____. **Provas: Lei 11.690, de 09.06.2008**. In: MOURA, M. T. A. (coord.). As reformas no processo penal: as novas leis de 2008 e os projetos de reforma. São Paulo: RT, 2008. 502 p.

GOMES FILHO, A. M.; BADARÓ, G. H. R. I. **Prova e sucedâneo de prova no processo penal brasileiro**. Revista Brasileira de Ciências Criminais, São Paulo, n. 65, 2007.

GOVIL, J.; GOVIL, J. **Ramifications of cyber crime and suggestive preventive measures**. In: IEEE EIT 2007 PROCEEDINGS, 2007. EIT'07. 6 p.

HOSMER, C. **Proving the integrity of digital evidence**. In: INTERNATIONAL JOURNAL OF DIGITAL EVIDENCE. Spring 2002, v.1(1), 2002.

KWAN, L.; RAY P.; STEPHENS G. **Towards a methodology for profiling cyber criminals**. In: Proceedings of the 41st Hawaii International Conference on System Science, Hawaii, 2008. 9 p.

LEE, S. H.; KIM, H. S.; LEE, S. J.; LIM, J. I. **Digital evidence collection process in integrity and memory information gathering**. In: Proceedings of the First International Workshop on Systematic Approaches to Digital Forensic Engineering, Taiwan, 2005. SADFE'05. 12 p.

LEIGLAND, R. **A formalization of digital forensics**. In: INTERNATIONAL JOURNAL OF DIGITAL EVIDENCE. Fall 2004, v.3(2), 2004.

MENDONÇA, A. B. **Nova reforma do código de processo penal**. São Paulo: Método, 2008. 320 p.

MEYERS, M.; ROGERS, M. **Computer forensics: the need for standardization and certification**. In: INTERNATIONAL JOURNAL OF DIGITAL EVIDENCE. Fall 2004, v.3 (2), 2004.

NUCCI, G. S. **Código de processo penal comentado**. 5. ed. rev. atual. e ampl. São Paulo: RT, 2006. 1215 p.

REFERÊNCIAS COMPLEMENTARES

BAGGILI, I. M.; MISLAN R.; ROGERS M. **Mobile Phone Forensics Tool Testing: A Database Driven Approach**. In: INTERNATIONAL JOURNAL OF DIGITAL EVIDENCE. Fall 2007, v. 6 (2), 2007. 11 p.

BLUM, R. M.S.O., BRUNO, M. G.S., Abrusio, J. C.(coord.) et. al. **Manual de direito eletrônico Internet**. São Paulo: Lex Editora, 2006. 682 p.

CAPANEMA, W. A. **O spam e as pragas digitais: uma visão jurídico-tecnológica**. São Paulo: LTr, 2009. 159 p.

CIARDHUÁIN, S.Ó. **An Extended Model of Cybercrime Investigations**. In: INTERNATIONAL JOURNAL OF DIGITAL EVIDENCE. Summer 2004, v.3 (1), 2004. 22 p.

CORRÊA, G. T**. Aspectos Jurídicos da Internet.** 3. ed. Ver. e atual. São Paulo: Saraiva, 2007. 145 p.

DE LUCCA, N.; SIMÃO FILHO, A. (coord.) et al. **Direito & Internet aspectos jurídicos relevantes**. São Paulo: Quartier Latin, 2008. 718p. v.II

DE LUCCA, N.; SIMÃO FILHO, A. (coord.) et al. **Direito & Internet aspectos jurídicos relevantes**. 2. ed. São Paulo: Quartier Latin, 2005. 543 p.

DOLAN, K. M. **Internet Auction Fraud: The Silent Victims**. In: JOURNAL OF ECONOMIC CRIME MANAGEMENT. Winter 2004, v.2 (1), 2004. 22 p.

ECO, U. **Como se faz uma tese**. 21. ed. Tradução de Gilson Cesar Cardoso de Souza. São Paulo: Perspectiva, 2007. 175 p.

GOMES FILHO, A. M. **Direito à prova no processo penal**. São Paulo: RT, 1997. 191 p.

GORDON, G. R.; WILLOX N. A. **The Ongoing Critical Threats Created by Identity Fraud: An Action Plan**. In: JOURNAL OF ECONOMIC CRIME MANAGEMENT, Summer 2006, v. 4 (1), 2006. 15 p.

GUPTA G; MAZUMDAR C; RAO M. S. **Digital Forensic Analysis of E-Mails: A Trusted E-Mail Protocol**. In: INTERNATIONAL JOURNAL OF DIGITAL EVIDENCE, Spring 2004, v. 2 (4), 2004. 11 p.

HALL, G. A.; DAVIS, W. P. **Toward Defining the Intersection of Forensics and Information Technology**. In: INTERNATIONAL JOURNAL OF DIGITAL EVIDENCE, Spring 2005, v.4 (1), 2005. 20 p.

LEE, H. C. **Cyber Crime and Challenges for Crime Investigation in the Information Era**. In: IEEE ISI 2008 Keynote Talk (II)

LIMA, P. M. F. **Crimes de computador e a segurança computacional**. Campinas: Millennium, 2005. 234 p.

MARSICO C. V.; ROGERS M. K. **iPod Forensics**. In: INTERNATIONAL JOURNAL OF DIGITAL EVIDENCE. Fall 2005, v.4 (2), 2005. 12 p.

MINISTÉRIO PÚBLICO FEDERAL E COMITÊ GESTOR DA INTERNET NO BRASIL. **Manual Prático de Investigação de Crimes Cibernéticos**. São Paulo, 2006. 100 p.

ROWLINGSON, R. **A Ten Step Process for Forensic Readiness**. In: INTERNATIONAL JOURNAL OF DIGITAL EVIDENCE. Winter 2004, v.2 (3). 28 p.

TONINI, P. **A prova no processo penal italiano**. Tradução de Alexandra Martins, Daniela Mróz. São Paulo: RT, 2008. 315 p.

VIEIRA, J. L. **Crimes na Internet: interpretados pelos tribunais: repertório de jurisprudência e legislação**. Bauru: Edipro, 2009. 342 p.

WHITCOMB, C. M. **An Historical Perspective of Digital Evidence: A Forensic Scientist's View**. In: INTERNATIONAL JOURNAL OF DIGITAL EVIDENCE. Spring 2002 v.1 (1), 2002.

ANEXOS

ANEXO A – Caso I: Relatório da Queixa Crime e Respectivo Laudo Pericial

Relatório da Queixa Crime

Relatório referente à Queixa Crime

Trata-se de Ação Penal Privada referente aos crimes contra honra: calúnia, injúria e difamação cometidos por meio da Internet, especificamente por meio de:

a) perfis falsos em site de relacionamento com o uso indevido do nome da querelante;
b) utilização indevida de imagem por meio de fotos e montagens de fotos disponibilizadas em sites eróticos;
c) criação de diversas contas de e-mail com o nome da querelante e uso indevido dos mesmos;
d) criação de vídeo disponibilizado em site de relacionamento;
e) postagem de conteúdo ilícito envolvendo o nome da querelante em blog;
f) envio por e-mail de mensagens ofensivas ao nome da querelante e também disponibilizadas em sites de relacionamento;
g) dados pessoais da querelante tais como nome, e-mail e números de telefones disponibilizados em sites eróticos como se fosse garota de programa;

Os crimes sob investigação por meio da referida Ação Penal Privada, quais sejam, crimes de calúnia, injúria e difamação cometidos por meio da Internet, conforme vimos anteriormente, são crimes que atentam contra a honra, ou seja, um valor social tutelado pelo direito, cometidos através de um sistema informático. Desta forma, não constituem nova modalidade de crime. A inovação nesses crimes é a maneira como foram praticados. São classificados como crimes informáticos de natureza mista ou imprópria.

Laudo Pericial

SECRETARIA DE SEGURANÇA PÚBLICA
SUPERINTENDÊNCIA DE POLÍCIA TÉCNICO-CIENTÍFICA
Instituto de Criminalística
Perito Criminal Dr. XXXX
Núcleo de Perícia de Informática

LAUDO Nº XXXXXXX

ACOMPAQNHA(M) A(S) PEÇAS(S) EXAMINADA(S), ACONDICIONADAS(S) EM SACO(S) PLÁSTICO(S) COM O(S) LACRE(S) DE NÚMERO (S) XXXXX.

Natureza da Ocorrência: “Crime contra a Honra”
Data do exame: XXXX
I.P. (Inquérito Policial) Nº XXXXX
Vítima(s): XXXX
Indiciado(s): A esclarecer.
Requisitante: Dr. XXXX – Delegado de Polícia – Delegacia XXXX
Relatores: nome de dois peritos criminais

SECRETARIA DE SEGURANÇA PÚBLICA
SUPERINTENDÊNCIA DE POLÍCIA TÉCNICO-CIENTÍFICA
Instituto de Criminalística
Perito Criminal Dr. XXXX
Núcleo de Perícia de Informática

Natureza da ocorrência: "Crime contra a honra"
Inquérito Policial nº XXXX

Laudo nº XXXX

Em XXXX, na cidade de XXXX e no Instituto de Criminalística XXXX, de conformidade com o disposto no artigo 178 do Decreto-Lei nº 3.689, de 03 de outubro de 1941, pelo Perito Criminal, Diretor deste Instituto, Dr. XXXXX, foram designados os peritos criminais XXXX e XXXX para procederem ao exame supra especificado, em atendimento à requisição do Delegado da XXXX, Dr. XXXX, datada de XXXX.

<u>Objetividade da Perícia:</u>

1. **"Verificar HD e mídias a fim de localizar e imprimir arquivos de mensagens enviadas através das caixas postais eletrônicas XXXXX, imprimindo o que for localizado."**
2. **"Verificar o HD a fim de localizar e imprimir arquivos que contenham os perfis XXXXXXX no site de relacionamentos XXXX ."**
3. **"Localizar e imprimir arquivos que tenham relação com o nome XXXXXX".**
4. **"Proceder a procura e recuperação de possíveis arquivos deletados que ensejam o crime de calúnia, injúria e difamação."**

CARACTERÍSTICAS DAS PEÇAS

Constituíram peças de exames:

1. Um disco rígido ostentando a marca “MAXTOR” e apresentado, entre outras características, a inscrição “XXXX” na parte superior.
2. Dezessete discos ópticos graváveis, por números de IC – 1 a IC – 17.

EXAMES:

1. Analisamos o conteúdo do disco rígido e dos discos ópticos recebidos para exame, utilizando softwares apropriados, inclusive, quando fosse o caso, um software para recuperação de arquivos apagados e dados não alocados.
2. Procuramos, no que fosse possível, responder aos quesitos apresentados, no capítulo “OBJETIVOS DA PERÍCIA”.

RESULTADOS:

Considerando os recursos técnicos e materiais disponíveis por ocasião da perícia e a quantidade total de dados encontrados nas peças examinadas (arquivos gravados, arquivos apagados e dados não locados), apresentamos os seguintes resultados:

1. Sobre o disco rígido recebido para exame:

1.1. Realizamos buscas por arquivos (do “Word”, do “Excel”, mensagens eletrônicas, páginas do site de relacionamento “XXXX”, etc) e dados não alocados, presentes nesse disco, que contivessem, pelo menos, alguns dos seguintes textos: XXXXXX. Dessa pesquisa, logramos somente encontrar dados não alocados (em forma de textos) onde está presente o texto XXXXX. Realizamos a impressão de alguns desses dados não alocados (devido à quantidade encontrada): anexos de 1 a 5.

1.2. Realizamos buscas por arquivos (do “Word”, do “Excel”, mensagens eletrônicas, páginas do site de relacionamento “XXXX”, etc.) e dados não alocados, presentes nesse disco, que contivessem pelo menos alguns dos seguintes textos: XXXXXXX.

1.2.1. Não logramos encontrar arquivo algum que contivesse o texto XXXXX. Esse texto também não foi encontrado nos dados não alocados.

1.2.2. Logramos encontrar alguns arquivos gravados, do tipo “htm” que apresentavam o texto XXXX. Alguns desses arquivos apresentavam semelhanças. Realizamos a impressão do conteúdo de dois desses arquivos: anexos 6 e 7.

1.2.3. Logramos encontrar um arquivo apagado que apresentava o texto XXXXXX. Realizamos a impressão parcial do seu conteúdo: anexo 8.

1.2.4. Logramos encontrar dados não alocados que apresentavam o texto XXXX. Realizamos a impressão de alguns desses dados não alocados (devido à quantidade encontrada): anexos 9 a 22.

1.2.5. Logramos encontrar alguns dados não alocados que apresentavam o texto XXXXX. Realizamos a impressão de alguns desses dados não alocados (devido à quantidade encontrada) anexos de 23 a 27.

2. Sobre os discos ópticos recebidos para exame:

2.1.Realizamos buscas por arquivos (do “Word”, do “Excel”, mensagens eletrônicas, páginas do site de relacionamento “XXXX”, etc), presentes nesses discos, que contivessem, pelo menos, alguns dos seguintes textos: XXXXXX.

2.1.2 Não logramos encontrar arquivo algum que obedecesse a esse critério.

2.2.Realizamos buscas por arquivos (do “Word”, do “Excel”, mensagens eletrônicas, páginas do site de relacionamento “XXXX”, etc), presentes nesses discos e que contivessem, pelo menos, alguns dos seguintes textos: XXXXXX.

2.2.1.Não logramos encontrar arquivo algum que contivesse o texto XXXXXXX.

2.2.2.Logramos encontrar arquivos que apresentam o texto XXXXX. Realizamos as impressões (totais e parciais) dos conteúdos de alguns desses arquivos (devido à quantidade encontrada): anexos de 28 a 52.

3. Observações:

3.1. Os dados não alocados estão divididos em grupos chamados TEXTO 1, TEXTO 2, etc, da mesma forma como foram obtidos, utilizando o software de análise.

3.2. Para os anexos que correspondam a conteúdos de arquivos (gravados ou apagados) escrevemos, nos rodapés, os números de arquivos.

ERA O QUE HAVIA A RELATAR

Este laudo vai impresso no anverso de 03(três) folhas de papel, acompanhado de 52 (cinquenta e dois) anexos. Uma cópia deste laudo, assinada e rubricada, permanece

arquivada neste Instituto. Acompanha(m) a(s) peça(s) examinada(s), acondicionada(s) em saco(s) plástico(s) com o(s) lacre(s) XXXX.

Localidade, data.

Assinatura dos peritos criminais

ANEXO B – Caso II: Relatório da Medida Cautelar de Busca e Apreensão e Respectivo Laudo Pericial

Relatório da Medida Cautelar de Busca e Apreensão

Relatório referente à Medida Cautelar de Busca e Apreensão

I - Trata-se de medida preliminar de Busca e Apreensão proposta perante o Juiz de Direito da Vara XXXX, requerida pela empresa XXXX (requerente), contra XXXX (requerido), funcionário da Requerente, em função de haver fortes indícios de que o requerido está relacionado a um grave incidente de vazamento de informações confidenciais, sendo investigado pelos crimes de violação de sigilo profissional, prática de concorrência desleal, ambos agrados pelo fato de a conduta acima descrita ter sido supostamente cometida com violação de dever inerente a cargo, ofício, ministério ou profissão.

II - A ação ilícita, sob investigação, foi supostamente praticada por meio de:

1. perfil com o nome do requerido, no *site* de relacionamentos XXXXXXX, postando fotos tiradas na dependência da requerida, ferindo manual de segurança da informação;

2. revelação de dados confidenciais da requerida em comunidade em site de relacionamento;

3. postagem de imagens de produto desenvolvido pela requerente (XXXX), o qual ainda não foi lançado e nem divulgado no mercado, bem como de documentos confidenciais atrelados ao aludido produto, divulgados nos *sites* XXXXX;

III - Os delitos ora investigados são os crimes de violação de sigilo profissional e prática de concorrência desleal cometidos por meio da Internet.
Conforme vimos anteriormente, são crimes que atentam contra um valor social tutelado pelo direito, cometidos através de um sistema informático. Desta forma, não constituem nova modalidade de crime, visto que a informatização da sociedade gera a informatização da delinquência. A inovação nesses crimes é a maneiro como

foram praticados. São classificados como crimes informáticos de natureza mista ou imprópria.

Laudo Pericial

EXMO. SR.. JUIZ DE DIREITO DA XX VARA CRIMINAL DA COMARCA DE XXXX

Autos n.o XXXXX
Requerente: XXXXXXX
Requerido: XXXXXXXX

XXXX, perito criminal nomeado por este N. Juizo, vem, mui respeitosamente, à presença de Vossa Excelência, nos autos em epigrafe, requerer a juntada do laudo técnico em anexo.

Nestes termos,
Pede deferimento.

XXXXXXX
Perito Criminal

GOVERNO DO ESTADO XXXX
POLICIA CIVI,L
DEP ARTAMENTO DE POLICIA TÉCNICO-CIENTIFICA
INSTITUTO DE CRIMINALISTICA

LAUDO DE EXAME EM MIDIAS DE ARMAZENAMENTO COMPUTACIONAL (HDs, CDs, DVDs, Disquetes, *Pen Drive),* CÂMERA FOTOGRAFICA DIGITAL E APARELHO CELULAR. (BUSCA E APREENSAO)

Aos XXXX dias do mês de XXXX do ano de XXXXX, nesta cidade de XXXX e no Instituto de Criminalística, pelo diretor Dr. XXXX foram designados os Peritos Criminais XXXX e XXXX, para procederem busca e apreensão em computadores e mídias de armazenamento computacional, a fim de atender ao despacho judicial, da lavra do MM. Juíz de Direito XXXXX, datada de XXXX, de origem da XX Vara Criminal da Comarca de XXXX.

1. HISTÓRICO: em atenção à designação supra, os peritos criminais, aos XXX dias do mês de XXXX de XXX, por volta das XXXX, acompanharam o oficial de justiça XXXXX, que cumpriu mandato de busca e apreensão na residência do senhor XXXXXX (requerido), localizada na Rua XXXXXXX, objetivando identificar mídias de armazenamento computacional *(Pen Drive,* discos rígidos, CDs, DVDS, disquetes etc.), celulares, câmeras fotográficas e computadores para que possam ser apreendidos e, posteriormente, analisados no IC/XX, levando em consideração os quesitos formulados pelos advogados: Dr. XXXXX e Dr. XXXXXXXX., que representam a parte requerente, empresa XXXX.

2. CONSIDERAÇÕES INICIAIS

   a) os advogados XXXXXXXXX e o assistente técnico Sr. XXXXXXX acompanharam a diligência;

   b) 0 Sr. XXXXXX (requerido), acompanhou os peritos e o oficial de justiça durante a diligência nas dependências internas da sua residência;

   c) o material apreendido (vide capitulo 4 adiante) foi levado para o Instituto de Criminalística para exames e emissão do respectivo laudo;

   d)Foram geradas imagens forenses (cópias "bit a bit") das mídias de armazenamento apreendidas *(HD, Pen Drive etc.),* ficando o assistente técnico com uma cópia de cada imagem gerada. Para o respectivo procedimento, foram utilizados o software forense *AcessData FTK Imager* e bloqueadores de escrita;

e) Para o presente trabalho, foram utilizadas as distribuições LINUX forenses HELIX (versão 3) e CAINE *(Computer Aided Investigative Environment,* versão 0.5) para análise dos dados armazenados nas imagens geradas.

3. LOCAL DA DILIGÊNCIA

a) Trata-se de residência de um piso, localizada em área urbana, construída em alvenaria, murada e gradeada, composta por uma garagem coberta, banheiro social, sala, varanda, cozinha, quintal e três quartos (um do Sr. XXXXX (requerido), um da Sra. XXXX - irmã do Sr. XXXXXX (requerido) - outro dos pais do Sr. XXXXXX (requerido).

Foto 01 da fachada do imóvel

XXXXXXXXX

b) No quarto do Sr. XXXXX (requerido), foram encontrados os seguintes equipamentos e mídias: 1 (um) microcomputador; 1 (um) *notebook* da marca XXX (localizado na penúltima gaveta da escrivaninha); 1 (um) aparelho de telefone celular da marca XXXX que estava com o Sr. XXXX (requerido); 1 (uma) câmera fotográfica digital da marca XXXX (localizada sobre a escrivaninha); 1 (um) disco rígido IDE (3.5") da marca XXX (localizado no guarda-roupa); 10 (dez) disquetes de 3 *V2* (localizados na primeira gaveta da mesa do microcomputador); 1 (um) porta *CD/DVD* contendo 18 (dezoito) mídias ópticas (17 CDs e 1 DVD), localizado no guarda-roupa; 1 (um) *Cable Modem* da marca TERAYON, modelo TJ716X, SIN: 507400510120, MAC ADDRESS: 00E06FE59116, localizado na mesa do microcomputador, de uma operadora de telecomunicações não identificada; 1 (um) roteador *Wireless* da marca D-LINK, modelo DI- 624, SIN: F31G172003245, MAC ADDRESS 00195B56D47E, localizado sobre o aparelho de som; 1 (um) pedaço de papel branco contendo entre outros, as inscrições "XXXX" e "XXXX", e manuscritos diversos (localizados na primeira gaveta da mesa do microcomputador). Vide fotos 01 a 07 adiante;

Fotos de 01 a 07 – XXXX

c) A Sra. XXXX (irmã do Sr.XXXX - requerido) entregou 1 (um) *notebook* da marca STI (SEMPTOSHIBA INFO) e 1(um) *Pen Drive* da marca KINGSTON, que estavam no seu quarto.

Foram feitas fotos de cada um dos equipamentos encontrados a serem periciados

Fotos - XXXX

4.MATERIAL APREENDIDO

a) 01 (uma) folha de papel de cor branca, medindo aproximadamente 15cmX21cm, apresentando no anverso as seguintes inscrições "XXXX", "XXXX", "XXXX","XXXX", entre outras, e no verso, manuscritos diversos;

b) 1 (um) *notebook* (computador portatil) da marca CCE, cor branca, medindo aproximadamente (AxLxC): 3x25x33cm; apresentando na base, uma plaqueta de identificação onde se lê as inscrições: XXXX", "PRODUZIDO POR: XXXX", entre outras; com disco rígido SATA de 2.5" da marca WESTERN DIGITAL, modelo WD1600BEVS-00USTO, número de série XXXX, de 160GB;

c) 1 (um) *notebook* da marca SEMP TOSHIBA, cor cinza, medindo aproximadamente (AxLxC): 3,5x23,5x33cm; apresentando na base, uma plaqueta de identificação onde se lê as inscrições XXXXXXXX, entre outras; com disco rígido SATA de 2.5" da marca WESTERNDIGITAL, modelo WD1200BEVS-22USTO, número de serie XXXXX, de 120GB.

d) 1 (um) disco rígido IDE de 3.5" da marca MAXTOR, modele D540X-4K, apresentando etiqueta onde se lê, entre outras, as inscrições XXXXXXX;

e) 10 (dez) disquetes de 3 '12: 1) sem marca aparente, cor preta, sem etiqueta, apresentando o manuscrito XXXX; 2) marca TDK, cor preta, sem etiqueta nem manuscrito; 3) marca NIPPONIC, apresentando etiqueta adesiva onde se lê os manuscritos XXXX; 4) marca NIPPONIC, apresentando etiqueta adesiva onde se lê os manuscritos XXXX; 5) marca IMATION, apresentando etiqueta adesiva onde se lê os manuscritos XXXX, marca IMATION, sem etiqueta, apresentando os manuscritos XXXX; 7) marca Star Life, apresentando etiqueta adesiva onde se lê as inscrições "Word 6.0", "for Windows", entre outras, e os manuscritos XXXX; 8) sem marca aparente, apresentando etiqueta adesiva onde se lê as inscrições XXXX, entre outras, e o manuscrito XXXX; 9) marca IMATION, apresentado etiqueta adesiva onde se lê os manuscritos XXXX; 10) sem marca aparente, apresentando parte de uma etiqueta adesiva onde se lê os manuscritos XXXXXX;

f) 1 (um) porta CD/DVD contendo 18 (dezoito) mídias ópticas (1 DVDR, 1 CD-ROM, 13 CDs): 1) tipo DVD-R, 4.7GB, marca TDK, apresentando os manuscritos XXXX, entre outras ilegíveis; 2) tipo CD-ROM, original, apresentando as inscrições XXXX,entre outras; 3) tipo CDR, 700MB, marca MAXELL, cor verde, apresentando os manuscritos XXXX; 4) tipo CD-R, 700MB, cor dourada, apresentando os manuscritos XXXX; 5) tipo CD-R, 700MB, marca BENQ, apresentando o manuscrito XXXX; 6) tipo CD-R, 700MB, marca MEMOREX,cor prata, apresentando os manuscritos XXXX; 7) tipo CD-R, 700MB, marca MEMOREX, cor dourada, onde se lê os manuscritos XXXX; 8) tipo CD-R, 700MB, marca BENQ, cor dourada, sem anotações; 9) tipo CDOR, 700MB, marca BENQ, cor dourada, apresentando o manuscrito XXXX; 10) tipo CD-R, 700MB, marca HP, core azul e prata; 11) tipo CD-R, 700MB, marca MAXELL, cor cinza, apresentando os manuscritos XXXX; 12) tipo CD-R, 700MB, marca BENQ, cor dourada, apresentando o manuscrito XXXX; 13) tipo CDR, 700MB, marca TDK, apresentando etiqueta onde se lê as inscrições XXXX; 14) tipo CD-R, 700MB, marca BENQ, cor dourada, apresentado o manuscrito

XXXX; 15) tipo CD-R, 700MB, marca BENQ, cor dourada, apresentando 0 manuscrito XXXX; 16) tipo CD-R, 700MB, marca TDK, cor prata, apresentando os manuscritos XXXX; 17) tipo CD-R, 700MB, marca TDK, cor prata, apresentando os manuscritos XXXX; 18) tipo CD-R, 700MB, marca BENQ, cor dourada, apresentando os manuscrito XXXXX;

g) 1 (um) aparelho de telefone celular da marca XXXX, de cor preta, medindo aproximadamente (AxLxC): lx5x10cm, apresentando etiqueta de identificação (localizada no compartimente da bateria), onde se lê as inscrições "MODELO: SGH-E256", "SSN: - E256GSMH", "N/S: 00428017", "IMEI: 354933/01/430017/6"; com bateria da mesma marca (modelo AB043446BN), cartao *SIM* (XXXXX) de 128KB da operadora de telefonia XXX e cartão de memória MicroSD de 1GB;

h) 1 (uma) câmera fotográfica digital da marca XXXX, modelo D- 435, cor prata, apresentando na base uma plaqueta de identificação onde se lê, entre outras, as inscrições XXXX e "MADE IN XXX", contendo um cartão de memória de 128MB da mesma marca, padrão XD e duas pilhas tipo AA recarregáveis da marca JWIN;

i) 1 (um) *Pen Drive* de cor branca, da marca XXXX, modelo DTI (Datatraveler) de 1GB, apresentando na lateral as inscrições XXXXX.

j) 1 (um) microcomputador ("CPU//) de marca genérica, apresentando a seguinte configurações: 1) gabinete tipo torre, medindo aproximadamente (AxLxC): 34x20x41,5cm, cor bege sem as tampas laterais, apresentando no setor traseiro uma plaqueta onde se Iê as inscrição XXXX; 2) placa-mãe com processador e ventoinha; 3) 1 (um) modulo de memoria; 3) 1 (um) leitor de CD da marca XXXX; 4) 1 (um) gravador de CD da marca LG; 5) 1 (uma) placa de Fax/Modem; 6)1 (uma) placa de rede; 7) 1 (uma) unidade de disquete 3 *V2;* 8) 1 (um) disco rígido IDE de 3.5// da marca SEAGATE, modelo ST310215A, numero de serie XXXX, de 10GB; 9) 1 (uma) fonte elétrica de 400W.

5. CONSTATAÇÕES: considerando o objetivo proposto, os peritos constataram os seguintes itens:

5.1 No documento

a) Apresenta no anverso diversas inscrições XXXX, sugerindo uma referência a um componente de Iinha de produção, identificado pelo código alfanumérico XXXX• No verso, apresenta um manuscrito de uma planilha mensal. Vide foto.

Fotos 08 e 09 – sigilosas.

5.2 NAS MIDIAS MAGNÉTICAS (DISQUETES *3112)* E Ó**PTICAS, NO *PEN DRIVE,* NO *NOTEBOOK* DA MARCA SEMP TOSHIBA E NO DISCO RIGIDO AVULSO DA MARCA MAXTOR:**

As mídias magnéticas e ópticas, o *notebook* da marca STI (SEMP TOSHIBA INFO) e o *Pen Drive* não apresentam qualquer elemento técnico indicativo, nem mesmo sugestivo, de armazenamento de dados referentes ao caso em questão. 0 disco rígido da marca MAXTOR não funciona, esta inoperante, prejudicando o exame.

5.3 NA CÂMARA FOTOGRÁFICA DIGITAL XXXX:

a) Encontra-se em bom estado de conservação e em perfeito funcionamento. A data e a hora do equipamento estão atualizadas;

b) A memória interna de 14MB não contém fotografia nem vídeo aparente. 0 Instituto não dispõe de cabo de dados compatível com o aparelho para recuperar arquivos porventura excluídos;

c) O cartão de memória *XD* contém 1 (um) arquivo de imagem (padrão JPEG) denominado P4170001.JPG, que contém um auto-retrato do Sr. XXXXXX (requerido) em sua residência. Os METADADOS produzidos pela câmera, que podem ser vistos na Imagem 01, informam que a marca e o modele do equipamento que produziu a foto é XXXXXXX;

d) Foi recuperado somente um arquivo excluído, de imagem (padrão JPEG), contendo também um auto-retrato do Sr. XXXXX (requerido), em sua residência.

Imagem 01 – Metadados do arquivo P4170001.JPG.

5.4 NO APARELHO CELULAR DE MARCA XXXX:

a) Encontra-se em bom estado de conservação e em perfeito funcionamento. A data e a hora do equipamento estão desatualizadas;

b) De acordo com a especificação do aparelho disponível no *site* da XXXX na Internet (www.XXXX.com). o equipamento possui a capacidade de produzir fotografias e vídeos de curta duração (resolução da câmera VGA, sem *flash,* vídeo no padrão 3GP/MPEG4), além de uma memória interna de 10MB;

c) A memória interna do aparelho contém 12 (doze) arquivos de imagem (padrão JPEG), contendo fotografias do Sr. XXXX (requerido), a maioria é auto-retrato. Um arquivo, denominado Foto-0002.jpg, contém um auto-retrato do Sr. XXXXX acompanhado de uma mulher não identificada, ambos vestindo uma roupa branca e um boné verde, que apresentam a inscrição "XXXX" em vermelho. Devido a inoperância da tecla de navegação "Opções", não foi possível copiar o respectivo arquivo, mas foi produzida uma foto no Instituto de Criminalística da câmera com a respectiva imagem. Vide Fotografia 11. Não há arquivo de vídeo aparente. O Instituto de Criminalística não dispõe de meios para recuperar arquivos porventura excluídos em memória interna de aparelho celular;

Foto 11 - Imagem reproduzida no visor do aparelho - sigilosa

d) O cartão de memória do aparelho celular contém dezenas de arquivos de imagem (padrão JPEG), de vídeo (padrões 3GP, MP4) e de música (padrão MP3). Foram recuperadas outras dezenas de arquivos. Nenhum dos arquivos possui referência à XXXX ou à empresa XXXX;

5.5 NO DISCO RÍGIDO DA MARCA SEAGATE DO MICROCOMPUTADOR

Obs: A data e a hora apresentada pela BIOS do microcomputador encontram-se atualizadas (GMT-4).

a) O disco rígido possui uma partição de 9,3GB (Sistema de Arquivos NTFS, setores: 19.534.977, bytes por setor: 512), doravante denominada P1, contendo aproximadamente 74.911 (setenta e quatro mil, novecentos e onze) arquivos, distribuídos em 3.791 (três mil, setecentas e noventa e uma) pastas. A maioria dos arquivos e das pastas é do sistema operacional e dos programas instalados;

b) O sistema operacional e o *Microsoft Windows XP Professional,* localizado em *P*1:*WINDOWS,* que de acordo com a data de criação dos arquivos, foi instalado em XXXXX;

c) Programas instalados sac: *Adobe Acrobat* (leitor de arquivos PDF), *ArcSoft Photoimpression* 6 (visualização e gerenciamento de imagens), *Microsoft Office* (pacote de escritório: editor de texto, planilha etc.), *IRPF* (imposto de renda), *MSN Messenger* (troca de mensagens e arquivos instantâneos pela Internet), XXXX *PC Studio* 3 (transferência de arquivos de celulares da marca XXXX);

d) A pasta *Pl: \Documents and Settings* \ possui as seguintes subpastas referentes as contas de usuário do sistema operacional instalado: "XXXX" (criada em XXXXXX – último acesso em XXXX); "TEMP.XXXXX.001" (criada em XXXX), ultima acesso em XXXX. Há também três pastas sem dados: "TEMP" (criada em XXXXXX, ultimo acesso em XXXXX), "TEMP.XXXX" (criada em XXXX, ultimo acesso em XXXXXX) e "TEMP.XXXX" (criada em XXXX, último acesso em XXXXX);

e) De acordo com o arquivo *SOFTWARE* do Registro do *MS Windows XP,* localizado em *Pl:\WINDOWS\system32\config, o* sistema operacional instalado está registrado em nome de "XXXX". Conforme imagem 02;

Imagem 02 – Trecho do registro do Windows XP instalado.

f) A pasta *"XXXX"* em *Pl: \Documents and Settings\XXXXX\Meus documentos\,* contem 30 (trinta) arquivos de imagem (padrao JPEG) com os nomes dos arquivos iniciados pelas letras DSC (padrao de nome de camera da marca SONY): 11 (onze) fotografias foram produzidas com 0 modele DSCP72, entre XXXXXX e XXXXX; 2 (duas) foram produzidas com 0 modele DSC-S500, no dia XXXX; 17 (dezessete) foram produzidas com o modele DSC-P43, entre XXXX e XXXX. As fotos não fazem referências a motocicletas nem à empresa XXXX;

g) As pastas *Contacts,* que armazenam as pastas dos usuários do serviço de mensagens instantâneas *MSN Messenger,* localizadas em *P*1:*Documents and Settings \XXXX*\() e *Pl :\Documents and Settings \XXXX\(2),* contém três usuários com referência ao nome do Sr. XXXX (requerido). Vide relação na Tabela 01;

Tabela 01 - Relação de usuários " XXXX" do MSN – Messenger

Tabela – XXXXXX

h) As pastas *Cookies,* que armazenam arquivos de controle criados pelos *sites* da Internet acessados, localizadas em *Pl: \Documents and Settings\XXXX*, *Pl:\Documents and Settings\XXXX \Configurações locais\ Temp* e *P*1:*Documents and Settings \TEMP.XXXX \Configurações locais\ Temp(3),* contém referência a 6 (seis) *sites* relacionados a XXXX. Vide relação Tabela 02;

Tabela 2 – relação dos arquivos Cookies

Tabela 2 – XXXXXX

i) Nas pastas de arquivos temporários de acesso a Internet pelo programa de navegação *Internet Explorer,* usando a conta *"TEMP.XXXX",* localizadas em *Pl:\Documents and Settings \TEMP.XXXX \Configurações locais\ Temporary Internet Files\Content.IE5* e *Pl :\Documents and Settings \TEMP.XXXX \Configurações locais\ Temp\ Temporary Internet Files \Content.IE5* foram localizados 14 (catorze) arquivos de imagem (padrão JPEG), contendo fotografias de XXXX. As imagens, alem de serem de baixa resolução,não contém dados da câmera fotográfica. Vide relação na Tabela 03 e o conteudo adiante;

Tabela - Relação das fotos com XXXX da Internet

Tabela – XXXXX

Fotos – XXXXXX

j)* As pastas *Pl: \Documents and *Settings\ TEMP.XXXX \ Configurações locais \Temp \Historico* e *Pl Pl: \Documents and Settings \TEMP.XXXX.OOl\Configurações locais\Historico* contém o histórico dos *sites* visitados no período de XXXX a XXXX, entre os quais, diversos perfis e comunidades do Orkut *(site* de relacionamento) e um sobre XXXX, relacionados na Tabela 04;

Tabela 4 - Relação de perfis e comunidades acessadas no Orkut

Tabela - XXXXXX
k) Nas pastas de arquivos temporários de acesso à Internet pelo programa de navegação *Internet Explorer,* usando a conta *"XXXX",* localizadas em *Pl:\Documents and Settings\XXXX\Configurações locais\ Temporary Internet Files\Content.IEg)* e *P1:\Documents and Settings\XXXX \Configurações locais\ Temp\Temporary Internet Files \Content.IEg,* foram localizados 8 (oito)arquivos de imagem (padrão JPEG e GIF) contendo fotografias de XXXX. As imagens, além de serem de baixa resolução, não contém dados da câmera fotográfica. Vide relação na Tabela 05 e conteúdo adiante;

Tabela 05 – Relação das imagens com XXX na Internet e fotos.

XXXXXX

I) As pastas *Pl:\Documents and Settings \XXXX\Configuraçõeslocais\Temp\Hist6rico* e *Pl:\Documents and Settings\XXXX\Configurações locais\Histórico* contém diversos

perfis e comunidades do Orkut, acessados no período de XXXX a XXXX, fora do escopo do exame;

m) 0 arquivo *Thumbs.db*[31], localizado na pasta *Pl:\Documents and Settings \TEMP.XXXX. 001 \Meus documentos \Minhas imagens,* contém 6 (seis) imagens em miniatura do Sr. XXXX (requerido), com o uniforme da empresa, e de XXXX. As imagens não contêm dados da câmera fotográfica. Como não possuem o nome original, as imagens foram nomeadas seguindo o padrão Imagem_Thumb_O?jpg (?=numero sequencial). Vide o conteúdo a seguir;

Imagens - XXXXX

n) Foram recuperadas 34 (trinta e quatro) imagens de XXXX e uma da logomarca da XXXX, algumas imagens estão incompletas. As imagens são de baixa resolução e não possuem dados da câmera nem da data que foram produzidas. Com exceção de três, as demais não possuem o nome original, sendo nomeadas seguindo o padrão Recuperado_O?jpg (?=numero sequencial). Vide o conteúdo a seguir;

Imagens – XXXX

O) A Tabela 06 contém o resultado da pesquisa das palavras-chaves XXXX independente de maiúscula ou minúscula, com ou sem espaço, com ou sem acento.

Tabela 6 - **Resultado das pesquisas das palavras-chaves**

Tabela – XXXX

5.6 NO DISCO RÍGIDO DO NOTEBOOK DA MARCA CCE

a) O disco rígido possui uma partição de 149GB (Sistema de Arquivos NTFS/ setores: 312.576.000/ bytes por setor: 512), doravante denominada P1/ contendo aproximadamente 110.005 (cento e dez mil e cinco) arquivos/ distribuídos em 14.017 (catorze mil e dezessete) pastas. A maioria dos arquivos e das pastas e do sistema operacional e dos programas instalados;

b) O sistema operacional e o *Microsoft Windows Vista Home Premium/*localizado em *Pl:\WINDOWS/* que de acordo com a data de criação dos arquivos/ foi instalado em XXXX;

c)Programas instalados são: *Adobe Acrobat Reader* (Ieitor de arquivos PDF)/ *Ares* (compartilhamento de arquivos)/ *Free Audio Packer* (conversor de arquivos de audio)/ *Google Earth* (visualizador de imagens de satelite)/ *Grisoft AVG* (antivlrus)/ *Microsoft Office* (pacote de escritório: editor de texto/ planilha etc.)/ *Mozilla Firefox*

31 0 arquivo Thumbs.db é criado pelo próprio sistema operacional Windows quando as imagens dos arquivos armazenados em uma determinada pasta são visualizadas no utilitário Explorer do Windows XP (na opção Exibir ->Miniaturas). Esse arquivo contém copias em miniatura (baixa resolução) das Imagens principais.

(navegador de Internet/ *browser), MSN Messenger* (troca de mensagens e arquivos instantâneos pela Internet), *Olympus Master* (programa para manipulação de fotos), WinRAR (compactor/descompactor de arquivos RAR);

d) A pasta *Pl:\Documents and Settings*\ possui uma subpasta denominada "XXXX// (criada em XXXX, ultimo acesso em XXXX/ por *volta* das XXXX) referente a conta de usuário do sistema operacional instalado;

e) De acordo com o arquivo *SOFTWARE*do Registro do MS Windows XP, localizado em *Pl:\WINDOWS\system32\config/ o* sistema operacional instalado esta registrado em nome de "XXXX". Vide Imagem 03;

Imagem 03 – Trecho do registro do MS Windows Vista instalado.

Imagem – XXXXX

f) 0 arquivo de usuário do *Excel* (pacote Office) denominado XXXX.*xls* (criado no disco em XXXX, último acesso em XXXX), armazenado na pasta *Pl :\XXXX \Documentos,* contem uma planilha intitulada XXXX*,* cujos valores correspondem parcialmente aos encontrados no verso do documento apreendido (seção 5.1). Vide o teor na Tabela 07;

Tabela 07 – conteúdo do documento XXXX.xls

Tabela – XXXXXXXX

g) Na pasta *Pl : \XXXX\,* foram localizados 32 (trinta e dois) arquivos de imagem e um de Vídeo amador (padrão 3GP/MP4) contendo imagens de XXXX e da logomarca da empresa XXXX. Vide relação na Tabela 08 e o conteúdo adiante;

h) 0 vídeo, com audio e duração de 48s (quarenta e oito segundos), mostra linhas de produção de XXXX, com funcionários vestindo uniformes iguais aos das fotos dos arquivos Foto-0097.jpg, Foto-0105.jpg e Foto-0106.jpg (vide conteúdo adiante). Aos vinte oito segundos, foi identificado um falante com timbre de voz masculina, pronunciando os seguintes dizeres: “XXXX", como se estivesse falando ao celular. Os dados técnicos do vídeo são compatíveis com o aparelho celular da marca XXXX, modelo XXXX;

TABELA 08 – RELAÇÃO DOS ARQUIVOS COM IMAGENS DE XXXX

TABELA – XXXXX

FOTOS – XXXX

VÍDEO – XXXX

i) A pasta *Meus arquivos recebidos,* localizado em *Pl: \ Users\xxxx\Documents\Meus arquivos recebidos,* contém ·12 (doze) arquivos de imagem (padrÃo JPEG) com os nomes dos arquivos iniciados pelas letras DSC (padrão de nome de câmera da marca SONY), contendo 12 (doze) fotografias produzidas com a câmera da marca

SONY, modelo DSC-W150, no dia XXXX. As fotos não fazem referência a XXXX nem a empresa XXXX;

j) A pasta *Contacts,* que armazena as pastas dos usuários do serviço de mensagens instantâneas *MSN Messenger,* em *Pl: \Users\XXXX* \ *Contacts,* contém três usuários com referência ao nome do Sr. XXXX (requerido). Vide relação na Tabela 09;

TABELA 09 – Relação do usuário "XXXX" do *MSN messenger*

TABELA – XXXX

k) 0 arquivo *Cookies.txt* do *navegador Firefox,* armazenado em *Pl : \Users\XXXX\AppData \Roaming \Mozilla \Firefox\Profiles\ g533ftff.default\,* contém referência a *sites* acessados relacionados
a XXXX. Vide relação na Tabela 10;

TABELA 10 – Registro de sites de XXXX no arquivo Cookies.txt

TABELA - XXXX

l) Foram recuperadas dezenas de imagens (padrões JPEG e PNG) de baixa resolução de diversas XXXX. Apenas três contém os nomes originais dos arquivos, os demais seguem o seguinte padrão: recuperado_?? .EXT, onde ?? = numero de sequencia e EXT = JPG ou PNG. Destaca-se o fragmento de imagem no arquivo denominado Recuperado_01.jpg, que contém os dados da marca (XXXX) e modelo (SGH-E256) da câmera que produziu a fotografia (em XXXX, por volta das XXXX). As demais imagens não possuem os respectivos dados;

IMAGENS RECUPERADAS – XXXXX

m) A Tabela 11 contém o resultado da pesquisa das palavras-chaves XXXX, independente de maiúscula ou minúscula, com ou sem espaço, com ou sem acento, ASCII ou Unicode, no todo ou como parte.

Tabelas 11 a 19 - Resultado das pesquisas das palavras-chaves.

Tabelas – XXXXX

6 CONCLUSÃO

Diante do exposto no corpo do presente laudo, levam os peritos a inferir que o Sr. XXXXX (requerido):

a) Produziu com o seu aparelho de telefone celular da marca XXXX, modelo SGH-E256, fotografias e vídeos de curta duração nas dependências da empresa XXXX;

b) Acessava sites de discussão relacionados a XXXXXX;

c) Tinha como contato no serviço de comunicação instantânea *MSN Messenger o* endereço eletrônico XXXX.

1) Queira o Sr. Perito descrever o local da diligencia.
Resposta: Vide capitulo 3. LOCAL DA DILIGÊNCIA.

2) Queira o Sr. Perito identificar e catalogar todas as máquinas e seus HDs, como também toda e qualquer mídia de armazenamento em geral, sem se limitar a pendrives, flash memory, smart memory, discos rígidos (incluindo HDs extemos USB, avulsos,desinstalados, não operantes etc.), DVDs, CD-ROMs, disquetes, zipdrives, fitas magneticas/DATjDDS, relógios com armazenamentos, celulares (com especial atenção,mas não se Iimitando a aparelho da marca XXXX)e IPOD.

Resposta: Vide capítulo 4. Material Apreendido.

3) Queira o Sr. Perito verificar se existem no local da diligência notas fiscais, recibos, ordens de serviços, mensagens, cartas, selos de garantia, etiquetas, manuais técnicos, embalagens, caixas e quaisquer outros documentos que indiquem ter havido compra, obtenção, instalação, substituição, venda, doação ou troca de equipamento de Informática ou algum componente, inclusive HDs, desde XXXX até a data da diligência.

Resposta: Nada encontrado.

4) Queira o Sr. Perito identificar e descrever a presença de equipamentos com configuração incompleta, como acessórios específicos para computadores, monitores de vídeo, teclados e pontos de rede não conectados a qualquer computador ou a existência de gabinetes sem disco rígido ou CPU.

Resposta: Somente um disco rígido IDE (3.5”) inoperante.

5) Queira o Sr. Perito identificar e descrever no local da diligência os recursos para comunicação de dados, incluindo conexão por cabos de rede (LAN, MAN, WAN), conexões ponto a ponto por radiofrequência, conexões wireless/wi-fi, conexões GRPSj Celular, Smartphone ou similares.

Resposta: Vide capítulo 3. LOCAL DA DILIGÊNCIA.

6) Queira a Sr. Perito gerar copias fiéis (clones "byte a byte") de todos as discos rígidos existentes no local. A cópia dever ser realizada através da metodologia e ferramentas que reproduzam integralmente o HD, inclusive os dados deletados, as áreas não alocadas, dados remanescentes de eventuais formatações anteriores, os arquivos do sistema operacional e assim por diante, tarefa usualmente realizada através do software "FTK" da ACESSDATA,via CD-ROM"bootaver:

Resposta: Procedimento efetuado. Vide capitulo 2. CONSIDERAÇÕES INICIAIS.

7) Queira a Sr. Perito copiar, "byte a byte” os dados de interesse pericial eventualmente presentes nos demais dispositivos digitais encontrados, como HDs

soltos, memórias, pen drives, disquetes, CD-ROMs, DVDs e demais dispositivos de armazenamento.

Resposta: Procedimento efetuado. Vide capitulo 2. CONSIDERAÇÕES INICIAIS.

8) Queira a Sr. Perito descrever o sistema operacional de cada dispositivo, seus códigos de licenciamento e as datas nas quais foram instalados e prover a descrição detalhada do conteúdo dos dispositivos digitais.

Resposta: Vide capítulo 5. DAS CONSTATAÇÕES.

9) Queira o Sr. Perito informar, no caso de ser encontrado aparelho celular na diligência (com especial atenção, mas não se limitando a aparelhos da marca XXXX), se possui capacidade para tirar fotos e filmar.

Resposta: Sim. Vide seção 5.4 do capítulo 5. DAS CONSTATAÇÕES.

10) Queira o Sr. Perito, utilizando software de investigação forense, analisar o celular apreendido a procura de fatos ou filmes no aparelho celular.

Resposta: Sim. Vide seção 5.4 do capítulo 5. DAS CONSTATAÇÕES.

11) Queira o Sr. Perito, se a resposta acima for positiva, detalhar quais fotos foram encontradas e se elas tem vínculo com o caso.

Resposta: Sim. Vide seção 5.4 do capítulo 5. DAS CONSTATAÇÕES.

12) Queira o Sr. Perito, se foi possível encontrar fotos ou filmes no aparelho celular, informar quantas destas fatos lembram o ambiente de trabalho da empresa XXXX.

Resposta: Sim. Uma fotografia.

13) Queira o Sr. Perito informar quais são os provedores de acesso utilizados nos dispositivos periciados.

Resposta: Prejudicado. Não foi possível identificar o provedor de acesso do Cable Modem encontrado.

14) Queira o Sr. Perito apurar para cada dispositivo a sua linha de tempo, mostrando cronologicamente as datas (mac time) de criação, alteração e deleção dos arquivos desde XXXX ate o dia da diligência. Favor listar todas as pastas (diretórios) e arquivos com suas datas, incluindo aqueles do sistema operacional. Com base nesses dados, favor esclarecer se a distribuição é normal ou há indícios de eventual formatação do dispositivo, reinstalação do sistema operacional, acréscimo ou eliminação de arquivos ou outro procedimento de maior significância na manipulação de arquivos.

Resposta: Prejudicado. 0 ICXX não dispõe de ferramentas para relacionar cronologicamente as datas de criação, alteração e deleção de arquivos e pastas.

15) Favor descrever se no material apreendido existe ou existiu qualquer software para eliminação de resíduos de arquivos deletados, eliminação de arquivos temporários, eliminação de cookies, apagamento de dados da área de swap ou similares. Caso positivo, descrever indicando data de instalação, execução e remoção do software.

Resposta: Não foi identificado nenhum elemento técnico indicativo de existência ou utilização de software para remoção de arquivos, pastas etc.

16) Queira o Sr. Perito examinar todos os dispositivos, abrangendo em sua análise tanto as pastas e arquivos ativos, assim como os arquivos deletados, fragmentos de dados, áreas não alocadas, área de swap, arquivos de hibernação (hiberfil etc.), áreas temporáriass, cookies, arquivos ".dat", arquivos log, arquivos históricos, registros do windows, metadados e demais dados técnicos existentes nos dispositivos, buscando qualquer vestígio da palavra XXXX. No caso afirmativo, gentileza detalhar em qual contexto esta palavra foi encontrada. Caso tenha sido encontrado um arquivo de imagem contendo este nome, favor reproduzir a imagem.

Resposta: Procedimento efetuado. Vide capítulo 5. DAS CONSTATAÇÕES.

17) Queira o Sr. Perito, através de análise forense digital, identificar em qual(is) HDs ou dispositivo de armazenamento podem ser encontradas fotos do novo modele da XXXX e qual data de criação e e alteração continha o arquivo.

Resposta: Vide capítulo 5. DAS CONSTATAÇÕES.

18) Queira o Sr. Perito exemplificar se foram encontrados vestígios de acesso a sites de XXXX, como: http://www.XXXX e outros.

Resposta: Vide capítulo 5. DAS CONSTATAÇÕES.

19) Queira o Sr. Perito exemplificar se (foram encontrados vestígios de acessos a sites com um suposto usuário XXXX.

Resposta: Nenhum vestígio encontrado.

20) Queira o Sr. Perito realizar as buscas em todos os tipos de arquivos, inclusive em arquivos de mensagens, imagem, documentos, cadastros, bancos de dados, planilha eletrônicas, arquivos compactados, arquivos protegidos por senhas, arquivos ocultos e similares, arquivos deletados, arquivos do sistema operacional, arquivos cifrados e outros, presentes em qualquer dispositivo de armazenamento, que possuam dados que possam conter, em seus nomes ou em seu conteudo, palavras como: XXXX.

Resposta: Pesquisa efetuada. Vide capítulo 5. DAS CONSTATAÇÕES.

21) Queira o Sr. Perito realizar as buscas em todos os tipos de arquivos, inclusive em arquivos de mensagens, imagens, documentos, cadastros, banco de dados, planilha eletrônica, arquivos compactados, arquivos protegidos por senhas, arquivos ocultos e similares, arquivos deletados, arquivos do sistema operacional, arquivos

cifrados e outros, presentes em qualquer dispositivo de armazenamento, que possam conter METADATA que correspondam a alguma câmera digital da marca XXXX.

Resposta: Pesquisa efetuada. Vide capítulo 5. DAS CONSTATAÇÕES.

22) Queira o Sr. Perito identificar a presença de softwares para comunicação,realizando buscas para cadastros de usuários, cadastro de contatos, mensagens, conversa ou chats com conteúdo de interesse pericial, abrangendo itens como Outlook (PST), Outlook Express (DBX), Lotus Notes, Webmails, IRC, ICQ, MSN, ORKUT, chats, fóruns, blogs, Skype e outros similares. Buscar indícios em arquivos ativos, deletários, temporários, de sistema etc. Queira verificar também os respectivos históricos de mensagens, logs e cadastros de interlocutores, dados cadastrais, userid, IPs (Internet Protocol) etc. que possam estar relacionados aos fatos em apuração.

Resposta: Pesquisa efetuada. Vide capítulo 5. DAS CONSTATAÇÕES.

23) Queira o Sr. Perito verificar detalhadamente nos clones dos disco rígidos a presença de indícios sobre o uso de sistemas remotos de mensagens tais como serviços Webmail ou similares, verificando e reconstituindo via html residente em arquivos temporários e em áreas não alocadas os acessos realizados de interesse pericial. Favor detalhar TODAS as contas de e-mail encontradas nos dispositivos de armazenamento e analisar se alguma delas está vinculada a sites de XXXX, como por exemplo: http://www. XXXX.

Resposta: Pesquisa efetuada. Vide capítulo 5. DAS CONSTATAÇÕES.

24) Queira o Sr. Perito considerar nos exames todos os dados de interesse pericial, incluindo mas não se limitando a nomes similares, variações de nomes, plural/singular, tempos de verbo, variações de gênero, presença ou ausência de acentuação, presença de caracteres especiais inseridos, existência ou não de espaços,hífens e quebras de parágrafos/páginas, presença da palavra chave como parte de um nome maior, qualquer variação de formatação etc..

Resposta: Pesquisa efetuada. Vide capítulo 5. DAS CONSTATAÇÕES.

25) Queira o Sr. Perito,em especial, realizar busca por dados existentes no interior dos arquivos de troca (pagefile.sys, etc.), em arquivos de cache e cookies, identificando trechos de códigos html que tenham qualquer relação com as questões em apuração. Solicita-se recuperar todas as telas armazenadas em pagefile.sys/swap sobre as questões de interesse pericial, abrangendo a recuperação de fragmentos html e páginas utilizadas.

Resposta: Pesquisa efetuada. Vide capítulo 5. DAS CONSTATAÇÕES.

26) Queira a Sr. Perito informar se nos arquivos encontrados referentes ao caso, há qualquer referência a origem dos dados, ou seja, de onde e como foram retiradas tais informações.

Resposta: Pesquisa efetuada. Vide capítulo 5. DAS CONSTATAÇÕES.

Nada mais havendo a relatar, encerra-se o presente laudo, contendo quarenta e duas (42) laudas, que relatado e digitado pelo primeiro perito, lido e achado conforme pelo segundo, assinam acordes.

XXXXXXXXXXXXXX
PERITOS CRIMINAIS

ANEXO C – Relatório do Pedido de Instauração de Inquérito Policial e Respectivo Parecer Técnico

Relatório do Pedido de Instauração de Inquérito Policial

Relatório referente ao Pedido de Instauração de Inquérito Policial

I - Trata-se de pedido de instauração de Inquérito Policial perante o Ilmo. Sr. Delegado de Polícia de Investigações Gerais de XXXXX feito pela instituição bancária XXXX, para apuração dos crimes de:

a) interceptação de comunicações informáticas e telemáticas;
b) quebra de sigilo bancário;
c) furto, mediante fraude ou destreza, e em concurso de mais de 02 (duas) pessoas e
d) formação de quadrilha.

II – Os supostos crimes foram praticados por meio de acessos ao sistema de Internet Banking Pessoa Física, da instituição bancária XXXX, realizando operações contestadas por seus correntistas, consistentes no pagamento de contas de consumo (água, luz, telefone etc), boletos bancários de natureza diversa e resgate de investimentos.

III – Os ilícitos sob investigação são os crimes comuns cometidos por meio da Internet. Conforme vimos anteriormente, são crimes que atentam contra o patrimônio, ou seja, um valor social tutelado pelo direito, cometidos através de um sistema informático. Desta forma, não constituem nova modalidade de crime, visto que a informatização da sociedade gera a informatização da delinquência. A inovação nesses crimes é a maneira como foram praticados. São classificados como crimes informáticos de natureza mista ou imprópria.

Parecer Técnico

RELATÓRIO XXXX

SISTEMA DE MONITORAMENTO XXX

ACESSO INDEVIDO A CONTAS

CONFIDENCIAL

Autor: Assistente técnico XXX

Data: XXX

1. Introdução

O objetivo deste relatório é a descrição de ocorrências acusadas como fraudulentas por clientes do XXXX, para diversas transações, realizados através da Internet.

2 Descrição da ocorrência

2.1 XXXX

Foram detectadas diversas transações na conta corrente da cliente XXXX, que não foram reconhecidas pela mesma, titular da conta corrente nº XXXX, agência XXXX e, portanto, consideradas indevidas, constituindo-se em transações realizados através da Internet, utilizando chaves de acesso válidas ao sistema Internet Banking Pessoa Física.

Mencionadas transações contemplam pagamentos de contas de consumo (água, energia elétrica e telefone), pagamentos de impostos, transferência e boletos bancários, conforme discriminação abaixo:

Data	Hora	Descrição	Acesso/Transação
XXXX	XXXX	XXXX	PG.FICHA COMP.OUTROS BCOS
XXXX	XXXX	XXXX	PG.FICHA COMP.OUTROS BCOS
XXXX	XXXX	XXXX	DOC
XXXX	XXXX	XXXX	CDC
XXXX	XXXX	XXXX	IPVA

3. Endereços IPs usados

Abaixo, seguem endereços IPs, data e horários utilizados para os acessos indevidos à conta do referido cliente:

Data	Hora	Acesso/Transação
XXXX	XXXX	XXXX
XXXX	XXXX	XXXX

4. Identificação dos Endereços IP no site "Registro.br"

Verificando os endereços IPs supra citados, segundo o Registro.br (órgão responsável por alocações de endereçamento IPs no Brasil), foi possível identificar que os endereços IPs estão sob responsabilidade do provedor e operadora de acesso XXXX, conforme anexo I.

A seguir é apresentada uma tabela que relaciona os endereços IPs à operadora utilizada:

4.1 XXXX

Data	Hora	Acesso	Operadora/Provedor

XXXX	XXXX	XXXX	XXXX
XXXX	XXXX	XXXX	XXXX

Dessa maneira, os referidos endereços IPs estão sendo utilizados através do serviço de acesso à Internet provido pela mencionada empresa para a prática de transferências acusada como indevidas pelos clientes do XXXX.

5. CONCLUSÃO

Assim, para localização do(s) responsável(eis) pelas transações tidas como indevidas pelo cliente desta instituição financeira, a única opção imediata é a identificação dos usuários da empresa XXXX, que utilizaram os endereços IP relacionados, nas datas e horários constantes na tabela prática abaixo:

Data	Hora	Acesso	Operadora/Provedor
XXXX	XXXX (GMT -3)	XXXX	XXXXX
XXXX	XXXX (GMT -3)	XXXX	XXXX

_____

XXXXXXXX

Assistente técnico

Anexo I – Consulta ao Registro.br para os endereços IPs pertencentes a XXXXXX.