Sabrina Rodrigues Santos

Perícia Forense em Sistemas Informatizados

Uma Abordagem Jurídica

DELFOS
Editora Digital

SABRINA RODRIGUES SANTOS

PERÍCIA FORENSE EM SISTEMAS INFORMATIZADOS

UMA ABORDAGEM JURÍDICA

SÃO PAULO – SP

2011

DELFOS
Editora Digital

S229p Santos, Sabrina Rodrigues.
Perícia forense em sistemas informatizados : uma abordagem jurídica [recurso eletrônico] /Sabrina Rodrigues Santos.
– livro digital. – São Paulo : Editora Delfos, 2011-

Sistema requerido: Adobe Acrobat Reader.
Modo de acesso: World Wide Web
<http://www.potti.com.br/home.html>
Forma de aquisição: As instruções para compra e aquisição das obras estão disponíveis no próprio site.
Obra concebida originalmente em versão digital.
ISBN 978-85-64514-00-3
Inclui bibliografia.

1. Direito 2. Direito – informática 3. Perícia forense computacional 4. Sistemas de informação 5. Crime cibernético. I. Título.

CDD 345.810

Bibliotecário Responsável: Renato Moreira de Oliveira
CRB 8/8090

Conselho Editorial: Ms. Álvaro da Cunha Caldeira
Ms. Sabrina Rodrigues Santos
Victor Hugo Pereira Gonçalves

Capa: Luiz Carlos Gonçalves

Diagramação: Ailton Roberto Oliveira

Revisão: Ms. Álvaro da Cunha Caldeira

DELFOS Editora Digital
Avenida Angélica nº 2632, cj. 64-b, São Paulo/SP
Brasil CEP 01228-220
Telefone 11 3258 4755

AGRADECIMENTOS

Agradeço ao amigo Ákio Nogueira Barbosa por compartilhar suas idéias sobre o imbricamento do Direito e as tecnologias, do que resultou a pesquisa sobre a Perícia Forense em Sistemas Informatizados.

Eterna gratidão a minha família pelo companheirismo.

“ A Justiça não pode produzir a Injustiça”,

A República, Platão

APRESENTAÇÃO

Esta obra se originou das pesquisas sobre o imbricamento do Direito com as tecnologias de comunicação e telecomunicação, com objetivo de fazer uma reflexão sobre a perícia forense em sistemas informatizados à luz da legislação em vigor, a partir da revisão do funcionamento e vulnerabilidades daqueles sistemas.

A perícia fornece elementos importantes para formar o convencimento consciente do juízo na solução do caso, mas a sua realização demanda técnicas específicas e alheias à ciência do Direito, cujo diálogo intenso entre os profissionais pode se mostrar eficiente e contribuir na educação para a inclusão digital e social e, por consequência, o uso racional dos mesmos.

Com o intuito de estimular o leitor a saber mais dos sistemas informatizados e refletir sobre a oportunidade de produzir a prova pericial, o estudo foi sistematizado a partir de três pontos principais: o funcionamento dos sistemas informatizados; os aspectos legais da perícia forense e sua importância como instrumento de educação e pacificação de conflitos; a importância do preparo dos profissionais na condução daquela prova, a fim de evitar equívocos que podem por em risco o direito de outrem. Para isso desenvolve a temática em sete capítulos, conforme segue.

O capítulo I consiste na introdução, oportunidade para apresentar o cenário atual e a prática de alguns ilícitos cometidos através de sistemas informatizados, cuja extensão dos danos podem ultrapassar os limites do individual, e a baixa sensibilidade dos profissionais do Direito a essas ocorrências, principalmente no Brasil face a informatização dos serviços judiciais e do processo. A partir disso foi possível orientar a pesquisa no sentido de oferecer alguma contribuição aos profissionais do Direito pouco familiarizados com o tema e estimular a discussão sobre os limites legais da prova pericial naqueles sistemas.

As pesquisas empreendidas neste trabalho permitiram avaliar o alto nível de complexidade que envolve a conexão de sistemas informatizados, bem como os ataques perpetrados contra estes. Por essa razão, no Capítulo II optou-se por apresentar as principais organizações comprometidas no combate e investigação dos crimes praticados mediante o uso das tecnologias de comunicação e telecomunicação, cuja execução e efeitos por vezes ultrapassam as fronteiras territoriais. Na sequência é feita revisão do termo “forense computacional” em face da inovação das tecnologias e do significado da prova pericial no Brasil.

No capítulo III é descrito o funcionamento dos sistemas informatizados e a estrutura de conexão para a internet de maneira simples, a fim de familiarizar o leitor com os principais conceitos, além de chamar sua atenção para alguns exemplos de ferramentas disponíveis na internet que proporcionam o anonimato do transgressor e facilitam a prática de ilícitos.

No capítulo IV faz-se uma abordagem jurídica da perícia forense aplicada aos sistemas

informatizados como instrumento de civilidade, na medida que ela contribui para a pacificação das partes e para educar a sociedade. Para corroborar essa idéia, foram utilizadas as obras de Dinamarco (2000) e de Santos (1997), seguindo-se reflexão sobre o momento oportuno de produzir a prova pericial.

Em seguida, no capítulo V, são apresentadas as técnicas para a realização da perícia forense em sistemas informatizados e a importância de se amparar nas melhores práticas face sua atualidade; o contraponto entre a busca de vestígios e a privacidade, a fim de atentar ao leitor os cuidados necessários para não comprometer a prova. E termina por demonstrar a contribuição do perito e assistentes na realização dos escopos sociais do processo (Dinamarco, 2000).

No capítulo VI é apresentado estudo de caso como forma de demonstrar os pontos críticos ao longo da instrução do processo civil e que podem comprometer o objetivo principal, que é demonstrar a existência de um fato e sua autoria.

Por derradeiro, o capítulo VII traz a conclusão das pesquisas e a sugestões que possam ser úteis aos pesquisadores e ao dia-a-dia dos profissionais.

ABREVIATURAS

Advanced Research Projects Agency	ARPA
Artigo	Art.
Agravo de Instrumento	Agr. Instr.
Associação Brasileira de Normas Técnicas	ABNT
Associação Nacional dos Peritos Criminais Federais	APCF
Associação Brasileira de Especialistas em Alta Tecnologia	ABEAT
Código Civil	CC
Código de Processo Civil	CPC
Código Penal	CP
Código de Processo Penal	CPP
Constituição Federal	CF
Comitê Gestor da Internet no Brasil	CGI
Companhia de Processamento de Dados do Estado de São Paulo	PRODESP
Computer Analysis and Response Team	CART
Diário Oficial Eletrônico	DOe
Domain Name System	DNS
Escola Politécnica da Universidade de São Paulo	EPUSP
Federal Bureau of Investigation	FBI
High Technology Crime Investigation Association	HTCIA
Hiper Text Markup Language	HTML
Information Technology Crime Investigation Manual	ITCM
International Association of Computer Investigable Specialists	IACIS
International Organization on Computer Evidence	IOCE
Internet Protocol	IP
Juizado Especial Cível	JEC
National Institute of Justice, United States Department of Justice	NIJ
Organização das Nações Unidas	ONU
Polícia Internacional	INTERPOL
Recurso Especial	REsp
Serviço de Perícias Informáticas	SEPINF
Scientific Working Group on Digital Evidence	SWGDE
Sistema de Pagamentos Brasileiro	SPB
Superior Tribunal de Justiça	STJ

Transfer Control Protocol	TCP
United States Computer Emergency Readness Team	CART

SUMÁRIO

PERÍCIA FORENSE EM SISTEMAS INFORMATIZADOS: UMA ABORDAGEM JURÍDICA

INTRODUÇÃO

O Século XX é marcado por acontecimentos sócio-econômicos e políticos de tal magnitude e impacto nas sociedades, que o caracterizaram como um dos períodos mais extraordinários da História da Humanidade. Entre eles, destacam-se a prosperidade das nações em suas diversas classes sociais combinada com o desenvolvimento tecnológico e sua dinâmica própria [1].

Isso é visível na década de 1990, quando se intensificou o uso dos computadores pessoais e também no âmbito das organizações. A conexão deles com a internet impulsionou a alteração dos padrões dos relacionamentos, na medida em que diminuiu o espaço e o tempo entre as pessoas sem que fosse necessária a presença física, conforme Lucca (2001, p.21 a 98).

De um lado as tecnologias de telecomunicação e comunicação proporcionaram aos cidadãos facilidades como comprar e vender; realizar aplicações financeiras, eleger seus representantes, indistintamente dispor de seus sentimentos, gostos e desgostos sem sair da sua cadeira e com apenas alguns *clicks* de *mouse,* a digitação de senhas e de dados.

De outro lado, nos últimos anos os cidadãos convivem com notícias diárias de ilícitos perpetrados com o uso daquelas tecnologias, que tipificados como crime ou não no Código Penal, violam os direitos das pessoas, quiçá da coletividade. Recentemente, o serviço de banda larga Virtua, oferecido pela empresa NET no Estado de São Paulo, foi atacado por um *cracker*. Ele acessou um servidor de DNS – *Domain Name System* da empresa com o intuito de redirecionar o serviço de *internet banking* do Banco Bradesco para uma página falsa que, inclusive, solicitava informações confidenciais. Os usuários constataram a fraude e não demoraram a alardear o feito na internet, segundo INFO Online (2009).

Ocorrências como esta preocupam os Estados, bem como vários segmentos da

[1] Eric Hobsbawn, historiador nascido em 1917 no Egito, brilhantemente traz a todos os inúmeros acontecimentos do século passado em suas obras, dentre as quais a esta pesquisa, se destacam "A Era dos extremos – a breve história do Século XX" e "Globalização, democracia e terrorismo". Esta bibliografia é importante para compreender como a gradativa informatização dos sistemas e das informações, combinada com as suas disponibilizações em larga escala, levaram aos mecanismos de governança corporativa, e no Brasil, a informatização do processo judicial e à virtualização dos serviços jurídicos como propostas de racionalização dos trabalhos pelo Poder Judiciário. Esses movimentos nos levam a refletir sobre o banco de dados como instrumento de poder, idéia essa lançada pelo Dr. Marco Aurélio Grecco em aula ministrada na ESA-OABSP no ano de 2008.

sociedade no Brasil e no mundo. Inclusive há anos que as várias nações vêm criando mecanismos legais de cooperação internacional para coibir e solucionar ilícitos perpetrados com o uso dos sistemas informatizados, como a Convenção da ONU contra o Crime Organizado Transnacional de 2000 e a Convenção de Budapeste sobre Cibercrimes de 2001.

O grau de conhecimento e desempenho dos transgressores para perpetrar ataques aos sistemas é elevado. Para coibir ilícitos como este, bem como apurar os fatos e sua autoria, peritos e técnicos ao redor do mundo mantém-se em contínuo desenvolvimento, através de estudos, pesquisas, treinamentos e intercâmbio de informações e experiências.

Dos profissionais do Direito, dedicados à defesa deste e à realização da Justiça, se espera conhecimento razoável do funcionamento dos sistemas informatizados e das práticas ilícitas cometidas através deles, pois que as habilidades comuns aos usuários são insuficientes a tal mister. Principalmente porque a desmaterialização dos serviços judiciários e do processo judicial, através da informatização, já é uma realidade no Brasil e riscos de ataque são previsíveis.

Tal conhecimento vai permitir a estes profissionais do Direito utilizarem a perícia no processo judicial com mais propriedade, pois sentir-se-ão aptos a manterem o diálogo com perito e assistentes. Isso porque nem sempre modalidades de prova como depoimento pessoal, oitiva de testemunhas e documentos são suficientes para constatar a existência e autoria dos fatos ocorridos através dos sistemas informatizados. Caso contrário, os usuários com alto nível de conhecimento sobre os sistemas e mesmo as organizações não adotariam rigorosos sistemas de segurança e de alto nível de complexidade, demandando do transgressor habilidades técnicas e cuidados para não deixar vestígios.

Na razão direta, os profissionais do Direto contribuem com a sociedade, na medida que o diálogo entre as partes e julgadores, considerado valoroso instrumento para educar sobre o funcionamento e uso racional dos sistemas informatizados, pode repercutir favoravelmente na sociedade.

A literatura sobre Direito e internet publicada no Brasil a partir de 2000, indica que o aumento da prática de ilícitos guarda alguma relação com a massificação do uso das tecnologias de comunicação e telecomunicação. Os temas versam sobre institutos jurídicos consolidados, tais como a relação de consumo, propriedade imaterial, contratos, dentre outros, agora adequados ao uso daquelas tecnologias, como o comércio eletrônico, contratos e documentos eletrônicos, marcas e nome de domínio, leilão eletrônico, além da violação dos direitos individuais e coletivos, como a invasão de privacidade e crimes.

Contudo, essa mesma literatura passa a largo da reflexão sobre o nível de complexidade que é provar a existência e a autoria dos fatos que resultaram em violação dos direitos, quando se trata de ilícito perpetrado com o uso das tecnologias de comunicação e telecomunicação, por

exemplo, como identificar e provar a autoria e existência de fraude contra o sistema bancário, a invasão de privacidade e uso de informações confidenciais, a difamação sob o manto do anonimato ou da falsa identidade. O referencial bibliográfico disponível no vernáculo pátrio relacionado à perícia em sistemas informatizados é voltado às pessoas da área técnica e que não têm familiaridade com os conceitos.

Essa percepção decorre também de duas verificações: 1) através da pesquisa nos portais do Tribunal de Justiça do Estado de São Paulo e do Superior Tribunal de Justiça, constatou-se resultados inexpressivos de julgamentos que indicam a realização de prova pericial no curso do processo; 2) no Brasil, a produção científica e os debates sobre a perícia em sistemas informatizados e o *modus operandi* dos transgressores circunscrevem-se aos peritos e técnicos, oriundos de departamentos da Polícia Federal, dos Institutos de Criminalística e alguns departamentos das faculdades de engenharia.

O nível de complexidade apontado anteriormente aumenta quando o ilícito perpetrado através dos sistemas informatizados se dá em dois ou mais territórios diferentes, momento que exsurge o conflito de leis como elemento complicador para a elucidação do caso.

Infelizmente, nesta primeira década do Século XXI, notadamente marcado pela globalização dos mercados e internacionalização das comunicações e finanças, os debates sobre a perícia e prova judicial não extrapolou os recintos dedicados à investigação e alcançou os profissionais do Direito que, a despeito da atualidade do tema objeto do estudo, foram pouco sensibilizados para atuar em processos judiciais que demandam a prova pericial.

Este cenário apresenta duas situações: a dificuldade do profissional do Direito em se preparar para enfrentá-los; e a demanda por literatura e cursos específicos sobre o tema.

Isso enseja o diálogo entre os profissionais do Direito e aqueles técnicos, porque a abordagem da perícia em sistemas informatizados pressupõe a interdiciplinaridade. Qualquer investigação ou perícia se realiza porque ao fato danoso se aplica uma hipótese definida em lei. Portanto, os limites para levá-las a efeito, é a legislação em vigor em cada país.

A convergência destas informações foi decisiva para determinar a pesquisa e redigi-la de modo que pudesse contribuir com outros interessados no tema.

O objetivo das pesquisas foi realizar uma abordagem jurídica da perícia forense aplicada aos sistemas informatizados, através da análise dos contornos legais e oportunidade para sua realização à luz da legislação em vigor, doutrina e jurisprudência.

Para melhor compreensão dos profissionais do Direito sobre a prova pericial propriamente dita, será apresentada descrição genérica do funcionamento daqueles sistemas, de alguns mecanismos facilitadores de condutas ilícitas e de práticas até aqui empreendidas.

A expectativa a partir deste estudo é de sensibilizá-los às questões que envolvem o

Direito e as tecnologias, disseminar os conceitos da perícia forense nos sistemas informatizados e a oportunidade para sua realização, além de estimular a educação com vistas a coibir a prática de ilícitos e a imposição de medidas punitivas eficazes. Por derradeiro, que ele seja útil como material de apoio aos interessados que iniciam os estudos sobre o tema.

CAPÍTULO I – PERÍCIA FORENSE COMPUTACIONAL

1.1. PANORAMA ATUAL

O nível de complexidade que envolve o funcionamento dos sistemas informatizados no modelo que se conhece nos dias de hoje, varia em razão do desejo e necessidade do proprietário e do usuário.

O nível de complexidade pode ser baixo, se forem considerados: a) alguns computadores conectados em rede, em um mesmo local físico e sem conexão com a internet; b) estrutura de redes de computadores, conectados ou não com a internet; c) estrutura de redes com acesso remoto, além de outros, até evoluir para o sistema bem complexo, como o SPB - Sistema de Pagamentos Brasileiro, implantado no país a partir do ano 2001. Todas essas estruturas, em tese, são vulneráveis a ataques.

Especialistas e interessados no tema ao redor do mundo há muito dispendem horas em discussões, pesquisas e treinamentos para conciliar o funcionamento dos sistemas informatizados, suas vulnerabilidades e o combate aos ilícitos através deles praticados.

As origens da internet, como se verá no próximo capítulo, data da década de 60, mas não tardou o aparecimento de entidades especializadas comprometidas com a pesquisa e desenvolvimento de recursos humanos e materiais para combater o ataque aos sistemas informatizados.

A atuação das referidas entidades também contribui com os esforços de cooperação internacional para combate ao crime e acredita-se que em alguma medida, podem contribuir com o desenvolvimento de pessoas e tecnologias de muitos países, que pelas circunstâncias sócio-econômicas, não possuem recursos suficientes para enfrentar aqueles ilícitos.

1.2. INSTITUIÇÕES COMPROMETIDAS COM O DESENVOLVIMENTO DA PERÍCIA FORENSE COMPUTACIONAL

Em meados do início da década de 1980 o FBI - *Federal Bureau of Investigation* iniciou movimento para investigar crimes cometidos com o uso de sistemas informatizados. Reuniu especialistas e pesquisadores e criou laboratórios, como o Computer Analysis and Response Team – CART. Com isso esperava responder à demanda da sociedade americana diante do aumento dos crimes cometidos com o uso das tecnologias de comunicação e telecomunicação. Também é destacada a atuação do CERT - United States Computer Emergency Readness Team.

A Polícia Internacional – INTERPOL foi criada em 1923 para combater os crimes

transfronteiriços e atualmente congrega 127 Estados Membros. Como os Estados Unidos, a Europa também já experimentava os dissabores e prejuízos da manipulação desautorizada e indevida dos dados em meio eletrônico, o que levou esta polícia internacional a reunir especialistas experientes e criar, em 1990, o EWPITC - European Working Party Information on Technology Crime.

Atualmente este grupo de trabalho desenvolve pesquisa sobre a investigação de crimes cometidos com o uso de sistemas informatizados e a compartilha com os membros da INTERPOL, além de produzir materiais de apoio, como o *Information Technology Crime Investigation Manual* – ITCIM, um guia de melhores práticas; além de realizar cursos.

As ações destas agências de investigação não são isoladas. Geus (2001) mapeou algumas instituições que unem esforços para solucionar aqueles crimes, bem como a padronização dos métodos e procedimentos, são desenvolvidos e compartilhados com outras entidades civis, sendo que dentre elas se destacam:

- IOCE - Internacional Organization on Computer Evidence, criada em 1995 e mantida com o objetivo de ser um fórum internacional sobre padronização da perícia forense em sistemas informatizados, estimular a troca de informações entre as agências participantes e sua disseminação, além de elaborar recomendações para seus membros;
- SWGDE - Scientific Working Group on Digital Evidence, criada em 1998 com objetivo de servir de canal de cooperação entre agências de perícia e participar dos esforços de padronização;
- HTCIA - High Technology Crime Investigation Association, instituição criada com objetivos semelhantes à SWGDE, também propõe a discussão de temas relacionados aos denominados crimes eletrônicos;
- IACIS - International Association of Computer Investigable Specialists, é associação com sede nos Estados Unidos e aberta a adesão de pessoas ao redor do mundo, composta por voluntários que se reúnem periodicamente para discutir e compartilhar informações, bem como publica o *The Journal of Computer Information Systems*, periódico de grande valia para os profissionais da área.

Além dessas entidades internacionais, outras desenvolvem trabalhos semelhantes aqui no Brasil:

- ABNT - Associação Brasileira de Normas Técnicas, criada em 1940 com o objetivo de elaborar, coordenar e difundir as normas técnicas no Brasil. Existem informações de que há grupo de trabalho no âmbito do Grupo de Segurança para discutir as melhores práticas de perícia forense aplicado aos sistemas informatizados, inclusive para colaborar com os esforços internacionais de padronização;
- APCF - Associação Nacional dos Peritos Criminais Federais, entidade civil representativa de

classe que também participa dos fóruns de discussão sobre perícia forense criminal;

- SEPINF - Serviço de Perícias Informáticas, área técnica da Polícia Federal composta por peritos com formação nas áreas de Ciência da Computação, Informática, Engenharia da Computação e semelhantes. Seus laboratórios estão localizados em várias cidades do país e cooperam com as secretarias de segurança pública estaduais. Além disso, participa ativamente do ICCYBER, evento bienal realizado pela ABEAT - Associação Brasileira de Especialistas em Alta Tecnologia;
- EPUSP - Escola Politécnica da Universidade de São Paulo, desenvolve pesquisas sobre este tema e, a partir de 2003, oferece um conjunto de disciplinas relacionadas à Ciência Forense Aplicada a Sistemas de Informação.

As entidades estrangeiras consultadas disponibilizam razoável volume de artigos, notícias, informações, ferramentas gratuitamente aos interessados neste tema, preocupação ou atenção que não se verifica por parte das entidades nacionais por motivos que se desconhece. Se assim o fizesse, daria contribuição significativa para a sociedade brasileira.

Da análise da leitura da literatura sobre o tema forense computacional e das propostas das referidas entidades, verificou-se o interesse e esforço significativos para a padronização de métodos e procedimentos.

Uma das justificativas de tais esforços propostas pelos especialistas é a realização da investigação de crimes praticados com o uso das tecnologias e executados em dois Estados ou mais. Nesses casos, nem sempre as normas que limitam a atividade da autoridade policial no curso da investigação são convergentes, ou seja, os requisitos legais para realizá-las, sem comprometimento da validade das provas, diferem de um país para outro.

Há que se respeitar o princípio da autodeterminação dos povos, consagrado no Direito Internacional, de que cada Estado tem autonomia para definir seu ordenamento jurídico, e o que não deve alcançar outro território. Tal ordenamento é determinado em razão do processo histórico, cultura, educação, condições sócio-econômicas. Quando há divergência entre a legislação dos Estados ocorre o conflito de leis. No Brasil, a solução está assentada nas regras constitucionais e na Lei de Introdução ao Código Civil.

Um dos aspectos negativos da padronização apontado por alguns especialistas brasileiros, é que a evolução das tecnologias de comunicação e telecomunicação tem uma dinâmica própria, ou seja, sofrem alterações constantes. Ao impor rígida sistemática de método e procedimento, corre-se o risco de tolher o trabalho do perito, pois a revisão da referida padronização não acompanharia aquela evolução.

Em ambos os casos, métodos e procedimentos padrão ou melhores práticas para a realização da perícia forense nos sistemas informatizados no Brasil, poderiam ser adotadas como

uso e costume [2], desde que não venham a afrontar o ordenamento interno.

A relação das entidades, o espectro de atuação de cada uma e as preocupações dos especialistas com as leis que limitam os contornos da perícia, são informações que proporcionam ao leitor ponto de partida para suas pesquisas, demonstrando ser fonte de consulta, além de proporcionar a possibilidade de troca de experiências.

1.3. REVISÃO DA TERMINOLOGIA "FORENSE COMPUTACIONAL" EM CONTRAPONTO COM A INOVAÇÃO TECNOLÓGICA

O uso correto dos termos em qualquer ciência é muito importante, pois deles depende o entendimento do leitor sobre determinado assunto.

No Direito, o conceito de determinado instituto pode variar em relação a outro conceito de ciência diferente. Acrescente-se a isso, que as hipóteses são definidas pela lei, inclusive a existência, validade e eficácia de terminado ato jurídico

Tem-se conhecimento de que o termo *computer forensic* foi cunhado pelo FBI em meados de 1980 e amplamente disseminado seu conceito como "ciência que estuda a aquisição, preservação, recuperação e análise de dados armazenados em formato eletrônico em algum tipo de mídia computacional". Os peritos naquela ciência afirmam que o resultado daquela perícia pode ser apenas informações indiretas, como evidências sobre a autoria do ilícito, ou informações diretas e decisivas para a elucidação de um caso (NOBLETT *et al* , 2000).

No Brasil aquele termo foi aportuguesado para forense computacional e amplamente difundido. Contudo, é de se indagar se o termo *computer forensic,* ou forense computacional, é apropriado para expressar o universo de mídias que os especialistas atualmente analisam e outras que advirão certamente por força da inovação tecnológica.

Quando a expressão *computer forensic* foi cunhada há mais de duas décadas, talvez não se vislumbrassem as inúmeras possibilidades de armazenamento de dados e informações que as tecnologias de comunicação e telecomunicação ofereceriam à sociedade, inclusive a criação de equipamentos com funções semelhantes às do computador, como os telefones celulares e, em breve no Brasil, a convergência digital das televisões.

Atualmente o grupo de trabalho EWPITC da INTERPOL promovem pesquisas, desenvolvimento de ferramentas e treinamento de pessoal também em tecnologias de internet sem

---

[2] Os usos e costumes são uma das fontes do Direito e servem para solucionar uma lacuna do ordenamento jurídico de um país e para dirimir os conflitos de interesses. Dentre os mais conhecidos cita-se os INCOTERMS, utilizados na compra e venda internacional de mercadorias, e as as práticas de auditoria interna ditadas pelo The International Instituto Auditor – The IIA. Sendo assim, a padronização de práticas de perícia forense em sistemas informatizados por instituição internacional amplamente reconhecida, desde que utilizadas largamente, poderiam ser tomadas como um uso e costume internacional.

fio, 3G, mensagens multimídia e “dinheiro virtual”.

A crítica ao termo *computer forensic* é que ela se afigura imprópria por tomar a parte (computadores) pelo todo (sistemas informatizados) e induz a pensar que esse tipo de perícia exclui outros equipamentos com as funções próprias dos computadores. E há demanda de perícia em tais objetos uma vez que os agressores utilizam toda sorte de instrumentos para levar à cabo seu intento [3].

A mera revisão do termo pode estimular a reflexão sobre os esforços de padronização e a adoção de melhores práticas de perícia forense, pois as tecnologias de comunicação e telecomunicação têm uma dinâmica própria.

Além disso, auxilia o profissional do Direito a refletir sobre o seu diálogo com o perito e assistentes, além de enriquecer o contraditório no curso da instrução processual, em especial na realização da prova pericial

A EPUSP, que já discute sobre isso há muito, optou por desenvolver disciplinas e pesquisas orientadas pela Ciência Forense Aplicada a Sistemas de Informação e há notícias de que seus docentes são simpáticos a idéia de roteiro de melhores práticas.

Embora essa discussão seja eminentemente técnica, sugere-se que os profissionais do Direito fiquem atentos às movimentações daquelas entidades relacionadas no item II.a, por dois motivos: ainda que o método e o procedimento para a realização da perícia seja orientado por uma organização estrangeira, devem observar os limites legais na sua realização; perito e assistentes devem demonstrá-los no laudo pericial e justificar a sua opção.

Por fim, ressalta-se que a perícia em sistemas informatizados no Brasil é assunto novo, poucas foram realizadas e apreciadas pelo Poder Judiciário e o desconhecimento por parte dos profissionais do Direito limita-o a extrair pouco da prova pericial.

---

[3] Durante as pesquisas foi feita uma busca com o termo “fraude”e “software” e obteve-se uma notícia de fraude de PABX perpetrada contra a EMBRATEL: “os fraudadores utilizam programas que geram repetidas chamadas para todos os diferentes ramais de um PABX suscetíveis à invasão. Assim que descobrem um ramal desprotegido que possibilite completar chamadas longa distância (DDD ou DDI), o ataque é feito usando as facilidades: "siga-me" , "disa*" e "correio de voz". Disponível em http://www.embratel.com.br/Embratel02/cda/portal/0,2997,MG_P_9289,00.html. Acesso em 15 de janeiro de 2009.

CAPÍTULO II - O FUNCIONAMENTO DOS SISTEMAS INFORMATIZADOS

A literatura sobre a história da internet é taxativa quanto a suas origens: a de que ela guarda relação estreita com a geopolítica que se desenvolvia no mundo a partir da Guerra Fria, e com a estratégia de segurança nacional dos Estados Unidos.

Tudo começou com a tecnologia de comutação de pacotes, que *grosso modo* é a repartição da informação em pedaços de dados e enviados em pacotes, separadamente e por caminhos diferentes, e reunidos na máquina do destinatário para apresentar a mensagem original, foi criada pela ARPA - Advanced Research Projects Agency, a partir das pesquisas e desenvolvimento de tecnologias pela Rand Corporation no período de 1962-1967. Estas pesquisas foram compartilhadas com universidades americanas e surgiu a ARPANET, com o intuito de implementar a rede pacotes. A demanda desta rede aumentou significativamente e em 1974 adveio o aperfeiçoamento do protocolo de comunicação através da criação do Transmission Control Protocol/Internet Protocol – TCP/IP, por Vinton Cerf, e a criação da Ethernet por Bob Metcalfe naquele ano, e cujo princípio de funcionamento consiste na interconexão de computadores próximos, conforme Rangel (1996).

O processo histórico da Humanidade foi importante para diversificar o uso da internet para além dos fins militares e de acadêmicos ao longo das décadas de 80 e 90. Assim, os sistemas informatizados passaram a ter papel relevante nas organizações e na vida das pessoas. Em algumas circunstâncias um sistema daqueles pode caber na palma da mão do leitor, que poderá levá-las consigo, ou armazená-las em qualquer lugar fora do alcance de seus olhos e suas mãos. Podem ser compartilhadas em um sistema de redes através da interligação de computadores, ou com o uso da internet.

Que a natureza destes sistemas permite facilidades, conforto e comodidade não é novidade. Mas há usuários que ignoram ser prejudicial seu uso sem critérios de segurança. Segundo o Comitê Gestor da Internet no Brasil – CGI (2006), eles são seguros se atenderem os requisitos de confidencialidade (dados somente disponíveis às pessoas autorizadas), integridade (dados não corrompidos ou prejudicados) e disponibilidade (acesso dos recursos do sistema sempre que necessários).

Portanto o binômio “sistemas informatizados e segurança” são indissociáveis, pois eventual falha no funcionamento de um pode comprometer o outro.

A seguir apresenta-se a configuração básica dos sistemas informatizados conectados em rede de computadores e internet, seguida de algumas ferramentas de ataque e informações úteis para a reflexão sobre possíveis focos da perícia técnica.

2.1. OS SISTEMAS INFORMATIZADOS COMO PLATAFORMA DE CONEXÃO E ARMAZENAMENTO DE DADOS

A leitura das obras técnicas sobre sistemas informatizados, possibilitou extrair algumas considerações básicas, tais como ser considerados suportes físicos dotados de mecanismos magnéticos, utilizados com objetivo de realizar uma ou mais funções. A quantidade e conteúdo dos dados e informações neles armazenados, não raro, sugerem cuidados e segurança especiais, sob pena de terceiros aproveitarem de suas vulnerabilidades e maliciosamente atentar contra eles, conforme Barbosa (2006) e Farmer e Venema (2007).

Sistemas informatizados podem realizar funções isoladamente ou não, com ou sem a interferência do ser humano.

Exemplo de sistema informatizado simples pode ser o disco CD, mídia utilizada para armazenamento de dados e informações. Individualmente ela não realiza qualquer função. A identificação do proprietário ou do usuário, no entanto, pode demandar várias ações caso aqueles não as identifiquem, pois ela não possui qualquer elemento visual estampado em sua face, por vezes apenas a marca do fabricante ou do distribuidor. Copiar os dados desta mídia ou corrompê-los, alterar seu conteúdo, ou mesmo desaparecer com ela, pode ser tarefa simples, bastando apenas o transgressor tê-la em sua posse.

A estrutura de redes de computadores interligados entre si varia em razão dos fins pretendidos por seu proprietário e das necessidades para execução de tarefas pelos usuários. Para isso, os recursos materiais, como equipamentos e programas, devem atender a alguns requisitos como eficiência, capacidade de armazenamento, velocidade, dentre outros. É prudente que cada usuário tenha uma senha e o acesso restrito, conforme as suas atribuições funcionais ou aos arquivos pessoais.

Os sistemas informatizados conectados à internet são estruturas com diferentes graus de complexidade, pois ensejam a conexão de vários computadores e outros equipamentos. Ou seja, além do computador, periféricos e *modem*, o usuário pode se conectar à internet através de vários programas, como o Outlook e Eldora, aplicativos de correio eletrônico; ou ainda acessar os sítios, ou *sites*, com a utilização de alguns programas de navegação, ou *browser*. Os mais conhecidos são o Internet Explorer, Mozilla, Netscape e Opera.

Geralmente para a conexão de computadores com a internet, são utilizados protocolos de comunicação. O Transmission Control of Protocol – TCP, é "um dos protocolos de comunicação utilizado entre os computadores conectados na Internet" (ICMCUSP).

O Internet Protocol – IP, é um endereço expressado por um único número de 32 bits, que pode identificar o computador conectado com a internet. É importante ressaltar que um único

endereço IP é atribuído a cada computador, e cada pacote de dados por ele transmitido, contém a informação do IP do remetente (endereço IP de origem) e para aquele que será remetido (endereço IP de destino)" (ABUSAR – Associação dos Usuários de Internet Rápida).

Face às dificuldades para lembrar dos protocolos IP para navegação em sítios, por exemplo, a Universidade de Wisconsin criou os primeiros servidores capazes de converter os números do endereço IP para um nome, os DNS, ou nomes de domínio (ABUSAR). Por exemplo, o endereço IP de uma organização *X* pode ser 200. 999.999.999.

É importante ressaltar que o endereço IP é atribuído pela empresa provedora de acesso à internet e inscrito a cada computador. Na hipótese de troca deste equipamento, o outro que lhe tomar o lugar poderá ser inscrito com o mesmo endereço IP e ser conectado à internet.

O funcionamento dos sistemas informatizados conectados em rede, na internet, ou não, implicam no armazenamento de dados e informações que podem ser identificados em mídias diversas.

Eles são passíveis de apropriação de informações por qualquer um e, em alguns casos, de ataques a partir de qualquer computador ligado a rede. As ocorrências mais comuns são o acesso desautorizado, implantação de programas maliciosos, furto de informações e fraude.

Seja qual for a configuração da rede e a forma de conexão com outros computadores, os proprietários e usuários devem adotar medidas de segurança ostensivas. Organizações zelosas de seus dados e informações mantém políticas de segurança que incluem programas de computador, treinamento de pessoal, cartilhas, distribuição e guarda de senhas, manual de procedimentos, dentre outros.

Essas noções elementares sobre o funcionamento dos sistemas informatizados e o acesso à internet são importantes para saber onde buscar evidências e outras informações relevantes para a elucidação do caso.

2.2. EXEMPLOS DE APLICATIVOS QUE PODEM SER UTILIZADOS PARA FINALIDADES MALICIOSAS

Os sistemas informatizados e a internet foram disponibilizados para a sociedade com as melhores intenções de seus criadores e inovadores. Ela pode ser utilizada para fins benéficos ou maléficos, do que depende da intenção do usuário. Assim como o avião, criado para que as pessoas pudessem percorrer longas distâncias em curto período de tempo e no ar. A destinação para fins bélicos quem dá é seu proprietário ou piloto.

A internet é um "espaço" imaterial, ao qual não se aplica o conceito de fronteiras como se conhece, tampouco à ela se aplica norma de qualquer país.

Há práticas maliciosas que induzem o usuário, mas não são consideradas ilegais, dentre as quais citem-se a intrusão através do redirecionamento do usuário para um sítio falso; a exposição através de *pop ups windows*, aquelas "janelinhas" que aparecem subitamente e sugerem ao usuário a acessar outro sítio ou digitar informações pessoais; ou ainda a execução automática de programas que instalam *cookies* com o objetivo de obter informações pessoais dos usuários e criar um banco de dados, conforme o CGI . Todas são modalidades do *phishing* [4].

A fraudes cometidas com o uso dos sistemas informatizados muitas vezes não é um fim em si mesma, mas um meio para a prática de outros ilícitos. Um usuário mal intencionado pode ter acesso a sistema informatizado e atribuir a outrem ação prejudicial, por exemplo, o acesso e alteração, subtração ou ainda supressão de dados de arquivo confidencial de uma organização, sem que o sistema esteja conectado com a internet.

Os ilícitos perpetrados através da internet geralmente são levados à efeito a partir da denominada engenharia social, entendida como aquela em "que alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para acesso não autorizado a computadores e informações" (CGI).

Manter o anonimato na internet não é algo difícil, a despeito de ser considerado ilegal (Art. 5o., inciso IV da Constituição Federal).

Poderá navegar através de endereço de IP dinâmico, porque cada a conexão à internet é atribuído um endereço IP diferente para o computador do usuário remetente das informações. O endereço de IP fixo é sempre o mesmo para o usuário.

Outra ferramenta que permite o acesso a um sítio através de um servidor intermediário, é o *proxy*, pois permite vários usuários compartilhar o acesso à internet, sem que sejam identificados. Embora otimize o uso da rede, não é confiável, ao que os técnicos recomendam o uso de outras ferramentas que possam garantir níveis de proteção.

Pesquisa rápida no buscador Google no dia 15 de janeiro de 2009, demonstrou que há inúmeros serviços de intermediação como este, disponíveis gratuitamente. Há empresas como a Sam Air, (http://www.samair.ru/) e a DNSOFTS (http://www.dnsofts.com/), que oferecem uma lista de IPs para navegar.

Há outros recursos de navegação privada, como o *private browsing,* um recurso adicional oferecido mas que não prejudica o histórico de navegação [5].

---

[4] Outra prática conhecida é o *phishing scam,* que consiste no envio de uma mensagem aos usuário, indistintamente, que geralmente indicam que o remetente é uma pessoa ou entidade reconhecida, como Delegacia da Receita Federal, bancos, dentre outros, com o objetivo de obter informações pessoais e/ou confidenciais e incorporá-las a uma base de dados. Uso desautorizado de marcas e identificações caracterizam no Brasil caracteriza crime de falsidade ideológica (Cartilha de Segurança do CGI).

[5] Ver. "Não deixe que descubram o que você faz quando usa a web", por Andrew Brandt (PC World/EUA). Disponível em http://pcworld.uol.com.br/dicas/2009/03/12/nao-deixe-que-descubram-o-que-voce-faz-quando-usa-a-web/ acessado em 26/03/2009.

Outro recurso que possibilita ações com efeitos diversos são os *cookies*, considerados por Silva Neto (2001, p.74): "indigestos biscoitos que os da webmaster tentam nos impingir".

De um lado, são úteis para facilitar a navegação mais rápida na internet, permitindo ao usuário armazenar dados e informações em seu *browser*, tais como lista de compras em sítios de comércio eletrônico, lista de sítios mais acessados, dentre outros (CGI). Por outro lado marcam os usuários muitas vezes sem que eles se dêem conta, além de facilitar a pratica do *phishing* [6].

O descarte descuidado de equipamentos e mídias também é uma boa fonte de informações para os transgressores, que podem utilizá-las para praticar a extorsão, fraude, falsidade ideológica, dentre outros.

A exemplo da lição de Sartre, "de que nada é negativo em si mesmo", os sistemas informatizados e a internet são instrumentos que podem ser usados para facilitar a vida das pessoas, ou prejudicá-las, cujo uso depende da intenção do usuário.

Depreende-se, pois, que os rumos da perícia forense devem levar em consideração todos os recursos disponíveis ao transgressor, pois ele se vale tanto das vulnerabilidades dos sistemas, como da inocência e despreparo das pessoas.

---

[6] O assunto é candente e sugere-se a leitura do artigo de Christian Hess Araya, *Derecho de la privacidad y cookies*, disponível na Revista Electrónica de Derecho Informático 2000.07 nº 24 http://www.vlex.com

CAPÍTULO III - O PROCESSO COMO VALOROSO INSTRUMENTO DE CIVILIDADE

A desmaterialização é uma das características marcantes do uso dos sistemas informatizados. Os conteúdos em suporte físico aos poucos são transferidos para o eletrônico.

Você pode ir a uma livraria e comprar um livro ou fazê-lo do aconchego do lar e através da internet. E em alguns dias vai receber o exemplar na porta de casa ou, quase que instantaneamente, no seu computador.

O agressor pode encontrar a sua vítima caminhando na rua, ou abordá-la através do acesso desautorizado aos seus dados e uso malicioso do que obteve. O criminoso pode invadir uma organização fisicamente, ou remotamente de qualquer lugar do Planeta. Bastam conhecimentos técnicos e cuidados para manter o anonimato.

Muitas das situações inusitadas e semelhantes a estas que se vivenciam nos dias de hoje, são levadas ao Poder Judiciário pelo cidadão na expectativa de uma solução que satisfaça os prejuízos e lhe desfaça os sentimentos de impotência e insegurança que lhe acometeram pela forma sorrateira e anônima do transgressor agir, o que assombra muitas pessoas.

Em face disso, é cada vez mais urgente "a aproximação da Justiça à população, feita sem intuitos demagógicos e corporativistas denunciados quanto a uma (sic) conhecida tentativa européia recente, é um dos pontos cardeais de uma "nova política judiciária" compatível com as exigências do tempo e com a visão pluralista dos objetivos do processo" (DINAMARCO, 2000, p. 227).

Este capítulo é dedicado a refletir como a prova pericial nos sistemas informatizados se insere na idéia do processo como instrumento de civilidade proposto por Cândido Rangel Dinamarco, sobre o contraponto entre os ônus da prova e o contraditório e a oportunidade de realizá-la.

3.1. A PERÍCIA TÉCNICA APLICADA AOS SISTEMAS INFORMATIZADOS PODE SER ÚTIL À PROPOSTA DE DINAMARCO, DO PROCESSO COMO INSTRUMENTO DE PACIFICAÇÃO SOCIAL E EDUCAÇÃO

Em meados de 2008, o Ministério Público Federal – MPF, obteve decisão favorável contra a Telefônica que obrigaria as empresas provedoras de acesso à internet rápida a repensar seu modelo de negócio. Tratava-se de venda casada, prática vedada pelo Código de Defesa do Consumidor e massivamente utilizada no país até então, constatada após a instrução processual que contemplou a prova pericial.

A despeito da decisão ser em primeira instância e passível de revisão pelo Tribunal

Regional Federal da 3a. Região, o juízo da 3a. Vara da Justiça Federal de Bauru atribuiu à sentença os efeitos *erga omnes.* A partir daquele julgamento, o usuário poderia escolher a empresa provedora de acesso à internet independente da empresa prestadora do serviço de conexão. Antes disso, as empresas de conexão indicavam as empresas provedoras, para com ela, o usuário acessar a internet. E quem buscou informações sobre possíveis ligações comerciais entre ambas, no Estado de São Paulo, verificou que elas praticavam a venda casada.

Este fato chamou a atenção para a pesquisa de julgamentos de processos com objeto da lide relacionada aos sistemas informatizados e internet. Realizou-se, então, pesquisa simples no sítio do STJ com as palavras "internet" e "privacidade" e verificou-se sete ocorrências no âmbito do direito penal, e apenas um deles determinava a realização da perícia técnica para determinar a certeza, conforme ementa a seguir transcrita:

> 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. 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. V.U. (RHC 18116/SP, Relator Ministro Hélio Quaglia Barbosa, 6a. Turma, Data do Julgamento 16/02/2006, Data da Publicação/Fonte DJ 06/03/2006, p. 443, RSTJ vol. 201, p. 636).

Foram feitas outras pesquisas aleatórias nos portais do STJ e Tribunais dos Estados de São Paulo e Rio de Janeiro, relacionadas àqueles termos, cujo resultado foi insatisfatório.

Uma hipótese é o processamento, em segredo de justiça, das ações que envolvem a perícia técnica nos sistemas informatizados, a fim de preservar as partes envolvidas e as informações confidenciais. Outra, se há processos com a realização de perícias que ainda não foram remetidos às instâncias superiores, ou ainda referidas ações terminadas por acordo.

Pode-se formular outras hipóteses: 1) se os cidadãos saberiam reconhecer quando os seus direitos são violados com o uso das tecnologias de comunicação e telecomunicação; 2) se na

ocorrência têm levado ao conhecimento do Poder Judiciário; 3) ainda se o cidadão é incrédulo sobre uma decisão favorável a ele; 4) ou apenas ignora a violação.

Em todos esses casos, o processo pode ser importante instrumento para prevenir práticas sorrateiras e acobertadas pelo anonimato.

A usual compreensão do processo como um meio de composição da lide, proposta por inúmeros processualistas modernos, inclusive Santos (1997, p. 9), já não satisfaz as necessidades da sociedade contemporânea, que clama por segurança nas relações e efetividade da justiça, principalmente naquelas questões que envolvem alguns de seus segmentos ou até ela como um todo.

Eminentes processualistas, atentos aos movimentos sócio-econômicos, refletem sobre a amplitude dos efeitos do processo judicial na sociedade.

Dinamarco (2000, p.149) fez revisão da doutrina processual e alargou o entendimento do significado do processo judicial: "todo instrumento como tal, é meio; e todo meio só é tal e se legitima, em função dos fins a que se destina. O raciocínio teleológico há de incluir, então, necessariamente, a fixação dos escopos do processo, ou seja, dos propósitos norteadores da sua instituição e das condutas dos agentes estatais que o utilizam".

Ele propôs a superação daquela idéia simplista, do processo como meio de composição da lide, para ser um instrumento de pacificação social (idem, p.12). O resultado pode ser o processo como um valoroso instrumento de civilidade.

Para alcançá-lo, seria necessário realizar os escopos:

- Social: pacificar com justiça e educação (ibdem, pp. 159-162, 317);
- Político: preservação da liberdade, participação e afirmação da autoridade do Estado e do seu ordenamento (Ibdem, pp. 162-164, 317);
- Jurídico: atuação da vontade concreta do direito (Ibdem, pp. 219-223, 317).

À exemplo do processo do MPF contra a Telefónica, cuja decisão foi formulada após intenso contraditório e diálogo com os técnicos, os ilícitos praticados com o uso dos sistemas informatizados devem ser julgados com o conhecimento sobre o seu funcionamento e fragilidades, a partir de provas robustas e com rigor.

Essas considerações permitiram relacionar estreitamente a perícia nos sistemas informatizados com o escopo social do processo, pois ao mesmo tempo que se instrumentaliza o processo, educa-se e pacifica.

3.2. OS ÔNUS DA PROVA E A DIALÉTICA DO CONTRADITÓRIO NO DIREITO CIVIL

Os ônus do processo são para todas as partes nele envolvidas. De um lado, o autor afirmar fatos e a violação dos seus direitos; e de outro, o réu defender-se. Também lhes incumbe o de provar: o autor a existência do fato; o réu, a inexistência daquele fato ou de que não se relaciona com ele, conforme Dinamarco (2000, pp. 247-254) e Santos (1997, pp 347-349).

Para Chiovenda, *apud* Santos (1997, p. 347) o ônus de provar se divide entre as partes e à cada uma, impondo-se a cada qual a iniciativa de demonstrar o que deseja sejam tidos por verdadeiros ao juiz. Não pode ser considerada tarefa fácil de cumprir, principalmente os processos que versam sobre ilícitos perpetrados com o uso dos sistemas informatizados, que demandam algum grau de conhecimento técnico para indicar evidências de violação de direitos.

Afinal, "a *verdade* que juiz busca no processo não se limita ao acerto do seu juízo histórico acerca dos fatos de interesse para a causa. *Ex facto oritur ius* e a representação de fatos passados ou presentes é a angustiante missão a ser cumprida mediante a experiência probatória", no entendimento de Dinamarco (2000, pp. 233).

O contraditório, cuja realização é compulsória por determinação constitucional [7], veio ao encontro das necessidades das partes envolvidas no processo, não somente para se por às alegações uma da outra, mas para manifestar-se sobre atos de terceiros em todo o curso do processo.

No presente estudo, acrescenta-se àquela dificuldade, a de se obter prova no exterior face às divergências das legislações do país onde se processa a ação e as daquele onde se pretende obter prova, conforme visto no item II.a. Também, a de se obter informações de empresas provedoras de conteúdos, ou ainda estabelecer a relação entre o computador utilizado para realizar o ilícito e o IP de acesso registrado no dia e no horário da ocorrência do ilícito.

Essas mesmas dificuldades podem ensejar a oportunidade de rever os conhecimentos sobre as tecnologias empregadas, afigurando-se saudável a dialética travada pelo contraditório no curso processo e o diálogo saudável entre partes, juiz, perito e assistentes, para elucidar o caso [8]. Com isso se cumpre a ampla defesa e se provê o juiz das informações necessárias a seu convencimento.

E se perfaz a educação de todos os envolvidos no processo sobre as tecnologias de comunicação e telecomunicação.

---

7 Art. 5o., XXXVII da Constituição Federal.

8 Arts. 420 a 439 do CPC; Arts. 158 a 184, CPP.

3.3. MOMENTOS PARA REALIZAR A PERÍCIA FORENSE NOS SISTEMAS INFORMATIZADOS

As tecnologias de comunicação e telecomunicação têm uma dinâmica especial e as informações armazenadas apresentam tempos de vida diferentes. Farmer e Venema apresentam tabela simples como guia aproximado com o ciclo de vida esperado dos dados, também denominada ordem de volatilidade, cujos números indicam quão variáveis são o tempo de existência dos dados, que variam de nanosegundos (ou menos) a anos [9]:

Tabela 1 – Ordem de volatilidade

Suporte	**Ciclo de vida**
registradores, memória periférica, caches, etc	nanossegundos
memória principal	dez nanossegundos
estado da arte	milissegundos
processos em execução	segundos
disco	minutos
disquetes, mídia de back up, etc	anos
CD-ROMs, impressões, etc	dezenas de anos

Fonte: FARMER & VENEMA, 2007, p. 6.

A interpretação dos números supra-indicados nos dá conta de que nem sempre é oportuno postergar a produção de prova nos sistemas informatizados porque os vestígios e indícios podem se perder.

Além da volatilidade dos dados, há circunstâncias em que o usuário, ou a pessoa mal intencionada, pode apagar os vestígios e indícios com a simples execução de um programa ou alteração do estado do equipamento (ligado-desligado), ou ainda com minas eletrônicas [10].

As circunstâncias que envolvem o "tempo de vida" são inúmeras e é preciso atentar o interessado a isso na produção da prova pericial.

O ordenamento jurídico nacional prevê a realização da perícia em dois momentos: antes do processo de conhecimento ou durante seu desenvolvimento.

---

[9] É um paradoxo a determinação da ordem de volatilidade dos dados nos diversos sistemas informatizados em contraponto às notícias de chantagem com dados obtidos de discos rígidos considerados lixos. Dentre as possibilidades de "fossilização" de tais dados é que são gravadas em meio magnético, cuja propriedade física permite a subscrição de dados em camadas, conforme estudos de FARMER & VENEMA, 2007.

[10] Conforme Farmer e Venema, Geus, dentre outros autores pesquisados.

No processo arbitral, a perícia pode constar do compromisso arbitral e, na sua falta, ser requerida pelas partes ou determinada pelo tribunal arbitral [11].

No caso do ilícito sugerir a ocorrência de crime, os fatos são apurados em sede de inquérito policial, cujas regras para sua realização são previstas nos artigos 4º a 23 do CPP. Na hipótese de ação penal pública [12], o inquérito será instaurado pela autoridade policial a partir da notícia do crime (de ofício), a requerimento da autoridade judicial, Ministério Público ou pelo ofendido (art. 5º, II, CPP). Na ação penal privada [13], a autoridade policial somente pode levar à efeito o inquérito se o ofendido levar-lhe o conhecimento a notícia do crime (art. 5o., par. 5o., CPP).

Em ambos os casos (ação penal privada ou pública), a realização de perícia forense no âmbito do inquérito policial pode deixar de ser realizada caso as autoridades, o Ministério Público ou ofendido tenham elementos suficientes para instaurá-la [14].

Nas ações cíveis, por outro lado, é a parte que escolhe o momento da realização da perícia.

Em todos esses casos, a realização da prova pericial, dentre outras permitidas pela legislação, está relacionada ao seu grau de utilidade e na razão direta da defesa dos direitos da pessoa.

O entendimento generalizado que se mantém entre os usuários dos sistemas informatizados é que os dados armazenados podem ter um tempo de vida efêmero. Isso induziria a deixar de reclamar a violação de seus direitos. Trata-se de idéia a ser revista por todos os usuários.

No processo cível, a prova pericial serve para constatar a existência de um fato e para determinar a autoria do ilícito. Os ilícitos perpetrados anonimamente ensejam a utilização da medida cautelar *ad perpetuam rei memorian* e a ata notarial, providências necessárias para obter informações a fim de se chegar ao transgressor.

Também pode ser utilizada caso haja risco de comprometimento do objeto da prova. Nos dois casos, o contraditório se estabelece apenas no âmbito da perícia técnica. Por exemplo, endereços de IPs, logs de acesso dentre outros.

---

[11] Art. 22. Poderá o árbitro ou o tribunal arbitral tomar o depoimento das partes, ouvir testemunhas e determinar a realização de perícias ou outras provas que julgar necessárias, mediante requerimento das partes ou de ofício", Lei no. 9.307 de 1996.

[12] "Art. 100 - A ação penal é pública, salvo quando a lei expressamente a declara privativa do ofendido. § 1º - A ação pública é promovida pelo Ministério Público, dependendo, quando a lei o exige, de representação do ofendido ou de requisição do Ministro da Justiça", CP.

[13] "Art. 100: § 2º - A ação de iniciativa privada é promovida mediante queixa do ofendido ou de quem tenha qualidade para representá-lo", CP.

[14] "Art. 6º Logo que tiver conhecimento da prática da infração penal, a autoridade policial deverá: (...)
VII - determinar, se for caso, que se proceda a exame de corpo de delito e a quaisquer outras perícias; (...) CPP.
"Art. 39, par. 5o. - O órgão do Ministério Público dispensará o inquérito, se com a representação forem oferecidos elementos que o habilitem a promover a ação penal, e, neste caso, oferecerá a denúncia no prazo de quinze dias", CPP.

No processo de conhecimento, a prova pericial se realiza durante a instrução processual para comprovar a existência de um fato. A realização das provas requeridas pelas partes é para esclarecer os pontos controvertidos do litígio [15], e cuja admissibilidade depende dos argumentos de autor e réu a justificá-las.

Casos complexos que envolvem sistemas informatizados, onde a testemunha ocular e o depoimento pessoal são pouco eficazes para elucidar os fatos, a perícia técnica pode ser decisiva e encurtar o longo caminho até a decisão final.

[15] "Art. 130. Caberá ao juiz, de ofício ou a requerimento da parte, determinar as provas necessárias à instrução do processo, indeferindo as diligências inúteis ou meramente protelatórias", CPC.

CAPÍTULO IV – PERÍCIA FORENSE APLICADA AOS SISTEMAS INFORMATIZADOS

O tempo de vida dos dados armazenados em meio eletrônico nos dá conta da fragilidade em manipulá-los sem comprometer sua estrutura. Além disso, elevá-lo a condição de prova robusta pressupõe uma série de atos sistematizados a lhe conferir credibilidade.

O ponto de partida da perícia forense aplicada aos sistemas informatizados é sua admissibilidade pelo juiz, do que segue às partes providenciar assistente técnico e quesitos relevantes.

Ao perito, após análise do processo e quesitos, definir a metodologia e procedimentos, enfim, todos os recursos e técnicas a serem empregadas no curso da perícia, além de proceder a elaboração da cadeia de custódia, conforme Geus *et al* (2001), Barbosa *et al* (2006) e Farmer e Venema (2007). Além de ser de grande valia para o exame das informações, elaboração do laudo e a resposta aos quesitos, é útil para validação da perícia.

A despeito de não haver padronização para a realização deste tipo de perícia, é comum os técnicos se orientarem pelo NIJ Guide, que sugere seqüência de ações, tais como:

a) relatar a descrição física do local onde ocorreu o ilícito, equipamentos e mídias lá dispostos, estado da máquina (ligado-desligado), inclusive com fotos de todo o ambiente, caso seja possível;

b) relacionar proprietários e usuários dos equipamentos, pessoas que têm acesso àquele ambiente, *logins*, disponibilização e guarda das senhas, sistemas de acesso com a internet e manual de uso, dentre outros;

c) relacionar os programas, funcionalidades do sistema, segurança, documentos de software e hardware, dentre outros.

A importância deste procedimento é gerar um histórico útil não só como fonte de informação aos técnicos quando da análise dos dados, elaboração do relatório e conclusão, mas também para contestar, eventualmente, a validade do procedimento e metodologia.

A análise das técnicas empreendidas para a realização da perícia forense computacional demonstra que os especialistas são unânimes em alguns pontos: criar e manter cadeia de custódia; manter a integridade da prova; copiar os arquivos objeto da perícia, respeitados os limites legais.

Como nas lições de Dinamarco (2000, p. 225), a "técnica está a serviço da eficiência do instrumento, assim como este está a serviço dos objetivos traçados pelo homem e todo o sistema deve estar a serviço dele".

Um dos aspectos da validade da perícia forense nos sistemas informatizados está

relacionada com a privacidade, ensejando dos Técnicos vários cuidados e em todas as suas fases e que serão vistas a seguir. Nessa oportunidade, evidencia-se não só as dificuldade das tarefas a serem desempenhadas, mas também o papel do papel dos peritos e assistentes na disseminação de alguns conhecimentos sobre as tecnologias de comunicação e telecomunicação, já imbricadas com o exercício da advocacia e o *modus operandi* dos tribunais.

4.1. A BUSCA DE VESTÍGIOS E O RESPEITO AO DIREITO FUNDAMENTAL À PRIVACIDADE

A privacidade é um dos temas discutidos pelos profissionais do Direito afeitos ao Direito da Informática. Não há consenso sobre o que é privado ou não na internet, se mensagens enviadas por meio eletrônico (por computadores e celulares) são de conteúdo aberto ou não.

No Brasil, o dever constitucional e infra-constitucional de sigilo e inviolabilidade da correspondência [16], são os parâmetros utilizados nas decisões [17].

Discorda desse posicionamento o CGI, que propõe serem "as mensagens que chegam à caixa postal do usuário normalmente armazenadas em um servidor de *e-mails* do provedor, até o usuário se conectar a internet e obter os *e-mails* do programa leitor". E que, "enquanto os *e-mails* estiverem no servidor, poderão ser lidas por pessoas que têm acesso à este servidor. Enquanto estiverem em trânsito, existe a possibilidade de serem lidos por alguma pessoa conectada à internet".

Esses debates servem para ilustrar as dificuldades que os técnicos poderão encontrar para realizar a perícia nos sistemas informatizados, pois nem sempre há informações no processo sobre eventuais lugares onde procurar por vestígios.

Farmer e Venema (2007, p. 04) encorajam seu leitor a "procurar qualquer coisa em qualquer lugar".

---

[16] Constituição Federal, Art. 5o., X – "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação"; Código Civil, Art. 186 - "Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito".

[17] AÇÃO DE OBRIGAÇÃO DE FAZER COM PRECEITO COMINATÓRIO - Mensagem eletrônica (e-mail), via internet com conteúdo difamatório anônimo - Prestador do serviço de correio eletrônico - Dever de prestar informação que permita a identificação do autor - Obrigação que não ofende o direito a privacidade e o sigilo das comunicações - Decisão reformada. Recurso provido (Agr. Instr. no. 4032894000, TJESP, Rel. Des. Antonio Maria, 3ª Câmara de Direito Privado, Registro em 20/12/2005, disponível em http://www.tj.sp.gov.br).
AGRAVO DE INSTRUMENTO. PEDIDO DE ANTECIPAÇÃO DE TUTELA ESPECÍFICA. Mensagens de correio eletrônico supostamente ofensivas a imagem de empresa, enviadas, anonimamente, a seus funcionários. Dados cadastrais do responsável do envio de tais mensagens que somente podem ser obtidos junto à recorrida por meio de ordem judicial. Legitimidade da agravante para postular a medida diante de seu direito de proprietária do chamado e-mail corporativo. Precedente do Colendo Superior do Trabalho e que se invoca para a solução da espécie. Presença dos requisitos do art. 461, § 3o. do CPC. Pedido improcedente. Agravo provido (Agr. Instr. no. 4882534900, TJESP, Rel. Des. A.C.Mathias Coltro, Registro em 12/03/2007, disponível em http://www.tj.sp.gov.br).

É prudente ter critérios para aplicar dessa idéia, pois quem procura algo deve saber o que está procurando, Caso contrário, o técnico incorrerá na invasão de privacidade e no desabono da prova, além de perder tempo no exame de informações que podem ou não ter relevância para a elucidação do caso.

No direito brasileiro, é vedado o uso da prova obtida por meios ilícitos nos processos judicial ou administrativo (Art. 5o., LVI, Constituição Federal). Para Nuvolone, *apud* Nery Junior (2009, p. 265), a prova vedada em sentido absoluto se dá na hipótese do sistema jurídico proibir em qualquer circunstância; e em sentido relativo, quando a legislação autoriza mediante o cumprimento de requisitos.

Por exemplo, o Código de Processo Penal define como prova ilícita aquela que é obtida em violação das normas constitucionais ou legais (Art. 157). Há regras de exceção, como a previsão constitucional de escuta telefônica mediante ordem judicial e para fins de investigação criminal ou para instruir processo penal (Art. 5o., XII). A locução "e" não deixa dúvidas que o expediente de escuta ou interceptação é restrito.

Ainda, vale mencionar haver juristas em cujo entendimento a prova realizada no processo penal, pode ser emprestada ao processo cível, em atenção a unidade da jurisdição e da teoria geral da prova. Mas para isso, é necessário que a parte contra quem foi produzida tenha participado efetivamente do processo penal de onde se emprestou, conforme Nery Junior (2009, pp. 264-269).

Também, se da prova ilícita derivar outra prova, esta última será considerada contaminada e, portanto, ilicitamente obtida.

Trata-se da *fruit of the poisonous tree doctrine*, em português a teoria dos frutos da árvore envenenada. Para Nery Junior, ela "consiste em que se deve considerar ineficazes no processo, e, portanto, não utilizáveis, não apenas as provas obtidas ilicitamente, mas também aquelas outras provas que, em si mesmas poderiam ser consideradas lícitas, se baseiam, derivam ou tiveram sua origem em informações ou dados conseguidos pela prova ilícita", (idem, p. 269).

Tratam-se de limites legais para a realização da perícia nos sistemas informatizados que devem ser observados, sob pena de comprometer a validade e eficácia da prova pericial.

4.2. OBTENÇÃO DE DADOS, FONTES DE INFORMAÇÕES, ANÁLISE FORENSE E APRESENTAÇÃO DO LAUDO

O entendimento comum entre os técnicos é que os ataques aos sistemas informatizados geralmente deixam vestígios das ações do transgressor, pois as informações e dados são arquivados

em meio magnético ou, no caso de armazenamento temporário de informações voláteis, em outros tipos de memória. Eles podem estar disponíveis em arquivos e equipamentos intactos ou não, o que depende da habilidade do transgressor em apagar os vestígios que deixou, e do perito em encontrá-los se aquele for descuidado.

Contudo, isso não significa sejam fáceis de localizar e mesmo visíveis aos olhos de pessoas comuns, pois carecem de conhecimentos técnicos de onde, como e quando eles podem ser encontrados.

A definição de Noblett para a *forense computacional* demonstra que ela é composta de, pelo menos, quatro fases, senão vejamos: aquisição, preservação, recuperação e análise de dados armazenados em formato eletrônico em algum tipo de mídia computacional.

Contudo, considera-se que a ela prescindem atos preparatórios, tais como a determinação dos procedimentos e métodos; a solicitação de ofícios às entidades que tenham informações relevantes para o sucesso da perícia, por exemplo, os provedores de acesso de conteúdo, de servidores corporativos; o agendamento de reunião e entrevistas; o eventual levantamento de informações de laboratórios equipados para acolher os materiais objetos da perícia. Tais atos incluem-se na preparação da cadeia de custódia, um dos elementos importantes na validação da perícia.

Segue-se, então, na busca e aquisição de dados conforme algumas ações, conforme relatório NIJ, como

- diligências ao local dos sistemas atacados para realizar levantamento de informações através de entrevistas com o proprietário, ou gestor, usuários; descrição do local físico e equipamentos; configuração da estrutura dos sistemas informatizados e conexões, estado da rede, dentre outros;
- identificação de todos os materiais recolhidos, estado de conservação e discriminação em documento próprio;
- relatório da cadeia de custódia.

É oportuno que as diligências ao local de busca de informações, equipamentos e dados, sejam realizadas pelo perito na companhia dos assistentes técnicos, do gestor dos sistemas informatizados objeto da perícia e testemunhas, a fim de conferir transparência ao longo dos procedimentos.

Manter a integridade das provas durante a realização da perícia é uma das grandes preocupações dos técnicos desde há muito. Por isso desenvolvem ferramentas de *softwares* com o intuito de auxiliá-los na realização daquela tarefa. Evitar o dano nos materiais colhidos depende da

utilização correta, destreza e qualificação dos profissionais naquela envolvidos.

A par dessas ferramentas, os experts são unânimes na idéia de fazer o "espelhamento", ou cópia, dos dados e informações contidas nos sistemas informatizados sempre que possível. Por exemplo, copiar os dados armazenados em todo o sistema informatizado de uma empresa multinacional pode se afigurar impossível diante do grande volume.

Não é raro o disco rígido, objeto da perícia, apresentar danos. Nessa hipótese, a recuperação precede a coleta de dados. Conforme Barbosa *et al* (2006) os danos que podem ocorrer no disco rígido e possibilidades de recuperação, como se pode ver a seguir:

- dano físico, tanto no *hardware* de suporte, como na mídia de armazenamento. No primeiro caso, os dados podem estar íntegros na superfície dos discos, contudo inacessíveis por problemas no disco rígido, o que demanda a substituição das partes comprometidas ou até a recuperação de pedaços de mídia. Contudo, os procedimentos podem emperrar por alguns problemas, tais como obter peças de reposição; laboratórios equipados e aptos para realizar a complexa tarefa; velocidade de obtenção de dados em detrimento do tempo para realização da perícia, ter habilidades e precisão;
- dano lógico, assim considerado aquele relacionado às estruturas descritoras de conteúdo, as quais indicam onde estão distribuídos os dados de um determinado arquivo. Os especialistas afirmam que arquivos removidos com os comandos *delete* ou *erase*, têm grandes chances de serem recuperados, parcial ou totalmente em alguns casos;
- dano por sobrescrita, considerado pela gravação de dados sobre outros. Para aqueles especialistas, é possível a recuperação de, pelo menos, duas camadas de dados sobrescritos.

A durabilidade dos dados arquivados em meio magnético depende da mídia onde estão gravados e políticas de armazenamento da organização. Farmer e Venema (2007, p. 171 e 175) afirmam que todos os dados são voláteis, opinião que é acompanhada por muitos especialistas. Por isso a preferência na coleta dos dados que podem sofrer alterações em curto espaço de tempo (item IV.c) e disponíveis em alguns locais, conforme a lista por aqueles sugerida:

- memória do dispositivo (há poucas ferramentas para isso);
- memória principal;
- obtenção do registro seqüencial, caso do sistema de arquivos com *jornaling*;
- obtenção do resultado transitório possível;
- captura das informações no e sobre o disco, através de cópia.

Estes locais possuem informações que podem se mostrar relevantes para a elucidação do

ilícito e para a constatação da existência do fato, tais como espaços de arquivos lógicos e subaproveitados; sistemas de arquivos; memória principal do sistema; arquivos de *log;* estado do sistema, com informações de sistema operacional, conexões de rede, dentre outros.

A coleta de dados em discos rígidos, em regra, é precedida de sua cópia, parcial ou total. A inconveniência de fazer cópia integral pode ser o espaço para armazenar todos os dados, do que se vê em Farmer e Venema (2007, p.171-175) e Barbosa *et al* (2006).

A análise da literatura permite concluir que a análise dos dados e informações coletados é tarefa complexa, porque implica no exame de todo material produzido (entrevistas e documentos), das mídias, dos sistema de arquivos e conexões, dos aplicativos, estrutura de rede e memórias dos sistemas. Trata-se do exame cuidadoso de cada um deles em particular e em conjunto, dependendo do caso, para constatar a existência do fato danoso e extensão dos prejuízos.

O laudo pericial é o resultado da coleta e análise dos dados e informações. Nele, o perito expõe todos os recursos, procedimentos e métodos empregados para levar a efeito seu encargo, suas conclusões. Em seguida, prossegue na resposta às perguntas formuladas pelo juízo e dos quesitos das partes.

Sendo a perícia forense um meio de transmitir ao juízo fatos interessantes à causa [18], cuja natureza dos elementos que constituem a prova exige conhecimentos especiais para poder extrair deles o máximo de informações.

Por isso é certo esperar que o laudo e respostas, apresentados em um único instrumento, sejam objetivos, concisos, com rigor científico, claros, em linguagem simples e de bom entendimento aos profissionais do Direito, com procedimentos e métodos fundamentados, resguardado o uso de terminologias técnico-científicas [19].

No processo cível os assistentes técnicos têm a oportunidade de apresentarem os seus laudos em prazo de 10 dias da intimação do laudo do perito, incluídas as respostas das perguntas e quesitos [20].

Ainda vale aqui mencionar que o juiz não está vinculado ao laudo pericial e, caso considere que o laudo do assistente técnico tenha cumprido os requisitos de clareza, concisão, objetividade, bom entendimento, coerente, e que melhor reflita a realidade dos fatos cuja existência se questiona, poderá considerá-lo, no todo ou em parte, conforme o entendimento do Superior Tribunal de Justiça [21].

---

[18] AMARAL SANTOS, p. 472.

[19] Os procedimentos da perícia forense devem observar as regras contidas nos arts. 420 a 439 do CPC e arts. 158 a 184 do CPP.

[20] Art. 433, parágrafo único do CPC.

[21] PROCESSO CIVIL. LIQUIDAÇÃO POR ARBITRAMENTO. LUCROS CESSANTES. PRESCRIÇÃO INTERCORRENTE NÃO CARACTERIZADA. RECURSO ESPECIAL. FUNDAMENTO INATACADO. CRITÉRIO DE APURAÇÃO DO QUANTUM. UTILIZAÇÃO DO LAUDO DO ASSISTENTE TÉCNICO.

A perícia demonstra ser um valioso instrumento, não só como prova, mas de desenvolvimento de tecnologias e pesquisa.

4.3. O PAPEL DO PERITO E ASSISTENTES

A qualidade do trabalho de peritos e assistentes técnicos, em processos relacionados a perícia em sistemas informatizados, permite aos profissionais do Direito o contato mais raso com a materialidade dos fatos em razão do anonimato que permeia os ataques aos sistemas informatizados.

Para isso, não basta somente a qualificação profissional [22], mas como exposto anteriormente, também o preparo e a *expertise* para analisar os dados e informações deixados nos sistemas e equipamentos, mas a compreensão sobre os contornos legais que a perícia deve obedecer e o sigilo profissional que permeia o procedimento em curso [23].

O diálogo entre os profissionais do Direito pode enriquecer o momento da perícia, porque se estabelece o contraditório agora com a participação de terceira pessoa – perito e assistentes. São lançadas luzes técnicas sobre as questões de fato e de direito, inclusive com a oportunidade de esclarecimentos dos pontos obscuros ou omissos da perícia em audiência.

Aos perito e assistentes, a possibilidade de interagir com aqueles profissionais e, na medida do possível, compreender a sistemática do processo e como se conduzir amparados pelo ordenamento jurídico interno, além de contribuir com as entidades de pesquisa, desenvolvimento e treinamento e com as autoridades de um país.

Esse momento pode se desbordar o processo para a sociedade, pois muitos cidadãos têm interesse direto nos resultados de alguns processos que mantém alguma semelhança com as suas aflições e prejuízos.

Evidencia-se a riqueza daquela oportunidade, de discutir ilícitos perpetrados através de sistemas informatizados através da abordagem interdisciplinar, pois tais ocorrências não têm precedentes na história da Humanidade, seja pelos meios empregados, seja pelo grau de

---

POSSIBILIDADE. (REsp 735015/BA, Rel. Min. Castro Filho, 3a. T., Julgamento em 29/11/2006, Publicação/Fonte DJ 18/12/2006, p. 372, LEXSTJ vol. 210 p. 180).

LOCAÇÃO. AÇÃO RENOVATORIA. FIXAÇÃO DO ALUGUEL DE ACORDO COM O LAUDO DO ASSISTENTE TÉCNICO DA RÉ. FIXADO O ALUGUEL PELO TRIBUNAL EM VALOR INFERIOR AO PLEITEADO NO RECURSO DA LOCADORA, INEXISTE VIOLAÇÃO AO PRINCIPIO TANTUM DEVOLUTUM QUANTUM APPELLATUM, JA QUE, NA FIXAÇÃO DO ALUGUEL JUSTO, OBJETIVO DA RENOVATORIA, NÃO ESTA O JUIZ ADSTRITO A DETERMINADO LAUDO OU AO PEDIDO DO LOCADOR. ALÉM DISSO, A OPERAÇÃO DE FIXAÇÃO DO VALOR LOCATICIO, COM BASE NOS ELEMENTOS DOS AUTOS, ENVOLVE QUESTÃO DE FATO, IRREVISIVEL NA VIA DO RECURSO ESPECIAL. RECURSO NÃO CONHECIDO.V.U. (Resp. 43401/SP, Relator Ministro Assis Toledo, 5a. T., Julgamento 06/04/1994, Publicação/Fonte DJ 25/04/1994 p. 9270).

[22] Conforme o Art. 159 do CPP; Art. 145 do CPP, incluídos os parágrafos e incisos de ambos os dispositivos.

[23] Arts. 25 a 27 do Código de Ética da OAB; Art. 7o. Alínea "a"do Guia do Profissional da Engenharia, da Arquitetura e da Agronomia para aplicação do Código de Ética. Disponível em http://www.confea.org.br/normativos/ . Acesso em 24/01/2009.

complexidade e extensão.

Além de satisfazer a necessidade de provar a autoria de um ilícito ou a existência de um fato, considera-se que a perícia forense em sistemas informatizados proporciona riqueza de informações, conhecimentos técnicos, notícias, pesquisas, dentre outras, aos profissionais do Direito, à luz dos escopos sociais do processo preconizado por Dinamarco (2000).

4.4. Estudo de Caso

No final de junho de 2007, foi noticiado pelos principais veículos de comunicação do país um fato à época inusitado: a publicação de uma conversa através de "sala de bate papo do MSN" no corpo de um despacho interlocutório exarado pelo MM. Juízo da 7a. Vara Cível do Foro Regional de Santana, e publicado no Diário Oficial eletrônico, o que levou o afastamento imediato do servidor da Justiça. As notícias sugeriam autoria desconhecida.

O principal suspeito, desde o início das investigações, foi o servidor Brasilino Soares Miranda, que já estava lotado no Juizado Especial Cível daquele Foro Regional há mais de mês, ou seja, muito antes da malfadada publicação.

Em novembro de 2007, os periódicos jornalísticos noticiaram o julgamento do processo administrativo, que resultou na sua demissão.

Considerada ocorrência grave no âmbito do Poder Judiciário Paulista, a expectativa da sociedade é a adoção de providências para verificar a autoria deste fato e respectiva penalidade. Nesse sentido, como poderia a perícia forense contribuir para a elucidação do caso, nos sistemas informatizados daquele Fórum?

A justificativa da parte interessada em realizar este tipo de prova seria a determinação do agente e modo de perpetrar o ilícito, informações essas relevantes para determinar eventuais tipos penais e violação de atividade funcional, bem como da reparação civil. Ainda, considera-se que tais informações sejam úteis para refletir e revisar os procedimentos de lançamento dos atos judiciais nos sistemas informatizados e respectiva publicação, além da política de segurança à eles relativos.

Em síntese, é preciso identificar com clareza o fato danoso a fim de constatar a sua existência, no caso a fraude no ato judicial levado à publicação. E, na medida do possível, responder perguntas chaves: quem, o que, como, quando, onde e porque se deu a fraude.

Isso possibilita fazer alguns questionamentos, inclusive como sugestão a uma eventual perícia técnica nos sistemas informatizados e em casos semelhantes à este:

a) quais as políticas de segurança implementadas, as práticas diuturnas e os procedimentos para disponibilização dos atos judiciais nos sistemas informatizados e remessa dos atos judiciais

para publicação;

b) quais as atribuições dos funcionários lotados no cartório e respectiva vara;

c) qual a prática de compartilhamento de equipamentos e guarda de *logins* e senhas;

d) qual a estrutura de rede e modo de disponibilização de IPs nos equipamentos.

Uma pesquisa sobre o procedimento para publicação dos atos judiciais pela Imprensa Oficial do Estado de São Paulo, levou a questionar, e até desconsiderar, a perícia técnica nas dependências, equipamentos e sistemas, pois que a instituição tem por objetivo apenas organizar e divulgar os atos dos três Poderes da República, conforme informações de seu portal.

Por isso a perícia técnica pode ser restrita aos recursos físicos, humanos e tecnológicos do cartório e respectiva vara, onde os supostos funcionários prejudicados exercem suas atividades, bem como do local e estação de trabalho do possível transgressor.

Ainda, a Microsoft, com sede das atividades nos Estados Unidos e responsável pelo aplicativo MSN, deveria ser oficiada para apresentar dados cadastrais das contas supostamente utilizadas pelos funcionários da 7a. Vara Cível do Foro de Santana. Se aquela conversa publicada existiu, o envio de informação dos IPs, respectivos *logins* e *logs* de acesso. Com isso seria possível determinar a existência da conversa e, conseqüentemente a autoria; se foi interceptada; ou ainda o uso desautorizado de *login* e senha por terceiro.

Quanto às perguntas do juízo e quesitos das partes, a rigor as informações relevantes devem estar relacionadas aos *logs* de acesso dos computadores das pessoas que tenham relação com o processo de criação e procedimentos de envio de atos judiciais para publicação no Diário Oficial eletrônico, a criação do ato judicial "fraudado" e alterações no(s) respectivo(s) arquivo(s) que o continha (computador, disquete ou CD); critérios de acessos e realização de tarefas a cada funcionário; prática de guarda de *logins* e senhas; programas disponíveis em cada máquina e critérios de uso; estrutura de redes do Fórum, endreços de IPs respectivo modo (manual ou automático), políticas de segurança e práticas diárias.

Uma pesquisa no portal da Imprensa Oficial possibilitou localizar algumas informações [24], inclusive um despacho sobre os contornos da prova pericial no âmbito do processo administrativo (Doe 21 de agosto de 2008, p. 118), cujos fragmentos que interessam ao presente estudo seguem abaixo:

> "Autos n.º 01/07 - Em atenção ao pedido de reconsideração e em relação aos esclarecimentos adicionais prestados pela I. Defensoria do Acusado:
> 1) Mantenho a decisão de indeferimento da expedição de ofícios para a Microsoft Informática Ltda. e Microsoft Corporation porque da simples leitura do texto verifica-se que o mesmo não foi gerado pelo Messenger ou MSN porque o programa não erra o nome dos interlocutores fazendo constar Lucianan" em vez de Luciana, nem faria

[24] Os processos judiciais para apurar responsabilidade civil por parte do funcionário condenado em processo administrativo e dos serventuários envolvidos no fato danoso, seguem abertos ao público na 14a. Vara da Fazenda Pública Estadual (processos nos. 053.08.104164-9 e 2007.261782-8).

> constar reticências e dois pontos ...:" e em determinados trechos apenas os dois pontos :" e nem faria constar a frase de um interlocutor no lugar da de outro, de forma que sequer há necessidade de prova pericial para esta circunstância. (..)
> 3.1) Indefiro os quesitos de nºs 1.7 , 1.8 , 2.1, 2.2 e 2.3. porque não se imputa ao acusado a geração do disquete de imprensa e sua transmissão. Aliás, pelo modo de operação do sistema Capcível tenho como incontroverso que o disquete de imprensa não foi gerado nem encaminhado pelo acusado à imprensa. Pelos motivos expostos no primeiro parágrafo acima (item 1), ficam indeferidos os quesitos 3.2.1 a 3.2.4.
> 3.2) Com o depósito intime-se os Srs. Peritos para iniciar o trabalho e entregar laudo em quinze dias.
> 4) Oficie-se à Prodesp indagando: I) Como é possível que o usuário 58301012554 (Brasilino Soares Miranda) tenha efetuado logoff no sistema às 19:14:20hs e um segundo depois, ou seja, 19:14:21hs o mesmo IP de número 10.34.13.193 tenha efetuado login com usuário 58301006405 (Antonio Jeová da Silva Santos)? II: Quando o sistema da CapCivel é desconectado involuntariamente (p.ex.: queda de energia, desconexão do cabo, desligamento do equipamento etc.) se o incidente fica registrado como logoff a exemplo de quando se opta pela opção sair" existente no programa. III) A quem pertence o login 58301012576. (...)"

Uma análise desta determinação judicial indica baixo nível de compreensão sobre as possibilidades de fraude através dos sistemas informatizados e internet. O leitor afeito ao tema entende possível a interceptação de mensagens rápidas ou de dados eletrônicos enviados pela internet, bem como seu tratamento para os fins que lhe sejam oportunos. Por isso, considera-se que a supressão desse meio de prova pode se afigurar prejudicial caso as demais provas não sejam conclusivas.

De outra feita, considera-se que o questionamento feito à Companhia de Processamento de Dados do Estado de São Paulo – PRODESP, sobre os supostos acessos pelo funcionário Brasilino em sua estação de trabalho e em seu próprio nome, e depois em nome do então juiz lotado na 7a. Vara Cível com mesmo IP, é relevante para responder outras questões.

Por exemplo, se o IP é disponibilizado a cada computador e sem a possibilidade de sua alteração, demonstra que os *logins* e senhas são compartilhados, o que compromete eventual política de segurança e a indicação do funcionário Brasilino como único transgressor, afinal, qualquer um poderia acessar os sistema em nome daquele juiz.

Contudo, se o IP foi atribuído de modo manual e pode ser disponibilizado em qualquer dos computadores cadastrados na rede do Foro Regional de Santana, qualquer pessoa com privilégios administrativos pode alterá-lo e utilizá-lo.

Em qualquer dos casos seria de bom alvitre realizar a perícia técnica nos computadores e mídias de todos os envolvidos no fato danoso com objetivo de obter prova robusta sobre a fraude.

Da análise do caso conclui-se que

- os procedimentos e práticas da 7a. Vara Cível, ao menos à época dos fatos, eram insatisfatórias para levar a bom termo as atividades judiciárias;

- as políticas de segurança determinadas pelo Poder Judiciário do Estado de São Paulo não eram cumpridas pelos funcionários daquela Vara, ao menos até a época dos fato danoso, o que potencializava a vulnerabilidade dos sistemas;
- caso seja excluída da perícia técnica a análise dos computadores dos funcionários envolvidos, pode-se perder a oportunidade de obter informações, quiçá até diretas sobre o transgressor.

A compreensão do funcionamento dos sistemas informatizados e diferentes graus de complexidade dos ilícitos perpetrados contra os órgãos decisórios do Poder Judiciário Paulista, ainda é insuficiente para determinar os contornos e alcance da perícia técnica em tais sistemas com precisão.

Em especial ao caso em exame, se a instrução do processo, em particular a prova pericial, não for conduzida com propriedade e rigor técnico e jurídico, poderá induzir a um julgamento tão danoso como fato que ensejou a respectiva ação, pois além de impor penalidade a um inocente poderá deixar o transgressor livre para a prática de outros ilícitos.

V. CONCLUSÃO

No curso da pesquisa deste trabalho sobre a perícia aplicada aos sistemas informatizados, tomou-se conhecimento de que no Brasil há grupos de pesquisa, associações de peritos em forense computacional e realização de eventos técnicos dos quais participam as autoridades nacionais e estrangeiras, pesquisadores e especialistas. Contudo a reflexão e debates não são levados à sociedade, mas ficam reservados. O nível das discussões e a qualidade dos trabalhos são altos e poderiam ser compartilhados com a sociedade, caso em que facilitaria a pesquisa pelos interessados e projetaria o Brasil como um dos centros difusores deste conhecimento especializado.

Na América do Norte e Europa, por outro lado, é desenvolvida intensa pesquisa e produção científica, além da perícia propriamente dita, e cuja literatura especializada é disponibilizada em meio físicos e eletrônico, gratuitos ou não. Essas ações conjugadas conferiram-lhes posição de destaque no meio e consolidaram-se como referência no assunto.

As dificuldades da pesquisa não se restringiram a parca literatura técnica forense sobre o assunto disponível no Brasil, mas também obras jurídicas relativas à prova no processo judicial. E, especificamente a prova pericial em sistemas informatizados, não foi encontrada alguma sequer, o que corrobora o entendimento que os profissionais do Direito têm poucos conhecimentos sobre as tecnologias de comunicação e telecomunicação, o que pode comprometer a compreensão da magnitude dos problemas do porvir.

Por isso é preciso ficar atento quanto ao argumento de "invasão de privacidade" e "prova ilícita" para restringir o âmbito da perícia nos sistemas informatizados e a atuação do perito ou para contestar o laudo. As centenas de pedidos de *habeas corpus* e as notícias jornalísticas dos últimos dois anos dá-nos conta dos desatinos por ignorância e o perigo da incriminação pela opinião pública.

Isso porque o desconhecimento daquelas tecnologias pode levar o profissional do Direito a refletir e emitir juízo de valor equivocado e induzir o público a erro. Essa crítica deve servir de estímulo ao estabelecimento de diálogo intenso na sociedade e os especialistas sobre referidas tecnologias, principalmente com aqueles profissionais que vão demandar e decidir em juízo. Nesse sentido, não é prudente pacificar a sociedade pela ignorância, sob pena de causar prejuízos de monta à sociedade como um todo.

O estudo de caso proporcionou um contato direto com uma situação que envolve crime, descumprimento de obrigação funcional e conseqüente responsabilização civil.

O fato foi lançado pela imprensa jornalística no final de junho de 2007 e em outubro do mesmo ano noticiada a suspensão do suposto transgressor, mas não a decisão final do processo

administrativo. Esse dado mostra o baixo comprometimento da imprensa com este tipo de notícia, pois além de ser reproduzida indiscriminadamente e sem critérios, como o tratamento da realidade dos fatos de maneira superficial e sem comprometimento de checar a sua veracidade, a sociedade não tem a informação do desfecho de casos emblemáticos como esse, que é da maior relevância se levarmos em consideração que a vida das pessoas estão imbricadas com as tecnologias de comunicação e telecomunicação.

Após a análise do caso, surgiram vários questionamentos, à luz da sugestão de Farmer e Venema (2007, p. 04), de que o leitor "deverá estar pronto para olhar em todos os lugares, procurando qualquer coisa, e deverá estar preparado quando localizar o que procura". Então formulou-se lista de medidas a serem consideradas pelo juízo e as partes:

- levantamento de todos os computadores, periféricos e outros equipamentos e mídias disponíveis e utilizadas no cartório respectiva vara judicial onde estão lotados os possíveis transgressor e vítima; fotografia dos locais;
- relação de usuários dos equipamentos; critérios de compartilhamento; autorização de acesso aos sistemas informatizados em razão da atribuição das tarefas de cada funcionário;
- levantamento dos IPs e modo de alteração (manual ou não); programas instalados e com execução reiterada, além da identificação dos equipamentos;
- *modus operandi* da entidade quanto ao processo de criação, elaboração e envio de atos processuais para publicação na Imprensa Oficial, bem como os responsáveis para tanto;
- estrutura de rede da instituição e administração dos sistemas informatizados; política de segurança aos sistemas informatizados;
- solicitação de informações à Microsoft dos dados cadastrais de eventuais contas de MSN utilizadas, bem como os IPs de acesso e histórico para o período que antecedeu a publicação, cuidando de manter sigilosa essa informação e apenas revelar nos autos caso haja conexão com os fatos, a fim de preservar a privacidade;
- solicitação de informações à Imprensa Oficial sobre o procedimento de remessa dos atos judiciais para publicação; informações de *login* e identificação do funcionário que enviou tal despacho desabonador, bem como do IP de onde partiu o ato judicial publicado e possibilidades de alteração dos caracteres;
- perícia no computador do suspeito e naqueles que guardam estreita relação com o ato ilícito;
- entrevistas com funcionários a fim de obter informações sobre práticas diuturnas de guarda de senhas; grau de comprometimento de cada um com a função; grau de entendimento sobre o funcionamento dos sistemas informatizados; acesso de terceiros ao local e nas estações de trabalho; outros.

O estudo também serviu para compreender melhor como a prova pericial pode ser

utilizada na estratégia de defesa sobre eventual direito violado, de cuja reflexão desdobraram-se outros questionamentos face ao futuro próximo e inevitável de informatização do processo e dos serviços judiciais e a virtualização dos serviços jurídicos.

Diante deste cenário, urge os cidadãos engajarem-se nos debates, propostas e soluções sobre as tecnologias de comunicação e telecomunicação disponíveis. Afinal, elas já estão incorporadas em seu dia a dia e a maioria daqueles cidadãos depende visceralmente delas.

Em especial os profissionais que atuam na área do Direito e desconhecem os sistemas informatizados e seu funcionamento e crêem, fielmente, que a perícia elucidará o caso, ou que trará informações relevantes para a defesa do Direito violado, ou ainda que oferece subsídios suficientes para a decisão, podem se enganar. Uma estratégia de defesa ou decisão erradas pode gerar alto custo para as partes envolvidas e à sociedade, pois podem abrir precedente pernicioso.

Por todos os motivos aqui relacionados e entre outros de igual importância mas que não guardam relação com o tema em exame, é importante os profissionais do Direito conhecerem os mecanismos dos sistemas informatizados e acompanharem a dinâmica das tecnologias de comunicação e telecomunicações, tomarem contato mais raso com essa realidade, o que é possível sem ingressar em um terreno tão arenoso como da Técnica e Engenharia.

O estudo contribui com a produção científica nacional e partilha com os colegas e interessados em geral, das preocupações, pesquisas, inovação, práticas, dentre outras ações.

Evidencia-se também, que se abriu oportunidade para os profissionais participarem, ativamente, das profundas alterações que se avizinham no exercício das carreiras jurídicas decorrentes da lei de informatização do processo judicial, da informatização dos serviços judiciários, dentre outros serviços públicos, notadamente as Receitas da União, Estados e Municípios.

BIBLIOGRAFIA

Associação Brasileira de Especialistas em Alta Tecnologia – ABEAT. Disponível em: < http://www.abeat.org.br/ > Acesso em 15/01/2009.

Associação Brasileira de Normas Técnicas – ABNT. Disponível em: <http://www.abnt.org.br/default.asp?resolucao=1280X800 >. Acesso em 15/01/2009.

Associação Nacional dos Peritos Criminais Federais – APCF. Disponível em: < http://www.apcf.org.br/%C3%81reaAberta/P%C3%A1ginaPrincipal/tabid/289/Default.aspx >. Acesso em 15/01/2009.

Associação dos Usuários de Internet Rápida – ABUSAR. *Glossário de Termos*. Disponível em: < http://www.abusar.org/418.htm >. Acesso em 15/01/2009.

BARBOSA, A. N. *Um sistema para análise ativa de comportamento de firewall.* Dissertação (Mestrado em Engenharia). São Paulo: EPUSP, 2007.

____; FERREIRA, M. S. J.; SANCHEZ, P. L. P . Técnicas de Recuperação de Dados Armazenados em Disco Rígido. In: 8º Simpósio Segurança em Informática, 2006, São José dos Campos. ANAIS SSI 2006. Rio de Janeiro : Fundação Biblioteca Nacional, 2006.

Código Civil. Disponível em: < http://www.planalto.gov.br/ccivil_03/LEIS/2002/L10406.htm >. Acesso em 15/01/2009.

Código Penal. Disponível em: < http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del2848.htm >. Acesso em 15/01/2009.

Código de Processo Civil. Disponível em: < http://www.planalto.gov.br/ccivil_03/LEIS/L5869.htm >. Acesso em 15/01/2009.

Código de Processo Penal. Disponível em: < http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del3689.htm > Acesso em 15/01/2009.

Comitê Gestor da Internet. *Cartilha de Segurança para Internet.* 2006. Disponível em: <

http://cartilha.cert.br >. Acesso em 15/01/2009.

Constituição Federal. Disponível em: < http://www.planalto.gov.br/ccivil_03/Constituicao/Constitui%C3%A7ao.htm > Acesso em 15/01/2009.

DINAMARCO, C. R. *A instrumentalidade do processo.* 8a. ed. São Paulo: Malheiros, 2000.

Escola Politécnica da Universidade de São Paulo – EPUSP. Disponível em: < http://www.poli.usp.br/Organizacao/Departamentos >. Acesso em 15/01/2009.

European Working Party Information on Technology Crime – EWPITC. Disponível em: <http://www.interpol.int/Public/TechnologyCrime/WorkingParties/default.asp >. Acesso em 15/01/2009.

FARMER, D. *Forensic Computer Analysis: An Introduction*. 2000. Disponível em: <http://www.ddj.com/184404242> Acesso em 15/01/2009.

____; VENEMA, W. *Perícia Forense Computacional: Teoria e Prática Aplicada*. São Paulo: Pearson Prentice-Hall, 2007.

Federal Bureau of Investigation – FBI – Laboratory. Disponível em: < http://www.fbi.gov/hq/lab/org/cart.htm > Acesso em 15/01/2009.

GEUS, P. L.; GUIMARÃES, C. C.; OLIVEIRA, F. de S.; REIS, M. A.. *Forense Computacional: aspectos legais e padronização.* 2001. Disponível em: < http://www.las.ic.unicamp.br/paulo/papers/2001-WSeg-flavio.oliveira-marcelo.reis-forense.pdf >. Acesso em 15/01/2009.

GRECCO FILHO, V. *Manual de Processo Penal*. 5a. ed. São Paulo: Saraiva, 1998.

High Technology Crime Investigation Association – HTCIA. Disponível em: <http://www.htcia.org/>. Acesso em 15/01/2009.

HOBSBAWM, Eric. *Globalização, Terrorismo e Democracia*. São Paulo: Cia. das Letras, 2008.

Imprensa Oficial do estado de São Paulo. Disponível em: < http://www.imprensaoficial.com.br > Acesso em 15/02/2009.

Instituto de Ciências Matemáticas e de Computação da Universidade de São Paulo – ICMCUSP – *Tutorial de HTML*. Disponível em: < http://www.icmc.usp.br/ensino/material/html/ >. Acesso em 15/01/2009.

International Association of Computer Investigable Specialists – IACIS. Disponível em: >http://www.iacis.com/>. Acesso em 15/01/2009.

Internacional Organization on Computer Evidence – IOCE. Disponível em: < http://www.ioce.org/core.php?ID=1 >. Acesso em 15/01/2009.

LUCCA, N. De; SIMÃO FILHO, A. (coord). *Direito e internet – aspectos jurídicos relevantes*. Bauru – SP: EDIPRO, 1a. Reimp., 2001.

NEGRÃO, T.; GOUVÊA, J. R. F.; BONDIOLI, L. G. A. *Código de Processo Civil e legislação processual em vigor*. 41a. ed. amp. at., São Paulo: Saraiva, 2009.

NERY JUNIOR, N.; NERY, R. M. A. *Código de Processo Civil Comentado*. 4a. ed. revista e ampliada. São Paulo: Revista dos Tribunais, 1999.

____. *Princípios do processo na Constituição Federal*. 9a. ed. rev., ampl. e atual. com as novas súmulas do STF (simples e vinculantes) e com a análise sobre a relativização da coisa julgada. São Paulo: Revista dos Tribunais, 2009.

NOBLETT, M. G.; POLLITT, M. M.; PRESLEY, L. A. *Recovering and Examining Computer Forensic Evidence; Forense Science Communications* outubro 2000. Vol. 2 N. 4; Federal Bureau of Investigation. Disponível em < http://translate.google.com.br/translate?hl=pt-BR&sl=en&u=http://www.fbi.gov/hq/lab/fsc/backissu/oct2000/computer.htm&sa=X&oi=translate&resnum=2&ct=result&prev=/search%3Fq%3Dfbi%2Bforensic%2Bcomputer%26hl%3Dpt-BR%26sa%3DG > Acesso em 15/01/2009.

Polícia Internacional – INTERPOL. Disponível em: <http://www.interpol.int/ >. Acesso em 15/01/2009.

RANGEL, Ricardo. “Do Sputnik a NSFNet”. 1996. Disponível em: <http://www.fe.unb.br/catedra/bibliovirtual/internet/a_historia_da_internet_1.htm > Acesso em 02/04/09.

REIS, M. A. *Forense computacional e sua aplicação em segurança imunológica*. Dissertação (Mestrado em Ciência da Computação). Campinas: UNICAMP, 2003. Disponível em < http://www.las.ic.unicamp.br/paulo/teses/20030226-MSc-Marcelo.Abdalla.dos.Reis-Forense.computacional.e.sua.aplicacao.em.seguranca.imunologica.pdf > Acesso em 15/01/2009.

SANTOS, M. A. *Primeiras linhas do Direito Processual*. 19a. ed. atual. e ampl. Vols. I e II. São Paulo: Saraiva, 1997.

Scientific Working Group on Digital Evidence – SWGDE. Disponível em: <http://www.swgde.org/>. Acesso em 15/01/2009.

SILVA, José Afonso. *Curso de Direito Constitucional Positivo*. 15a. ed. Rev. - São Paulo, SP: Malheiros Editores, 1998.

SILVA NETO, Amaro Moraes. *Privacidade na internet: um enfoque jurídico.* Bauru, SP: EDIPRO, 2001.

STRENGER, Irineu. *Direito Internacional Privado.* 3a. ed. aum. - São Paulo: LTr, 1996.

United States Computer Emergency Readness Team – US-CERT. Disponível em <http://www.cert.org/tech_tips/FBI_investigates_crime.html >. Acesso em 15/01/2009.

Universidade Federal de São Carlos . SOS - Informática FAQ (Frequently Asked *Question, ou Perguntas Freqüentemente Feitas)* < http://www.ufscar.br/~suporte/faq00.php#Section_7 > Acesso em 15/01/2009.

ZMOGINSKI, F. *Cracker invade virtua e muda dns do Bradesco.* In INFO Online. Notícia disponível em: < http://info.abril.uol.com.br/noticias/tecnologia-pessoal/cracker-invade-virtua-e-muda-dns-do-bradesco-15042009-36.shl > Acesso em 15/04/2009.

Fim