Anonimato *On-line* e Responsabilização Penal (Objetiva) em Cibercrimes (Agosto 2010)

Maciel Colli

***Resumo*—O presente artigo busca traçar e explorar questões controversas existentes para a responsabilização penal de sujeitos que cometem delitos por meio da *internet* — infrações penais que, pela natureza do meio em que são praticadas, serão aqui denominadas de *cibercrimes*. Com fundamento neste problema busca-se analisar quais são os limites aos quais a investigação preliminar policial e o processo penal estarão atrelados em razão do anonimato *on-line* ciberespacial, bem como apresentar possíveis hipóteses/respostas que viabilizariam a superação de referidos limites, tornando a investigação criminal dos *cibercrimes* mais eficiente e eficaz.**

***Palavras-Chave*—Anonimato *On-line*, Cibercrimes, Crimes Virtuais, Investigação Policial, Responsabilidade Penal.**

I. A *Internet* e a Dialética do Anonimato *On-line*

A *internet* revolucionou a maneira como a informação é transmitida e como as pessoas se comportam. KEITH HART ressalta a dualidade existente no universo comportamental do indivíduo urbano contemporâneo: o comportamento *virtual* e o *real*. O autor associa, respectivamente, a estes comportamentos os termos *on-line* e *off-line* [1]. A utilização destes conceitos para o esclarecimento do significado do termo *on-line* parece salutar. De fato, a tradução literal *em linha* poderia conduzir às remotas tecnologias de fios telefônicos, hoje em dia já em ascendente desuso graças ao surgimento de novos recursos trazidos pelo avanço da engenharia de materiais. Como bem observado, os dois *mundos* coexistem e complementam-se; o indivíduo ao ingressar no mundo *on-line* (*virtualizado*) traz consigo as características do seu comportamento no mundo *off-line* (*real/tangível*). Estabelece-se aí a dialética *virtual-real*, na qual a denominada realidade *virtual* torna-se o palco principal. O estabelecimento dessa dialética é fundamental para a compreensão dos *cibercrimes* cometidos na *internet*.

A partir de uma conduta exercida no mundo *real*, como, por exemplo, digitar um texto ou clicar em algum *hyperlink*, pode-se exercer, simultaneamente, uma ação e um resultado no mundo *virtualizado*, como por exemplo, a publicação de algum vídeo ou texto. Para melhor compreensão desta diversidade de termos, faz-se necessário o estabelecimento, breve, das diferenças entre o *virtual* e o *real*.

Ao analisar-se o ambiente *sui generis* do *ciberespaço*, verifica-se que dentre as suas características está a possibilidade de dissipação presencial no *espaço-tempo*: *onde estou se estou em todo o lugar* [2]. A conjugação da *existência* em dois *mundos* – *off-line* e *on-line* – faz com que as características de um não estejam necessariamente vinculadas ao outro. Ao ingressar no ambiente *on-line*, inevitavelmente, estarão agregados a um sujeito *virtual* as características de outro sujeito, o *real*. Porém, ao contrário do sujeito do mundo *real* (*off-line*), o qual ao manter relações interpessoais possuirá uma *representação única* perante um grupo social, o *sujeito on-line* representará uma espécie de *camaleão pixelado*, podendo assumir a *identidade* que bem entender ou mais lhe convier. É justamente nesta possibilidade de se modelar uma *individualidade on-line* que reside a questão do *anonimato on-line*.

O *anonimato on-line* fornece uma liberdade inatingível no mundo *real*. Seja em *websites de relacionamento*, seja em conversas através de mensageiros instantâneos (*instant messengers*), seja através de dados armazenados em bancos de dados de quem procura emprego; em qualquer destes *ambientes* do *ambiente on-line*, a liberdade para se assumir características de gênero, idade e religião é ilimitada. Essa ampla liberdade permite a qualquer pessoa assumir uma *personalidade* ou *identidade* que poderá corresponder ou não a da pessoa do mundo *off-line*. O *tudo posso fazer* e o *ser quem eu quiser*, entretanto, possuem limites.

II. O *Underground* e o Perfil *Cibercriminoso*

A sala é escura. Os móveis e apetrechos que a ocupam são de pouca relevância econômica. *Posters* pendurados nas paredes exibem o saudosismo digital – protagonistas de *games*, anúncios publicitários de *OSes* [3] antigos. O aparato geralmente é amplo, de aparência fragmentada, ou melhor, recém montada. A luz que ilumina o ambiente é uma só, vem do monitor ligado. Nele predomina uma cor, o verde. O fundo da tela, escuro, contrasta com a cor traçante de letras e números – estes em conjuntos indecifráveis para os *homens comuns*. A cena possui apenas um protagonista, apenas uma fala. Em geral, estereotipado no indivíduo jovem, detentor de incomparável conhecimento matemático e de linguagens de programação. Posto na frente do instrumento irradiante, o *ser iluminado* atravessa qualquer barreira. A partir de seu computador, o habitante deste escuro ambiente desloca-se em minúsculas frações de tempo ao redor do mundo. Move-se do *mainframe* do banco ao *servidor* da faculdade, em microssegundos. O <*enter*> [4] dá vazão ao intelecto. Comandos organizados surtem efeitos: *./configure, make,*

make install, ./run, rm. Ação e (múltipla) reação. Barreiras intransponíveis permeabilizam-se diante do *exploit* [5]; desmoronam como um castelo de areia com a água do mar. Em geral, composto de poucas linhas, mas considerado um *secret spot* [6] para o *descobridor* malicioso, o *exploit* tem poder avassalador sobre programas ou máquinas vulneráveis. É a porta cuja maçaneta foi sutilmente removida. Se não corrigido, e espalhada a notícia de sua existência, traduz-se em uma das poucas certezas do *mundo digital*: nenhum sistema é impenetrável.

Apesar de espalhafatoso, o relato representa a imagem, muitas vezes equivocada, daqueles sujeitos que, valendo-se de seus conhecimentos sobre instrumentos eletrônicos, invadem sistemas operacionais ou descobrem falhas em determinados *softwares* e/ou *hardwares*. A fantasia *falaciosa* de letras e números em *3D* que saltitam na tela dos computadores, de recursos gráficos preciosos e de ambientes assemelhados a canais do sistema de detritos municipais é meramente cinematográfica. Tenta representar valores ligados a um suposto *movimento underground*, na qual o *hacker* é sujeito emblemático. Tirando o sujeito jovem, o aparato (recém) montado e os parcos móveis que integram o ambiente, há diversa realidade.

O *underground cibercriminoso* é falacioso e estabelece o ideal *wannabe* [7] de quem idolatra – e de quem teme – a figura do *invasor*. Não há sujeito *mais underground* – primazia da imagem/estilo e da *ideologia invasora* – que possa ser equiparado ao sujeito *mais criativo*, *mais conhecedor, mais oportunista* ou, inevitavelmente, *mais sortudo*. A atribuição destas características – *criatividade, conhecimento*, *oportunidade* e *sorte* – serve, na verdade, para ilustrar um suposto perfil dos sujeitos que praticaram *cibercrimes* a partir da invasão e/ou manipulação de computadores, redes e/ou pessoas. Nada obsta, salienta-se, que estas atribuições não sejam necessárias a prática de outros tantos crimes que tenham na *internet* o seu meio, instrumento ou objeto material. Para a invasão de redes e sistemas operacionais, a quebra de chaves de criptografia (*cracking*), o *spamming*, o *phishing* e outros eventos danosos, aquelas características possivelmente estarão presentes.

Criatividade pra quê? Que o diga John T. DRAPER, vulgo *captain crunch*, cujo pseudônimo deriva da manobra por ele utilizada para fazer ligações de longa distância – no Brasil conhecidas como *DDD* – a partir de um apito que vinha nas embalagens de um cereal com esse nome, em 1972 [8]. Valendo-se de um brinquedo, e da construção de um equipamento chamado *blue box*, o *phreaker* [9] passou a ter acesso e controle sobre ligações em telefones públicos, sem que para isso fosse necessário depositar moedas.A manobra foi primorosa. Usando o apito, *cap'n'crunch*' emulava a mesma freqüência sonora (2600 HZ) que o telefone público usava ao ser *creditado* para *liberar* uma conexão. Ao conseguir essa *autorização* da central telefônica, bastava usar uma *blue box* – a qual emulava os tons enviados por um aparelho de telefone comum – para que a conexão a longa distância com qualquer telefone fosse completada.

Conhecimento sobre o quê? Matemática, lógica e comportamento humano. Trata-se de conhecimento específico nas áreas que envolvem a comunicação entre os homens e entre estes e as máquinas. Para que surta efeitos, a comunicação do sujeito *invasor* deverá ser feita de forma convincente não apenas com seres humanos, mas também com as máquinas. Quanto maior a afinidade com a *linguagem da máquina*, maior será a possibilidade de se alcançar determinado objetivo através da organização de algarismos e letras em forma de códigos. O *faça o que eu quero* traduz-se na facilidade em lidar com os meios fornecidos através de comandos de interpretação das diversas linguagens de computadores. Quanto maior o *vocabulário maquinário*, maiores as chances de se fazer entender. Em relação ao comportamento humano também é necessário ao *invasor* um bom discurso e uma boa técnica de *vergamento social*. O *social engineering* [10] é o exemplo por excelência do uso da manipulação do comportamento humano. Valendo-se de subterfúgios tendentes a fragilizar e subverter o comportamento emocional de seu *alvo*, o *invasor* consegue, muitas vezes, informações e dados preciosos para a remoção de algum obstáculo do caminho de seu objetivo.

Oportunidade de quem? Sem dúvida, de um exemplo como o de Kevin POULSEN. Em 1º de junho de 1990, a rádio 102.7 KIIS-FM de Los Angeles, Estados Unidos da América, deu seguimento ao seu concurso *Win a Porsche by Friday* (Ganhe um *Porsche* na Sexta-Feira). O 102º sujeito a ligar para a central telefônica da rádio, após uma sequência de determinadas músicas, seria o felizardo ganhador de um *Porsche*. Com a ajuda de dois amigos, Ronald AUSTIN e Justin PETERSON, Kevin POULSEN promoveu um *takeover* [11] das 25 linhas telefônicas da rádio, bloqueando a recepção das ligações oriundas de linhas externas, deixando livre o caminho apenas para um número telefônico: o seu [12].

Sorte por quê? Muitos dos *exploits* e *backdoors* utilizados para se penetrar em um sistema protegido decorrem do descobrimento casuístico de falhas e *portas abertas* deixadas pelo próprio desenvolvedor originário do *software*.

Diante de um cenário *virtualizado* ou *real*, com base no ideal *wannabe* há pouco apresentado, ou com base nos exemplos fáticos relatados, os computadores e a *internet* – *novos* instrumentos de um tempo que está em acelerada *velocidade* – podem ter a sua finalidade *positiva* (benéfica) desviada, transformando-se em utilitários de atividades que, sendo antijurídicas ou não, resultam em dano e/ou prejuízo alheio. Condutas já criminalizadas – e, portanto, antijurídicas –, como o estelionato e a falsificação de documentos, podem vir a ser executadas também por meio dos novos recursos eletrônico-computacionais. Estas infrações penais são, geralmente, denominadas *cibercrimes*, e os sujeitos que os cometem são alcunhados de *cibercriminosos*.

III. Identidade Qualitativa e Numérica: A Cisão entre Máquinas e Indivíduos

Em termos gerais, uma pessoa é *individualizada* socialmente (no mundo *off*-line) por sua *identidade visual*. O

reconhecimento das características de uma pessoa, tais como feições faciais, altura, e voz fazem com que se associe este rol de qualidades a um nome; há uma espécie de *concretização qualitativa*. O reconhecimento e a identidade *legal* de uma pessoa, por outro lado, são feitos, em geral, por um documento ao qual se atribui um elemento identificador – por exemplo, um número. Este documento identificará a *individualidade* de uma pessoa em um determinado período de tempo em um determinado território – por exemplo, número de passaporte e número do Registro Geral. Tem-se aqui uma espécie de *concretização numérica*.

A *identidade* e o *reconhecimento* na *rede mundial de computadores* são feitos de modo semelhante aos dois modelos anteriormente apresentados; em verdade, pode-se dizer que são mescladas características da *concretização qualitativa* e *numérica*. Diferenciam-se, porém, em três importantes aspectos: a) não há – ou pelos menos não deveria haver [13] – *identidade na rede* (*concretização qualitativa*) sem identidade numérica, ou seja, para se identificar [14] o *host A* como um computador que faz parte de uma rede, será necessário atribuir-se um *endereço numérico* a ele – *por exemplo*, um *endereço IP*; b) a identidade, seja ela *qualitativa* (*individualidade* de características na rede) ou *numérica* (endereço), será sempre de um computador, jamais de um sujeito; c) um *endereço numérico* – por exemplo, um *endereço IP* – pode ser atribuído em um curto período de tempo (horas) a diferentes computadores, não podendo, entretanto, (em tese [15]) possuírem o mesmo *endereço*, ao mesmo tempo, dois ou mais computadores – individualmente considerados.

Não serão aprofundados os estudos a respeito do protocolo *IP*, pois se estaria fugindo do foco do presente estudo. Por ora é importante ter em mente que um *endereço IP* é, basicamente, o atributo que identifica um computador em uma rede [16] (*qualitativa* e *numericamente*). Assim, pode-se ter uma rede sem fio (*WLAN*) composta por um *host A* (*endereço IP*: 192.168.0.2), um *host B* (*endereço IP*: 192.168.0.3) e um roteador 802.11 (*endereço IP*: 192.168.0.1). Cada uma das máquinas detentoras destes *endereços IPs* terá associada a si um novo identificador, qual seja, o *endereço MAC*. O *endereço MAC* é um número exclusivo identificador de uma interface de rede que faz a comunicação de uma máquina com outra, por exemplo, uma placa de rede (*Ethernet*). Cada interface de rede possuirá um número exclusivo de *endereço MAC*.

O chamado protocolo *ARP* é responsável pela realização da correlação *endereço IP x endereço MAC* em uma rede [17]. Por exemplo, o *host A* quer saber onde está o *host B*; para tanto, envia um *ARP Request packet* perguntando: *quem tem o IP X?* O *host B*, que possui o *IP X,* ao perceber que o seu *endereço* foi *requerido*, responderá com um *ARP Reply packet*, informando: *eu tenho o IP X e o meu endereço MAC é Y.* Desta maneira forma-se a rota de comunicação de dados entre um *requerente* (*host A*) e um *requerido* (*host B*).

Um computador, portanto, ao ingressar em uma rede passa a ter um *endereço IP* exclusivo. A comunicação com outros computadores e sistemas desta mesma rede será feita com base no *endereço MAC* da sua interface de rede, cuja correlação com o primeiro (*endereço IP*) será feita através do protocolo *ARP*.

Quando se cogita em *anonimato on-line*, na verdade, o que se quer dar a entender é que esse *anonimato* é, em princípio, *aparente*, pois mesmo o *mais anônimo* dos sujeitos de um *website de relacionamento* – por exemplo, o sujeito que mais omite informações a seu respeito – utilizará um computador cujo *endereço IP* – atribuído ao seu computador – será identificado quando conectado à *internet*, ou quando realizada alguma ação em referido *website*.

IV. A Problemática do Anonimato *On-line* para a Responsabilização Penal de Cibercriminosos

Apesar da aparente facilidade em se identificar um sujeito na *internet* a partir de seu *endereço IP*, há duas questões importantes que serão problemáticas para qualquer órgão policial incumbido da investigação de um *cibercrime* [18]: a) a correlação, em um determinado espaço de tempo, entre *endereço IP x máquina*; b) a correlação, em um determinado espaço de tempo, entre *máquina x sujeito que a opera*.

Em relação ao primeiro problema, a dificuldade estará no rastreamento de um *endereço IP* e conseqüente associação a uma *máquina* – para, posterior, associação de autoria de um *cibercrime* a um sujeito, o qual será o suposto detentor da máquina e do *endereço IP* suspeito. Para melhor compreensão deste problema, traz-se o seguinte exemplo: um determinado *endereço IP X* é gravado pelos servidores de um banco que foi furtado. O furto se realizou a partir de uma operação bancária não-autorizada por meio da *internet*, às 12 horas, do dia 4 de maio de 2009. Como descobrir a que máquina este *endereço IP X* pertencia?

Em tese, para se descobrir qual máquina executou referida operação, naquele momento, busca-se inicialmente a identificação do *endereço IP* – no presente exemplo, de número *X*. Identificado o *endereço IP* responsável pela operação não autorizada, parte-se para a análise de qual provedor de *internet* possuía referido *endereço IP* – na verdade, a máquina do sujeito que fez a operação possui um *IP* que é *emprestado* pelo provedor, isto é, provedores de acesso à *internet* possuem uma gama de endereços *IPs* a sua disposição, os quais serão atribuídos aos seus *clientes* no momento da conexão destes à *internet*. Identificado o provedor de acesso, identifica-se sob qual *conta de usuário* estava sendo utilizado referido *IP* em referido momento, a fim de se descobrir, a seguir, quem teria feito a transação bancária.

Pois bem, a questão que se faz é a seguinte: identificado o *IP,* identificado o provedor detentor daquele *IP,* identificada a *conta do usuário*, e igualmente, identificado o *contratante* do serviço de acesso a *internet* detentor daquela *conta de usuário*, há um juízo positivo para a *aparência* de suspeição a respeito da máquina e do sujeito que praticou o suposto *cibercrime?* A resposta só pode ser negativa. E a razão para esta resposta está estampada no primeiro exemplo que foi apresentado nesta

pesquisa. Se ao adentrar na *WLAN*, o *invasor* passa a fazer parte dela, tendo um *IP interno* atribuído ao seu computador, bem como acesso à *internet* a partir do roteador *wireless*, qual *endereço IP* estaria gravado como sendo *aparentemente* do autor no exemplo anterior? O *endereço IP X* gravado pelos servidores do banco seria aquele obtido pelo roteador *wireless* no momento de sua conexão com o provedor de *internet*. Ou seja, o acesso que é feito pelo *invasor* é intermediado e feito a partir deste dispositivo, e os registros que irão aparecer serão, portanto, não do *invasor*, mas sim do *IP* atribuído ao roteador *wireless* no momento em que este estabeleceu uma conexão com a *internet*.

Pergunta-se: de quem é a máquina, a *conta de usuário* e o contrato com o provedor da *internet* neste caso? Do *invasor*? A resposta novamente é negativa. O *sujeito* a quem a *aparente autoria* de um *cibercrime* seria atribuída, seria o dono do roteador *wireless,* quem anteriormente havia contratado a prestação de serviço de acesso a *internet* com um provedor cujo *IP* gravado é apontado como sendo o utilizado no delito. Neste exemplo, para que a investigação possa localizar o eventual e *aparente* autor de referido *cibercrime* será necessário analisar o *data logging* [19] – se existir – do próprio roteador para se tentar localizar o endereço *MAC* do suposto *invasor*. Identificado o *MAC*, ter-se-ia uma identidade única, podendo-se, a partir daí, correlacionar-se *endereço IP x máquina*. Entretanto, diante deste risco de identificação, é comum que os *invasores* utilizem um programa que falsifica o *MAC* identificador (*MAC spoofing*), fazendo com que um dos poucos elementos que poderia relacionar *endereço IP x máquina* desapareça.

O segundo problema é ainda mais grave. A correlação, em um determinado espaço de tempo, entre *máquina x sujeito que a opera*. Como pode haver *aparência* de autoria do cometimento de um *cibercrime* a partir de um computador de uso público, ou ainda, no caso do cometimento de um *cibercrime* por meio de um computador utilizado por uma família de 8 pessoas, algumas maiores, outras menores de idade? Este problema está ligado ao que já foi exposto anteriormente: a identidade, seja ela *qualitativa* ou *numérica*, será sempre de um computador, jamais de um sujeito. Não há como se *automatizar* o direcionamento de uma investigação preliminar com base apenas no nome do *titular* de um contrato de acesso a *internet*.

V. Hipóteses e Alternativas à Atividade Investigativa: Em Busca de uma Maior Eficiência e Eficácia na Repressão e na Responsabilização Penal de Cibercrimes

A investigação preliminar policial e a utilização de medidas cautelares restritivas de direitos voltadas a um sujeito *aparentemente* suspeito devem ser embasadas em circunstâncias que corroborem com drásticas ações. A ausência de *indícios aparentes de autoria*, em situações como as descritas, enseja uma ação investigativa voltada meramente a sua função simbólica, desvinculada de outras funções [20] – igualmente relevantes – como o resguardo a acusações infundadas. No caso de uma instauração investigativa baseada na mera presunção de suspeição a partir da titularidade do contrato de acesso a *internet – automatização incriminadora* – a atividade policial estaria, claramente, orientada sob a ótica de responsabilização objetiva do Direito Penal, o que deve ser repudiado a todo custo.

O que deve ficar muito claro é que qualquer identificação ou rastreamento que possa ser feito na *internet*, ou em qualquer outra rede de computadores, será de números – endereços *IP, MAC*, por exemplo – e de máquinas, jamais de sujeitos.

A partir da apresentação destes dois pressupostos correlacionais – correlação *endereço IP x máquina* e correlação *máquina x sujeito que a opera* –, uma maneira de contornar os problemas daí surgidos é a seguinte: o indiciamento e a responsabilização do *sujeito que opera uma máquina*, e a partir dela comete um *cibercrime*, poderão ser realizados desde que haja a prisão em flagrante [21] com a *máquina operante* (ligada). Esta proposta tem em vista não apenas a investigação preliminar – que busca *vestígios de materialidade* e *indícios de autoria* –, mas também a ação penal dela decorrente. Afinal de contas, o Inquérito Policial – fase pré-processual – representa o *instrumento a serviço do instrumento* [22]. Por este motivo, para se evitar que uma operação que se prolonga por vasto período de tempo acabe em *nada*, é imprescindível que sua execução seja feita de maneira organizada, com atendimento à legalidade e com vista ao processo penal.

A primeira correlação – *endereço IP x máquina* – estaria satisfeita a partir da flagrância da *máquina operante*, a segunda correlação – *máquina x sujeito que a opera* –, a partir da prisão em flagrante. A primeira está para a configuração (e confirmação) da *materialidade* do delito, assim como a segunda está para a *aparência* de indícios de autoria. Veja-se o porquê destas afirmações. Em primeiro lugar, deve-se levar em consideração que dentre os *cibercrimes* há uma boa parte deles cuja natureza é de *crime permanente* [23], ou seja, sua consumação se prolonga no tempo enquanto durar o delito. Em particular, esta modalidade interessará, pois nestes *cibercrimes* que se prolongam no tempo – como, por exemplo, o compartilhamento ilícito de arquivos durante meses com um computador ligado – estará caracterizada a *permanência* da infração penal. A flagrância da *máquina operante* nos *cibercrimes* desta natureza será essencial, pois com ela *ligada* será possível correlacionar-se os dois elementos necessários à robustez (e confirmação) da *materialidade* do delito, quais sejam, o *endereço IP* e a *máquina operante* que está sendo utilizada para cometer o *cibercrime permanente*.

A segunda correlação – *máquina x sujeito que a opera* – é ainda de maior relevância, pois leva em consideração a pessoa que será alvo não apenas da investigação preliminar policial, mas também de eventual processo penal dela decorrente. O custo trazido por uma conseqüente estigmatização social decorrente de uma acusação infundada deve ser evitada ao máximo, razão pela qual para que isto seja evitado deve-se partir da necessidade de observância não apenas

da *possibilidade* da ocorrência de um delito como critério para a instauração do inquérito policial, mas igualmente da necessidade de um juízo mínimo de *probabilidade* da existência de uma infração penal, e, consequentemente, de indícios *suficientes* de autoria, os quais embasariam a ação penal [24]. Parte-se do pressuposto que as análises de *data mining* [25] ou *data carving* [26] podem levar à coleta de vestígios de *materialidade* em computadores e dispositivos de armazenamento utilizados em um *cibercrime* – atividade por excelência da perícia informática. Porém, para que se possa coadunar as informações angariadas a partir destes procedimentos – *materialidade* do *data mining* e/ou *data carving* – à responsabilização e identificação pessoal do sujeito – *indícios de autoria suficientes* – tem-se como indispensável a prisão em flagrante deste, quem, operando uma *máquina* associada à determinado endereço *IP*, estaria a cometer um delito *permanente* [27].

Portanto, em se tratando de uma *investigação preliminar policial* de um *cibercrime*, em especial se de natureza *permanente*, crê-se e sustenta-se ser necessária não só a prisão em flagrante do *sujeito* suspeito que opera uma *máquina* associada a um *endereço IP*, mas também que esta mesma máquina esteja *operante*. O risco do não atendimento a estes requisitos aqui apresentados poderia ensejar: a) para a *investigação preliminar policial:* a ausência de vestígios de *materialidade* (máquina desligada) e/ou a ausência de indícios *suficientes* de autoria (prisão em flagrante do sujeito passivo), a ensejar posterior *trancamento* do processo penal pela via do *Habeas Corpus* ou posterior *arquivamento* de inquérito policial pelo órgão competente; b) para a *ação penal*: a ausência de *justa causa* a ensejar a falta de uma das condições da ação penal [28], restando como conseqüência a rejeição da denúncia ou queixa (artigo 395 e 396, do Código de Processo Penal) [29].

Referências

[1] HART, Keith. Notes towards an anthropology of the internet. **Horizontes antropológicos**, Porto Alegre, v. 10, Nº 21, 2004. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0104-71832004000100002&lng=en&nrm=iso>. Acesso em: 27 ago. 2007.

[2] Já diria Paul VIRILIO: *Living present, here and there at the same time: where am I if I am everywhere?* (Vivendo o presente, aqui e lá ao mesmo tempo: onde estou eu se estou em todos os lugares?) (VIRILIO, Paul. **Inertia Polar.** Londres: Sage Publications, 2000. p. 83).

[3] *Operating System* (Sistema Operacional).

[4] Tecla que executa comandos em *Personal Computers*.

[5] Um *exploit* é o instrumento utilizado para explorar (daí o termo *exploit*, verbo inglês que significa *explorar*) uma vulnerabilidade existente em um *software* ou *hardware*. A execução do *exploit* geralmente é feita sob a forma de *buffer overflows*, os quais ocorrem quando um programa ao gravar uma informação em uma variável acaba passando maior quantidade de dados que a que estava prevista pelo programa. Isto faz com que haja a possibilidade de execução de um código malicioso arbitrário, o qual ao ser posicionado dentro da área de memória do processo em questão ocasiona a falha de estouro de *buffer* (ou *buffer overflow*) (ANTONIOLI, Rafael. **Detecção e Tratamento de Intrusões em Plataformas Baseadas no XEN.** Dissertação (Mestrado em Ciências da Computação) - Faculdade de Informática, Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2008. p. 64).

[6] A gíria é utilizada por surfistas para fazer referência a um lugar pouco explorado e considerado um pequeno paraíso; um local privilegiado por ser pouco conhecido e surfado, no qual ondas formidáveis quebram. O segredo por parte daqueles que conhecem o *secret spot* faz com que o ponto pouco conhecido seja guardado a sete-chaves, assim como o *exploit* descoberto. Ambos fornecem privilégios aos seus descobridores: aos surfistas o deleite, aos *exploiters* o controle sobre a falha.

[7] Aquele que imita, idolatra ou quer ser igual à outra pessoa, em geral a imagem idealizada do *hacker invasor* (gíria derivada do inglês *want to be*, ou *querer ser*). Daqui igualmente deriva o termo *script kiddie*, que é o sujeito que se utiliza de *exploits* ou *scripts* descobertos ou criados por outros para explorar vulnerabilidades. A falta de conhecimento a ensejar o descobrimento de novos *exploits* ou de criar os seus próprios *scripts* para explorar falhas, faz com que esta seja considerada uma atitude infantil, de *garotada* (daí o termo *kiddie*, derivado do inglês *kid*, ou criança/infantil).

[8] O brinquedo (apito) que vinha dentro da embalagem do cereal *Captain Crunch* era capaz de produzir uma freqüência exata de 2600 Hz. Essa freqüência era igual aquela enviada pelo aparelho de telefone público para a sua central a fim de que fosse alcançado o modo operador (*operator mode*). O uso do apito simulava o envio da freqüência do telefone público à central telefônica, indicando que a partir dali deveria ser feita uma conexão de longa distância (*trunk line connection*). Aprimorando o sistema, John T. Draper desenvolveu as chamadas *blue boxes*, que eram na verdade instrumentos geradores de tons de freqüências que permitiam a *comunicação* com a central telefônica e posterior controle sobre o destino das ligações, sem que houvesse qualquer gasto em moedas para o *phreaker* (DRAPER, John T. The origins of Captain Crunch. **The Real Captain Crunch.** Disponível em: <http://www.webcrunchers.com/crunch/origins.html>. Acesso em: 08 mar. 2009).

[9] O *phreaking* guarda com as telecomunicações a mesma relação que o *hacking* guarda com os sistemas de informações. O termo deriva de *phone freaking* (em inglês algo como mutação em telefones) e refere-se à técnica de explorar vulnerabilidades nos sistemas de telecomunicações, em geral de telefonia. A prática do *phreaking* desenvolveu-se a partir de experimentos inicialmente realizados no MIT (*Machassussets Institute of Tecnology*) nos anos 60. A partir da emulação de freqüências utilizadas para gerar telefonemas, os *phreakers* do MIT eram considerados *entusiastas da nova tecnologia* (SCHWABACH, Aaron. **Internet and the Law:** Technology, societies, and compromises. Santa Barbara: Abc-Clio, 2005. p. 265).

[10] O *social engineering* será melhor abordado no segundo capítulo do presente trabalho, ao qual remetemos o leitor.

[11] Tomar controle de algo; neste caso específico, desconectando todas as linhas telefônicas que não a de Kevin Poulsen.

[12] LITTMAN, Jonathan. **The Watchman:** the twisted life and crimes of serial hacker Kevin Poulsen. Boston: Little, Brown and Company, 1997. pp. 3 a 4 e 214 a 235.

[13] Adicionamos esta observação, pois no exemplo da interceptação de *packets* para invasão da *rede WLAN* por meio do *ARP Reply Attack*, vimos que, por exemplo, um *host A* com o *endereço 192.168.0.2* pode fazer-se passar pelo *host B* através do envio de *packets ARP* informando que possui na verdade o *endereço* do *host B*, por exemplo, *192.168.0.3*. Trata-se de um procedimento conhecido como *ARP Spoofing* (parte de um *ARP Poisoning*), no qual um *host X*, com um *endereço X*, faz-se passar por *N hosts* e *N endereços* (XIAO,Yang; PAN, Yi. **Security in Distributed and Networking Systems.** Singapura: World Scientific, 2007. pp. 7 a 9).

[14] E aqui estamos nos referindo ao conjunto de características individuais de um computador, que o faz ser *único* em uma rede: como por exemplo, seu *sistema operacional*, *hardware, dispositivos a ele ligados*.

[15] Como já foi explicado anteriormente, se houver o uso do *IP spoofing*, uma mesma máquina poderá se passar por duas máquinas, possuindo um *IP* verdadeiro e um *IP* falso.

[16] TANENBAUM, Andrew S. **Computer Networks.** 4. ed. Nova Jersey: Prentice Hall PTR, 2003. pp. 436 a 438.

[17] TANENBAUM, Andrew S. **Computer**... pp. 450 a 452.

[18] Nesta pesquisa serão considerados sinônimos de *cibercrimes*: *crimes cibernéticos*, *crimes informáticos pela internet*, *crimes praticados pela*

internet. A ligação entre *cibernética*, *ciberespaço* e *crimes informáticos* permite que se compreenda o instituto do *cibercrime* como sendo aquele no qual um ou mais computador(es), equipamentos telemáticos ou dispositivos eletrônicos, interligados por meio de uma rede de comunicação, são utilizados, por um ou mais indivíduos, no cometimento de uma, ou mais, conduta(s) criminalizada(s), ou são alvo(s) desta(s). O homem interagindo com uma máquina – retroalimentando-a com informações por meio de mensagens – através de uma rede de computadores (*cibernética*) interligados (*ciberespaço*), agindo conforme uma conduta previamente criminalizada (*crime informático*) estereotiparia um modelo de *cibercrime*.

[19] Através do *data logging* um sistema operacional coleta, continuamente, informações objetivas a seu respeito para posterior análise e interpretação. Durante este procedimento não há interferência com as atividades dos usuários, apenas o registro do que foi feito por eles no sistema. Os *logs* servem para identificar rastros deixados por computadores quando feita alguma conexão, bem como para saber que tipo de atividade (exemplo, quais comandos foram executados) foi desempenhada (STEPHANIDIS, Constantine; JACKO, Julie. **Human-computer interaction:** theory and practice (II). V. 2. Filadélfia: Lawrence Erlbaum Associates, 2003. p. 482).

[20] LOPES JUNIOR, Aury. **Sistemas de investigação preliminar no processo penal.** Rio de Janeiro: Lumen juris, 2003.pp. 44 a 63.

[21] Franco Cordero ensinava que a *flagrância* decorria do verbo latino *flagro,* o qual indicava uma combustão ou incêndio. A ocorrência ou não da flagrância deveria ser feita a partir da sincronia *fato-percepção*. Em relação às infrações penais a *flagrância* poderia ser associada ao estado em que o autor é pego quando realiza o fato ou logo após tê-lo cometido. (CORDERO, Franco. **Procedimiento Penal.** Tomo I. Bogotá: Temis, 2000. Pp. 410 a 412). Na doutrina nacional, há certa divergência quanto ao conceito e entendimento do que caracterizaria a flagrância. Eugênio Pacceli defende a idéia de *imediatidade*, ou seja, do momento em que ocorre o fato. *Por flagrante se deve entender a relação de imediatidade entre o fato ou evento e sua captação ou conhecimento*. (OLIVEIRA, Eugênio Pacelli de. **Curso de Processo Penal**... p. 410). Carnelutti, por outro lado, refere-se à flagrância em razão da *visibilidade* do fato ou evento. O flagrante seria não a *atualidade*, mas sim a *visibilidade* do delito (CARNELUTTI, Francesco. **Elementos de Direito Processual Penal:** Volume 4. 1. ed. Rio de Janeiro: Forense, 1965. p. 63).

[22] LOPES JUNIOR, Aury. **Sistemas**... pp. 42 a 43.

[23] BITENCOURT, Cezar. **Tratado de Direito Penal.** 10. ed. São Paulo: Saraiva, 2006. pp. 265 a 266.

[24] LOPES JUNIOR, Aury. **Sistemas**... pp. 51 a 54 e 55 a 60.

[25] O *data mining* é um procedimento por meio do qual se extrai informações interpretáveis de uma grande quantidade de dados. O termo vem do inglês *data* (dados) *mining* (extração). Em *Computer Forensics* (perícia em computadores) o *data mining* pode ser realizado após o procedimento do *disk imaging* (em português, espelhamento) (cópia fiel e idêntica) do dispositivo de armazenamento analisado (HAND, D. J.; MANNILA ,Heikki; SMYTH, Padhraic. **Principles of data mining.** Cambridge: MIT Press, 2001. pp1 a 5).

[26] O *data carving,* semelhantemente ao *data mining,* é um procedimento de recuperação de dados. Porém, ao contrário do *data mining* cujos dados podem ser localizados por possuírem referência no *sistema de arquivos* de uma *partição*, no *data carving* as informações de localização de determinado arquivo (*system allocation information*) foram perdidas – seja porque o arquivo foi *deletado*, seja porque o *disco rígido* foi formatado (DICKERMAN, Daniel. **Advanced Data Carving.** Disponível em:< http://sandbox.dfrws.org/2006/dickerman/Dickerman DFRWS 2006 Challenge Final Submission.pdf>. Acesso em: 27 abr. 2009).

[27] Um exemplo que chama a atenção diz respeito justamente a questão que aqui é trazida sobre a necessidade de apreensão da máquina operante e do sujeito que a opera. Na notícia veiculada pela Agência de Notícias da Polícia Federal brasileira, em 18 de maio de 2009 (http://www.dpf.gov.br/DCS/noticias/2009/Maio/18052009_OpTurco.html), o seguinte texto é apresentado: *Nas buscas os policiais irão acessar os computadores dos suspeitos para confirmar a existência de imagens de pornografia infantil. Caso o material seja encontrado, os responsáveis serão presos em flagrante.* Apesar de se tratar de mera veiculação de uma notícia, a ensejar, portanto a inexigibilidade de conhecimento técnico ou científico ligado ao processo penal, percebe-se que se houvesse a localização de referido material pornográfico infantil na máquina dos suspeitos, não poderíamos cogitar de prisão em flagrante, pois inexistente a flagrância, a *chama* do delito. A medida cautelar que poderia ser decretada, se preenchidos todos os pressupostos e requisitos necessários, neste caso, seria a prisão preventiva, jamais a pré-cautelar e precária prisão em flagrante.

[28] LOPES JUNIOR, Aury. (Re)pensando as condições da ação processual penal desde as categorias jurídicas próprias do processo penal. *In:* FAYET JÚNIOR, Ney; MAYA, André Machado (orgs.). **Ciências Penais e Sociedade Complexa.** Porto Alegre: Núria Fabris, 2008. pp. 86 a 87 e 94 a 99.

[29] BRASIL. **Decreto-lei Nº 3.689, de 3 de outubro de 1941** (**Código de Processo Penal).** Brasília, 1941. Disponível em: <http://www.planalto.gov.br/CCIVIL/Decreto-Lei/Del3689Compilado.htm>. Acesso em 03 abr. 2009.

MACIEL COLLI é autor do livro *Cibercrimes: Limites e Perspectivas à Investigação Policial de Crimes Cibernéticos* (Editora Juruá, 2010). Advogado em Santa Catarina (OAB/SC 29.785-B). Mestre em Ciências Criminais (PUC-RS). Especialista em Ciências Penais (PUC-RS). Docente da Pós-Graduação (Especialização) em Direito Penal e Processual Penal e da Graduação em Direito na Universidade do Oeste de Santa Catarina (UNOESC). Coordenador Regional, em Santa Catarina, do Instituto Brasileiro de Direito Processual Penal (IBRAPP). Membro do Grupo de Pesquisas, cadastrado no CNPq e vinculado à Pontifícia Universidade Católica do Rio Grande do Sul (PUC-RS), *Processo Penal e Estado Democrático de Direito: a Instrumentalidade Constitucional (Garantista) como Limitação do Poder Punitivo*. Membro do Instituto Brasileiro de Ciências Criminais (IBCCRIM). Currículo *lattes*: http://lattes.cnpq.br/6804979392849552. (*e-mail*: maciel@processopenal.com.br).