JOSÉ RICARDO SIMÕES RODRIGUES

CRIMES DE INFORMÁTICA E A LEGISLAÇÃO BRASILEIRA

LAVRAS
MINAS GERAIS — BRASIL
2004

JOSÉ RICARDO SIMÕES RODRIGUES

CRIMES DE INFORMÁTICA E A LEGISLAÇÃO BRASILEIRA

Monografia apresentada como requisito para obtenção do grau de Especialista em Administração de Redes Linux do Curso de Pós-Graduação *Lato Sensu* em Administração de Redes Linux do Departamento de Ciência da Computação da Universidade Federal de Lavras.

Orientadora:
Professora Msc. Kátia Cilene Amaral Uchôa

Co-Orientador:
Professor Msc. Joaquim Quinteiro Uchôa

LAVRAS
MINAS GERAIS — BRASIL
2004

JOSÉ RICARDO SIMÕES RODRIGUES

CRIMES DE INFORMÁTICA E A LEGISLAÇÃO BRASILEIRA

Monografia apresentada como requisito para obtenção do grau de Especialista em Administração de Redes Linux do Curso de Pós-Graduação *Lato Sensu* em Administração de Redes Linux do Departamento de Ciência da Computação da Universidade Federal de Lavras.

APROVADA em 29 de fevereiro de 2004.

Professora Msc. Kátia Cilene Amaral Uchôa
UFLA
(Orientadora)

Professor Msc. Joaquim Quinteiro Uchôa
UFLA
(Co-Orientador)

Professor Msc. Willian Soares Lacerda
UFLA
(Membro)

Lavras
Minas Gerais — Brasil
2004

"Alguns qualificam o espaço cibernético como um novo mundo, um mundo virtual, mas não podemos nos equivocar. Não há dois mundos diferentes, um real e outro virtual, mas apenas um, no qual se devem aplicar e respeitar os mesmos valores de liberdade e dignidade da pessoa".

Jacques Chirac

Resumo

Novos agrupamentos sociais surgem com a cultura digital. De outra banda, onde há relação social, há norma reguladora. Exsurge dessa nova realidade pelo menos dois novos segmentos do Direito, a saber, o Direito Civil Informático e o Direito Penal Informático. O foco deste estudo é o segundo segmento: o conjunto de normas reguladoras da prevenção, repressão e finalmente punição dos fatos e atos atentadores contra o uso, segurança (sigilo também) e transmissão de informações em sistemas interligados em rede no Brasil.

Sumário

Lista de Figuras

Lista de Tabelas

Lista de siglas e abreviaturas

ANEEL ..... Agência Nacional de Energia Elétrica *Página 81*

ARPA ..... *Advanced Resources Projects Agency* Agência de Pesquisa de Projetos Avançados *Página 14*

BBS ..... *Bulletin Board System* Sistema eletrônico de quadro de avisos *Página 27*

CE ..... *Council of Europe* Conselho da Europa *Página 33*

CERN ..... *European Organization for Nuclear Research* Organização Européia para Pesquisa Nuclear *Página 36*

CERT ..... *Computer Emergency Response Team* Equipe de resposta a emergências computacionais *Página 100*

CF ..... Constituição Federal *Página 95*

CGCE ..... Câmara de Gestão da Crise de Energia *Página 81*

CMA ..... *Computer Missuse Act* *Página 44*

CNUDCI ..... Comissão das Nações Unidas para o Direito Comercial Internacional *Página 69*

CP ..... Código Penal *Página 13*

CPP ..... Código de Processo Penal *Página 88*

DNS ..... *Domain Name Service* Serviço de nomes de domínio *Página 99*

DoS..... *Denial of Service* Negação de serviço *Página 43*

DPN..... Domínio de primeiro nível *Página 18*

ECA..... Estatuto da criança e do adolescente *Página 92*

FAPESP..... Fundação de Amparo à Pesquisa de São Paulo *Página 15*

FBI..... *Federal Bureau of Investigation* Escritório Federal de Investigação *Página 57*

FTP..... *File Transfer Protocol* Protocolo para transferência de arquivos *Página 27*

HC..... *Habeas corpus* *Página 92*

HD..... *Hard disk* Disco rígido *Página 85*

HTML..... *Hypertext Markup Language* Linguagem de marcação de hipertexto *Página 81*

IDS..... *Intrusion Detection System* Sistema de Detecção de Intrusos *Página 90*

IMAP..... *Internet Message Access Protocol* Protocolo para acesso à mensagens da internet *Página 99*

IP..... *Internet Protocol* Protocolo internet *Página 38*

IRC..... *Internet Relay Chat* Rede de Bate-Papo *Página 27*

NBSO..... *Network Information Center BR Security Office* Escritório Brasileiro de Segurança do Centro de Informação de Redes *Página 24*

NSFnet..... *National Science Foundation Net* Rede da Fundação Nacional de Ciência *Página 15*

NTP ..... *Network time protocol* Protocolo de tempo para rede *Página 98*

OEA ..... Organização dos Estados Americanos *Página 26*

RAM..... *Ramdon Access Memory* Memória de acesso aleatório *Página 30*

SMTP ..... *Simple Mail Transfer Protocol* Protocolo simples para transferência de correio *Página 97*

SO ..... Sistema Operacional *Página 30*

SSH..... *Secure Shell* Aviso de comando seguro *Página 99*

SSL ..... *Secure Sockets Layer* Camada de soquetes segura *Página 99*

STF..... Supremo Tribunal Federal *Página 81*

TCP/UDP ... *Transmission Control Protocol/User Data Protocol* Protocolo de controle de transmissão/Protocolo de dados do usuário *Página 98*

UCP ..... Unidade central de processamento *Página 32*

WAP..... *Wireless Application Protocol* Protocolo de aplicação sem-fio *Página 101*

WEP..... *Wired Equivalent Privacy* Uma função do padrão 802.11 que oferece criptografia *Página 101*

WLAN..... *Wireless Local area network* Rede local sem-fio *Página 101*

WWW..... *World Wide Web* Rede de Alcance Mundial *Página 35*

Introdução

O advento da internet[1] possibilitou à sociedade moderna adquirir, armazenar e difundir uma vasta quantidade de informações que vão desde assuntos escolares, pesquisas, culinária até tratados científicos. Como não poderia deixar de ser, questões jurídicas acabam por surgir em meio a essa gigantesca revolução tecnológica.

Dados da United Nation Statistics Division (2003) informam que a internet brasileira possuía, em 2002, 14.300.000 pessoas conectados à rede. Essas novas relações surgidas com o advento da internet trouxeram questões que já deveriam ter começado a ser pensadas e refletidas pelos operadores do direito.

A livre circulação de idéias e manifestação do pensamento nessa mídia eletrônica por excelência surge como o principal valor a ser protegido pelas regras do Direito. Em seguida, ganham corpo as questões tradicional-

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

mente ligadas à propriedade. Propriedade e uso da informação, propriedade e direito autoral no uso de imagem e de criações intelectuais; marcas comerciais e outros signos distintivos.

Por fim, vem à tona as atividades com finalidade lucrativa para a forma digital, ou a circulação de bens intangíveis, transacionados na internet. É o comércio eletrônico.

Além disso, a internet, como se sabe, não possui proprietário e tem como característica principal a liberdade ilimitada de seus usuários. A inexistência, assim, de linhas delimitadoras recai para a circulação da informação digital e o acesso à rede acarretam neo-problemas para a disciplina jurídica. Entretanto uma coisa é certa: esse território existe e não pode ficar imune ao Direito.

Há duas posições diversas quanto à regulamentação da Rede Internacional:

A visão clássica: dizem que a anarquia prepondera na internet, inviabilizando a aplicação de qualquer norma ou princípio do direito;

Visão Norte-Americana: pretendem a aplicação da lei na internet em qualquer das situações. Detalhe: sua própria lei e jurisprudência.

O alerta que se faz é que os abusos cometidos na internet e que hoje são destacados na imprensa como novidade, em pouco tempo podem vir a se tornar rotina, e sendo assim, é de suma importância o preparo dos juristas para esse novo desafio.

O propósito deste trabalho é desenvolver um estudo que possa informar as dimensões desse problema expondo as lacunas existentes em nossa legislação e demonstrar a necessidade da reunião de esforços no sentido de criar uma legislação que impeça a utilização indevida da internet.

Despertada a necessidade de criação de uma legislação para coordenar as relações humanas, impedindo a utilização indevida da internet o autor deste trabalho entende por bem, diante da vasta problemática acerca desse assunto, ater-se à questão dos crimes cometidos via internet e que não são punidos pela legislação penal.

Inclui-se no nosso objetivo específico suscitar breves polêmicas sobre um dos neo-problemas que a informática trouxe para a humanidade e, conseqüentemente, para o Direito em sentido amplo: o aparecimento dos *hackers*, micreiros ou ciberladrões (invasores de contas bancárias, *e.g.*), o que faremos com o enfoque voltado para o Direito Positivo Brasileiro. Para tanto, usaremos como método de trabalho o dedutivo, em que se parte de um conhecimento geral para um particular, onde o nosso tema, referindo-se ao enquadramento do direito na era digital, ficará circunscrita à sua relação com o Direito Penal.

A pesquisa será baseada em dados bibliográficos que enfoquem o tema de forma geral e de forma específica, principalmente, artigos em revistas especializadas, livros e jornais.

Novos agrupamentos sociais surgem com a cultura digital. Tais agrupamentos (clãs *crackers* e *hackers*, *e.g.*) possuem organização própria e fortemente baseada na meritocracia. Os autores das infrações nem sempre buscam vantagens materiais em sua conduta antijurídica. Antes, objetivam transpor as barreiras da rede para buscar satisfação pessoal, reconhecimento do grupo ou com interesses ideológicos. Portanto faz-se necessária pesquisa dos elementos volitivos dos delinqüentes, para uma melhor constituição de instrumentos coercitivos.

A presente investigação justifica-se porque atualmente a legislação pátria possui uma lacuna quando se trata de processar e julgar crimes informáticos. Países como os Estados Unidos da América ou Portugal já regula-

ram a matéria. No Brasil há apenas projetos de lei em discussão na Câmara dos Deputados. A jurisprudência dos tribunais brasileiros é pacífica quanto ao uso dos atuais dispositivos processuais e penais para o processamento e julgamento dos crimes ditos digitais e nosso Código Penal (CP) é datado de 1940 em sua parte especial. Assim, figura-se muito difícil a aplicação de tal parte especial aos crimes puros de informática.

Nossa hipótese é que há possibilidade, sim, de aplicação dos dispositivos penais no processamento e julgamento dos crimes informáticos, mas há, também, uma certa dificuldade na tipificação da conduta do infrator. Há que se fazer, também, uma revisão do conceito de crime pois é inegável a dicotomia entre delito comum e delito de informática. O Direito Criminal da Informática deve ser desenvolvido rapidamente, de modo a serem sistematizadas normas que atinjam os crimes tipificados na prática e que são cometidos com o emprego de computadores e sistemas, desenvolvendo proteção à privacidade, a instrumentalização da produção de provas (inclusive reciclando o próprio conceito de provas).

1 Noções preliminares

1.1 Um pouco da história da internet

Segundo Zakon (2003), um dos marcos principais da história da internet é o ano de 1969 quando a ARPANet comissionada pelo Departamento da Defesa para realizar pesquisa sobre redes constrói uma rede com quatro nós ligando três universidades e um instituto de pesquisa.

É verdade que o embrião da internet nasceu bem antes, durante a guerra fria através de projetos desenvolvidos pelo Departamento de Defesa dos Estados Unidos. A intenção era constituir uma rede de computadores para a comunicação dos principais centros militares de comando que pudessem sobreviver a um possível ataque nuclear e que atendesse a seguintes exigências:

- não fosse vulnerável a ataque militar, pois sendo Washington atacada, outros pontos deveriam estar funcionando;
- não existisse um centro de comando, pois no caso de um ataque o centro seria o primeiro lugar a ser atacado; e
- possuísse flexibilidade para adaptar-se as mais diversas situações possíveis.

Inicialmente, a rede era composta por quatro supercomputadores de laboratórios de pesquisas, a qual foi denominada *Advanced Resources Projects Agency* (ARPA).

A rede mundial de computadores, a internet, passou a ser utilizada nos moldes conhecidos hoje a partir do ano de 1970, quando os pesquisadores começaram a utilizar o correio eletrônico para troca de informações. No ano de 1980, a rede foi dividida em ARPAnet, de caráter civil, e a MILnet, com finalidades militares.

Posteriormente, já em 1985, criou-se a *National Science Foundation Net* (NSFnet) que objetivava interligar todos os maiores centros americanos de pesquisa. Em 1986, a NSFnet e a ARPAnet fundiram-se, dando origem à internet, que foi liberada para uso comercial em 1987, surgindo, então, os primeiros provedores de acesso comercial a partir de 1993.

As primeiras conexões do Brasil foram feitas em 1988, pela Fundação de Amparo à Pesquisa de São Paulo (FAPESP) e pelo Laboratório Nacional de Computação Científica do Rio de Janeiro, criando-se uma Rede Nacional de Pesquisa em 1989 pelo Ministério da Ciência e Tecnologia. A utilização comercial da internet no Brasil ocorreu no ano de 1995, facultando-se as empresas denominadas provedores de acesso comercializar o acesso à rede mundial de computadores.

A internet é uma gigantesca rede mundial de computadores em que não há um único lugar que a controla, sua organização se dá através dos administradores das redes que a compõe e dos próprios usuários. Os computadores conectados a internet estão ligados através de linhas comuns de telefone, linhas de comunicação privada, cabos submarinos, canais de satélite e diversos outros meios de telecomunicação.

Não há dúvidas que a sociedade mundial tem sofrido e vai sofrer

grandes mudanças sociais e culturais radicais nos próximos anos em razão desse fenômeno denominado internet, já podendo ser considerada como um dos mais revolucionários eventos da história da humanidade.

1.2 Importância da internet

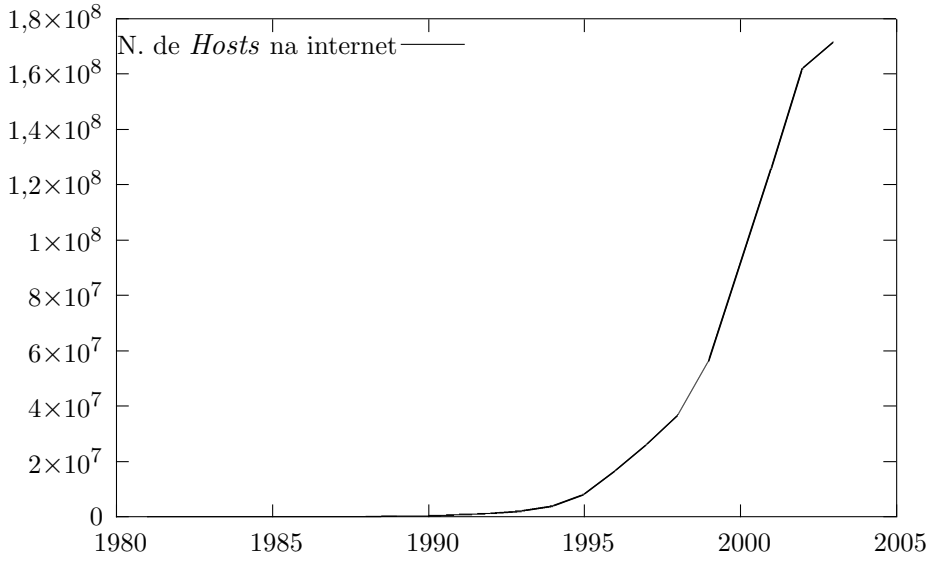

Figura 1: Pesquisa por domínios da internet - Número de *Hosts* na internet

Fonte: Internet Software Consortium (2003).

Há quem diga que o século XX, foi o que mais propiciou as mais relevantes transformações na história da humanidade.

As formas de comunicações inventadas foram as mais diversas, note-se que há 500 anos surgiu a imprensa; há 160 anos, o telégrafo; há 120 anos, o telefone; há 95 anos, o rádio e há 50 anos, a televisão. As mudanças no mundo se fazem de forma exageradamente rápida, a partir das quais surgem inovações das mais variadas, as quais permitem ao homem melhor conviver

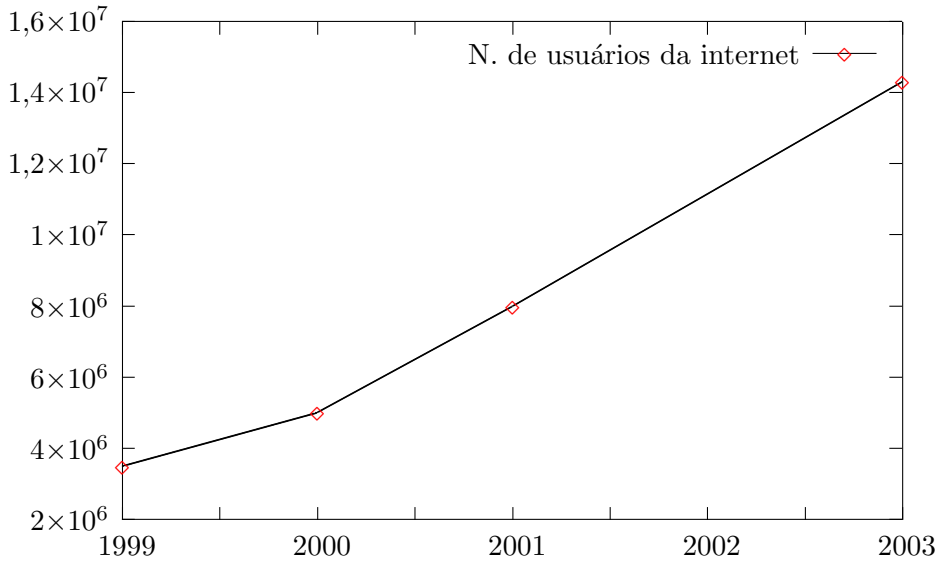

Figura 2: Crescimento do N. de usuários da internet no Brasil

Fonte: United Nation Statistics Division (2003).

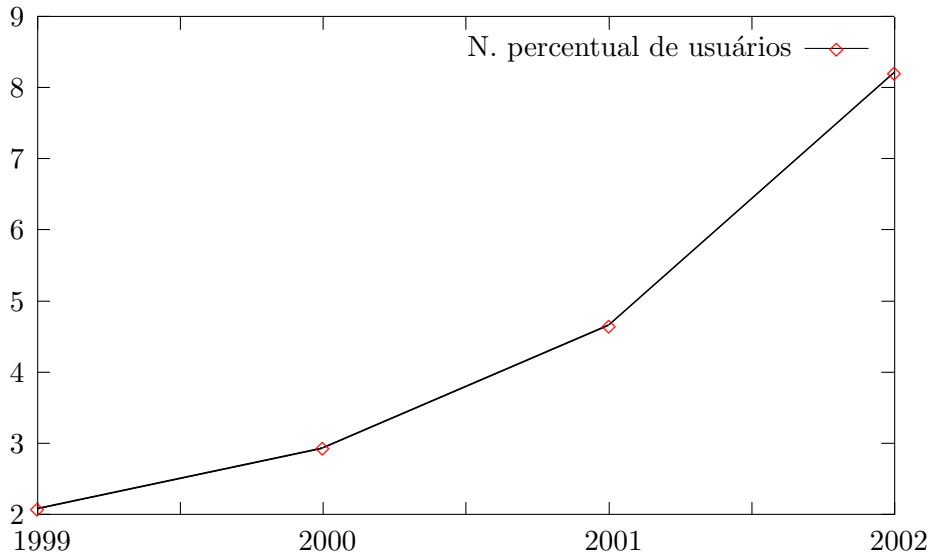

Figura 3: N. de usuários da internet no Brasil a cada cem brasileiros

Fonte: United Nation Statistics Division (2003).

e melhor conhecer a si e a seus semelhantes.

Essa revolução da humanidade é relatada por Losso (1998) da seguinte forma:

> De fato, da então revolucionária máquina de escrever evoluiu-se aos poderosos computadores; do rangedor carro de bois aos céleres aviões supersônicos; do engenhoso gramofone aos fidelíssimos sons dos CDs; do rádio de fugitivas ondas à eficiente televisão digital; do temível bisturi às cirurgias a *laser*; dos documentos copiados em bem desempenhadas letras góticas ao fantástico fax; ao então inovador telégrafo sem fio à impressionante internet; do mecanismo cartesiano ao pensamento sistêmico.

O fenômeno da informatização, o qual encontra-se consolidado em nossa sociedade, passou a ter ainda maior importância nos últimos anos, pois aumentou a quantidade de usuários da internet, corroborando a assertiva de que a rede mundial tornou-se um evento cada vez mais presente no nosso cotidiano.

Dados da United Nation Statistics Division (2003), dão conta de que no Brasil existam quatorze milhões e trezentos mil usuários da rede. Nos gráficos das figuras 2 na página 20 e 3 na página precedente visualizamos o crescimento desse número.

O crescimento da informação disponível só foi possível em razão de fatos ocorridos no campo do processamento eletrônico de dados e no de computadores. A expansão dessa informação tem se dado em razão da criação dessa enorme Rede Internacional que permite aos computadores compartilharem serviços e comunicarem-se diretamente como se fossem parte de uma grande engrenagem. Esse instrumento de comunicação tem atingido proporções sem precedentes, vide as tabelas 3 na página 24, 2 na próxima página e 1 na página seguinte.

A utilização da internet surgiu diante do mundo de informações, cu-

Tabela 1: Domínios registrados por DPN

DPN	Quantidade	%
COM.BR	485129	91,16
ORG.BR	14943	2,81
IND.BR	3575	0,67
ADV.BR	3405	0,64
NOM.BR	2023	0,38
Outros	23037	4,36
Total	532112	-

Fonte: Comite Gestor da Internet no Brasil (2003a). Posição em 10/12/2003.

Tabela 2: Número de *Hosts* na América do Sul

Posição	País	*Hosts*
1º	Brasil (.br)	2.237.527
2º	Argentina (.ar)	495.920
3º	Chile (.cl)	135.155
4	Uruguai (.uy)	78.660
5º	Colômbia (.co)	55.626
6º	Venezuela (.ve)	24.138
7º	Peru (.pe)	19.447
8º	Paraguai (.py)	4.351
9º	Equador (.ec)	2.648
10º	Bolívia (.bo)	1.413

Fonte: Comite Gestor da Internet no Brasil (2003b). Posição em janeiro de 2003.

Tabela 3: Posição dos Países por Número de *Hosts*

Posição	País	*Hosts*
1º	Estados Unidos	120.571.516
2º	Japão (.jp)	9.260.117
3º	Itália (.it)	3.864.315
4º	Canadá (.ca)	2.993.982
5º	Alemanha (.de)	2.891.407
6º	Reino Unido (.uk)	2.583.753
7º	Austrália (.au)	2.564.339
8º	Holanda (.nl)	2.415.286
9º	Brasil (.br)	2.237.527
10º	Taiwan (.tw)	2.170.233

Fonte: Comite Gestor da Internet no Brasil (2003b). Posição em Janeiro de 2003.

riosidades e lazer a que o usuário tem acesso dos mais variados e inusitados pontos do planeta. Com isso têm-se verificado uma miscigenação de culturas, dados e descobertas numa velocidade espantosa.

A importância da rede é tamanha que a mídia sempre a tem em pauta, dando origem a revistas especializadas e encartes próprios nos jornais e revistas, demonstrando que é impossível ficar alheio a essa tecnologia, mormente diante da globalização.

O uso do computador é necessário em todos os segmentos econômicos e sociais e, por isso, o direito não poderia ficar ausente a essa nova realidade. A Rede Mundial de Computadores tem servido de instrumento à educação, tornado o computador, na mão de professores capacitados, um excelente meio de ensino.

No Brasil, advogados e clientes com interesses em decisões do Supremo Tribunal Federal, poderão acessar *site* com fins a obter a íntegra do acórdão desejado; em São Paulo, a Polícia Civil aceita ocorrências pelo computador. Enfim, essa rede pode desburocratizar o serviço público e permitir

ao cidadão exercer a plenitude de seus direitos. As compras realizadas na internet vão de CDs a carros, sendo a parte mais visível e colorida da era do comércio eletrônico.

1.3 Conceito jurídico de internet

A internet, ainda segundo Losso (1998), pode ser entendida como:

> Uma rede transnacional de computadores interligados com a finalidade de trocar informações diversas e na qual o usuário ingressa, por vários meios, mas sempre acaba por realizar fato jurídico, gerando conseqüências inúmeras nas mais diversas localidades.

Já para Willing (1997, p. 30), a definição de internet é a seguinte:

> A internet é uma rede mundial, não regulamentada, de sistemas de computadores, conectados por comunicações de fio de alta velocidade e compartilhando um protocolo comum que lhes permite comunicar-se.

Da primeira definição extraímos os seguintes elementos:

- a formação de uma rede que não está restrita a apenas um país. As informações dentro da rede cruzam as fronteiras virtuais de vários países sem quaisquer barreiras ou limitações, acionando-se os mais variados ordenamentos jurídicos;
- vários são os objetivos da internet, que vai do entretenimento até o uso comercial da informação;
- o acesso do usuário pode ser feito por meio de um *notebook*, computador pessoal ou terminais públicos situados em bibliotecas, todos conectados através de modem, placas de rede ou outro dispositivo de interface;

- o usuário da rede pode praticar ato jurídico até pelo simples recebimento de um *e-mail* ou a visualização de uma página, uma vez que tal ato pode gerar conseqüências variadas.

Da última definição, o elemento mais importante é a não regulamentação. Esse elemento é que traz problemas sob o aspecto jurídico, pois a falta de regulamentação legal dificulta inibir os abusos que eventualmente ocorram na utilização da internet.

1.4 A internet e os tribunais

Segundo o art. 5º, inciso XXXV, da Constituição Federal do Brasil, a norma legal jamais poderá excluir da apreciação do Poder Judiciário quaisquer lesões ou ameaças a direito que o cidadão venha sofrer. Tal princípio, denominado doutrinariamente de *princípio da inafastabilidade*, assunto mais detidamente analisado na seção 3.2.2.3 na página 77, resumidamente, força o Judiciário a apreciar qualquer tipo de questão que seja levada aos seus Tribunais, mesmo que não haja qualquer norma sobre tal questão.

1.5 Existe um Direito da Informática?

A práxis muitas vezes antecede a discussão de sua validade. Por exemplo, a utilização da terminologia *Direito da Informática* se tornou muito comum antes mesmo de se discutir se este conjunto de termos é correto. Nas adjacências desse tema, existem outros de importância complementar, os quais serão discutidos a seguir.

1.5.1 Direito da Informática e Informática Jurídica

Direito da informática é um ramo de atuação normativa coerciva, como boa parte do Direito, e estatal, objetivando um dever-ser da conduta, através de uma técnica social específica visando um fim social. Informática jurídica é uma técnica do ramo da informática voltada à prática do direito, desenvolvendo o que a informática tem de mais útil para as atividades relacionadas ao direito, na qual se destaca, por enquanto, os *Software*, bastante popularizados perante a comunidade jurídica.

Materialmente, os objetos do direito da informática são o *hardware* (base rígida), *software*[1], redes, etc. Obviamente, não serão todos os materiais produzidos pela informática ou para a informática tratados como bens jurídicos, apenas aqueles com relevância e repercussão jurídica, destacando-se entre estes os que possuem destaque social, seja positiva ou negativamente, na forma econômica ou sentimental, à longo ou curto prazo, como uma atividade nova ou um novo meio prático para realização de atividades antigas. Logicamente, os seus usos, efeitos, finalidades e atividades correlatas deverão ser analisados pelos intérpretes e construtores do direito para a correta avaliação da sua importância no sistema social.

A informática veio trazer ao mundo do direito muitas inovações, quase todas positivas. É possível, hoje, remeter peças judiciais através de diversos aparelhos eletrônicos, parcela relevante dos nossos bancos de dados foi substituída por meios de armazenamento eletrônico, diminuindo substancialmente o espaço físico necessário para o funcionamento de um escritório ou repartição pública, além de variados materiais voltados especificamente à gestão dos negócios, diminuindo o tempo gasto pelos operários do direito na sua rotina habitual, facilitando e democratizando o acesso à informação acerca do trâmite processual, por exemplo.

[1] Não se excluindo desta acepção o *vírus*, como qualquer outro programa executável

1.5.2 Formas de Organização do Direito

O Direito se organiza em diferentes ramos utilizando-se de três formas principais.

A organização pedagógica, a primeira a ser aqui tratada, é um tipo de organização voltada ao modo de ensino, que, por razões óbvias, pode ou não se auxiliar dos outros dois modos de organização. A divisão neste sistema não é complexa, ou seja, as matérias estão dispostas de forma a se integrar entre si numa visão ampla e preliminar sobre o direito, com limitações no que tange a aplicação do direito na vida prática. Aqui, nesta organização, destacam-se matérias propedêuticas que auxiliam na compreensão dos fenômenos jurídicos, e que não fazem parte objetiva do sistema normativo.

A segunda forma de organização deriva-se da análise científica, é uma organização sistemática do tema, em especialidade de matérias. Nesta, estão destacadas diferentes campos, sendo imprescindível que cada tópico possua certa autonomia perante aos demais, com campo normativo e científico próprio, além de pesquisadores especialmente dedicados ao objeto em análise, se caracterizando por um conjunto de princípios e institutos relativamente independentes perante o conjunto legislativo. Logicamente, nesta independência se respeita a hierarquia e complementaridade (seja analogicamente ou diretamente) que as diferentes áreas normativas fornecem a outras. Assim, pode-se perceber que um mesmo objeto material, como o comércio, por exemplo, pode ser analisado sobre diferentes pontos de vista normativos, sem que haja qualquer conflito normativo. Muito embora os diferentes planos no mundo concreto possam se mostrar inseparáveis e coesos, na abstração, cada um destes tópicos possui uma distinção que deriva ou do interesse científico, ou do interesse social, que, através do legislador, preferiu distinguir determinado campo com princípios e normas próprias para uma

atuação mais coerente com a vontade social.

A terceira e última forma que trataremos se refere a uma organização problemática. Nesta organização, não está evidente a independência científica, mas, na verdade, o estudo de campos do direito de forma interrelacionada visando uma determinada função social, solucionando um determinado problema. Assim surgem as expressões: direito empresarial, do consumidor, rural, industrial, comercial, e também o Direito da Informática, como um conjunto de materiais úteis a estas estruturas sociais.

Com espeque nas definições supra, temos que o direito da informática é na verdade parte da ciência jurídica responsável por regulamentar as informáticas, atuando, assim, em diversos outros ramos do direito:

Material e processual civil: assinatura digital, contratos no mundo virtual; registro de domínios; seguro de bens virtuais ou informatizados; responsabilidade civil, perturbações em geral, invasão da privacidade e destruição de propriedade virtual ou informatizada; provas ilícitas; direitos autorais sobre *software* e *hardware*; controle legal do conteúdo e forma dos *Software*; competência territorial; *juntada* regular de documentos; ciência e prazos; atividades irregulares no processo; composição judicial por meios eletrônicos;

Penal: diferenciação dos crimes de informática puros e impuros; valoração e pena; discussão acerca da tipicidade ou inaplicabilidade de dispositivos velhos em atividades realizadas através de aparelhagem eletrônica, classificação dos criminosos pelo tipo aplicável, competência territorial em crimes à distância, por exemplo;

Tributário: tributação de atividades econômicas realizadas por via eletrônica, distinção das atividades, aplicação ou não de certas normas tributárias; incidência tributária territorial; regulamentação e legiti-

mação da informática como uma forma de pagamento, declaração de tributos;

Trabalhista: no *networking*, ou trabalho realizado à distância através de instrumentos informatizados; incidência legislativa em se tratando de *networking* em diferentes países.

Vemos que o direito da informática não é um ramo autônomo, mas um conglomerado atípico dos mais variados campos legislativos, resultado da revolução tecnológica pela qual passa nossa sociedade contemporânea. Pode parecer que a autonomia derive das modificações sociais que reclamam novos princípios e normas, mas a revolução tecnológica é a mais recente fase da revolução industrial, que se desenvolve para exigir nova postura frente às atividades sociais eminentemente inovadoras, cujo tratamento, apesar de se tornar especial em determinadas ocasiões, não se distingue em essência das outras atividades e estruturas existentes cujo tratamento se dá pelas matérias clássicas do Direito moderno.

1.6 A legislação e a internet

A história tem demonstrado que as condutas humanas evoluem no decorrer do tempo. Dessas novas condutas surgidas algumas podem não ser desejáveis para a sociedade ou para o Estado. É bem verdade que o Estado está sempre atento a essas novas condutas e busca os meios necessários (edição de regulamentos incriminadores) para desestimular sua prática e aplicar sanções, quando tratarem-se de condutas criminais.

Pinheiro (2000) nos relata o seguinte:

> No final do século XIX um cidadão alemão foi preso acusado de furto de energia elétrica. Os advogados do acusado, entretanto, observaram que não existia na legisla-

> ção penal alemã tal delito, pois a energia elétrica não tinha status de coisa, e somente coisa poderia ser passível de furto. O tribunal absolveu o réu ao entender que a lei penal não permite interpretação analógica. Com isso, o legislador alemão providenciou logo um dispositivo legal que tipificasse como crime o furto de energia elétrica, pois sem a mesma, aqueles que viessem a desviar a energia elétrica ficariam impunes.

Atento à atualidade, Pinheiro (2000) continua e nos informa que :

> Pouco mais de um século se passou e nossos tribunais se deparam com um problema que, em tese, é bem semelhante ao vivido pela Alemanha. Com a popularização da internet em todo o mundo, milhares de pessoas começaram a se utilizar deste meio. Contemporaneamente se percebe que nem todos a utilizam de maneira sensata, e acreditando que a internet é um espaço livre, acabam por exceder em suas condutas fazendo surgir com isso novas modalidades de delito: os crimes de informática.

Os gráficos das figuras 5 na página 34 e 4 na página 33 mostram algumas estatísticas referentes ao crescimento de incidentes de segurança reportados ao *Network Information Center BR Security Office* (NBSO), corroborando a afirmação de Pinheiro (2000) acerca do crescimento da deleinqência na rede mundial de computadores.

Estas condutas delituosoas, novidades que são ao nosso ordenamento jurídico, são interpretadas, na opinião de Pinheiro (2000), como todos os atos ilícitos praticados mediante uso de recursos da rede internet ou outra rede e que venham a causar algum tipo de dano, seja ele patrimonial ou moral, ao ofendido.

Os assim ditos *Cibercrimes* podem ser classificados em delitos de informática puros, mistos e comuns, segundo a classificação encontrada na seção 2.5 na página 64.

Devido ao vácuo existente em nossa legislação, há possibildiade de

se punir apenas crimes de informática que estejam previstos na legislação incriminadora existente, no caso, os crimes de informática mistos.

O Estado Brasileiro, atendendo aos anseios da sociedade e às pressões internacionais[2], está em vias de unir-se ao pequeno grupo de países que conta com legislação específica para a punição de crimes de informática.

A comissão de Ciência e Tecnologia, Comunicação e Informática da Câmara dos Deputados aprovou, em novembro de 2003, a Redação Final oferecida pelo Relator, Dep José Ivo Sartori, para o Projeto de Lei de N. 84/99[3] de autoria do deputado Luiz Piauhylino (PSDB-PE), presidente da comissão, e que define os crimes cometidos na área de informática.

Tal Projeto de Lei atualmente encontra-se no Senado Federal[4], em atenção ao bicameralimo existente no processo legislativo brasileiro.

As ações dos *crackers*, de apagar, destruir, modificar ou inutilizar total ou parcialmente, dado ou programa de computador, de forma indevida ou não autorizada deverão serem punidas com um a três anos de detenção e multa[5].

Para Pinheiro (2000), deve-se levar em consideração sim, a urgência que se perfaz em nosso contexto, mas sobretudo, não se pode permitir que o Estado, sob o pretexto de atribuir maior segurança aos usuários da rede,

[2]Na Reunião de Ministros da Justiça e procuradores dos países integrantes da OEA realizada em março de 2000, um dos principais temas foi a criação de mecanismos para coibir a ação criminosa na internet.

[3]O andamento do Projeto de Lei na Cãmara dos Deputados pode ser consultado em `http://www.camara.gov.br/Internet/sileg/Prop_Detalhe.asp?id=15028`.

[4]O andamento do Projeto de Lei no Senado pode ser consultado em `http://www2.senado.gov.br/sf/atividade/Materia/Detalhes.asp?p_cod_mate=63967`.

[5]Ementa do Projeto de Lei 84/99: Altera o Decreto-Lei N. 2848, de 07 de dezembro de 1940 - Código Penal e a Lei N. 9296, de 24 de julho de 1996, e dá outras providências. Dispõe sobre os crimes cometidos na área de informática, e suas penalidades, dispondo que o acesso de terceiros, não autorizados pelos respectivos interessados, a informações privadas mantidas em redes de computadores, dependerá de prévia autorização judicial.
Trata-se, portanto, de Lei que altera o Código Penal Brasileiro.

viole os direitos de liberdade de expressão do cidadão.

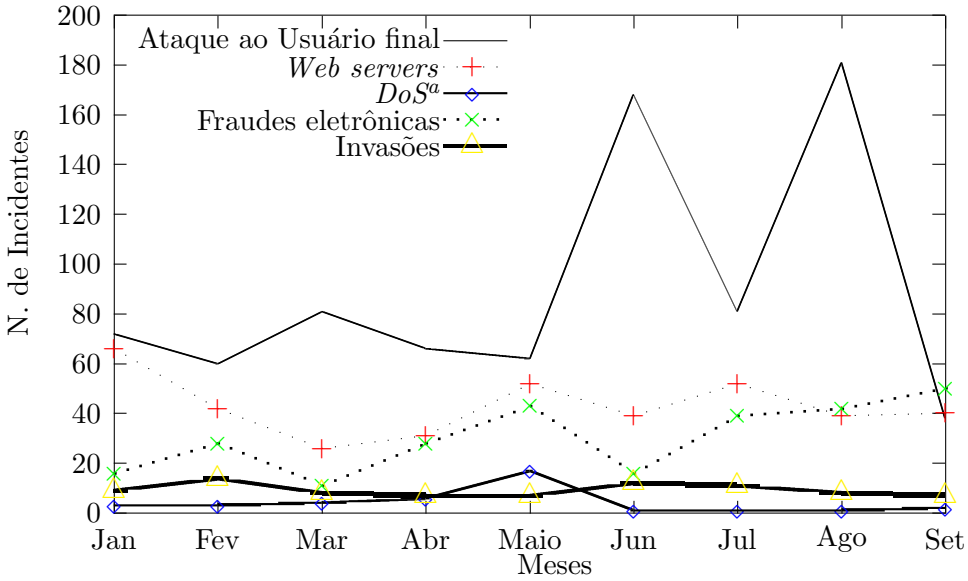

Figura 4: Incidentes reportados ao NBSO (Ataque ao Usuário final, *Web Servers*, *DoS*, fraudes e invasões) - Janeiro a Setembro de 2003

Fonte: NIC BR Security Office (2003a).

[a] *Denial of service*, negação de serviço. Ataque que consiste em sobrecarregar um servidor com um alto volume de requisições, provocando sua queda.

1.7 A legislação e o Direito Penal da informática

O Direito Penal de Informática caracteriza-se pela sua absoluta pobreza. A Parte Especial do CP data de 1940 e as normas incriminadoras são de um tempo em que sequer existia o computador, de modo que as normas vigentes somente podem ser aplicadas aos crimes de informática de forma incidental a tais hipóteses.

O legislador brasileiro somente preocupou-se com o mau uso do com-

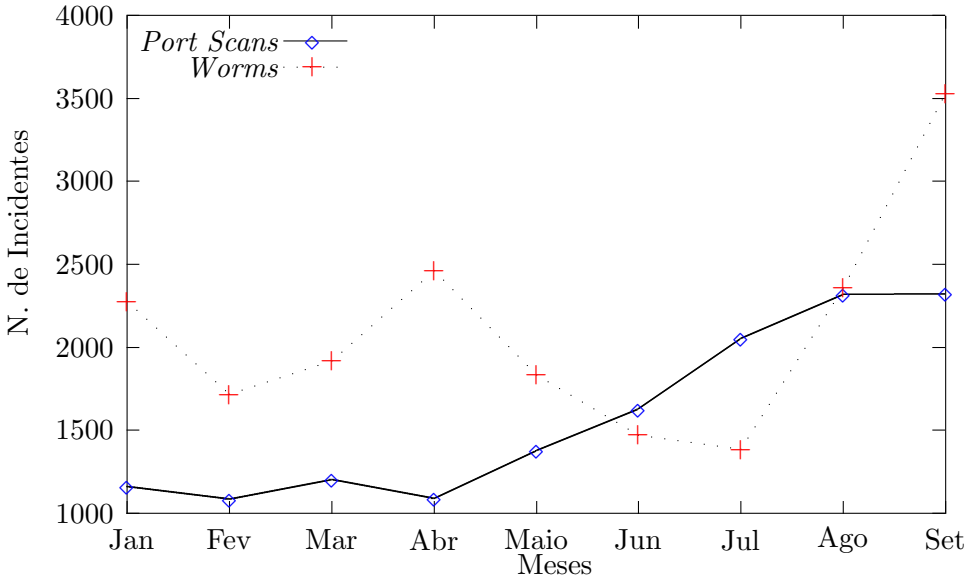

Figura 5: Incidentes reportados ao NBSO (*Port Scans* e *Worms*)- Janeiro a Setembro de 2003

Fonte: NIC BR Security Office (2003a). Janeiro a setembro de 2003.

putador, vez que a legislação existente dirige-se especificamente à pirataria de *software*, talvez por causa dos *lobbies* da indústria, jamais ao crime de informática por excelência, vide (BRASIL, 1998b) e (BRASIL, 1998a).

Também os doutrinadores brasileiros acompanham a tendência internacional que protege o *software* ao entendimento do que seja direito autoral. O legislador aceita essa posição. Para tanto, a Lei 7.646, de 18 de dezembro de 1987[6], definiu em seus artigos 35 e 37 dois crimes que expressam esse entendimento:

> Art. 35 - Violar direitos de autor de programas de computador:
> Pena: Detenção, 6 (seis) meses a 2 (dois) anos e multa.
> Art. 37 - Importar, expor, manter em depósito, para fins de comercialização, programas de computador de origem externa não cadastrados:
> Pena: Detenção, de 1 (um) ano a 4 (quatro) anos e multa.

O artigo 35 retrata, com clareza meridiana, o objetivo do legislador em proteger o direito autoral, sem, contudo, mesmo assim, ser caracterizado como um crime de informática, e, sim, crime contra o direito autoral.

O artigo 37 cria a figura típica de contrabando de informática. O objeto jurídico é, tão somente, o erário público, prejudicado pela evasão da renda e da proteção dos *software* nacionais. Também, a norma carrega a amplitude da incidência genérica, tal como, no artigo 334 do CP, o delito de contrabando e descaminho.

Pela simples leitura, vê-se que as regras legais citadas são manifestamente imperfeitas e insuficientes para os fins que se destinam. Tanto assim, que com a mudança em matéria de política de informática, o delito de contrabando de *software* não cadastrado já não tem mais razão de existir, vez que, hoje, não mais é necessário que seja cadastrado junto ao órgão

[6]Tal lei foi revogada expressamente pela Lei N. 9.609 de 19 de fevereiro de 1998 (Lei do *Software*) que regula a mesma matéria.

competente.

Ainda, ao apreço da norma nacional, que tem por finalidade, apenas, proteger a propriedade intelectual, em relação ao programa de computador, como manifestação de propriedade imaterial, fazendo-o da mesma forma que o CP o faz, para a violação do direito autoral em geral. Todavia, a pena prevista é, em muito mais gravosa que a determinada pela Lei Penal (detenção de três meses a um ano e multa).

O sistema legal ainda contempla proteção às condutas lesivas contra a ordem econômica e contra as relações de consumo. No âmbito da ordem tributária, a Lei N. 8.137 de 27 de dezembro de 1990, define uma nova forma de mau uso do computador, qual seja, ação de utilizar ou divulgar programa de processamento de dados que permita ao contribuinte possuir informação contábil diversa que é , por lei, fornecida à Fazenda Pública, sendo apenado com detenção de seis meses a dois anos e multa. É, pois, um programa de computador destinado a permitir a fraude fiscal.

Ante essa paupérrima legislação, o aplicador do direito é obrigado a servir-se dos delitos tradicionais para o combate aos crimes de informática, dada a inexistência de lei específica para a tutela dos sistemas informáticos ou redes de computadores. Têm-se que muitas das condutas que caracterizam os crimes de informática, poderiam ser enquadradas na figura típica do estelionato ou invasão de privacidade.

Todavia a velocidade do desenvolvimento tecnológico no setor de informática, não garante que se possa, eternamente, manter a aplicação do nosso CP, ou seja, o enquadramento dos crimes comuns às condutas típicas do delitos de informática. Some-se a essa dificuldade presente, as diversas doutrinas e correntes que pululam a matéria criminal de informática, e mais, as próprias divergências em torno da aplicação do Direito Alternativo e a corrente que defende programa de descriminalização, que vertem profundas

dificuldades ao aplicador do direito.

1.8 Perfil médio do autor de delitos de informática

Trata-se da figura do criminoso digital, cujo perfil é diverso daqueles que se utilizam de uma arma branca ou de fogo para intimidar ou assaltar pessoas, por ser alguém geralmente jovem, muito inteligente, que senta confortavelmente atrás de uma máquina, e com alguma paciência pode dar desfalques milionários em bancos, surrupiar cartões de crédito de cidadãos inocentes ou até deixar um estado inteiro sem energia elétrica.

1.8.1 Tipos de sujeitos ativos

Os cibercriminosos são verdadeiros fanáticos pela informática, cujo passatempo preferido é interceptar mensagens digitais e/ou invadir os computadores alheios, descobrindo segredos e, algumas vezes, até mesmo deixando instituições bancárias, industriais ou militares em verdadeiro pânico. Alguns deles são apenas amadores em busca de diversão e emoções fortes. Outros sem embargo, possuem índole diversa, e são fraudadores, espertalhões modernos que desejam auferir vantagem ilícitas, como por exemplo surrupiar contas bancárias, ao adentrarem nos sistemas de instituições financeiras, ou roubarem segredos industriais.

No jargão dos iniciados, um jovem que recentemente ganhou um computador e já quer invadir o Pentágono com programinhas simples, obtidos na internet (as chamados receitas de bolo), é chamado de *lamer* e além de ser relativamente inofensivo, é desprezado por quem entende de informática.

Há, também, os famosos *hackers* que na verdade são jovens que tem conhecimentos reais de programação e de sistemas operacionais de computadores, conhece as falhas do sistema de segurança e, por diversão (como

uma espécie de desafio), procura conhecer novas falhas e usa técnicas próprias de invasão, desprezando as ditas *receitas de bolo*, além de não gostarem de ser confundidos com criminosos, pois limitam-se a invadir sistemas pelo prazer de ultrapassar as barreiras lhe impostas, sem todavia, destruírem os mesmos ou se utilizarem das informações pessoais para fins pessoais ou de terceiros.

Os verdadeiros criminosos são os chamados *crackers*, conhecidos também como *hackers* aéticos, aqueles que invadem sistemas, roubam arquivos, destroem discos rígidos, espalham vírus, fazem espionagem industrial e lavagem de dinheiro sujo internacional. Este é o indivíduo nocivo a sociedade digital do novo milênio, pois as polícias e a sociedade ainda não estão preparadas para contê-los.

Aliás, o termo *cracker* foi cunhado em 1985 pelos próprios *hackers*, como inequívoco objetivo de não serem confundidos com aqueles. Segundo definição de Neto (2000), *crakers* são aqueles que rompem a segurança de um sistema em busca de informações confidenciais com o objetivo de causar dano ou obter vantagens pessoais.

Há grandes diferenças entre os *hackers* e os *crackers*, sendo aquele atiçado exclusivamente pelo desafio intelectual de romper as defesas de um sistema operacional e aí encerrar sua batalha mental, já o segundo inicia sua batalha quando do rompimento das defesas do sistema operacional sob ataque, tendo em vista a obtenção de benefícios para si ou para outrem, sempre em dentrimento de terceiros.

Por fim, os *phreakers* são especialistas em fraudar sistemas de telecomunicações, principalmente linhas telefônicas convencionais e celulares, fazendo uso desses meios gratuitamente ou às custas de terceiros. Muitos *crackers* são também *phreakers*: procuram modos de fazer repetidas conexões a computadores que estão atacando sem pagar por elas, bem como

tornar difícil ou impossível o rastreamento de suas atividades.

Há ainda os *cyberpunks* e os *cyberterrorists*, que desenvolvem vírus de computador perigosos, como os *Trojan horses* (cavalos de Tróia) e as *Logic bombs*, com a finalidade de sabotar redes de computadores e em alguns casos propiciar o chamado *Denial of Service* (DoS), com a queda dos sistemas de grandes provedores, por exemplo, impossibilitando o acesso de usuários e causando prejuízos econômicos.

O cibercrime é, sem dúvidas, um fruto da globalização, de um planeta que passa a não ter fronteiras e nem distâncias, em que não há alfandegas para o tráfego da informação, fazendo surgir a figura do sociopata anônimo que usa o computador para dar vazão ao seu ego em busca da fama, ainda que apenas pelo seu codinome, mesmo que ela provenha da invasão dos *sites* do Pentágono, da quebra de sigilo telefônico de sua cidade, com a interrupção do sistema de metrô de Nova Iorque ou o desvio de rota de um satélite de telecomunicações. O que importa é o impacto do feito a divulgação do mesmo.

Embora no submundo cibernético essas diferentes designações ainda façam algum sentido e tenham importância, o certo é que, hoje, para a grande maioria das pessoas, a palavra *hacker* serve para designar o criminoso eletrônico, o ciberdelinqüente. E isto mesmo na Europa e nos Estados Unidos, onde já se vem abandonando a classificação um tanto quanto maniqueísta acima assinalada, vide, a esse propósito, o *Computer Missuse Act* (CMA), de 1990[7], que, seguindo esse caminho, procurou qualificar dois tipos de *hackers*:

O *inside hacker*: indivíduo que tem acesso legítimo ao sistema, mas que o utiliza indevidamente ou exorbita do nível de acesso que lhe foi permi-

[7]Lei britânica sobre crimes informáticos, aprovada pelo Parlamento.

tido, para obter informações classificadas. Em geral, são funcionários da empresa vítima ou servidores públicos na organização atingida;

O *outsider hacker*: que vem a ser o indivíduo que obtém acesso a computador ou a rede, por via externa, com uso de um *modem*, sem autorização.

1.8.1.1 O perfil do sujeito ativo

O perfil do criminoso, baseado em pesquisa empírica, indica jovens inteligentes, com um bom nível de escolaridade, com idade entre 16 e 32 anos, do sexo masculino, caucasianos, audaciosos e aventureiros, com inteligência bem acima da média e movidos pelo desafio da superação do conhecimento. Além do sentimento de anonimato, que bloqueia seus parâmetros de entendimento para avaliar sua conduta como ilegal, sempre alegando ignorância do crime e, simplesmente, uma brincadeira.

Segundo Leite (1999), é possível descrever as principais características daqueles que praticam crimes por computador, na atualidade. Os dados tomados por ele referem apenas a agentes internos de empresas e não a *crackers* ou *hackers*, mas merecem ser analisados:

- Idade: 18 a 35 anos;
- Sexo: masculino, na maioria;
- Função: administrador de alto nível;
- Perfil: estável no emprego, brilhante, ativo, motivado, diligente, de confiança (acima de qualquer suspeita), laborioso, primeiro a chegar e o último a sair, não tira férias, zeloso com relações pessoais, preocupado com a manutenção do prestígio, individualista, gosta de resolver problemas de forma independente;

- Antecedentes Criminais: nenhum;
- Método: executando uma ação ordinária no curso de uma operação de sistema normal e legal, como por exemplo: cálculo de salário, contas a receber, pagamentos de fornecedores, transferência de fundos, etc.
- Reações ao ser apanhado:
  - *Isso não é crime*
  - *Eu não prejudiquei ninguém*
  - *Todo mundo faz isso*
  - *Eu apenas tentei demonstrar ao meu superior que isto é possível ser feito*

Costa (1998), estudando o perfil do delinqüente de informática, inclusive as condutas dos *crackers* e dos *hackers*, diz que é inequívoca a idéia de que esses criminosos digitais são sempre *experts*, detentores do conhecimento necessário ao cometimento do ilícito de informática.

Dispõe, ainda, o estudo do referido advogado que:

> Através das inumeráveis compilações que circulam pelo mundo da informática, são os crimes dessa espécie cometidos à égide da *special opportunity crimes*, qual sejam, os crimes afeitos à oportunidade, perpetrados por agentes que tem a sua ocupação profissional ao manuseio de computadores e sistemas, em várias atividades humanas, e em razão dessa ocupação cometem delitos, invariavelmente, contra seus empregadores. (COSTA, 1998)

A conclusão que se chega quando comparamos os diversos estudos sobre esse tipo de delinqüente é que em qualquer parte do mundo eles mantém esse perfil, que dificulta ao máximo que seja surpreendido em ação delituosa ou que se suspeite dele.

2 Natureza jurídica do Direito Informático

2.1 Sistemas computacionais

Ressaltamos, antes de adentrarmos na definição de sistema de computador, que são distintos os conceitos de sistema de computador e sistema operacional. Além dessa terminologia, o sistema operacional possui outras pouco usuais: sistema supervisor, sistema monitor, e sistema de executivo.

Barron (1973, p. 11) diz que o Sistema Operacional (SO) é um dos principais componentes do computador e foi desenvolvido como resposta à necessidade de maximizar a utilização do processador central e dos dispositivos periféricos. Com exceção das máquinas pequenas, é impossível operar um computador se, no mesmo, não existir algum tipo de sistema. Da mesma forma, um sistema danificado pode causar efeitos negativos à capacidade de processamento da máquina. Os SOs proporcionam ainda uma maior comunicabilidade entre os usuários e o computador.

Para mostrar quanto os sistemas operacionais revolucionaram o campo da computação, ainda Barron (1973, p. 11-12) relata de que modo era realizada a operação do computador antes do advento dos sistemas operacionais, demonstrando o quanto era penoso operar um computador antes de criarem os sistemas operacionais. Além de operar, o usuário tinha que entender também de programação, o que dificultava muito o acesso das pessoas leigas

ao computador (basta lembrar dos lendários cartões perfurados).

Tendo já conhecimento de algumas funções dos sistemas operacionais, pode-se definí-lo como sendo um programa de computador que, após ser carregado (*loaded*) no computador por meio de um processo chamado de *boot*[1], controlará todos os outros programas daquele computador. Estes outros programas são chamados de programas aplicativos. Os aplicativos, por seu turno, fazem uso do sistema operacional para realizar as tarefas[2] solicitadas pelos usuários externos.

Guimarães (1989, p. 12), acerca do SO, nos apresenta o seguinte conceito:

> Sistemas operacionais são simplesmente uma coleção de programas inteiramente análogos aos de um programa do usuário, isto é, uma seqüência de instruções executadas pelo(s) mesmo(s) processador(es) que executa(m) as instruções do programa do usuário; é verdade que algumas dessas instruções não são, em geral, acessíveis ao usuário comum ... mas a característica fundamental permanece, que é a de *software* sobreposto funcionalmente ao *hardware*.

Ainda em Guimarães (1989, p. 12), temos que sistema operacional é uma extensão ou vestimenta do *hardware* que torna o trabalho do programador mais eficiente e menos sujeito a erros.

Visto o conceito de sistema de computador, pode-se enumerar agora as suas principais funções:

1. Apresentar ao usuário uma máquina mais flexível e adequada para programar do que aquela que o *hardware* nú apresenta; ele, o sistema

[1] Por *boot*, entendemos ser o procedimento executado pelo processador para carregar um sistema operacional na *Ramdon Access Memory* (RAM)

[2] O termo tarefa (tradução do termo inglês *job*) é utilizado para designar um conjunto de passos (seqüência de atividades computacionais) a ser executado pelo aplicativo

operacional, torna a comunicação do homem com a máquina mais natural e inteligível.

2. Possibilitar o uso eficiente e controlado dos vários componentes de *hardware* que constituem o sistema como um todo: processador, memória principal e secundária, canais de Entrada/Saída, controladores, periféricos, etc.

3. Possibilitar a diversos usuários o uso compartilhado e protegido dos diversos componentes de *hardware* e de *software* do sistema de modo que o sistema seja utilizado de maneira mais eficiente e que usuários possam se beneficiar do trabalho de outros e cooperarem entre si na execução de projetos complexos.

Existem vários sistemas operacionais, diferindo uns dos outros pelo principal tipo de serviços que eles proporcionam aos usuários e, principalmente, o modo pelo qual executam tais tarefas. Os três tipos mais recorrentes são os sistemas do tipo lote (*batch*), nos quais as tarefas dos usuários são agrupadas fisicamente e processadas seqüencialmente uma após a outra; os sistemas de tempo repartido (*time-sharing*), cada comando do usuário é interpretado e executado em seguida; e os sistemas de tempo real que são voltados para aplicações de medição e controle que exigem o monitoramento contínuo, pois suas tarefas devem ser respondidas em um intervalo de tempo prefixado

Percebe-se, então, que o sistema operacional, *software* essencial ao funcionamento do computador, permite um maior aproveitamento dos recursos físicos, denominados de *hardware*. O sistema operacional não funciona sem o *hardware*, nem este executa as tarefas se não estiver sob o controle de um sistema operacional.

Em uma análise menos superficial, pode-se dizer que o *hardware*

compreende os dispositivos periféricos e os dispositivos internos. Estes são os elementos essenciais ao funcionamento do computador, eles estão presentes em todo e qualquer tipo de computador, são eles: Unidade central de processamento (UCP); memória; circuito de entrada e saída, também chamado de placa-mãe (é a placa principal do computador onde se encaixam o processador, a memória e as placas de expansão). Os dispositivos periféricos são aqueles que propiciam um incremento às funções do computador, não são essenciais ao funcionamento do mesmo, mas possibilitam um maior aproveitamento da máquina.

Será considerado sistema de computador aquele conjunto de dispositivos e programas essenciais ao funcionamento de um computador. Desse modo, é pacífico entre os diversos autores que sistema de computador consiste em um complexo formado por *hardware* e *software* destinado à realização de determinada função. Sistema de computador é o conjunto indissociável formado pelo sistema operacional mais os dispositivos internos, ambos os elementos essenciais das categorias *hardware* e *software* respectivamente.

Nossa definição de sistema de computador foi construída a partir de definições já existentes em legislações estrangeiras.

Consultando a legislação estrangeira, foi encontrada a definição de sistema de computador em uma convenção elaborada pelos Estados signatários do *Council of Europe* (CE). A definição encontra-se no artigo primeiro do *Draft Convention on Cybercrime*:

> Artigo 1 - Definições
> Para os propósitos desta Convenção:
> a. "Sistema de computador" é um dispositivo[3] ou um conjunto de dispositivos interconectados, que executam o processamento automático de dados (ou qualquer outra

[3]O autor deste trabalho utiliza o vernáculo *dispositivo* no sentido de um *hardware* (parte física do computador) que é capaz de receber e enviar dados.

> função) de acordo com os comandos de um programa[4]. (COUNCIL OF EUROPE, 2000)

Foi encontrada definição semelhante na legislação portuguesa na Lei N. 10/91 de 29 de abril:

> Sistema informático - o conjunto constituído por um ou mais computadores, equipamento periférico e suporte lógico que assegura o processamento de dados. (PORTUGAL, 1991)

Percebemos que essas definições são bem mais amplas, não se atendo às partes essenciais do sistema de computador (sistema operacional e dispositivos internos). Tal amplitude é justificável por razões práticas, pois quis o legislador não somente proteger as partes principais de um sistema de computador. O legislador, ao dizer que o sistema de computador é um conjunto de dispositivos interconectados, assim o faz para proteger a lesão a qualquer parte do sistema de computador, não se limitando às partes essenciais ao funcionamento do mesmo, pois como veremos em seguida, podem ocorrer danos ao sistema de computador sem que o funcionamento do mesmo seja comprometido. Tais definições com maior amplitude são importantes quando da tutela de redes de computadores, que se tratam de sistemas de computadores em sentido bem mais amplo.

2.1.1 Sistema de computador enquanto um bem jurídico

Conceituado o sistema de computador, cabe agora verificar se o mesmo é um bem jurídico, devendo assim receber proteção jurídica.

Bem jurídico, segundo Toledo (2000, p. 16) citando Welzel, é um bem

[4]No original:
Article 1 - Definitions
For the purposes of this Convention:
a."computer system" means any device or a group of inter-connected devices, which pursuant to a program performs automatic processing of data [or any other function].

vital ou individual que, devido ao seu significado social, é juridicamente protegido. Mário (2000, p. 253), por seu turno, já define bens jurídicos como sendo, primeiramente, aqueles de natureza patrimonial, que possuem valor econômico apreciável, em outras palavras, tudo aquilo que tem valor econômico e que integre o patrimônio de uma pessoa é considerado bem jurídico. Adverte, entretanto que não só os bens de natureza patrimonial são bens jurídicos, há também aqueles que, *mesmo não integrando o patrimônio do sujeito, são suscetíveis de proteção legal*.

Percebe-se então que ambas as definições não são excludentes. A de Welzel citado por Toledo é mais ampla, apelando para o significado social. Todo bem que possua significado social é protegido pelo Direito. Já Mário tenta imprimir uma classificação com critérios objetivos, patrimonialidade ou não do bem. Se tiver caráter patrimonial, é considerado bem jurídico. Se não tiver, pode ser que seja considerado bem jurídico. Esta última categoria acaba por deixar a classificação de Mário tão subjetiva quanto a de Welzel. O que não é problema, pois como afirmou Toledo (2000, p. 16) bem jurídico é, pois, toda situação social desejada que o direito quer garantir contra lesões.

Resta agora saber se o sistema de computador possui significado social, demandando proteção legal. Como é sabido, a internet, grosso modo, é uma interligação entre sistemas de computadores. Antes do advento da internet é óbvio que existiam os sistemas de computadores, no entanto, não havia possibilidade de comunicação de um sistema com o outro. Nesse sentido, é elucidativa a explicação de Ramonet:

> Se as origens da rede remontam ao fim dos anos 60, seu verdadeiro nascimento data de 1974 quando, respondendo a um desejo do Pentágono, Vint Cerf, professor da universidade da Califórnia, em Los Angeles, aprimorou a norma comum que permitiu conectar todos os computadores e lhe deu um nome: internet. Vint Cerf tinha

> descoberto que os computadores, assim como os homens, são gregários; além disso, nunca são tão eficazes a não ser quando estão conectados a outros computadores. (RAMONET, 1998, p. 143)

Ramonet (1998, p. 143) diz ainda que a internet só se desenvolveu maciçamente com o aprimoramento da *World Wide Web* (WWW), abreviadamente, *web*, pelos pesquisadores do *European Organization for Nuclear Research* (CERN) em Genebra. A teia mundial, baseada em uma concepção de hipertexto, transformou a internet num ambiente mais acessível ao usuário sem conhecimentos profundos em informática. Com o desenvolvimento desse tipo de interface, tornou-se possível que qualquer pessoa leiga navegar pela internet. Graças a isso, duplica todos os anos o número de computadores conectados no mundo e, de três em três meses, o número de *web sites*, vide estatísticas relativas ao número de brasileiros conectados no gráfico da figura 2 na página 20 e acerca do registro de domínios no Brasil na tabela 1 na página 23.

Fez-se esse breve histórico da internet para mostrar a importância dos sistemas de computadores interligados em rede para a sociedade contemporânea. Com a interligação dos sistemas, vários tipos de serviços passaram a serem prestados pela internet, várias informações passaram a ser disponibilizadas na *web*. Essa interligação de computadores (ou sistema de computadores) ampliou significativamente o leque de funções que um computador isolado poderia oferecer. Surge então uma nova necessidade: a proteção daquilo que possibilita toda essa teia de informações e serviços. Faz-se mister, nesse panorama, que se garanta proteção jurídica do sistema de computador, pois é evidente a importância do mesmo para a sociedade contemporânea e, com o advento da internet, esse bem jurídico ficou mais exposto a ataques.

Começa-se a falar então na proteção da integridade e disponibilidade

do sistema. A integridade do sistema consiste em o mesmo não ser alterado por pessoas que não estejam autorizadas. Disponibilidade, por seu turno, é a característica de o sistema sempre estar disponível para que sejam realizadas as funções para as quais ele fora planejado.

Conclui-se, dessa forma, que com o surgimento da internet o significado social do sistema de computador foi ampliado, tendo ele várias utilidades para a sociedade contemporânea. Cogita-se agora na proteção da integridade e disponibilidade dos sistemas de computador.

2.2 Internet, Ciberespaço e Direito Penal

É muito antiga a noção de que Direito e Sociedade são elementos inseparáveis. "Onde estiver o homem, aí deve estar o Direito", diziam os romanos. A cada dia a Ciência Jurídica se torna mais presente na vida dos indivíduos, porque sempre as relações sociais vão-se tornando mais complexas.

A internet, a grande rede de computadores, tornou essa percepção ainda mais clara. Não obstante nos primeiros anos da rede tenham surgido mitos sobre sua imunidade ao Direito, esse tempo passou e já se percebe a necessidade de mecanismos de auto-regulação e hetero-regulação, principalmente por causa do caráter ambivalente da internet.

Bastos (1989), nos seus Comentários à Constituição do Brasil, percebeu essa questão, ao asseverar que evolução tecnológica torna possível uma devassa na vida íntima das pessoas, insuspeitada por ocasião das primeiras declarações de direitos. Força é convir que não se pode prescindir do Direito, para efeito da prevenção, da reparação civil e da resposta penal, quando necessária.

Tendo em vista as origens da internet, poderia ser um contra-senso

defender a idéia de que o ciberespaço co-existe com o mundo real como uma sociedade libertária ou anárquica. Isto porque a cibernética — que se aplica inteiramente ao estudo da interação entre homens e computadores — é a ciência do controle. A própria rede mundial de computadores, como um sub-produto da Guerra Fria, foi pensada, ainda com o nome de Arpanet para propiciar uma vantagem estratégica para os Estados Unidos, em caso de uma conflagração nuclear global contra a hoje extinta União Soviética.

Como dito anteriormente, a WWW, que popularizou a internet, propiciando interatividade e o uso de sons e imagens na rede, foi desenvolvida em 1990 no CERN, pelo cientista Tim Berners-Lee. O CERN é uma organização internacional de pesquisas nucleares em física de partículas, situada nas proximidades de Genebra, na Suíça, e fundada em 1954. Atualmente, a sua convenção-constituinte tem a ratificação de vinte Estados-partes.

Além dessa origem pouco vinculada à idéia de liberdade, a grande rede não tem existência autônoma. As relações que se desenvolvem nela têm repercussões no *mundo real*. O virtual e o real são apenas figuras de linguagem (um falso dilema), não definindo, de fato, dois mundos diferentes, não dependentes. Em verdade, tudo o que se passa no ciberespaço acontece na dimensão humana e depende dela.

Por conseguinte, a vida *on-line* nada mais é do que, em alguns casos, uma reprodução da vida *real* somada a uma nova forma de interagir. Ou seja, representa diferente modo de vida ou de atuação social que está sujeito às mesmas restrições e limitações ético-jurídicas e morais aplicáveis à vida comum (não eletrônica), e que são imprescindíveis à convivência. Tudo tendo em mira que não existem direitos absolutos e que os sujeitos ou atores desse palco virtual e os objetos desejados, protegidos ou ofendidos são elementos da cultura ou do interesse humano.

Mas a internet não é só isso. No que nos interessa, a revolução tec-

nológica propiciada pelos computadores e a interconexão dessas máquinas em grandes redes mundiais, extremamente capilarizadas, é algo sem precedentes na história humana, acarretado uma revolução jurídica de vastas proporções, que atinge institutos do Direito tributário, comercial, do consumidor, temas de direitos autorais e traz implicações à administração da Justiça, à cidadania e à privacidade.

Não é por outra razão que, do ponto de vista cartorial (direito registrário), a internet já conta com uma estrutura legal no País, representada pelo Comitê Gestor da internet no Brasil, que delegou suas atribuições à FAPESP, e tem regulamentado principalmente a adoção, o registro e a manutenção de nomes de domínio na rede brasileira.

Assim, verifica-se que não passam mesmo de mitos as proposições de que a internet é um espaço sem leis ou terra de ninguém, em que haveria liberdade absoluta e onde não seria possível fazer atuar o Direito Penal ou qualquer outra norma jurídica.

Estabelecido que a incidência do Direito é uma necessidade inafastável para a harmonização das relações jurídicas ciberespaciais, é preciso rebater outra falsa idéia a respeito da internet: a de que seriam necessárias muitas leis novas para a proteção dos bens jurídicos a serem tutelados pelo Direito Penal da internet.

Destarte, a legislação aplicável aos conflitos cibernéticos será a já vigente, com algumas adequações na esfera infraconstitucional. Como norma-base, teremos a Constituição Federal, servindo as demais leis para a proteção dos bens jurídicos atingidos por meio do computador, sendo plenamente aplicáveis o Código Civil, o Código de Defesa do Consumidor, a Lei dos Direitos Autorais, a Lei do *Software* e o próprio CP, sem olvidar a Lei do *Habeas Data*.

Os bens jurídicos ameaçados ou lesados por crimes informáticos merecerão proteção por meio de tutela reparatória e de tutela inibitória. Quando isso seja insuficiente, deve incidir a tutela penal, fundada em leis vigentes e em tratados internacionais, sempre tendo em mira o princípio da inafastabilidade[5] da jurisdição, previsto no art. 5º, inciso XXXV, da Constituição Federal.

A atuação do Direito Penal será imprescindível em alguns casos, por conta da natureza dos bens jurídicos em jogo. Pois, pela *web* e no ciberespaço circulam valores, informações sensíveis, dados confidenciais, elementos que são objeto de delitos ou que propiciam a prática de crimes de variadas espécies. Nas vias telemáticas, transitam nomes próprios, endereços e números de telefone, números de cartões de crédito, números de cédulas de identidade, informações bancárias, placas de veículos, fotografias, arquivos de voz, preferências sexuais e gostos pessoais, opiniões e idéias sensíveis, dados escolares, registros médicos e informes policiais, dados sobre o local de trabalho, os nomes dos amigos e familiares, o número do *Internet Protocol* (IP), o nome do provedor de acesso, a versão do navegador de internet (*browser*), o tipo e versão do sistema operacional instalado no computador.

A interceptação de tais informações e dados ou a sua devassa não autorizada devem ser, de algum modo, tipificadas, a fim de proteger esses bens que são relevantes à segurança das relações cibernéticas e à realização da personalidade humana no espaço eletrônico.

LESSIG (1999, p. 4), especialista norte-americano em Direito da internet, adverte que a própria arquitetura dos programas de computador que permitem o funcionamento da internet como ela é pode se prestar à regulação da vida dos cidadãos *on-line* tanto quanto qualquer norma jurídica.

Uma nova sociedade, a sociedade do ciberespaço, surgiu nos anos

[5] A esse respeito vide a seção 3.2.2.3 na página 77 deste trabalho.

noventa, tornando-se o novo foco de utopias. Ainda segundo LESSIG:

> Como na Europa pós-comunista, as primeiras idéias sobre ciberespaço se desvencilharam das garras do Estado. Mas aqui o vínculo era ainda mais forte que na Europa pós-comunista. A reivindicação agora era que o governo não regulasse mais o ciberespaço, ele era essencialmente e individualmente livre. Os governos poderiam ameaçar, mas essa conduta não pode ser controlada; leis podem proibir, mas elas seriam sem sentido. Não havia escolha sobre qual governo instalar. - nenhum poderia reinar. Ciberespaço seria uma sociedade bem diferente. Teria uma definição e direção, mas construída de baixo para cima e nunca na direção do Estado. A sociedade desse espaço seria cheia de entidades ordenadas por si sós, livre de governantes e dos jogos políticos[6]. (LESSIG, 1999, p. 4)

A idéia anárquica de internet tem nítida relação — que ora apontamos — com o movimento abolicionista. No entanto, segundo LESSIG (1999, p. 5), a etimologia da palavra *ciberespaço* remete à cibernética, que é a ciência do controle à distância.

Posicionando-se, LESSIG pontua que não há liberdade absoluta na internet e que não se pode falar no afastamento total do Estado. O ideal seria haver uma constituição para a internet, não no sentido de documento jurídico escrito — como entenderia um publicista —, mas com o significado de arquitetura ou moldura, que estruture, comporte, coordene e harmonize os poderes jurídicos e sociais, a fim de proteger os valores fundamentais da sociedade e da cibercultura.

[6]No original: "As in post-Communist Europe, first thoughts about cyberspace tied freedom to the disappearance of the state. But here the bond was even stronger than in post-Communist Europe. The claim now was that government *could not* regulate cyberspace, that cyberspace was essencially, and unavoidably, free. Governments could threaten, but behavior could not be controlled; laws could be passed, but they would be meaningless. There was no choice about which government to install — none could reign. Cyberspace would be a society of a very different sort. There would be a definition and direction, but built from the bottom up, and never through the direction of a state. The society of this space would be a fully self-ordering entity, cleansed of governors and free from political hacks."Tradução do autor.

Essa moldura deve ser um produto consciente e fruto do esforço de cientistas, usuários, empresas e Estado, pois:

> Ciberespaço, por si só não fará promessas de liberdade. Por si só, o ciberespaço se tornará uma perfeita ferramenta de controle. Controle. Não necessariamente controle pelo governo, e não necessariamente controle de algum mal do final do fascismo. Mas o argumento desse livro é que a mão invisível do ciberespaço está construindo uma estrutura que é bem o oposto do que era o ciberespaço no seu surgimento. A mão invisível, através do comércio, está construindo uma estrutura de perfeito controle — uma estrutura que faria possível uma regulamentação de alta eficácia.[7]. (LESSIG, 1999, p. 5)

Mais adiante, LESSIG (1999, p. 193) arrola suas perplexidades diante das implicações do ciberespaço sobre o Direito, declarando que:

> Essa conduta foi primeiramente ordinariamente governada sob uma jurisdição, ou sob duas jurisdições em coordenação. Agora irá sistematicamente ser governada sob múltiplas jurisdições não-coordenadas. Como poderia uma lei lidar com isso?[8].

Ou seja, como será possível enfrentar o problema do conflito real de diferentes ordens jurídicas nacionais, em decorrência de fatos ocorridos no ciberespaço ou na internet?

A mudança das concepções a respeito dos *hackers*, dá idéia de como o Direito tem lidado com conflitos entre as normas do ciberespaço e as da comunidade do espaço real. Isto porque, no início, a internet era um mundo

[7]No original: "Cyberspace, left to itself, will no fulfill the promise of freedom. Left to itself, cyberspace will become a perfect tool of control. Control. Not necessarily control by government, and not necessarrily control to some evil, fascist end. But the argument of this book is that the invisible hand of cyberspace is building an architecture that is quite the opposite of what it was at cyberspace´s birth. The invisible hand, through commerce, is constructing an architecture that perfects control — an architecture that makes possible highly efficient regulation". Tradução do autor.

[8]No original: "Behavior was once governed ordinarily within one jurisdiction, or within two coordinating jurisdictions. Now it will sistematically be governed within multiple, non-coordinating jurisdictions. How can law handle this?"Tradução do autor

de *softwares* e sistemas abertos, no qual valiosos arquivos e informações financeiras não eram acessíveis *on-line*.

Todavia, com o avanço do cibercomércio, as coisas mudaram, e foi necessário estabelecer novas regras de segurança na rede, fazendo surgir um evidente conflito entre a cibercultura *hacker* e os interesses financeiros e econômicos das empresas e as preocupações estratégicas e de segurança do governo.

> Enquanto estas culturas estavam em conflito, a lei do espaço-real agiu rapidamente. A lei trabalhou impiedosamente para matar determinados tipos de comunidade *on-line*. A lei tornou o comportamento dos *hackers* um crime, e o governo fez uso de métodos agressivos para combatê-la. Alguns casos proeminentes e de grande divulgação foram usados redefinir comportamento 'inofensivo' dos *hackers* naquilo que a lei poderia chamar de comportamento 'criminoso'. A lei apagou assim toda a ambigüidade sobre o que poderia ser bom em *hacking*[9]. (LESSIG, 1999, p. 194)

Exemplo disso foi o que se deu com Robert Tappin Morris, da Universidade de Cornell, que foi condenado a três anos de detenção, com direito a *sursis* (*probation*), pela Justiça Federal norte-americana, por violar o *Computer Fraud and Abuse Act*[10] de 1986. Essa lei tipifica o crime de acesso doloso a computadores de interesse federal sem autorização, quando esse acesso cause dano ou impeça o acesso de usuários autorizados. Morris programou um *worm*[11] para mostrar as falhas do programa de *e-mail Sendmail*, acabando por contaminar computadores federais, congelando-os

[9] No original: "As these cultures came into conflict, real-space law quickly took sides. Law worked ruthlessly to kill a certain kind of on-line community. The law made the emphhackers behavior a crime, and the government took aggressive steps to combat it. A few prominent and well-publicized cases were used to redefine the emphhackers´ 'harmless behavior' into what the law could call 'criminal'. The law thus erased any ambiguity about the good in hacking ". Tradução do autor.

[10] Lei federal norte-americana que trata dos crimes de informática.

[11] Programa de computador que se auto-replica automaticamente.

ou deixando-os *off-line*.

Por conseguinte, embora repudiando o exagero de certas tipificações, não há como negar a interação entre a internet e o Direito Penal. Isto porque o ciberespaço e sua cultura própria não estão fora do mundo. E, estando neste mundo, invariavelmente acabarão por sujeitar-se ao Direito, para a regulação dos abusos que possam ser cometidos pelo Estado contra a comunidade cibernética e para a prevenção de ações ilícitas e ilegítimas de membros da sociedade informatizada contra bens jurídicos valiosos para toda pessoa ou organização humana.

2.3 A reserva legal

No direito penal brasileiro vige o *princípio da reserva legal*, previsto constitucionalmente. Tal princípio, imiscuido no texto Constitucional, enuncia que:

> Art. 5º. ...
> XXXIX — Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal[12].

Podemos dizer que o princípio da legalidade (ou da reserva legal) tem significado político, no sentido de ser uma garantia constitucional dos direitos do homem, daí o fato de estar previsto na Carta Magna como inciso do artigo 5º. Constitui a garantia fundamental da liberdade civil, que não consiste em fazer tudo o que se quer, mas somente aquilo que a lei permite. À lei e somente a ela compete fixar as limitações que destacam a atividade criminosa da atividade legítima. Esta é a condição de segurança e liberdade individual.

Portanto, não há crime sem que, antes de sua prática por algum

[12]Cf. também art. 1º do Código Penal Brasileiro.

indivíduo, haja uma lei descrevendo-o como fato punível, ou seja tipificando-o. É lícita e isenta de qualquer punição, pois, qualquer conduta que não se encontre definida em lei penal incriminadora.

Com o advento da teoria da tipicidade, o princípio da reserva legal ganhou muito de técnica. Típico é o fato que se amolda à conduta criminosa descrita em lei. É necessário que o tipo (conjunto de elementos descritivos do crime contido na lei penal) tenha sido definido *antes* da prática delituosa. Daí falar-se em anterioridade da lei penal incriminadora. Assim, o art. 1º do CP, contém em seu texto dois princípios:

1. Princípio da legalidade (ou de reserva legal) — não há crime sem lei que o defina; não há pena sem cominação legal.

2. Princípio da anterioridade — não há crime sem lei anterior que o defina; não há pena sem prévia imposição legal. Para que haja crime é preciso que o fato que o constitui seja cometido após a entrada em vigor da lei incriminadora que o define.

2.3.1 Origem histórica do princípio da reserva legal e Direito comparado

São muitos os entendimentos dos doutrinadores com relação à origem e evolução histórica do princípio da reserva legal. Alguns, apontam a Magna Carta do Rei João Sem Terra, em 1.215, na Inglaterra, outros dizem que suas raízes encontram-se no direito ibérico, nas Cortes de Leão, em 1.186, no reinado de Afonso IX.

Não obstante o seu antigo traçado rudimentar, o certo é que na Idade Média permitia-se a criação de crime por meio da analogia, do arbítrio judicial e do arbítrio do rei. Foi somente no século XVIII que Montesquieu, em sua famosa obra *O espírito das leis* (1.748), dando seqüência às idéias

iniciadas por John Locke, no século XVII, desenvolveu a teoria da separação dos Poderes, proibindo a analogia penal. Montesquieu dizia que só a lei pode proibir, e o que não é proibido é permitido, dando assim inegável contribuição ao desenvolvimento do conceito de liberdade.

Beccaria, na obra *Dos delitos e das penas*, também preconiza que só as leis podem fixar as penas de cada delito e que o direito de fazer as leis penais é tarefa exclusiva do legislador. Todavia, com a nitidez atual surgiu o princípio da reserva legal, pela primeira vez, apenas na legislação austríaca de 1.787. A Revolução Francesa, dois anos mais tarde, sob a influência da doutrina da divisão dos Poderes de Montesquieu, consagrou-o na Declaração dos Direitos do Homem e do Cidadão, de 26 de agosto de 1789. E, a partir de então, não se conteve mais a expansão do princípio, que se generalizou, instalando-se nas Constituições de diversos países, chegando ao Brasil pelo texto da Constituição do Império, em 1824, reproduzido pelas Constituições de 1891, 1934, 1937, 1946, 1967 e 1969. Na Constituição vigente, o princípio está consagrado no art. 5º, inciso XXXIX.

O princípio da reserva legal não existe no Direito Penal inglês; lá o costume é a fonte de criação das normas incriminadoras. Outra exceção ao princípio da reserva legal é encontrada na Escócia, que admite o emprego da analogia como fonte criadora de infrações penais.

Alguns países, amparados por regimes autoritários, despreocupados com a garantia da liberdade individual, reagiram ao princípio da reserva legal. Isso ocorreu na doutrina dos comunistas russos e no nacional-socialismo alemão. Efetivamente, o Código soviético de 1926 admitia a aplicação da lei penal por analogia. Essa situação perdurou até a reforma legislativa de 25 de dezembro de 1958, que trouxe de volta o princípio da legalidade.

Já a doutrina do nacional-socialismo alemão, sob a liderança de Adolf Hitler, também admitia o emprego analógico da lei penal. E ainda conside-

rava delito a conduta que contrariava a sã consciência do povo. Portanto, além da analogia, permitia-se o arbítrio judicial como fonte criadora de infrações penais. O CP alemão atual adota o princípio da legalidade.

2.4 Condutas lesivas na área da tecnologia e sua tipificação

Evidentemente, é melhor para a segurança de todos nós a existência da reserva legal no Direito Penal. Na atual conjuntura, entretanto, na área da tecnologia, telemática, informática, etc., surgem determinadas condutas lesivas que merecem (às pressas) tipificação criminosa e que, justamente por não estarem previstas em lei como *crime*, são consideradas atípicas, isto é, não há que se falar em crime, nem em punição na esfera criminal.

Existem diversos projetos de lei em andamento no Congresso Nacional que tratam da invasão de computadores e até mesmo descrevem a utilização da técnica da chamada (no jargão da informática) *engenharia social* como meio para a prática criminosa no tema, tratando inclusive da exploração de vulnerabilidades tecnológicas e processuais. A aparente morosidade na elaboração das normas (no caso, criminais) acontece em razão de aspectos técnicos, isto é, não se pode deixar de observar determinadas regras na tipificação. Considerar determinada conduta como crime é tarefa de alta responsabilidade.

Gomes (2001) escreveu:

> Há muito reivindica-se no Brasil a criminalização específica dos crimes informáticos. Com o advento da Lei n. 9.983/00 (de 14/07/00), que entrou em vigor no dia 15/10/2000, surgiram no cenário jurídico-penal brasileiro algumas tipificações. (...) São tipificações, entretanto, muito específicas e que visam a proteger primordialmente a previdência social e a administração pública. Não im-

> pede, portanto, a necessidade de uma lei penal mais geral.

A informática pode ser vista como um fator criminógeno na medida em que:

1. abre novos horizontes ao delinqüente (que dela pode valer-se para cometer infindáveis delitos — é a instrumentalização da informática);
2. permite não só o cometimento de novos delitos (p.ex.: utilização abusiva da informação armazenada em detrimento da privacidade, intimidade e imagem das vítimas) como a potencialização dos delitos tradicionais (estelionato, racismo, pedofilia, crimes contra a honra etc.);
3. dá ensejo, de outro lado, não só aos delitos cometidos com o computador (*computer crime*), senão também os cometidos contra o computador (contra o *hardware*), o *software* ou mesmo contra a própria informação);
4. o crime informático pode ser cometido:
   - no momento da entrada dos dados (*input*);
   - na programação;
   - no processamento dos dados;
   - na saída dos dados (*output*);
   - na comunicação eletrônica;
5. em todo o *iter criminis* pode ser utilizado o computador, é dizer,
   - no planejamento do crime;
   - na preparação do crime;
   - na sua execução;

- e inclusive na fase posterior para seu encobrimento (destruição de provas);

6. permite o desenvolvimento tanto de uma criminalidade privada (de particulares, pessoas físicas ou jurídicas) como pública (criminalidade estatal, que não só pode disseminar o uso da informática para controlar as pessoas, como também abusar das informações, tudo em flagrante violação aos direitos e garantias fundamentais típicas do Estado de Direito).

Dentre tantos outros aspectos criminológicos da questão, impõe-se ressaltar que o delinqüente informático cada vez mais se distancia do *protótipo* (do *hacker*[13] jornalisticamente forjado) que é o estudante de classe média, com alta especialização informática, bom nível de escolaridade, inteligente etc.

Hoje tais delinqüentes são, em geral, pessoas que trabalham no ramo informático, normalmente empregadas, não tão jovens nem inteligentes; são *insiders*, vinculados a empresas (em regra). Sua característica central consiste na pouca motivabilidade em relação à norma (raramente se sensibiliza com a punição penal). Motivos para delinqüir: ânimo de lucro, perspectiva de promoção, vingança, apenas para chamar a atenção etc. A vítima da criminalidade informática é a pessoa jurídica *par excellence* (de direito público ou de direito privado). Em regra conta com grande poder econômico, mas

[13]Realmente o termo *hacker* foi jornalisticamente forjado; entretanto para nós ainda conceitua-se como indivíduos com um grande conhecimento de informática e que podem utilizar seus extraordinários conhecimentos na área para atividades lícitas ou criminosas, em especial a invasão de sistemas de computadores, criação de vírus etc. Vide a esse propósito a definição de *hacker* constante de Raymond (2003):"1. Pessoa que gosta de explorar os detalhes de sistemas programáveis e como expandir suas capacidades, em oposição à maioria dos usuários que preferem aprender o mínimo necessário."(No original: "1. A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary". Tradução do autor.)

mesmo assim praticamente não denuncia o delito contra ela cometido. Por isso mesmo, é a vítima a grande aliada do delinqüente. Neste momento, a tendência mais notada consiste na prática do delito informático para espionagem, tanto de empresa contra empresa, como de país contra país.

Do ponto de vista político-criminal pode-se afirmar que a freqüência da criminalidade informática, suas drásticas conseqüências lesivas, a intensidade dos ataques, a importância dos bens jurídicos envolvidos (intimidade, privacidade, patrimônio, segredo industrial, segredo comercial, segredo empresarial etc.) justificam a intervenção do Direito Penal nessa área. De qualquer modo, como já salientamos, não se pode esquecer que esse instrumento é subsidiário (só se legitima quando outros meios de controle formais — Direito Civil, Administrativo etc — ou informais forem inidôneos) e fragmentário (apenas os ataques mais intensos ao bem jurídico é que autoriza a sanção penal). Direito Penal é a *ultima ratio*; a pena criminal é a *extrema ratio*. No restrito, subsidiário e fragmentário campo do Direito Penal podem tão-somente aparecer:

1. crimes *contra* o próprio sistema de informatização (danos aos programas, danos aos dados etc.);

2. crimes cometidos *por meio* do sistema informatizado (crimes novos, como violação de segredo, acesso indevido e danos a programas e dados etc)[14].

Os chamados crimes impróprios (ou impuros), que são os tradicionais estelionato, pedofilia, racismo etc, cometidos pelo computador, já estão definidos no ordenamento jurídico e nesse caso é totalmente desaconselhável a *bis in idem* criminalizador. Justamente nessa linha político-criminal incriminadora vem o Projeto de Lei (PL) 84/99, de autoria do deputado Luiz

[14] A esse respeito, a classificação dos delitos relacionados à informática, vide a seção 2.5 na página 64 deste trabalho.

Piauhylino (PSDB-PE), que prevê sete delitos informáticos e suas respectivas penas. Espera-se que os legisladores dêem a devida atenção ao assunto e aprovem brevemente a lei penal geral sobre os delitos informáticos.

O estelionato continua sendo estelionato, a velha apropriação indébita, continua sendo apropriação indébita. O mesmo raciocínio deve ser feito para os crimes contra a inviolabilidade dos segredos, dos crimes de concorrência desleal, etc. Independentemente da esfera criminal, também não podemos nos esquecer da responsabilidade civil, tanto no campo da culpa contratual como da aquiliana (culpa extracontratual) - que é aquela que não deriva de contrato, mas de violação ao dever legal de conduta — ao dever genérico de não lesar a outrem — *neminem laedere*, determinado de forma geral no art. 927, do Código Civil. Desta infração, surge a obrigação de ressarcimento do prejuízo causado. Ao lesado, incumbe o ônus de provar a culpa ou o dolo do causador do dano e independe de qualquer ação criminal. A propósito, citamos o Novo Código Civil (BRASIL, 2003, p. 58-59, 144 e 146.):

> 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.
> Art. 187. Comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestadamente os limites impostos pelo seu fim econômico, social, pela boa-fé ou pelos bons costumes.
> ⋮
> Art. 927. Aquele que por ato ilícito (art. 186 e 187), causar dano a outrem, é obrigado repará-lo.
> ⋮
> Art. 935. A responsabilidade civil é independente da criminal, não se podendo questionar mais sobre a existência do fato, ou sobre quem seja o seu autor, quando estas questões se acharem decididas no juízo criminal.
> ⋮

Art. 944. A indenização mede-se pela extensão do dano.

A despeito da esfera criminal, no mínimo, podemos contar com a responsabilização civil do invasor.

2.5 Classificação dos delitos de informática

A taxionomia mais aceita é a propugnada por Hervé Croze e Yves Bismuth, ambos citados em Ferreira (1992, p. 214-215), e que distingue duas categorias de crimes informáticos:

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

No primeiro caso, temos o delito de informática propriamente dito, aparecendo o computador como meio e meta, podendo ser objetos de tais condutas o computador, seus periféricos, os dados ou o suporte lógico da máquina e as informações que guardar. No segundo caso, o computador é apenas o meio de execução, para a consumação do crime-fim, sendo mais comuns nesta espécie as práticas ilícitas de natureza patrimonial, as que atentam contra a liberdade individual e contra o direito de autor.

Na doutrina brasileira, tem-se asseverado que os crimes informáticos podem ser puros (próprios) e impuros (impróprios). Serão puros ou próprios, aqueles que sejam praticados por computador e se realizem ou se consumem também em meio eletrônico. Neles, a informática (segurança dos sistemas, titularidade das informações e integridade dos dados, da máquina e periféricos) é o objeto jurídico tutelado.

Já os crimes eletrônicos impuros ou impróprios são aqueles em que o agente se vale do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço real, ameaçando ou lesando outros bens, não-computacionais ou diversos da informática.

Assim, os crimes informáticos dividem-se em crimes contra o computador e crimes por meio do computador, em que este serve de instrumento para atingir uma meta. O uso indevido do computador ou de um sistema informático (em si um fato tipificável) servirá de meio para a consumação do crime-fim. O crime de fraude eletrônica de cartões de crédito serve de exemplo.

Os crimes de computador, em geral, são definidos na doutrina norte-americana como *special opportunity crimes*, pois são cometidos por pessoas cuja ocupação profissional implica o uso cotidiano de microcomputadores, não estando excluída, evidentemente, a possibilidade de serem perpetrados por meros diletantes.

3 Crimes informáticos

3.1 A autoria de crimes informáticos

Já assinalada a importância da legalidade também no Direito Penal da Informática, vide seção 2.3 na página 56, é preciso ver que na sua operacionalização quase sempre haverá uma grande dificuldade de determinar, nos delitos informáticos, a autoria da conduta ilícita.

Diferentemente do mundo dito *real*, no ciberespaço o exame da identidade e a autenticação dessa identidade não podem ser feitos visualmente, ou pela verificação de documentos ou de elementos identificadores já em si evidentes, como placas de veículos ou a aparência física, por exemplo.

Quando um indivíduo está conectado à rede, são-lhe necessários apenas dois elementos identificadores: o endereço da máquina que envia as informações à internet e o endereço da máquina que recebe tais dados. Esses endereços são chamados de IP, sendo representados por números, que revelam quase nada sobre o usuário da internet e muito pouco sobre os dados que estão sendo transmitidos.

No ciberespaço, há razoáveis e fundadas preocupações quanto à autenticidade dos documentos telemáticos e quanto à sua integridade. O incômodo de ter de conviver com tal cenário pode ser afastado mediante a aplicação de técnicas de criptografia na modalidade assimétrica, em que se

utiliza um sistema de chaves públicas e chaves privadas, diferentes entre si, que possibilitam um elevado grau de segurança[1].

Contudo, no que pertine à atribuição da autoria do documento, mensagem ou da conduta ilícita, os problemas processuais persistem, porque, salvo quando o usuário do computador faça uso de uma assinatura digital, dificilmente se poderá determinar quem praticou determinada conduta.

A assinatura digital confere certa autenticidade ao documento ou mensagem, permitindo que se presuma que o indivíduo **A** foi o autor da conduta investigada. Mas o problema reside exatamente aí. Como a internet não é auto-autenticada a definição de autoria fica no campo da presunção. E, para o Direito Penal, não servem presunções, ainda mais quando se admite a possibilidade de condenação.

O único método realmente seguro de atribuição de autoria em crimes informáticos é o que se funda no exame da atuação do responsável penal, quando este se tenha valido de elementos corporais para obter acesso a redes ou computadores. Há mecanismos que somente validam acesso mediante a verificação de dados biométricos do indivíduo. Sem isso a entrada no sistema é vedada. As formas mais comuns são a análise do fundo do olho do usuário ou a leitura eletrônica de impressão digital, ou, ainda, a análise da voz do usuário.

Tais questões se inserem no âmbito da segurança digital, preocupação constante dos analistas de sistemas e cientistas da computação, que têm a missão de desenvolver rotinas que permitam conferir autenticidade, integridade, confidencialidade, irretratabilidade e disponibilidade aos dados e informações que transitam em meio telemático. Naturalmente, tais técnicas e preocupações respondem também a necessidades do Direito Penal Informático e do decorrente processo penal.

[1] A esse respeito, noções introdutórias podem ser encontradas em (UCHÔA, 2003, p. 17).

Como já assinalado, a segurança de um sistema depende do uso de senhas, de assinatura digital ou eletrônica, de certificação digital, da criptografia por chaves assimétricas, da esteganografia[2], além de requerer a cooperação do usuário no sentido de não compartilhar senhas, de visitar apenas *sites* seguros[3], de instalar e configurar programas de proteção, como *anti-sniffers*, *firewalls*, anti-vírus e bloqueadores de conteúdo.

Como dito, somente os mecanismos de assinatura eletrônica, certificação digital e de análise biométrica podem conferir algum grau de certeza quanto à autoria da mensagem, da informação, ou da transmissão, se considerado o problema no prisma penal.

Mas a criptografia avançada assimétrica, tanto quanto a internet e a informática, em si mesma ambivalente, de um lado se presta a proteger a privacidade de cidadãos honestos e os segredos industriais e comerciais de empresas, presta-se também a assegurar tranqüilidade para ciberdelinqüentes, espaço sereno para transações bancárias ilícitas e campo fértil para o terrorismo e outras práticas criminosas, colocando os órgãos investigativos do Estado em difícil posição e, conseqüentemente, minando a defesa social.

Segundo Shapiro:

> Antes da expansão da disponibilidade massiça de criptografia forte, havia sempre a possibilidade de que comunicações remotas pudessem ser interceptadas e lidas por agentes do Estado (ou por bisbilhoteiros da vida privada). Embora o governo, supostamente, pudesse investigar as condutas daqueles que estivessem engajados em atividades ilegais, funcionários desleais podiam abusar desse poder, grampeando linhas de cidadãos com condutas irreprimíveis — ou, antes do advento do telefone, apreendendo comunicações escritas. A criptografia forte muda isso, pois, mesmo que a interceptação não autori-

[2]Uso de imagens, como *marcas d'água* digitais, para confirmar a autenticidade e integridade de um documento cifrado.

[3]Identificados pelo protocolo `https://`, onde o *s* significa *secure*.

> zada ocorra, a mensagem continua incompreensível. Isso faz um balanceamento de forças entre indivíduos e o Estado. Nos permite manter nossos segredos longe do Estado.[4] (SHAPIRO, 1999, p. 75)

Ainda segundo Shapiro (1999) citando Luis Freeh, Diretor do *Federal Bureau of Investigation* (FBI):

> O obscuro espectro da expansão da disponibilidade massiça de criptografia robusta, virtualmente indecifrável, é uma das maiores dificuldades que os sistemas legais terão no século que se aproxima[5]. (SHAPIRO, 1999, p. 75)

E Shapirocontinua:

> Antes da disponibilidade de criptografia forte, naturalmente, um criminoso pode ter tentado ser esquivado das autoridades. Porém, o Estado poderia responder com suas ferramentas privilegiadas de investigação — muito provavelmente a interceptação de linhas de comunicações. Agora, segundo estes representantes governamentais, essa vantagem foi efetivamente tomada do Estado. Criptogra-fia forte significa que os esforços da lei não podem mais ter acesso a mensagens em texto plano. A única solução, dizem tais representantes, é permitir ao Estado reter esta vantagem[6]. (SHAPIRO, 1999, p. 75)

[4]No original: "Before the widespread availbility of strong encryption, there was always the possibility that remote communications would be intercepted and read by the state (or by private snoops). Though government was only supposed to eavesdrop on those who were engaging in illegal conduct, rogue officials could abuse that power, tapping the lines of law-abiding citizens — or, before the advent of the phone, seizing written communications. Strong encryption changes this, because even unauthorized interception of an encrypted message occurs, the message will be incomprehensible. This changes the balance of power between individuals and the state. It allows us to keep secrets from government."Tradução do autor.

[5]No original: "The looming spectre of the widespread use of robust, virtually unbreakable encryption is one of the most difficult problems confronting law enforcement as the next century approaches". Tradução do autor.

[6]No original: "Prior to the avaibility of strong encryption, of course, a criminal might have tried to evade the cops. But the state could respond with its privileged investigative tools - most likely, wiretapping. Now these government officials say, the upper hand has been effectively taken from state. Strong encryption means law enforcement can no longer get timely access to the plain text of messages. The only solution, these officials say, is to allow the state to retain its advantage."Tradução do autor.

A reserva de tecnologia pelo governo se daria das seguintes formas:

1. Proibição de acesso a ferramentas de codificação poderosas a qualquer cidadão;

2. Desenvolvimento de padrão governamental de cifração para difusão na indústria e entre os usuários;

3. Proibição de exportação de programas de codificação, tipificando tal conduta como criminosa;

4. A criação do sistema de molho de chaves (*key escrow system*), pelo qual o usuário de criptografia ficaria obrigado a enviar a um órgão central de controle uma cópia de sua chave privada de cifração. Essa autoridade central, mediante ordem judicial, poderia decodificar a messagem supostamente ilícita e entregá-la aos agentes públicos investigantes.

Shapiro critica essas tentativas de controle governamental, asseverando que:

> ... os esforços governamentais de regulamentação podem ter um efeito contrário ao pretendido, diminuindo a segurança de todos os indivíduos enquanto afeta os criminosos afinal ... O que é importante aqui são as cada vez mais intrincadas maneiras em que o estado pode, no curso de uma perseguição legítima, limitar o controle de indivíduos sem justificação — e sem intenção de fazê-lo[7]. (SHAPIRO, 1999, p. 79)

Ou seja, estamos diante dos velhos conflitos entre direitos fundamentais e interesse público, entre segurança pública e privacidade, entre ação

[7]No original: "The government effort to regulate code could have the opposite of its intented effect, diminishing individual security while hardly affecting criminals at all ... What´s important here is to see the increasingly intricate ways in which the state may, in the course of legitimate pursuits, limit individual control without justification — and without meaning to do so."Tradução do autor.

do Estado e a intimidade do indivíduo, questões que somente se resolvem por critérios de proporcionalidade e mediante a análise do valor dos bens jurídicos postos em confronto.

O certo é que, enquanto o Direito Constitucional e o próprio Direito Penal não alcançam consenso quanto à forma de tratamento de tais conflitos, a criminalidade informática tem ido avante, sempre com horizontes mais largos e maior destreza do que o Estado, principalmente no tocante à ocultação de condutas eletrônicas ilícitas e ao encobrimento de suas autorias. Os *hackers* dominam várias técnicas para assegurar-lhes o anonimato, a exemplo:

1. do uso de *test accounts*, que são contas fornecidas gratuita e temporariamente por alguns provedores e que podem ser obtidas a partir de dados pessoais e informações falsas;

2. utilização de serviços de *proxy servers*[8], alguns disponíveis gratuitamente e usados até a partir de *browsers*[9];

3. da utilização de *anonymous remailers*, contas que retransmitem emails enviados por meio de provedores de internet que garantem o anonimato;

4. clonagem de celulares para acesso à internet, de modo a inviabilizar a identificação do local da chamada e de seu autor, mediante rastreamento do sinal;

5. utilização de celulares pré-pagos, pois tais aparelhos podem ser adquiridos com dados pessoais falsos e são de difícil rastreamento.

[8]Um *proxy server* age basicamente como um procurador, fazendo requisições a outros servidores em seu próprio nome, usando técnicas de mascaramento de IPs. Isso permite navegar de modo completamente anônimo.

[9]Navegadores. Aplicativos para acesso, principalmente, ao conteúdo da *WWW*.

Por isso Spinello (1999, p. 38) assevera que "anonimato eletrônico também frustra o empenho dos legisladores para assegurar responsabilidades individuais em suas ações *on-line*"[10]. E isto implica impunidade, em se tratando de criminalidade informática.

Essas e outras questões, ainda sem respostas, põem-se diante dos penalistas e dos estudiosos do Direito Penal. Espera-se, apenas, que sejam breves os embates e as polêmicas, pois o crime na era da internet se consuma na velocidade da luz.

3.2 Questões processuais

3.2.1 Questões de jurisdição e competência

Teem-se observado que os legisladores preocupam-se em regular as questões internáuticas, quanto ao direito substantivo, ou seja, quanto à criminalidade, pirataria de programas, bases de dados, propriedade intelectual, dentre muitos outros, não cuidando porém, de averiguar se a estrutura do direito processual vigente, está adaptada aos desafios exigidos.

Exemplo máximo é o caso da jurisdição e da competência para o conhecimento e pronunciamento do direito da internet. Essa questão se impõe quando surge a indagação seguinte: quem seria o juízo competente, por exemplo, para julgar lide envolvendo internautas, (*lato senso*) de países, ou de localidades distintas, onde **A**, sem sair fisicamente do seu território, provoca um dano em um direito de **B** através da internet? Neste caso, **B** pretende reaver seu prejuízo demandando contra **A** uma ação para fins de indenização de danos com base no art. 927 do Código Civil, vide página 63. Em que foro deve propor a ação? Pode haver foro privilegiado? E

[10] "eletronic anonymity also frustrates lawmakers efforts to hold individuals accountable for they on-line actions". Tradução do autor.

quanto ao princípio jurisdicional de aderência ao território e da competência territorial, como fica em relação à internet como elemento de comunicação sem fronteiras?

Dificuldades desta natureza não podem ser renegadas ao segundo plano. Antes, devem ser enfrentadas e superadas por aqueles que pretendem disciplinar a matéria. Daí dizer-se da essencialidade, para o direito material, de sua instrumentalidade.

3.2.2 Conceituação

3.2.2.1 Jurisdição

A própria conceituação de jurisdição (*iuris dictio*, ou dizer o direito), a define como uma função cabível ao Estado para prover a garantia e atuação do direito, com o firme propósito de resolução dos conflitos. O império da norma é ministrado e aplicado pelo Estado de forma a garantir a paz social.

A sociedade, por si só, não pode se auto tutelar para prover a resolução dos conflitos decorrentes da interação de seus direitos. Sabemos, por exemplo, que, salvo expressa concessão legal, é ilícito o emprego da auto defesa para prevalecer direitos, sob pena de incorrer em exercício arbitrário das próprias razões.

Neste caso, é inevitável estabelecer critérios para distinguir a jurisdição, em que aponta o seu caráter substitutivo como sendo a necessária intervenção do Estado em substituição das partes titulares, interessadas no conflito, para de forma imparcial, conhecer, decidir e executar o direito pretenso.

Adverte-se que o Estado aqui referido pressupõe àquele que controla o Ordenamento Jurídico e dispõe de meios concretos para aplicação

da norma objetiva. Deduz-se claramente, a figura do Estado real, com territorialidade, soberania e autonomia.

Entretanto, o que pode ocorrer quando se pretende suscitar um direito que paira sobre uma virtualidade? Como identificar o Estado ao qual se recorrer, quando os elementos primários identificadores da jurisdição sobrepujarem as fronteiras desta territorialidade, soberania e autonomia? É de se asseverar, por exemplo, que no caso em estudo, a internet têm como seu elemento caracterizador, o objetivo de estabelecer comunicação sem fronteiras e promover a interação de pessoas em diversas localidades do planeta. Porquanto, foge-se à fixação territorial de um direito **A** ou **B**, supostamente sujeitos à jurisdição estatal. Neste caso, o direito internáutico, seja ele qual for, contrapõe-se a pelo menos um dos princípios elementares da jurisdição; o da aderência ao território.

Os princípios da Jurisdição, doutrinariamente, têm caráter universal e constituem-se de elementos essenciais para a concretude do exercício jurisdicional. Não obstante a importância dos princípios da investidura, indelegabilidade, inafastabilidade e o da inércia, para atendermos ao estreito objeto da nossa pesquisa, enfocamos basicamente dois; o princípio de aderência ao território e o da inafastabilidade, que são correlatos.

3.2.2.2 Princípio da aderência ao território

O princípio da aderência ao território pressupõe que, para que a jurisdição seja exercida, há que haver correlação com um território. Ensinanos Alvim que:

> Não se pode falar de jurisdição, senão enquanto correlata com determinada área territorial do Estado. Tal limite estabelece, inclusive, limite à atividade jurisdicional dos juízes, que, fora do território sujeito por lei à sua autoridade, não podem exercê-la. (ALVIM, 2000, p. 61).

Pellegrini e Dinamarco, também preceituam o seguinte:

> No princípio da aderência ao território manifesta-se, em primeiro lugar, a limitação da própria soberania nacional ao território do país: assim como os órgãos do Poder Executivo ou Legislativo, também os magistrados só têm autoridade nos limites territoriais do Estado. (PELLEGRINI; DINAMARCO, 1992, p. 118)

Entende-se assim, que este princípio tem o escopo de dar ao Estado limites de atuação em seus poderes. Norteia-se claramente pela autonomia e soberania dos outros Estados que, da mesma forma, delimitam suas atuações.

Isto é perfeitamente explicável sob o ponto de vista jurídico-político: do ponto de vista político, excetuando-se os períodos de guerra e de dominação de culturas imperialistas, como as do médio oriente, asiáticas e a norte americana, em que há intensa dominação de Estados totalitários sobre Estados minoritários, quer por razões religiosas, quer por razões políticas, o mundo vivencia hoje um ambiente de respeito às soberanias e autonomias dos Estados.

A pacificação social e a redefinição da estrutura geopolítica mundial, experimentada com o pós-guerra (II Grande Guerra), como o fim da União das Repúblicas Socialistas Soviéticas e a criação de novos Estados, como os oriundos da Iugoslávia, por exemplo, fortaleceram os conceitos de respeito aos limites físicos, políticos, culturais e sociais de cada nação, que consubstanciaram em suas constituições princípios pautados na hegemonia e harmonia das relações internas e internacionais.

Desta forma, guardar respeito à soberania alheia ficou de tal forma arraigada, que os Estados definem em suas próprias leis internas, o respeito a este princípio.

Além disso, os Estados estabeleceram acordos de cooperação para a

realização de atos que atendam a interesses recíprocos, dentre os quais se encaixam alguns de ordem jurídica, como, por exemplo, cartas precatórias e rogatórias, tudo com o objetivo de não invadir a soberania e autonomia do Estado cooperado, que atenderá espontaneamente à solicitação, caso haja previsibilidade legal.

Do ponto de vista jurídico, os limites da Jurisdição encerram os limites do império da Lei. Ora, é juridicamente impossível fazer valer o cumprimento de uma norma alienígena em um território onde a lei emanada e que se quer ver cumprida, sequer tem força coercitiva.

Ademais, o Estado não tem interesse em se ocupar de questões jurídicas supranacionais, face a inalcançabilidade e ineficácia prática da aplicabilidade de suas normas em terras estrangeiras. Mesmo porquê, como já mencionado, quando se fizer necessário o cumprimento de uma lei em um caso específico, em que se pretenda punir agente nacional residente no exterior e passível da incidência de alguma norma legal válida em seu país de origem, existem mecanismos jurídicos devidamente apropriados, inobstante os inúmeros acordos e tratados internacionais firmados entre os Estados.

Aqui, entretanto, comporta mais uma nuance da Jurisdição, que diz respeito à sua extensão. Mais uma vez recorremos a Alvim que define:

> Em obediência a um dever genérico internacional, de reconhecer os demais Estados como soberanos, nos limites de seus respectivos territórios, todo Estado, ainda que em medida diversa, reconhece a atividade desenvolvida pelos demais, mas sem detrimento da própria soberania. Com este objetivo, o Estado expede atos de vontade própria, cujo conteúdo esteja em conformidade com os atos de vontade do Estado estrangeiro. Em vista desta atividade legislativa estrangeira, o Estado nacional prescreve normas preliminares que traçam os limites dentro dos quais o legislador reconhece o direito alienígena, como regra de relações que interessam concomitantemente a estrangeiros e nacionais. Em virtude dessas normas de

> aplicação, o juiz aplica direito estrangeiro, mas como direito nacionalizado e não como direito estrangeiro. A vontade de que o juiz atua somente pode ser a do Estado de que ele é órgão. (ALVIM, 2000, p. 64-65)

Efetivamente, o que se pode deduzir do que foi dito, é que o direito será albergado de uma forma ou de outra, ainda que a Tutela Jurisdicional do Estado esteja limitada pela territorialidade. Mas, como podemos interpretar estas lições à guisa do problema maior: a internet? Como traduzir o princípio da territorialidade para parâmetros de relações jurídicas sem territorialidade?

3.2.2.3 Princípio da inafastabilidade

Como referido, de uma forma ou de outra, o direito tutelado será apreciado. Não pode haver omissão ou afastamento do Estado na administração da Jurisdição. É dever precípuo do Estado, fazer valer o enunciado de direito, estabelecendo o equilíbrio social.

Neste sentido, o Estado, no exercício de sua atividade jurisdicional, não pode se escusar de conhecer a pretensão deduzida pelas partes, sob nenhuma alegação. Este princípio está enunciado pela Constituição Federal Brasileira no artigo 5º, inciso XXXV:

> Art. 5º. Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade nos seguintes termos:
> ⋮
> XXXV — a lei não excluirá da apreciação do Poder Judiciário lesão ou ameaça a direito;

Quando os textos constitucionais, internacionais e legislativos reconhecem, hoje, um direito de acesso aos tribunais este direito concebe-se

como uma dupla dimensão:

1. um direito de defesa ante os tribunais e contra atos dos poderes públicos;

2. um direito de proteção do particular através de tribunais do Estado no sentido de este o proteger perante a violação dos seus direitos por terceiros (dever de proteção do Estado e direito do particular a exigir esta proteção).

A intervenção do Estado para defender os direitos dos particulares perante outros particulares torna claro que o particular só pode, em geral, ver dirimidos os seus litígios perante outros indivíduos através de órgãos jurisdicionais do Estado. Esta *dependência* do direito à proteção jurisdicional do Estado (criação de tribunais, processos jurisdicionais) justifica a afirmação corrente de que o conteúdo essencial do direito de acesso aos tribunais é a garantia da via judiciária (*garantia da via judicial*, *garantia da proteção judicial*, *garantia de proteção jurídica através dos tribunais*).

Tem-se então, que o princípio da inafastabilidade constitui um dos elementos mais importantes da *jurisdictio* e reflete um dever constitucional do Estado de manter a ordem interna e promover a pacificação social.

Porém, mais uma vez, levanta-se uma questão referente a internet. Tendo este princípio, correlação direta com o princípio da aderência ao território em que, somente o tribunal que exerce a jurisdição sobre determinado limite territorial será o garantidor do acesso à justiça proclamado pelo princípio constitucional, como interpretar, por exemplo, a ausência de jurisdição de um outro tribunal, em apreciar dano provocado por internautas de distintas localidades, em contra partida à garantia do acesso à justiça? Poderia um agente **A** domiciliado em território brasileiro, tendo sido prejudicado

pelo agente **B** que é espanhol, mas que praticou o ato lesivo em território japonês, onde passava suas férias, requerer do tribunal japonês a reparação de seu danos? Poderia o tribunal japonês declinar de apreciar o direito por se declarar incompetente e sem jurisdição? Poderia o tribunal japonês recusar a garantia de acesso à justiça?

3.2.2.4 Competência

Vimos que a jurisdição é função do Estado, que no exercício de seu poder de agir, equilibra as relações e estabelece a soberania de uma nação. Aqui a visão é, não só, jurídica, mas do ponto de vista legislativo e administrativo. A noção de jurisdição como poder é temerária e insuficiente, posto que a jurisdição é um *poder-dever* do Estado. Assim, para além de um poder emana-se uma função no exercício do dever estatal.

Mas a jurisdição, apesar de una, necessita de uma distribuição ou de um compartilhamento de funções (competências), posto que, em razão da matéria, das partes, do território, do valor e da função.

Estas distribuições são necessárias ao completo desempenho do Estado no exercício de sua função jurisdicional. A esta distribuição de atribuições chamamos de competência. Doutrinariamente, tem-se que o requisito da competência resulta do fato de o poder jurisdicional ser repartido, segundo diversos critérios, por numerosos tribunais. Cada um dos órgãos judiciários, por virtude da divisão operada a diferentes níveis, fica apenas com o poder de julgar num círculo limitado de ações, e não em todas as ações que os interessados pretendam submeter à sua apreciação jurisdicional.

Tais entendimentos se justificam pela multiplicidade de órgãos jurisdicionais e de foros territoriais. Se o Estado pretende desenvolver suas funções a contento, bem como aplicar seu poder estatal de forma a atender

às necessidades sociais da população e garantir sua soberania e autonomia, deve fazê-lo de maneira que possa maximizar os mecanismos de sua atuação. Sendo o Estado um ente despersonalizado, necessita de descentralizar-se em vários órgãos e atuar através dos tribunais e magistrados espalhados pelo território, que desempenharão cada um, nos limites que lhe forem impostos por lei, a jurisdição.

Dentre todas estas divisões doutrinárias sobre a competência, para não falar em outras, definidas também por lei, interessa-nos a competência em razão do território, por razões óbvias. Se a nós nos cabe investigar o princípio jurisdicional de aderência ao território, cabe a nós explorar também, os limites territoriais da competência, tudo em face do já mencionado direito informático.

3.2.3 Competência em razão do território

A competência territorial atende ao princípio jurisdicional de aderência ao território por estarem, obviamente, intimamente relacionadas. Esta competência diz respeito àquela que o juiz ou tribunal terá para conhecer, processar, julgar e executar o direito contido na pretensão deduzida no âmbito dos limites físicos de atuação de sua jurisdição.

É pois, neste sentido, que o foro da comarca de Lavras, Minas Gerais, por exemplo, será o competente para julgar matéria, definida em lei, que tenha assento nos limites territoriais da região em que tem abrangida sua jurisdição, mesmo que, outros tribunais sejam providos de jurisdição e competência para julgar matéria idêntica. O que os distingue aqui é a limitação da extensão territorial, ou de alcance do braço jurisdicional para aquela questão.

A competência territorial ou competência em razão do território é

a que resulta de aos vários tribunais da mesma espécie e do mesmo grau de jurisdição ser atribuída uma circunscrição, ou seja, uma área geográfica própria de competência, e de a lei localizar as ações nas diferentes circunscrições, mediante o elemento de conexão que para esse efeito reputa decisivo.

Os elementos de conexão: foro do réu, foro do autor, foro do bem imóvel, foro obrigacional, foro hereditário e foro da execução, são decisivos para estabelecer os limites territoriais em que se deve assentar a fixação da competência. São critérios de justiça e de razoabilidade.

Há, entretanto, outro critério doutrinário de relevante importância para o processo civil. Trata-se do interesse direto sobre a matéria. Se a matéria envolver interesse público, não há como se contemplar a mutabilidade do foro competente, porquanto se trata de um direito indisponível, este tendo que correr onde a lei assim o definir. Desta forma, a competência assume os caracteres de improrrogabilidade e de absolutibilidade. Se, entretanto, decorrer de interesses individuais das partes, este pode ser convencionado e pode ser mudado a qualquer tempo, assumindo assim, o caráter de relatividade.

Ressalva Santos (2002, p. 263) que no processo penal, esta distinção não apresenta maior importância, porque, quer seja absoluta, quer, relativa, o juiz deve *ex officio* declarar-se incompetente.

Ainda no estudo da competência territorial, temos que esta competência guarda plena correspondência com a competência internacional. A competência do Estado para prover a sua jurisdição está aqui disposta no sentido amplo. Não só a competência interna, mas também, na externa. Não pode o juiz ou o tribunal nacional ter competência para julgar casos ocorridos no estrangeiro, pois como se viu, além do alcance da jurisdição limitar-se pela territorialidade, a inferência de um tribunal na esfera de outro tribunal com a mesma possibilidade de julgar a matéria, geraria o chamado

conflito de competência internacional. Entretanto, mais uma vez alertamos para as excepcionalidades previstas em leis, tratados e convenções.

3.2.4 Questões processuais de jurisdição e competência

Muito embora a jurisdição e a competência sejam matérias de execução eminentemente processual, é no direito material constitucional e infraconstitucional que elas encontraram guarida legislativa. Citadas já nos tempos do direito romano, somente na década de 60 passaram a ser objeto de estudos mais apurados, posto que, na altura, novas idéias políticas iam surgindo sobre aglutinação de mercados e blocos econômicos (globalização). Naquele preciso momento histórico, os interessados no assunto, pertinentemente, entenderam de regulamentá-las em um espectro mais abrangente.

Assim, com o firme propósito de estender alguns aspectos jurisdicionais, dantes concentrados e limitados nos Estados unitários, firmou-se a Convenção de Bruxelas, protocolada por vários países da Comunidade Européia em setembro de 1968. Este diploma legal acabou por atender, em parte, as dificuldades que seriam enfrentadas com o comércio eletrônico, pois é ele que normaliza até os dias de hoje as disciplinas que tratam da jurisdição e competência, notadamente, as de âmbito internacional. Embora avançado para o seu tempo, não tinha como ter previsto no corpo do texto convencionado o surgimento da internet, posto que a mesma só se deu no ano seguinte, em 1969. Entretanto, o preciosismo dos convencionadores da época, tem ajudado a solver, em medidas limitadas, vários dos problemas gerados pelo uso da rede.

A previsão legal limita-se ao espectro civil e comercial. E é neste último que incide o pilar de quase toda problemática envolvendo a jurisdição e competência na internet.

Os países desenvolvidos são os maiores concentradores de relações negociais e comerciais, onde a compra e venda e circulação de mercadorias envolve bilhões de euros, dólares ou qualquer outro papel-moeda de grande valor. Mas é de lá que também saem os maiores investimentos em tecnologia informática. Toda esta estrutura mercadológica ganhou uma nova dimensão com o surgimento dos *e-Commerce* e *e-Business*, que tiveram desenvolvimento acentuado principalmente nos Estados Unidos e no Japão.

Pessoas físicas (singulares) e jurídicas (coletivas) passaram a gerir imensas transações via internet, comprando e vendendo mercadorias em rede. Em pouco tempo, metade das transações negociais passou a ser feita pela nova via tecnológica da informática. Entretanto, com a mesma rapidez, este comércio começou a enfrentar problemas de diversas ordens; técnicas, de apoio logístico, fiscal (tributário) e jurídicos.

E aqui, não obstante a essência do texto da Convenção de Bruxelas poder ser aplicada a qualquer caso prático de conflito de jurisdição ou competência no âmbito do comércio internacional, é inevitável que se assevere, que o texto já está obsoleto. Quando por exemplo, faz preterir questões fiscais e aduaneiras, deixa de contemplar muito dos outros questionamentos incidentes sobre jurisdição e competência na rede.

A questão tributária é ponto importante também no cenário da internet, porém não é o tema de nossa abordagem. O que se quer mostrar é a superação gradativa da Convenção de Bruxelas para o pleno disciplinamento da matéria.

Neste sentido, a Comissão das Nações Unidas para o Direito Comercial Internacional (CNUDCI), com sede em Viena e criada para harmonizar e unificar as progressivas mudanças na estrutura do mercado internacional, em complementação às normas pactuadas na Convenção de Bruxelas, bem como, para incorporar às demais diretivas européias existentes, dentre elas

a 2000/31/CE, desenvolveu o que é considerado hoje, o melhor modelo de gestão comercial internacional via internet[11].

Este modelo prevê, além de outros pontos, a validade dos dados armazenados em suporte informático como meio de prova em litígio, a questão do momento de formação dos contratos eletrônicos e principalmente, a despeito das questões aqui tratadas, definindo regras sobre o local de recebimento e envio de mensagens de dados eletrônicos. Esta última tem suma importância para o direito internacional privado, pois dela depende não só a apuração do foro competente, mas também a determinação da lei a ser aplicada à uma determinada relação contratual. A lei estabeleceu assim, uma regra básica: a de que as mensagens são consideradas como enviadas e recebidas no local de estabelecimento do remetente e do destinatário (art. 15, item 4 da Lei Modelo).

Entende-se por estabelecimento, a sede física das partes envolvidas na interação. Sede física subentende-se o domicílio residencial ou comercial e não o domicílio informático. Muitos juristas doutrinam que o domicílio informático, conhecido como endereço eletrônico, tem relevância para a fixação da competência e jurisdição, posto que, é através dele que o eventual ato lesivo será veiculado, ou seja, é através do endereçamento eletrônico situado no *Site*, ou na *Home Page* que o agente se utilizará para, por exemplo, passar *spam*[12]. Assim, o endereçamento eletrônico seria o espaço virtual de identificação do agente utilizador[13], mas não necessariamente o seu domicí-

[11] Model Law on Electronic Commerce. Veja texto na íntegra na página `http://www.uncitral.org`.

[12] Diz-se do conjunto de mensagens enviadas por *e-mail* ao destinatário, que não foram solicitadas. (Publicidades, textos religiosos, boletins econômicos, etc.) Estas mensagens costumam sobrecarregar a caixa de correio eletrônico e provocar danos ao usuário. O ato de transmissão do *SPAM* é muito combatido no mundo comercial e jurídico. Em alguns países, como a França, por exemplo, já existem legislações que disciplinam e punem o uso do correio eletrônico, ou *e-mail*. A comunidade jurídica vem se empenhando em legislar a atividade dos *SPAMMERS* como são conhecidos os que enviam as mensagens indesejáveis, ou *lixo eletrônico*

[13] Há casos em que não se pode identificar o agente causador do dano, pois o endereça-

lio legal.

Ora, é evidente que não se pode entender o endereço eletrônico como sendo o domicílio do agente. Aqui há que se esclarecer fatores de limitações técnicas e, porque não dizer, jurídicas. O endereço eletrônico não tem abrigo no computador do agente transgressor. O mesmo, como já mencionado, é um espaço virtual disponibilizado na rede por um provedor de acesso, que pode estar localizado em qualquer parte do globo. Assim, por exemplo, o agente **A** pode residir no Brasil e o seu provedor **X** ficar localizado na França. Nem por isso o agente **A** deixaria de ter acesso ao seu computador para navegar na internet. O que o endereço eletrônico faz é permitir a comunicação entre redes em várias escalas e, como os demais serviços da rede, totalmente sem limitações quanto ao seu emprego e uso. Portanto, não se pode fixar o foro de competência do Estado francês para punir o agente **A**, pois o domicílio, ou o estabelecimento deste está no Brasil.

Entendemos neste caso, que o ato está atrelado ao princípio subjetivo, ou seja, será sempre do sujeito transgressor a responsabilidade direta pelo dano causado e como tal, terá o braço imperioso da lei que alcançá-lo em seu domicílio real. Neste sentido, a Lei Modelo também prevê a impossibilidade das instituições provedoras terem foro de competência. Essa regra tem a grande virtude de afastar (salvo quando as partes acordam o contrário, pois a regra do artigo 15 da Lei Modelo não é cogente, ressalvando expressamente a possibilidade de as partes convencionarem de modo diferente — direito disponível já mencionado) a possibilidade de ser tomada a localização do provedor, como local para definir questões relativas à jurisdição.

Os provedores de acesso à internet são os intermediários da comuni-

mento eletrônico está situado em outro domínio. Entende-se por domínio, o nome de uma área reservada em um servidor, que indica a marca a que pertence a página eletrônica

cação eletrônica, pois funcionam como condutores das mensagens de dados, que armazenam em seus sistemas. Quando se trata de definir um problema relacionado à jurisdição, sempre se questiona a possibilidade de se adotar o estabelecimento físico do provedor como o foro competente. A nova regra supera esse problema adicional, justamente quando delimita o foro competente como sendo o do estabelecimento de uma das partes envolvidas na relação contratual, nunca o do simples intermediário da comunicação informática.

A regra em comento (art. 15 da Lei Modelo) tem ainda outro ponto positivo que merece destaque. É o de estabelecer uma presunção irrefutável quanto a um fato jurídico: o de que o local de expedição ou recebimento de uma mensagem eletrônica será sempre o do estabelecimento dos contraentes, independentemente da localização física da pessoa deles. A lei introduz uma clara distinção entre o local considerado de envio ou recepção da mensagem (que será sempre o do estabelecimento, salvo convenção em contrário) e o lugar em que eventualmente possa estar localizada a parte no momento em que efetivamente a remete ou recebe. Por força dessa regra, é indiferente se um dos contraentes envia ou recebe a mensagem em local situado fora do território de jurisdição ao qual está vinculado seu estabelecimento.

Por exemplo, pode ocorrer de a parte enviar ou receber mensagem de *e-mail* por ocasião de viagem a lugar remoto, distante da localidade de seu estabelecimento, onde se conecta a outro provedor para aceder a internet. Tal circunstância em nada altera a presunção legal. Sempre que outras normas jurídicas (*p. ex.*, normas relativas à formação dos contratos ou normas de Direito internacional privado) requererem que se determine o lugar de recepção ou de expedição de uma mensagem eletrônica de dados, deve-se recorrer à fórmula do lugar do estabelecimento.

É importante observar que a intenção da lei foi a de estabelecer,

como elemento determinante, um vínculo razoável entre a parte e o que se considere lugar de expedição ou recepção de uma mensagem eletrônica de dados, e que o outro contraente possa facilmente identificar esse lugar. Isso é perceptível nas alíneas a e b do seu artigo 15, que plantou regras subsidiárias para as hipóteses em que a parte tem múltiplos estabelecimentos ou não possui nenhum. Para o primeiro desses casos, a lei indica como o lugar que se considera enviada ou recebida a mensagem aquele que guarde a relação mais estreita com a transação subjacente ou, caso não exista transação subjacente, o seu estabelecimento principal. No segundo deles, quando a parte não possui estabelecimento comercial, a solução criada pela lei foi a de se levar em conta a sua residência habitual. Essa última regra, como se vê, tem aplicação para os casos em que o participante da comunicação eletrônica é uma pessoa física ou age em seu nome.

Vê-se pois, que a Lei Modelo atingiu seu escopo e traçou um novo marco no ordenamento jurídico mundial, notadamente quanto às questões de jurisdição e competência para solver lides internáuticas.

Atrelada às demais Convenções e Diretivas européias, a Lei fez transpor aos Estados a complementação das regras essenciais, mas com lacunas quanto às concepções iniciais e tradicionais de jurisdição e competência, abordadas no intróito deste trabalho. As conceituações clássicas, doutrinárias ou não, apontadas inicialmente sobre jurisdição e competência, embora plenamente vigentes e, até mesmo, por constituírem a essência da atividade jurisdicional do Estado, necessitavam sobremaneira de uma imediata ampliação de seu alcance, principalmente no que concerne aos traumas jurídicos provocados pelo surgimento da rede.

Mas, não só os europeus se preocuparam com a conformação de um novo direito processual internacional. Também nos Estados Unidos muitos esforços vêm sendo feitos pelo Congresso Norte-americano em aprovar leis

que regulamentem a matéria. Entretanto, enquanto não a tem por completo delineada, vigora-se pelas terras ianques o princípio jurisdicional chamado de *minimum contact*, ou seja, uma mínima relação existencial entre o sujeito ativo ou passivo do dano provocado na relação comercial eletrônica e a jurisdição do Estado em que o ato foi praticado. Trata-se de nítida exclusão a tese dantes ventilada de que poderia ser foro competente também, o foro eletrônico. Na aplicação deste princípio, a Corte Federal do Estado de Ohio decidiu pelo caso *Compuserve vs. Patterson*. O caso se tornou famoso pela dissidência que provocou no entendimento dos tribunais de lá.

Em suma, tratou-se de um caso em que um usuário residente no Texas que tinha firmado contrato com a Compuserve, provedora americana com sede no estado de Ohio se envolveu em uma pendência judicial com a mesma. Esta para ver dirimida e garantida sua pretensão, suscitou a apreciação da Corte Federal de Ohio. No contrato houvera sido firmado que seria a referida corte de Ohio, a competente para conhecer de eventual lide. Entretanto, a Corte se julgou incompetente para julgar a questão, face ao que chamou de inexistência de um critério de coligação física que vinculasse o usuário do Texas à esfera jurisdicional do Estado.

Este entendimento não pode prosperar, por infringir o princípio elementar do direito processual, que trata de direitos disponíveis. Como se viu ao longo de toda a exposição, a lei consagra que as partes podem eleger a sede do foro competente quando assim o permitir. Isto ocorre, *v.g.*, quando o direito não envolver interesse público e a norma não for cogente. Agindo assim, a douta Corte Judicial Federal americana preteriu um direito contratual garantido. Entendendo desta mesma forma, tal decisão foi reformada pela corte superior, que em grau de apelação sentenciou que a estipulação contratual de que o Estado de Ohio seria o competente para julgar a matéria, atenderia por completo o critério da mínima correlação *sujeito-jurisdição*.

Ou seja, a Corte Federal de Ohio teria fundamentos jurisdicionais suficientes para julgar o caso.

De outro modo, este entendimento também é esposado pela legislação que diz respeito à figura jurídica do consumidor, que já se encontra devidamente legislada e regulada em quase todo o globo. Na realidade, a Convenção de Bruxelas já a contemplava na Secção IV, artigo 13 e seguintes e estipulava um foro especial para este tipo de contratante, é o chamado foro privilegiado. No Brasil, como em outros países, o consumidor tem forte influência nas disputas do *e-Commerce*, mas é reconhecidamente sujeito à vulnerabilidade em relação ao contratante fornecedor. Deste modo, a legislação brasileira, Lei N. 8.078/90, Código de Defesa do Consumidor, amparou aquele que é reconhecidamente a parte hipossuficiente na relação contratual, instituindo inclusive, a inversão do ônus da prova com o objetivo de facilitar a sua defesa.

Os consumidores que atuam pela via eletrônica são, hoje, uma realidade irrefutável. As autoridades européias vêm demonstrando grande preocupação quanto a afirmação dos direitos a serem protegidos no *e-Commerce*. Mas a proposta de Diretiva de Comércio Eletrônico apresentada recebeu críticas fervorosas, pois, apesar de as críticas atingirem outros pontos da Proposta, no seu cerne esteve o princípio do país de origem. Este princípio significaria que os provedores de serviços da sociedade da informação teriam que respeitar (apenas) a legislação do Estado-membro no qual estivessem estabelecidos, mas já não a legislação de outros Estados-membros nos quais os seus serviços pudessem ser recebidos. Em conseqüência da aplicação universal deste princípio, os direitos dos consumidores poderiam ser afetados por várias razões. Primeiro, os prestadores destes serviços procurariam estabelecer-se em Estados-membros com padrões normativos de proteção dos consumidores menos exigentes. Com efeito, estando sujeitos

apenas à legislação de um Estado-membro, os prestadores destes serviços poderiam ser conduzidos a escolher o Estado-membro com padrões normativos menos exigentes em matérias de direitos dos consumidores, para aí se estabelecerem.

4 Punição e prevenção dos crimes de informática

4.1 Bens jurídicos sob tutela e possíveis condutas criminais

A advogada Nigri (1992) elenca algumas condutas que poderiam ser passíveis de tipificação. Esta lista, segundo a autora, é exemplificativa, podendo ser ampliada. Tais condutas são baseadas em modelos internacionais, levando-se em conta a legislação já existente nessa área em diversos países, como Estados Unidos e Inglaterra.

- **Acesso indevido aos sistemas de computador:** Ganhar acesso ou tentar ganhar acesso, indevidamente, a um sistema de computador ou a uma rede de computadores, fazendo o sistema produzir alguma função.

  O simples acesso indevido a um computador, ou a uma rede de computadores, é punido. Pune-se o acesso não autorizado ou o indivíduo que excede os limites de sua autorização. O agente deve estar ciente, no momento do crime, que ele não estava autorizado a ter acesso ao sistema. O agente pode cometer tal crime fisicamente ou remotamente (através de um modem). Basta que o computador responda ao comando do agente indevidamente autorizado para tipificar-se o crime.

O bem jurídico tutelado neste caso é a integridade do sistema e conseqüentemente preservação das informações armazenadas no sistema.

- **Acesso indevido com o intuito de cometer crime mais grave:** Ganhar acesso ou tentar ganhar acesso, indevidamente, a um sistema de computador ou a uma rede de computadores com o intuito de cometer crime mais grave.

  Várias formas qualificadas são previstas, tais como: causar dano, obter vantagem, alterar programas, devassar o sigilo de informações contidas em sistemas. Crime mais grave pode incluir fraude eleitoral, crime de calúnia, injúria e difamação, entre outros.

- **Violação de sistemas de processamento de dados através de senha de outrem:** Utilizar senha de outrem sem a devida autorização com o intuito de ganhar acesso ao computador ou a rede de computadores.

  A utilização de senha de outrem também é prevista como forma qualificada do acesso não autorizado.

- **Fraude através do uso do computador:** Apropriar-se indevidamente de valores através da manipulação de qualquer sistema de processamento de dados, obtendo assim vantagem econômica para si ou para outrem.

  O bem jurídico neste caso é de caráter financeiro: dinheiro, ações, valores. A expressão *qualquer sistema* inclui computadores e redes de computadores diversas, tais como redes bancárias, do mercado de ações, caixa automáticas de serviços bancários.

- **Furto de informações contidas no computador:** Apropriar-se indevidamente de informações contidas em qualquer sistema de processamento de dados, seja temporária ou permanentemente.

Protege-se aqui o direito à informação e ao acesso e uso legítimo da mesma parte do usuário. Protege-se igualmente a privacidade e integralidade do sistema.

- **Falsificação de documentos com o uso da tecnologia do computador:** Alterar, apagar ou falsificar documento através de sistema de computador e seus periféricos e usar este documento falso com o intuito de induzir alguém em erro. Incorre no mesmo crime a pessoa que usa documento sabendo ser ele falso.

  Para efeitos penais, equipara-se documento o dado constante no sistema de computador e qualquer suporte físico tais como: disquete, fita, disco compacto, cd-rom, ou qualquer aparelho usado para armazenar informação seja por meio mecânico, ótico ou eletrônico.

- **Sabotagem:** Impedir ou prevenir o funcionamento de um computador ou de um programa de computador, temporária ou permanentemente, interferindo no sistema de forma a causar distúrbios no mesmo.

  O bem jurídico tutelado é a integridade do sistema, permitindo assim seu funcionamento normal.

- **Danos ao computador e às informações armazenadas no computador:** Causar danos ao computador, destruir, inutilizar, alterar, apagar, suprimir ou modificar os dados e informações contidas no computador, temporaria ou permanentemente, total ou parcialmente.

  O bem jurídico tutelado é a integridade do sistema, permitindo assim seu funcionamento normal.

  Pode haver superposição entre o crime de sabotagem e o de dano. No crime de sabotagem o criminoso tem a intenção de causar distúrbio no funcionamento normal do sistema. Por exemplo, fazer com que o sistema fique lento. Já no crime de dano a intenção é danificar o

sistema.

- **Aquisição ilícita de segredos industriais ou comerciais:** Adquirir segredos industriais ou comerciais ou informações de caráter confidencial com intenção de causar danos financeiros ou obter vantagem pecuniária para si ou para outrem.

  O bem jurídico a ser protegido é o segredo industrial ou comercial.

- **Uso não autorizado de computador — furto de tempo do sistema:** Utilizar sem autorização de quem de direito, ou abusar da autorização que lhe foi conferida, sistema de processamento de dados, de modo a causar perda significativa de recursos.

  O furto de tempo de sistema de processamento de dados visa evitar abusos, normalmente realizados por empregados que utilizam o sistema de computador do empregador para desempenhar tarefas particulares sem a devida autorização do mesmo. O objetivo é, por exemplo, penalizar a pessoa que resolve estabelecer seu próprio negócio às custas do empregador. Uma grande dificuldade neste crime é estabelecer-se a pena a ser atribuída. Uma pena de multa seria aconselhável; ocorre que é difícil calcular-se a quantidade de eletricidade despendida pelo agente. Um bom parâmetro seria estabelecer o valor de mercado da atividade realizada pelo perpetrador do delito.

- **Cópia/uso ilícito de programa de computador:** Reproduzir, modificar, distribuir, importar, exportar, usar programa de computador protegido por lei com o intuito de obter vantagem pecuniária para si ou para outrem sem a devida autorização do autor do programa.

  O bem jurídico a ser protegido é o direito de propriedade de seu autor original ou do detentor da licença para comercialização.

- **Violação de direito autoral:** Usar ou ganhar acesso a rede de

computadores com o intuito de reproduzir, distribuir obras literárias, artísticas e/ou científicas protegidas.

- **Criação, inserção e distribuição de vírus:** Criar, inserir e distribuir programa de computador contendo informações capazes de destruir, modificar, alterar, impedir ou interferir no funcionamento próprio de um sistema de computador ou provocar resultado diverso do esperado ao sistema, com o fim de causar dano físico ou material a outrem ou obter qualquer vantagem para si ou para outrem.

  Para fins penais é irrelevante se o programa maléfico não causa dano ou modificação do sistema.

  Pretende-se aqui punir logo de início a criação do vírus eletrônico, independente do fato de eles serem maléficos ou benéficos ao sistema. Mesmo o vírus mais inocente pode causar a lentidão do sistema, fazendo com que o funcionamento do computador seja afetado. O bem jurídico tutelado é a integralidade do sistema, permitindo assim seu funcionamento normal, e, em caso de dano físico, o bem juridicamente tutelado é a vida.

- **Espionagem:** Obter acesso ilícito a um sistema de computadores com o intuito de apropriar-se de informações confidenciais ligadas a segurança nacional para furtar, copiar, vender ou transferir para outrem.

  Pretende-se aqui proteger sistemas de computadores relativas a segurança nacional assim como a integridade de tais sistemas e informações.

- **Interceptação indevida de telecomunicações:** Interceptar indevidamente a comunicação entre computadores através de grampos durante a transmissão de dados com o intuito de invadir a privacidade do usuário.

- **Violação de base de dados pessoais:** Violar base de dados de caráter pessoal obtendo informações confidenciais do indivíduo.

  O objeto aqui é proteger o indivíduo e suas informações pessoais que podem estar contidas em base de dados bancária, médica, policial, por exemplo. O bem jurídico tutelado é a privacidade.

- **Abuso de Rede ou correio eletrônico:** Usar ou ganhar acesso a rede de computadores com o intuito de disseminar informações fraudulentas ou que gerem crime mais grave.

  Pune-se aqui a utilização de rede de computador para disseminar informações fraudulentas tais como distribuição de programas de computador, de forma a violar direito de autor, ou a distribuição de senhas para quebra de sistema de segurança por *hacker*. Pode-se incluir aqui também a disseminação de pornografia, incitação ao nazismo e racismo através da rede.

4.2 Relato de casos

Nesta seção, mostraremos as condutas levantadas que reiteradamente têm colocado em ameaça a integridade e disponibilidade dos sistemas de computador. Dentre os relatos de casos, haverá também relato de casos ocorridos fora do Brasil, o que não prejudica a pesquisa, pois há possibilidade fática de ocorrem no país. No entanto, os relatos de casos de invasões em outros países são mais satisfatórios.

- **Acesso não-autorizado a sistemas de computadores.** Em linha geral, o acesso não-autorizado ao sistema pode ser praticado de duas formas: com a utilização de senhas que dêem acesso ao sistema e também através das falhas do sistema. O acesso através da utilização

de senha pode ocorrer quando um funcionário de uma empresa, *e. g.*, revela sua senha a um terceiro e este acessa indevidamente o sistema da mesma.

Outro caso de acesso não-autorizado por senha cadastrada no sistema se dá quando, por exemplo, um funcionário de uma empresa é demitido e o seu cadastro ainda permanece no banco de dados da mesma. Como será relatado a seguir, este funcionário ainda com acesso, por vingança, pode danificar o sistema da mesma causando prejuízos. Há também o acesso através de falhas dos sistemas, são as conhecidas *invasões* praticadas pelos *crackers*. Vale ressaltar que esta pesquisa trata apenas de analisar condutas lesivas ao sistema de computador em si, não importando, portanto, se com o acesso não-autorizado viola-se a privacidade, por exemplo. Aqui serão analisadas tão somente as condutas que lesionam ou que potencialmente podem lesionar o sistema de computador, impedindo ou dificultando que ele realize a tarefa para a qual fora destinado.

Hipótese 1: Trata-se de acesso não-autorizado obtido com a utilização de senha cadastrada no sistema. Ocorreu em outubro de 2002. Patrick McKenna que trabalhava para a empresa Bricsnet foi demitido em 20 de outubro de 2000. A empresa, por descuido, não cancelou o cadastro do funcionário no sistema. Dessa forma, ele ainda podia ter acesso ao sistema como se ainda fosse funcionário. No mesmo dia em que fora demitido, McKenna acessou remotamente, via Internet, o sistema da empresa[1].

Ao acessar os computadores da empresa, este funcionário poderia ter apagado dados essenciais ao funcionamento do sistema, causando prejuízos consideráveis para a mesma (ameaça à inte-

[1] Relato completo do caso encontra-se em `http://www.cybercrime.gov/McKennaSent.htm`.

gridade do sistema). Outra atitude que poderia ter ocorrido seria a utilização dos recursos daquele sistema para benefícios pessoais, como, por exemplo hospedar um *site* (ameaça à disponibilidade do sistema). Neste caso de acesso não-autorizado, o que é relevante é a potencialidade de danos à integridade e disponibilidade dos sistemas acessados, pois o indivíduo não estava autorizado e, mesmo sem permissão, acessou aquele sistema.

Hipótese 2: O segundo caso diz respeito à ação *cracker*, às pessoas que buscam falhas nos sistemas e, por esses *buracos*, passam a ter o controle do mesmo. Há vários casos, os mais comuns são as invasões aos *sites*[2]. Os *crackers* invadem o sistema em que o *site* está hospedado e fazem uma modificação apenas no texto do *site*. É como se fosse um aviso para os administradores do *site* que o sistema dele está com falhas. A alteração não é dos arquivos de funcionamento do sistema, mas sim de arquivos *Hypertext Markup Language* (HTML)[3], por exemplo, apenas indicando que eles *estiveram lá*, servindo também para mostrar que a integridade e disponibilidade daquele sistema estavam ameaçadas.

Um caso recente que merece ser citado foi a invasão da página oficial da Câmara de Gestão da Crise de Energia (CGCE)[4]. O *hacker Darko - ph4z3n* invadiu o sistema que hospedava o *site* retirou todos os serviços do ar e ainda deixou as seguintes mensagens:

> *Ainda bem que nós estamos aki (sic) antes do apagão, né...; Esse plano de economia deve-*

[2]Há várias páginas que disponibilizam em seus arquivos esses *sites* invadidos, os chamados *defaced sites*: `www.attrition.org` e `www.hacker.com.br` são exemplos

[3]Linguagem de marcação de hipertexto. Essa linguagem é usada para a formatação das páginas da *web*.

[4]A URL é `http://www.energiabrasil.gov.br`, hoje, evidentemente, sem o *defacement*

ria ser revisto[5].

Não obstante ter retirado os serviços do ar, o *hacker* não danificou o sistema, pois apenas alterou o conteúdo da página. No entanto, o fato de ter alterado o conteúdo, mostra que ele poderia ter danificado os arquivos de sistema, causando assim prejuízos ainda maiores. O mesmo ocorreu com os *sites* do Supremo Tribunal Federal (STF) e Agência Nacional de Energia Elétrica (ANEEL)[6], que foram invadidos como forma de protesto contra o racionamento de energia.

O importante, neste tipo de invasão, é o potencial que os *crackers* têm de afetar a integridade e disponibilidade dos sistemas de computadores. Eles poderiam ter danificado arquivos de sistema. No entanto, apenas colocaram em risco a integridade e disponibilidade do sistema de hospedagem do *site*.

- **Utilização dos recursos do sistema indevidamente.** Têm-se aqui casos que afetam diretamente a disponibilidade do sistema. Disponibilidade do sistema significa o mesmo estar disponível para realizar as tarefas para o qual fora concebido. Serão apresentados, aqui, dois casos exemplificativos.

  Hipótese 1: Os principais casos deste tipo de conduta ocorrem com os chamados ataques DoS (denial of service). De forma simplificada, nestes tipos de ataque, o *cracker* através de um microcomputador controla vários outros computadores que previamente foram infectados com um tipo específico de vírus. No controle desses *computadores-zumbi*, os *crackers* começam bombardear o provedor ou servidor alvo. Este provedor/servidor, ao receber

[5] Maiores informações em `http://www.estadao.com.br/agestado/noticias/2001/jun/14/125.htm`

[6] O *site* desfigurado da ANEEL pode ser acessado pelo seguinte link: `http://www.attrition.org/mirror/attrition/2000/11/07/hidroweb.aneel.gov.br/`

essa quantidade excessiva de mensagens, *cai*, ficando fora do ar. Nestes casos, o sistema de computador não chega a ser danificado, mas é utilizado de maneira exaustiva, ficando assim fora de serviço ou extremamente lento. Ou seja, utilizam-se os recursos do sistema de maneira excessiva, impedindo que ele seja executado para as finalidades para as quais fora concebido.

Um caso que merece ser citado foi o ataque feito por um grupo *cracker* ao *site* da Casa Branca: os invasores enviaram uma grande quantidade de dados para o *site*, provocando uma sobrecarga. Dessa forma, as páginas da Casa Branca ficaram inacessíveis por cerca de seis horas. Segundo oficiais, o conteúdo do *site* não foi danificado nem alterado[7]. Esse tipo de ataque, como se pode perceber, não prejudica a integridade do sistema, apenas faz com que ele não esteja disponível para a realização da tarefa para a qual ele fora programado. Em outras palavras, ataques DoS afetam a disponibilidade do sistema.

Hipótese 2: Outra hipótese possível, porém não muito divulgada, talvez por seu pequeno potencial lesivo, se comparada com as outras, ocorre quando algum *cracker* invade um sistema ou utiliza uma senha de terceiro para acessá-lo e, a partir desse acesso não-autorizado, desvia os recursos dos sistemas para a realização de atividades sem ter pagado ou ter sido autorizado para usufruir as mesmas.

Vários casos são açambarcados por essa hipótese. Ocorrem casos de *hackers* que invadem o sistema de provedor e, tendo o controle dos recursos, instalam servidores de *Internet Relay Chat* (IRC)[8]. Há casos também de *hackers* que utilizam os recursos do provedor

[7] Notícia em: `http://www.estadao.com.br/agestado/noticias/2001/mai/05/11.htm`
[8] Compreende as conhecidas redes de bate-papo.

invadido para armazenar arquivos de seu interesse. Em outros, o *cracker* utiliza senhas indevidas para ter acesso à internet, ou seja, ele não paga por esse serviço, no entanto, utiliza-se dele. Como já foi dito, aqui cabem vários casos de utilização indevida dos recursos do sistema. No entanto, esses casos são menos graves que os advindos de ataques DoS, pois nestes a indisponibilidade do sistema chega a ser máxima. Já, nestes apresentados nesta seção, a disponibilidade é reduzida, mas o sistema ainda continua funcionando, continua *no ar*.

- **Alteração ou destruição de dados essenciais ao funcionamento do sistema.** Tratam-se aqui de hipóteses nas quais a pessoa já possui acesso autorizado ao sistema e dolosamente o danifica ou ainda de *hackers* que invadem o sistema e depois o danifica. Cabe nesta conduta a ação dos vírus de computador, que danificam arquivos essenciais ao sistema Essas condutas afetam diretamente a integridade do sistema, fazendo-o funcionar de forma indevida ou ainda levando à sua total perda.

  Hipótese 1: O caso que será apresentado não foi praticado por um *cracker*, foi fruto de uma perícia para testar a segurança dos sistemas telefônicos de São Paulo. Nada obstante, serve perfeitamente para ilustrar um caso de acesso não autorizado seguido de destruição de dados essenciais ao funcionamento do sistema. Um laudo produzido pelo Instituto de Criminalística, órgão da Secretaria da Segurança Pública de São Paulo, concluiu que qualquer pessoa munida de um computador pessoal, *modem*[9] e um bom conhecimento em informática poderia tirar do ar os sistemas telefônicos paulista e carioca, deixando sem comunicação alguns

[9]Dispositivo para acesso discado a computadores ou redes de computadores como a internet.

milhões de pessoas e empresas que utilizam as linhas para transmitir dados. O *cracker* poderia excluir dados ou mesmo impedir o funcionamento de todo o sistema de telefonia. Na simulação da invasão, o perito conseguiu, depois de algumas tentativas, invadir os computadores centrais das duas empresas, sem que elas se dessem conta. A principal causa da fragilidade desses sistemas estaria na falta de pessoal qualificado para tratar do assunto, aliada ao desconhecimento propriamente dito dos riscos que seus sistemas de informática estão correndo. Além disso, há o fato de os *crackers* estarem sempre se atualizando e estudando as chaves que permitem invadir os computadores alheios. A verdade é que não existe nenhum sistema de computação completamente inexpugnável. Mesmo as redes militares americanas já sofreram ataques de *hackers*. Mas também é certo que existem meios de aumentar a segurança dessas redes.

Este caso mostra indubitavelmente que se fosse um *cracker* que tivesse invadido o sistema de telefonia, ele poderia ter simplesmente derrubado tal sistema, causando prejuízos incalculáveis. Vê-se que aqui a agressão é direta contra a integridade do sistema que, por via reflexa, também ocasiona a indisponibilidade do mesmo.

Hipótese 2: Outro caso de destruição ou alteração de sistema pode ser praticado por funcionário que tenha a senha e dolosamente lesiona o sistema afetando sua integridade. As estatísticas desse tipo de conduta são altas. Segundo Módulo Security (2003, p. 7), 53% das invasões a sistemas de computadores são praticadas por funcionários insatisfeitos da própria empresa. Aqui o dano se dá por ato de quem estar autorizado a acessar o sistema.

Hipótese 3: Uma terceira hipótese que pode ser citada é a destrui-

ção de dados essenciais ao funcionamento pelos chamados vírus de computador. Os vírus podem danificar o sistema, lesando a integridade do mesmo. Há vários tipos de vírus, com as mais diversas finalidades, no entanto, só interessa para esta pesquisa aqueles que danificam o sistema.

Um caso que pode ser citado é o recente vírus O EIC.Trojan, um programa DOS (de apenas 68 bytes) que corrompe o setor de inicialização do *Hard disk* (HD) tornando impossível a partida do sistema. Para escapar à vigilância dos antivírus, o trojan é programado com código similar aos dos arquivos *Standard Anti-virus Test File* (Eicar), que são testes-padrão para identificar a presença de vírus no computador. Além de danificar o setor de boot do disco, o vírus também pode programar outros setores do HD, destruindo pastas e arquivos. Nas máquinas contaminadas, talvez seja possível recuperar o sistema, mediante a reconstrução do setor de boot. No entanto, a programação em outras partes do disco pode também levar à destruição do sistema. Nesse caso não há outra alternativa senão formatar o HD e reinstalar o Microsoft Windows[10].

- **Produzir ou disseminar vírus de computador.** A produção de um vírus de computador é uma ameaça à integridade do sistema. A pessoa, ao produzir um vírus de computador, cria potencialmente a possibilidade de se destruir um sistema de computador. *Disseminar*, por seu turno, ocorre quando uma pessoa, embora não tenha fabricado um vírus, passa-o a outras pessoas. Tal conduta também se caracteriza pela potencialidade de dano aos sistemas de computadores.

  O caso do vírus *I Love You* é exemplificativo. O estudante filipino

[10] O EIC.Trojan, como a maioria esmagadora dos vírus, é específico para a plataforma da Microsoft.

Onel de Guzman criou o vírus e este se espalhou pela Internet por acidente. No entanto, nada obstante ele apenas ter criado o vírus, sem intenção de espalhá-lo pela internet, pode-se dizer que a conduta dele, ao criar um vírus era potencialmente lesiva, o que se concretizou com a disseminação do mesmo pela Internet.

4.3 Legislação a ser usada

A legislação aplicável aos conflitos cibernéticos será a já vigente, com algumas adequações na esfera infraconstitucional. Como norma-base, teremos a Constituição Federal, servindo as demais leis para a proteção dos bens jurídicos atingidos por meio do computador, sendo plenamente aplicáveis o Código Civil, o Código de Defesa do Consumidor, a Lei dos Direitos Autorais, a Lei do Software e o próprio CP, sem olvidar a Lei do *Habeas Data*.

Aras (2001) elenca alguns tipos penais, que descrevem crimes de informática, já existentes. São eles:

1. O artigo 10 da Lei Federal N. 9.296/1996, que considera crime, punível com reclusão de 2 a 4 anos e multa:

   > Art. 10 - Realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo de Justiça, sem autorização judicial ou com objetivos não autorizados em lei.

2. O artigo 153, § 1°-A do CP, com a redação dada pela Lei Federal N. 9983/2000, que tipifica o crime de divulgação de segredo punindo-o com detenção de 1 a 4 anos

> Art. 153 ...
> § 1°-A - Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública.

3. O artigo 313-A, do CP, introduzido pela Lei N. 9983/2000, que tipificou o crime de inserção de dados falsos em sistemas de informações, com a seguinte redação e punindo-o com pena de reclusão, de 2 a 12 anos e multa:

> Art. 313-A - Inserir ou facilitar o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano.

4. O artigo 313-B, do CP, introduzido pela Lei n.° 9983/2000, que tipificou o crime de modificação ou alteração não autorizada de sistema de informações, com a seguinte redação e cominando-lhe pena de detenção, de 3 meses a 2 anos, e multa:

> Art.313-B - Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente.

5. O artigo 325, §1°, incisos I e II, introduzidos pela Lei N. 9983/2000, tipificando novas formas de violação de sigilo funcional, nas condutas de quem:

> Art. 325...
> § 1º ...

> I - permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou bancos da Administração Pública.
> II - se utiliza, indevidamente, do acesso restrito.

Ambos sancionados com penas de detenção de 6 meses a 2 anos, ou multa;

6. O artigo 12, caput, §§ 1° e 2°, da Lei Federal N. 9609/1998, que tipifica o crime de violação de direitos de autor de programa de computador, punindo-o com detenção de 6 meses a 2 anos, ou multa; ou com pena de reclusão de 1 a 4 anos e multa, se agente visa lucro;

7. O artigo 12, inciso V, da Lei N. 8137/1990, que considera crime

> Art. 12 ...
> V - Utilizar ou divulgar programa de processamento de dados que permita ao sujeito passivo da obrigação tributária possuir informação contábil daquela que é, por lei, fornecida à Fazenda Pública.

8. O artigo 72 da Lei N. 9504/1997, que cuida de três tipos penais eletrônicos de natureza eleitoral.

> Art. 72. Constituem crimes, puníveis com reclusão, de cinco a dez anos:
> I - obter acesso a sistema de tratamento automático de dados usado pelo serviço eleitoral, a fim de evitar a apuração ou a contagem de votos;
> II - desenvolver ou introduzir comando, instrução, ou programa de computador capaz de destruir, apagar, eliminar, alterar, gravar ou transmitir dado, instrução ou programa ou provocar qualquer outro resultado diverso do esperado em sistema de tratamento automático de dados usados pelo serviço eleitoral;

> III - causar, propositadamente, dano físico ao equipamento usado na votação ou na totatalização de votos ou suas pastas.

Verifica-se, portanto, a preocupação dos legisladores infraconstitucionais de protegerem bens informáticos e de assegurar, na esfera penal, a proteção a dados de interesse da Administração Pública e da privacidade telemática do indivíduo.

Como se pode verificar, a legislação existente não é suficiente para garantir a punição do criminoso fazendo-se necessária uma tipificação indubidosa e eficaz, com condutas ainda não tipificadas em lei.

4.4 As provas

A idéia de que a internet é um novo espaço em que os delitos costumam ficar impunes, como já dissemos, carece de fundamentos. As mesmas vantagens que a Rede trás ao delinqüente moderno podem também ser de serventia para técnicos que participam das investigações em busca de provas e evidências da identidade e origem do suposto infrator.

As novas técnicas e modalidades geram um outro tipo de investigação que podem ter resultados inequívocos na determinação da autoria e mecânica de um delito, porém exige do investigador um conhecimento bem mais específico da matéria. Por outro lado, a grande inovação que a internet proporciona as técnicas de investigação, é a possibilidade de obter uma cópia exata dos elementos que fizeram parte da transação ilícita. Desde mensagens transmitidas pelos participantes até os próprios efeitos e mecânica do delito.

O Código de Processo Penal (CPP) prescreve no seu artigo 158 que,

quando a infração deixar vestígios será indispensável o exame de corpo de delito, ou seja, é necessário que se colha as provas da existência do crime por intermédio da perícia técnica. Em uma definição simplificada, prova é qualquer informação com valor comprobatório, seja para confirmar ou rejeitar uma determinada hipótese.

Segundo Gomes (2002), o primeiro passo para o levantamento das evidências é a obtenção de uma mandado judicial dando amplos poderes à equipe de respostas a incidentes para fazer uma devassa na máquina examinada. Tal procedimento, apesar de dispensável, é de grande importância, pois geralmente subestima-se a dimensão de um incidente, e no curso da investigação descobre-se algo que não se estava procurando, mas é de grande importância, talvez maior que o próprio incidente.

A obtenção dos elementos de provas deve sempre observar os limites constitucionais e suas regras estão devidamente expressas na Lei de Interceptação Telefônica, porém nosso aparato técnico ainda deixa a desejar. Inúmeras são as ferramentas auxiliares na persecução penal, e a primeira delas é a base de dados *WHOIS*[11] e no Brasil a FAPESP ambas de acesso público e gratuito que permitem conhecer a titularidade de um domínio e seus responsáveis administrativos e financeiros. Das informações ali contidas consta o nome, o domicílio, e o telefone, assim como o IP do servidor primário e secundário.

Um exemplo é o caso de iniciar uma investigação para obter provas sobre uma máquina que foi invadida e teve dados roubados. No decurso da investigação descobre-se que o funcionário que usava a máquina, estava executando diversos programas maliciosos com o intuito de invadir o servidor da rede, além disso, enviou dados sigilosos, por *e-mail*, para a concorrên-

[11] O serviço WHOIS é uma base de dados com acesso público onde podemos obter, entre outras informações, o responsável (pessoa física ou jurídica) por certo domínio da rede. O serviço brasileiro pode ser acedido em `http://registro.br`.

cia. Se caso os investigadores não estivessem munidos de mandado judicial para fazer uma devassa no *e-mail* do funcionário, as provas obtidas seriam tidas como ilícitas e imprestáveis para embasar uma ação judicial ou uma demissão.

A regra geral a ser aplicada para resguardar as evidências de um crime de informática após um ataque, como o furto de dados, por exemplo, é: se você não tem total certeza do que está fazendo não faça nada, chame alguém que entenda. Tal regra é de extrema importância pois se está trabalhando com informações que são extremamente voláteis e a perda de alguns dados poderá inviabilizar toda a investigação.

Se caso o usuário continue operando a máquina poderá haver alteração da hora e data do sistema, subscrição de dados no disco rígido etc.. E se por ventura a máquina for desligada, muitos dados importantes, como o registro e o conteúdo da memória, estado das conexões de rede e dos processos em execução serão perdidos. Devido a isso, recomenda-se manter a máquina ligada, sem uso, e chamar o mais rápido possível a equipe de resposta a incidentes.

A equipe de resposta a incidentes deverá chegar ao local o mais rápido possível, isolar a área, controlar o acesso de pessoas, desligar a máquina da rede e iniciar a coleta de provas fazendo uma imagem do disco rígido da máquina atacada, gravando tudo em uma mídia não regravável, inclusive utilizando algum sistema criptográfico ou de paridade com a finalidade de garantir a integridade dos dados. Além de etiquetar as mídias e anotar todos os passos tomados.

Com relação aos procedimentos de cópia ou *backup* dos dados da máquina atacada, é necessário, ainda segundo Gomes, que se faça distinção entre imagem e cópia.

> Na primeira, existe a preocupação, que não existe na segunda, de se colocar cada bit de dado no mesmo local que se encontrava originalmente no disco rígido, no mesmo cilindro do mesmo cluster. Com isso, obtém-se um retrato fiel do disco que se está examinando. Como a imagem não pode ser alterada, pois se encontra em uma mídia não regravável, já se tem uma prova para embasar uma ação judicial. Ademais, os peritos poderão simular, em laboratório, o funcionamento da máquina no momento do ataque, podendo descobrir novas evidências e o modo de agir do criminoso. Além disso, as provas poderão passar por outras perícias ou contraprovas. (GOMES, 2002).

Após ou concomitantemente ao exame da máquina atacada a equipe de resposta deverá fazer uma análise física e lógica de toda a rede recolhendo os *logs* dos *firewalls*, *Intrusion Detection System* (IDS), antivírus, roteadores e sistemas de controle de acesso físico.

Concluído o levantamento de todos os dados já se terá em mãos uma grande quantidade de provas, mas que ainda encontra-se em estado bruto sendo necessário o envio de todo material para a perícia técnica ou para a perícia da equipe de respostas a incidentes, levando-se sempre em consideração que o Código de Processo Penal art. 159, § 1º determina que: Não havendo peritos oficiais, ou seja, aqueles que são investidos na função por lei, é necessário que o exame seja feito por duas pessoas idôneas, portadoras de diploma de curso superior, escolhidas de preferência, entre as que tiverem habilitação técnica relacionada à natureza do exame. Ademais, conforme o entendimento solidificado dos nossos tribunais, a perícia feita por uma só pessoa é nula.

E ainda, segundo o CPP art. 160 os peritos elaborarão um laudo pericial onde descreverão minuciosamente o que examinarem e responderão aos quesitos formulados. Tais quesitos são questões estabelecidas sobre um assunto específico, que exigem respostas, opiniões e pareceres, como por

exemplo: É possível determinar se a máquina periciada foi invadida? A que horas? Houve algum dado copiado? Quais foram os comandos executados?

Portanto, somente após o laudo pericial será possível determinar o que aconteceu, se houve algum crime e qual foi o delito perpetrado. Aqui, encerra-se todo o processo de levantamento da provas e será possível dar início a uma ação judicial.

Também existem outras ferramentas que permitem através da análise do correio eletrônico chegar a sua origem e traçar a rota desde a mesma. Como visto existem numerosas fontes de informação de acesso público, que permitem associar a direção de correio eletrônico a uma pessoa determinada sem alterar o titular.

Especificamente no caso de *e-mail* gratuito, se pode conhecer a identidade do usuário, estando os servidores desse tipo obrigados a facilitar os dados de seus usuários a autoridade judicial que o requerer. Apesar de tantas ferramentas existem alguns obstáculos que devem superados não somente no que tange ao Brasil, tendo em vista a característica de transnacionalidade desse tipo de delito. Dentre eles temos: a escassez de meios técnicos, burocracia do judiciário no momento da emissão dos competentes mandados e principalmente os problemas de jurisdição.

Como se vê, a produção de provas nos crimes de informática é um processo demorado, caro e exige pessoal altamente especializado onde um único erro acarreta a imprestabilidade das provas. Diante disso, o usuário doméstico fica indefeso, pois dificilmente poderá contratar pessoal capacitado para colher as provas e a Polícia, apesar do grande avanço das delegacias especializadas nos crimes de informática, pouco poderá fazer.

4.5 Julgados

Aqui apresentamos alguns julgados proferidos pelo Judiciário brasileiro. A jurisprudência é escassa mas já parece bem sedimentada, com uma orientação bem definida.

Neste *Habeas corpus* a tônica é a já apresentada quando discutimos acerca dos crimes impróprios na seção 2.4 na página 62, ou seja, o que há de novo é a forma com a qual o crime já tipificado foi consumado e não um novo crime. Não há que se falar em aplicação da lei por analogia. Novas técnicas para cometimento de ilícitos não criam, necessariamente novos crimes.

> *Habeas corpus* 76689/PB, Rel. Min. Sepúlveda Pertence, 1ª Turma, STF.
> Ementa: Crime de Computador: publicação de cena de sexo infanto-juvenil (Estatuto da criança e do adolescente (ECA), art. 241), mediante inserção em rede BBS/Internet de computadores, atribuída a menores: tipicidade: prova pericial necessária à demonstração da autoria: *Habeas corpus* (HC) deferido em parte.
> 1. O tipo cogitado - na modalidade de 'publicar cena de sexo explícito ou pornográfica envolvendo criança ou adolescente' — ao contrário do que sucede por exemplo aos da Lei de Imprensa, no tocante ao processo da publicação incriminada é uma norma aberta: basta-lhe à realização do núcleo da ação punível a idoneidade técnica do veículo utilizado à difusão da imagem para número indeterminado de pessoas, que parece indiscutível na inserção de fotos obscenas em rede BBS/Internet de computador. 2. Não se trata no caso, pois, de colmatar lacuna da lei incriminadora por analogia: uma vez que se compreenda na decisão típica da conduta criminada, o meio técnico empregado para realizá-la pode até ser de invenção posterior à edição da lei penal: a invenção da pólvora não reclamou redefinição do homicídio para tornar explícito que nela se compreendia a morte dada a outrem mediante arma de fogo. 3. Se a solução da controvérsia de fato sobre a autoria da inserção incriminada pende de informações técnicas de telemática que ainda pairam acima do conhecimento do homem comum,

impõe-se a realização de prova pericial.

O caso a seguir apontado abordou a distinção entre *hardware* e *software* e o tratamento jurídico que ambos recebem, em regimes diferenciados.

> Tribunal de Alçada Criminal do Estado de São Paulo. Apelação 669.353/2, julgada em 28.08.91, publicada na RJDTACRIM, volume 12, página 69. Relator: Penteado Navarro.
> Ementa: CRIME CONTRA A PROPRIEDADE INDUSTRIAL - *Hardware* e *software* - Proteção jurídica de um e de outro por ramo distinto do direito privado - Entendimento - Proteção constitucional.
> ***Hardware* e *software* não se confundem no campo jurídico**. *Hardware* está em âmbito do Direito de Propriedade Industrial. *Software* está em âmbito do Direito Autoral. Não se confunde, pois, *software* com o correspondente suporte (disquete, fita cassete, ou *chip*), que se constitui em seu corpo mecânico (assim como disco é o suporte da música, esta obra intelectual protegida). Programa e disquete não se confundem, não dando ensejo a crime de violação de marca de industria ou comércio e de concorrência desleal. - Genericamente a propriedade de marca está protegida pela Constituição da República (art. 5º, XXIX). Porém, essa proteção não é ilimitada, visto que incide somente na classe correspondente à atividade, conforme o disposto no art. 53, caput, do Código de Propriedade Industrial. A lei leva em conta o gênero de comércio ou indústria, sem cogitar de identidade ou semelhança, entre os produtos ou artigo, mas da identidade ou da afinidade dos ramos de negócio. (destacado do original).

No texto do acórdão, destaca-se a seguinte passagem:

> Logo, a Apelante investiu contra texto expresso de lei e ainda, o que é pior, denominou os disquetes de *software* quando eles são um corpo mecânico para armazenar dados do computador, ou seja, fazem parte dos componente denominados *hardware*.
> Cometeu, assim, erro grosseiro, já que o programa ou sistema é uma manifestação intelectual usada no funcionamento do computador ou máquina.

> No campo jurídico, a **diferença entre o *hardware* e o *software*** é tão distante que o primeiro está no âmbito de incidência do Direito de Propriedade Industrial, enquanto que o segundo pertence ao Direito Autoral. (destacado do original).

E mais adiante:

> Demais, em recente acórdão do egrégio Tribunal de Justiça (Apelação Cível n. 126.690-1), tomado por unanimidade de votos, esta relatoria fez a seguinte citação: 'o *software* — que é gravado em disquete, fita cassete ou *chip* (pastilha) — representa um conjunto de instruções estruturado em códigos e edificado em linguagem própria que possibilita à máquina (computador) realizar suas finalidades (arquivo de textos, edição. operação de cálculos, gráficos etc.) ... não se confunde, pois, *software* com o correspondente suporte (disquete, fita cassete ou *chip*), que se constitui em seu corpo mecânico (assim como disco é o suporte da musica, esta, a obra intelectual protegida)'....

Selecionamos dois casos relativos a apreensão de computadores. No primeiro, trata-se de uma decisão em mandado de segurança que envolvia uma ordem de apreensão, deferida em juízo cautelar, com o objetivo de apurar a comprovação de infração às disposições criminais da Lei 7.646/87[12]:

> MANDADO DE SEGURANÇA - Número Do Processo: 0081767800 - Comarca De Origem: Curitiba - Orgão Julgador: Segundo Grupo De Câmaras Criminais. Data De Julgamento: 13.12.95 - Relator: Juiz Milani De Moura. Decisão: Unânime, confirmada a liminar para conceder, em definitivo, o *mandamus*. Número De Arquivo Do Acordão: 301 Ramo Do Direito: Criminal Data De Publicação: 09.02.96.
> Ementa: MANDADO DE SEGURANÇA - impetração visando desconstituir busca e apreensão de computadores - apreensão de computadores - apreensão deferida em medida cautelar objetivando colher a materialidade

[12]Tal lei foi revogada expressamente pela Lei N. 9.609 de 19 de fevereiro de 1998 (Lei do *Software*)que regula a mesma matéria.

> de eventual delito cunhado no art. 35, da lei N. 7.646/87 (Lei do *Software*) - objetos não sujeitos a vistoria de que trata o art. 38, parágrafo único, da citada lei - excesso desnecessário na busca e apreensão - ilegalidade caracterizada - afronta ao direito de propriedade - segurança concedida.
> Não sendo os bens necessários ao deslinde da questão, não interessando, inclusive, à eventual ação penal, por não sujeitos à vistoria de que trata o parágrafo único, do art. 38, da Lei do *Software*, forçoso é reconhecer que houve excesso na ordenada busca e apreensão, a pretexto de se colher material para formação de corpo de delito, constituindo-se, assim, a medida, em flagrante ilegalidade, ferindo direito líquido e certo da proprietária impetrante, reparável via *mandamus*.

No segundo, o assunto a merecer destaque é a validade das provas obtidas através da análise da memória de computador apreendido.

> Supremo Tribunal Federal. Ação Penal Originária307, julgada em 13.12.94, publicada no DJ de 13.10.95. Relator:Ilmar Galvão.
> Ementa: AÇÃO CRIMINAL. CP. Corrupção Passiva (Art. 317, Caput), Corrupção Ativa De Testemunha (Art. 343), Coação No Curso Do Processo (Art. 344), Supressão De Documento (Art. 305) E Falsidade Ideológica (Art. 299). Preliminares: Inadmissibilidade de provas consideradas obtidas por meio ilícito e incompetência do Supremo Tribunal Federal para os crimes do Art. 299, a ausência de conexão com o de corrupção passiva, que determinou a instauração do processo perante essa corte, posto que atribuído, entre outros, A Presidente da República.

A ementa não é suficientemete esclarecedora, mas no corpo do acórdão estão as disposições realmente úteis, como se pode ver:

> 1. ...
> 1.1. Inadmissibilidade, como prova, de laudos de degravação de conversa telefônica e de registros contidos na memória de micro computador, obtidos por meios ilícitos (art. 5., LVI, da Constituição Federal); no primeiro caso, por se tratar de gravação realizada por um

> dos interlocutores, sem conhecimento do outro, havendo a degravação sido feita com inobservância do princípio do contraditório, e utilizada com violação a privacidade alheia (art. 5º, X, da Constituição Federal (CF)); e, no segundo caso, por estar-se diante de micro computador que, além de ter sido apreendido com violação de domicílio, teve a memória nele contida sido degravada ao arrepio da garantia da inviolabilidade da intimidade das pessoas (art. 5º, X e XI, da CF).
> 1.2. Improcedência da acusação. Relativamente ao primeiro episódio, em virtude não apenas da inexistência de prova de que a alegada ajuda eleitoral decorreu de solicitação que tenha sido feita direta ou indiretamente, pelo primeiro acusado, mas também por não haver sido apontado ato de ofício configurador de transação ou comércio com o cargo então por ele exercido. No que concerne ao segundo, pelo duplo motivo de não haver qualquer referência, na degravação sido feita com inobservância do principio do contraditório, e utilizada com violação à privacidade alheia (art. 5º, X, da CF); e, no segundo caso, por estar-se diante de micro computador que, além de ter sido apreendido com violação de domicílio, teve a memória nele contida sido degravada ao arrepio da garantia da inviolabilidade da intimidade das pessoas (art. 5º, X e XI, da CF).

Cabe salientar que se trata do acórdão do julgamento do caso Collor e P. C. Farias, junto ao Supremo Tribunal Federal, no qual as provas obtidas através das memórias dos computadores apreendidos não foram consideradas válidas, como se viu.

Sob a argumentação de que é vivido hoje um momento de forte presença dos recursos tecnológicos, no caso a seguir apresentado foi decidido pela admissibilidade inicial de gravação magnética.

> AGRAVO DE INSTRUMENTO. Número Do Processo: 0076684100. Comarca De Origem: Curitiba. Orgão Julgador: Sétima Câmara Cível. Data De Julgamento: 17.04.95. Relator: Juiz Conv. Ruy Cunha Sobrinho. Decisão: Unânime, Negado Provimento. Número De Arquivo Do Acordão: 3704 Data De Publicação: 05.05.95.

> Jurisprudência: Revista Da Associação Dos Magistrados Do Paraná 31/28. Rt 599/66. Rt 603/178. Rt 620/150. Ementa: PROCESSUAL CIVIL - Prova - Gravação Magnética - Admissibilidade. AGRAVO IMPROVIDO. Na era da informática não se pode excluir 'a priori' prova que se pretende produzir através de gravação magnética.

O julgamento de *Habeas-Corpus* adiante trata da possibilidade jurídica de interceptação de fluxo de dados.

> Acórdão HC15026/SC
> *HABEAS CORPUS* 2000/0126493-1
> Relator Min. VICENTE LEAL
> Data da Decisão: 24/09/2002 Orgão Julgador: T6 - SEXTA TURMA.
> Ementa: CONSTITUCIONAL. Processual Penal. *Habeas-Corpus*. Sigilo De Dados. Quebra. Busca E Apreensão. Indícios De Crime. Investigação Criminal. Legalidade. CF, ART. 5º, XII. LEIS 9.034/95 E 9.296/96. Embora a Carta Magna, no capítulo das franquias democráticas ponha em destaque o direito à privacidade, contém expressa ressalva para admitir a quebra do sigilo para fins de investigação criminal ou instrução processual penal (art. 5º, XII), por ordem judicial. - A jurisprudência pretoriana é unissonante na afirmação de que o direito ao sigilo bancário, bem como ao sigilo de dados, a despeito de sua magnitude constitucional, não é um direito absoluto, cedendo espaço quando presente em maior dimensão o interesse público. - A legislação integrativa do canon constitucional autoriza, em sede de persecução criminal, mediante autorização judicial, "o acesso a dados, documentos e informações fiscais, bancários, financeiras e eleitorais"(Lei N. 9.034/95, art. 2º, III), bem como "a interceptação do fluxo de comunicações em sistema de informática e telemática"(Lei N. 9.296/96, art. 1º, parágrafo único). — *Habeas-corpus* denegado.

4.6 Formas de prevenção

Esta seção é um resumo das principais recomendações contidas em NIC BR Security Office (2003b), um guia com informações para configurar, administrar e operar redes ligadas à internet de forma mais segura.

4.6.1 Políticas

Uchôa (2003) recomenda que a elaboração de uma política de segurança e de uso é prioridade em um ambiente computacional.

1. elaboração de uma política de segurança, com apoio da administração da organização;
2. divulgação da política de segurança entre os usuários da rede;
3. elaboração e divulgação de uma política de uso aceitável.

4.6.2 Instalação e Configuração Segura de Sistemas

1. Antes da instalação:
   (a) planejamento dos propósitos e serviços do sistema;
   (b) definição do particionamento do disco;
   (c) provisão de mídias e documentação necessárias à instalação.
2. Durante a instalação:
   (a) escolha de uma senha forte para o administrador;
   (b) instalação do mínimo de pacotes, com o sistema fora da rede;
   (c) documentação da instalação no *logbook*.

3. Após a instalação:

   (a) desativação de serviços instalados e não utilizados;

   (b) instalação de correções de segurança; configuração do servidor *Simple Mail Transfer Protocol* (SMTP), fechando o *relay*;

   (c) configuração do *proxy web*[13], ajustando os controles de acesso.

4. Antes de conectar o sistema em rede:

   (a) verificação das portas *Transmission Control Protocol/User Data Protocol* (TCP/UDP) abertas, usando um comando como o *netstat*;

   (b) ajuste nas regras de *firewall* apropriadas, para liberar o tráfego para o novo sistema.

4.6.3 Administração e Operação Segura de Redes e Sistemas

1. Educação dos usuários:

   (a) divulgação de documentos de educação do usuário, sobre segurança de redes[14].

2. Ajuste do relógio:

   (a) instalação e configuração de um servidor local de tempo (por exemplo, *Network time protocol* (NTP));

   (b) sincronização dos relógios dos sistemas da rede com o relógio do servidor local de tempo;

[13] Um *proxy web* é um *software* que media o acesso entre um cliente e um servidor web. Tipicamente, situa-se numa rede local, entre o resto das máquinas da rede e a Internet. É um elemento fundamental na segurança de uma rede e assegura o controle dos conteúdos a que se pode aceder

[14] Um documento introdutório é a "Cartilha de Segurança para a Internet", disponível em `http://www.nbso.nic.br/docs/cartilha/`.

(c) ajuste do *timezone* dos sistemas.

3. Equipes de administradores:

   (a) criação de listas de discussão para a comunicação entre os administradores de redes e sistemas da organização;

   (b) estabelecimento de procedimentos e/ou instalação de ferramentas para controle de alterações na configuração dos sistemas;

   (c) estabelecimento de procedimentos e/ou instalação de ferramentas que permitam um controle sobre a utilização de contas privilegiadas (*root* e *Administrator*).

4. Logs:

   (a) habilitação do *logging* em sistemas e serviços;

   (b) estabelecimento de um procedimento de armazenamento de *logs*;

   (c) instalação e configuração de um *loghost* centralizado;

   (d) estabelecimento de um procedimento de monitoramento de *logs*;

   (e) instalação de ferramentas de monitoramento automatizado e de sumarização de *logs*.

5. Cuidados com *Domain Name Service* (DNS):

   (a) limitação de transferências de zona nos servidores DNS mestres e escravos;

   (b) separação de servidores com autoridade e recursivos; configuração do servidor DNS para execução com privilégios mínimos;

   (c) preservação de informações sensíveis (incluindo versão do serviço) registradas no DNS;

   (d) configuração do DNS reverso para todos os *hosts* da rede.

6. Informações de contato:

   (a) implementação dos *e-mails abuse* e *security*;

   (b) atualização dos contatos (especialmente o técnico) no WHOIS/-serviço de registro.

7. Eliminação de protocolos sem criptografia:

   (a) substituição de aplicativos como Telnet, FTP, rlogin, rsh e rexec por *Secure Shell* (SSH);

   (b) substituição de POP3 e *Internet Message Access Protocol* (IMAP) sem criptografia por soluções de *e-mail* com criptografia (POP3 ou IMAP sobre *Secure Sockets Layer* (SSL), *Webmail* sobre HTTPS).

8. Cuidados com redes reservadas:

   (a) filtragem dos endereços pertencentes a redes reservadas e não alocadas;

   (b) configuração de tabelas de *hosts* e/ou servidores DNS privados quando são utilizados internamente endereços de redes reservadas.

9. Políticas de *backup* e restauração de sistemas:

   (a) definição da periodicidade dos *backups*;

   (b) definição dos dados que devem ser copiados;

   (c) escolha de um local adequado para o armazenamento dos *backups*;

   (d) estabelecimento de um procedimento de verificação de *backups*;

   (e) estabelecimento de um procedimento para a restauração de sistemas a partir do *backup*.

10. Como manter-se informado:

    (a) inscrição nas listas de anúncios de segurança dos fornecedores de *software* e/ou *hardware*;

    (b) inscrição nas listas de administradores e/ou usuários dos produtos usados na sua rede;

    (c) inscrição na lista de alertas de segurança do *Computer Emergency Response Team* (CERT).

11. Precauções contra engenharia social:

    (a) treinamento de usuários e administradores contra possíveis tentativas de descoberta de informações sobre a rede da organização;

    (b) busca e remoção de documentos que contenham tais informações e que estejam disponíveis nos servidores de rede;

    (c) preservação de informações sensíveis ao solicitar auxílio em fóruns públicos na internet.

12. Uso eficaz de *firewalls*:

    (a) escolha de um *firewall* que rode em um ambiente com o qual os administradores estejam acostumados;

    (b) instalação de *firewalls* em pontos estratégicos da rede, incluindo, possivelmente, *firewalls* internos;

    (c) uso de uma DMZ[15] para confinamento dos servidores públicos;

    (d) implementação de *ingress* e *egress filtering* no perímetro da rede.

13. Redes wireless:

[15] A abreviação vem de ***de****militarized* ***z****one* e é usada para designar uma subrede que encontra-se entre uma rede interna, como uma LAN privada, e uma rede insegura e externa, como a internet.

(a) definição de uma política de Uso da Rede *Wireless*;

(b) posicionamento cuidadoso dos APs visando minimizar o vazamento de sinal;

(c) segregação da rede *Wireless Local area network* (WLAN) da rede interna da instituição;

(d) uso de *Wired Equivalent Privacy* (WEP);

(e) uso de criptografia na aplicação (SSH, SSL, etc);

(f) adoção de *Wireless Application Protocol* (WAP) e 802.11i[16], quando disponíveis;

(g) mudança da configuração default dos APs (senhas, SSID[17], SNMP *communities*, etc);

(h) desligamento do broadcast de SSID;

(i) proteção dos clientes *wireless* (aplicação de *patches*, uso de *firewall* pessoal, antivírus, etc.);

(j) monitoração da rede *wireless*.

4.7 Condutas recomendadas em caso de *hacking*

Mesmo tendo instalado firewall e um IDS, são necessários certos cuidados quando um incidente de segurança acontece (note que não dissemos *se*, porque um incidente acontecerá mais cedo ou mais tarde).

Para estar bem preparado é necessário saber que atitudes tomar com relação a um incidente de segurança. Uma boa alternativa, reportada em INTERPOL (2000), é seguir o roteiro abaixo:

[16]Padrão IEEE que especifica meio de acesso e camada física para redes sem fio de 1 e 2 Mbps, com con exões entre dispositivos fixos, portáteis e móveis dentro de uma área local.

[17]Um identificador fixo ao pacote de dados que são enviados sobre uma WLAN e que funciona como uma senha para entrada em uma WLAN particular

Preparação : Este estágio cobre coisas como a política, suporte da gerência, o treinamento e as relações com os as autoridades legais.

Identificação : Como identificar um incidente, equipe de funcionários responsáveis, uma coordenação com os fornecedores de equipamentos/*software* de rede.

Contenção : Criar uma equipe no local para examinar a situação. *Backup* do sistema. Determinação do risco (de o sistema voltar funcionar).

Erradicação : Fazer análise da vulnerabilidade. Remova a causa do incidente. Valide o sistema.

Continuação : Desenvolva um relatório para continuação das atividades.

O que foi dito na seção 4.4 na página 107 deve ser seguido pela equipe de contenção objetivando munir as autoridades competentes de subsídios para fins de futura investigação dos agentes causadores do incidente.

Conclusões

Quando da conclusão deste trabalho o autor constatou que uma das muitas dificuldades que o tema propõe é a difícil interação dos idiomas utilizados, tanto pelo direito como pela informática, haja vista que o desconhecimento da terminologia leva o examinador a incorrer em equívocos na interpretação jurídica de condutas específicas e características da ciência informática.

O Direito Penal de Informática, como referencial científico, já é entre nós indelevelmente presente, inobstante que alguns assim não o reconheçam. Daqueles que o estudam, percebemos a nítida preocupação com a variedade e a velocidade com que se aprimoram os métodos delitivos, pois os números que orbitam a informática, a cada dia que passa, nos são apresentados em cifras elevadíssimas. Ao mesmo tempo em que cresce o uso de computadores, na mesma proporção multiplicam-se os métodos delitivos, que envolvem o conjunto informático.

Os conceitos compilados expõem a polêmica e a controvérsia, em razão da natureza e da complexidade do tema. Somando a essas, entende o autor que estes delitos devem ser prismados à ótica do objeto material, do bem juridicamente protegido (ou a ser protegido). Em razão disto, o autor afirma serem os crimes de informática todos aqueles em que o agente se utiliza dos meios informáticos como instrumento ou fim do delito.

A partir deste conceito, possibilitou que estes crimes fossem classificados em três categorias: puros, mistos e comuns, vide 2.5 na página 64.

Esta classificação permite que o legislador elabore normas próprias para coibir tais práticas delitivas, ao mesmo tempo em que pode aperfeiçoar as normas existentes e com isto abranger o universo deste tipo de crime.

O autor sugere que sejam incluídas qualificadoras pelo uso dos meios informáticos, às normas penais vigentes. Normas estas que atenderiam aos delitos mistos e comuns, restando ao legislador a criação de norma específica a atender aos delitos puros de informática.

Foi também exposta, embora que de forma sucinta, a aplicabilidade das normas penais existentes à algumas condutas, demonstrando, assim, ser possível a utilização das normas vigentes a estes delitos, embora saibamos serem deficientes para suportar os métodos criminais desta natureza. Também é de ser ressaltado que não ocorre o uso da lei penal vigente a estes delitos, pelo desconhecimento dos aplicadores do direito, o que tem remetido o delinqüente informático à impunidade. Credita-se, pois, tal afirmação, à complexidade e natureza dos delitos, que requerem dos aplicadores do direito sólidos conhecimentos de informática e de áreas afins.

De outra banda, pelos vários delitos descritos ao longo deste trabalho e, em especial aqueles que são perpetrados via internet, nos foi dado perceber a profunda preocupação da comunidade penal de vários países com o crescimento de métodos sofisticados delitivos perpetrados através de infovias.

A exemplo do tratamento que foi dado ao cheque[1], é, pois, por oportuno que seja editada legislação unificada sobre crimes desta natureza, até porque o crescimento vertical da tecnologia de informática, por via de conseqüência, traz consigo, na mesma proporção, estes delitos. Também, é de ser alertado que com a oferta de infovias, se potencializam os delitos mul-

[1] A Lei Uniforme é adotada em forma de convenção por inúmeros países. Tal lei lança as bases para que seja construída legislação acerca dos títulos ao portador do tipo cheque.

tinacionais, que por sua peculiaridade hoje oferecem profundas dificuldades no que concerne à competência para julgar tais delitos multinacionais.

Os métodos e exemplos de delitos que elencamos nos asseveram que ao Brasil é muito importante que esteja preparado e na vanguarda deste tema para poder enfrentar com eficácia esses novos crimes.

Uma das constatações que aflora, embora que subsidiária ao tema deste trabalho, é que cresce de forma quase que incontida a corrida ao domínio da informática, pois o poder que emana do controle da ciência informática assemelha-se ao poder emanado pelos detentores da tecnologia nuclear em passado não muito distante. Também por estes motivos devem ser otimizados os procedimentos de pesquisa, intercâmbio e aquisição de tecnologia, bem como, seja propiciado e incentivado o estudo jurídico do direito voltado à informática,

Calcado nestas razões e constatações, reitera o autor que urge ao legislador pátrio dote os operadores do direito desta ferramenta, já imprescindível. Tais medidas visam a que o país tenha meios adequados para enfrentar esta nova realidade jurídica que é a informática e seus efeitos na vida do Estado e dos cidadãos.

Tratou-se aqui apenas da parte criminal do Direito Informático.

Como expusemos brevemente na página 1.5.2 na página 29, o Direito Informático também, evidentemente, tem implicações civis. Podemos discutir a validade da assinatura digital, os contratos no mundo celebrados via internet, a parte registral da rede (registro de domínios), seguro de bens virtuais ou informatizados, responsabilidade civil, perturbações em geral, invasão da privacidade e destruição de propriedade eletrônica ou informatizada, direitos autorais sobre *software* e *hardware*, controle legal do conteúdo e forma do *software*. E mais, em Direito Processual Civil, competência ter-

ritorial, *juntada* regular de documentos, ciência e prazos, atividades irregulares no processo e composição judicial por meios eletrônicos.

Há, portanto, um novo mundo de relações civis e comerciais ainda não completamente reguladas e que carecem da atenção não somente dos legisladores mas também de pesquisadores e doutrinadores.

Referências

ALVIM, J. E. C. *Elementos de Teoria Geral do Processo*. 7. ed. Rio de Janeiro: Pesquisar, 2000.

ARAS, W. Crimes de informática: Uma nova criminalidade. jun 2001. Disponível em: <www.direitocriminal.com.br>. Acesso em: 11 de junho de 2002.

BARRON, D. W. *Sistemas Operativos*. Buenos Aires: Editorial Kapelusz, 1973. 11 p.

BASTOS, C. R. *Comentários à constituição do Brasil*. São Paulo: Saraiva, 1989.

BRASIL. Lei do Software. *Lei N. 9.609 , de 19 de fevereiro de 1998*. Brasília, DF: Presidência da República — Subchefia para Assuntos Jurídicos, 1998. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L9609.htm>. Acesso em: 07 de maio de 2003.

BRASIL. Lei dos Direitos Autorais. *Lei N. 9.610, de 19 de fevereiro de 1998*. Brasília, DF: Presidência da República — Subchefia para Assuntos Jurídicos, 1998. Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências. Disponível em:

BRASIL. Lei N. 10.406 de 10 de janeiro de 2002. *Novo Código Civil Brasileiro*. São Paulo: Escala, 2003. 302 p. Lei em vigor a partir de 11/01/2003. Apresentação e comentários de Celso Russomano.

COMITE GESTOR DA INTERNET NO BRASIL. Domínios Registrados por DPN. *Comitê Gestor da Internet no Brasil*, dez 2003. Disponível em: <http://registro.br/estatisticas.html>. Acesso em: 10 de dezembro de 2003.

COMITE GESTOR DA INTERNET NO BRASIL. Indicadores: Crescimento da Internet. *Comitê Gestor da Internet no Brasil*, jan 2003. Dispo-

nível em: <http://www.cg.org.br/indicadores/brasil-mundo.htm>. Acesso em: 10 de dezembro de 2003.

COSTA, M. A. O. O Direito e a Internet. São Paulo, nov 1998. Disponível em: <http://www.trlex.com.br/resenha/marco/marco.htm>. Acesso em: 20 de dezembro de 1999.

COUNCIL OF EUROPE. Draft Convention on Cybercrime. n. 19, 2000. Disponível em: <http://www.usdoj.gov/criminal/cybercrime/coedraft-.htm>. Acesso em: 8 de dezembro 2000.

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

GOMES, L. F. Crimes informáticos: Primeiros delitos e aspectos criminológicos e político-criminais. *Direito Criminal*, mar 2001. Disponível em: <http:/www.direitocriminal.com.br>. Acesso em: 07 de maio de 2003.

GOMES, R. R. Como colher provas de um crime virtual? *Módulo Security Magazine*, dez 2002. Disponível em: <http://www.modulo.com.br-/pt/page_i.jsp?page=3&catid=2&objid=310>. Acesso em: 11 de junho de 2003.

GUIMARÃES, C. C. *Princípios de sistemas operacionais*. Rio de Janeiro: Campus, 1989. 12 p.

INTERNET SOFTWARE CONSORTIUM. Internet Domain Survey: Number of internet hosts. jan 2003. Disponível em: <http://www.isc.org/>. Acesso em: 10 de dezembro de 2003.

INTERPOL. *IT Security and crime prevention methods*. 2000. Disponível em: <http://www.interpol.com/Public/TechnologyCrime/CrimePrev-/ITSecurity.asp>. Acesso em: 10 de dezembro de 2003.

LEITE, C. H. Crimes por computador. jul 1999. Disponível em: <http:-//www.mingus.modulo.com.br/clip_22.htm>. Acesso em: 20 de agosto de 2000.

LESSIG, L. *Code and other laws of cyberspace*. Nova Iorque: Basic Books, 1999.

LOSSO, F. M. Internet, um desafio jurídico. *Infojur*, 1998. Disponível em: <http://ccj.ufsc.br/infojus>. Acesso em: 07 de maio de 2003.

MÁRIO, C. *Instituições de Direito Civil*. Rio de Janeiro: Forense, 2000. 253 p.

MÓDULO SECURITY. 9ª Pesquisa Nacional de Segurança da Informação. *Módulo Security Magazine*, nov 2003. Disponível em: <http://www-.modulo.com.br/pdf/nona_pesquisa_modulo.pdf>. Acesso em: 10 de dezembro de 2003.

NETO, A. M. S. Resgatemos os hackers. *Jus Navigandi*, Teresina, jan 2000. Disponível em: <www.jus.com.br/doutina/hackers.html>. Acesso em: 05 de outubro de 2000.

NIC BR SECURITY OFFICE. Estatísticas dos incidentes reportados ao NBSO. set 2003. Disponível em: <http://www.nbso.nic.br/stats-/incidentes/>. Acesso em: 10 de dezembro de 2003.

NIC BR SECURITY OFFICE. Práticas de segurança para administradores de redes internet. mai 2003. Disponível em: <http://www.nbso.nic.br/docs-/seg-adm-redes/>. Acesso em: 10 de dezembro de 2003.

NIGRI, D. F. Crime e informática: um novo fenômeno jurídico. *Revista Trimestral de Jurisprudência dos Estados*, v. 16, n. 100, mai 1992.

PELLEGRINI, A.; DINAMARCO, C. R. *Teoria Geral do Processo*. 9. ed. Rio de Janeiro: Malheiros, 1992.

PINHEIRO, R. C. Os cybercrimes na esfera jurídica brasileira. *Jus Navigandi*, Teresina, n. 44, ago 2000. Disponível em: <http://www1.jus.com.br-/doutrina/texto.asp?id=1830>. Acesso em: 07 de maio de 2003.

PORTUGAL. Lei da Proteção de Dados Pessoais face à Informática. *Lei N. 10 de 29 de abril de 1991*. Lisboa: [s.n.], 1991.

RAMONET, I. *Geopolítica do Caos*. Petrópolis: Vozes, 1998. 142 p.

RAYMOND, E. S. *The Jargon File*: version 4.4.6. out 2003. Disponível em: <http://catb.org/~esr/jargon/>. Acesso em: 10 de dezembro de 2003.

SANTOS, M. A. *Primeiras Linhas de Direito Processual Civil*. São Paulo: Saraiva, 2002. 386 p.

SHAPIRO, A. L. *The control revolution*: how the internet in putting individuals in charge and changing the world we know. Nova Iorque: Public Affairs, 1999. 75 p.

SPINELLO, R. A. *Cyberethics*: morality and law in cyberspace. Londres: Jones and Bartlett, 1999. 38 p.

TOLEDO, F. de A. *Princípios Básicos de Direito Penal*. São Paulo: Saraiva, 2000. 16 p.

UCHÔA, J. Q. *Segurança em redes e criptografia*. Lavras: UFLA/FAEPE, 2003. 59 p. Curso de Pós-Graduação *Lato Sensu* (Especialização) em Administração de Redes Linux.

UCHÔA, K. C. A.; ALVES, R. M. *Introdução à Cibercultura*. Lavras: UFLA/FAEPE, 2002. 94 p. Curso de Pós-Graduação *Lato Sensu* (Especialização) em Administração de Redes Linux.

UNITED NATION STATISTICS DIVISION. Millennium Indicators. 2003. Disponível em: <http://unstats.un.org/unsd/mi>. Acesso em: 10 de dezembro de 2003.

WILLING, D. S. A internet e a Constituição dos Estados Unidos. *Consulex*, I, jan 1997.

ZAKON, R. H. *Hobbes' Internet Timeline v. 6.1*. 2003. Disponível em: <http://www.simonevb.com/hobbestimeline/>. Acesso em: 10 de dezembro de 2003.