UNIVERSIDADE FEDERAL DE CAMPINA GRANDE
CENTRO DE CIÊNCIAS JURÍDICAS E SOCIAIS
UNIDADE ACADÊMICA DE DIREITO
CURSO DE DIREITO

KILMARA BATISTA ESTRELA

C R I M E S D I G I T A I S

SOUSA - PB

2003

KILMARA BATISTA ESTRELA

C R I M E S D I G I T A I S

Monografia apresentada ao Curso de Direito do Centro de Ciências Jurídicas e Sociais da Universidade Federal de Campina Grande, como requisito parcial para obtenção do título de Bacharela em Ciências Jurídicas e Sociais - Direito.

Orientadora: Professora Ma. Adriana de Abreu Mascarenhas.

SOUSA - PB

2003

E823c Estrela, Kilmara Batista.
Crimes digitais. / Kilmara Batista Estrela. - Sousa - PB: [s.n], 2003.

54 f.

Orientadora: Professora Ma. Adriana de Abreu Mascarenhas.

Monografia - Universidade Federal de Campina Grande; Centro de Formação de Professores; Curso de Bacharelado em Ciências Jurídicas e Sociais - Direito.

1. Crimes digitais. 2. Crimes cibernéticos. 3. Responsabilidade – crimes na internet 4. Crimes digitais mistos. 5. Crimes digitais comuns. 6. Prevenção contra crimes digitais. I. Mascarenhas, Adriana de Abreu. II. Título.

CDU: 343.451:004(043.1)

Elaboração da Ficha Catalográfica:

Johnny Rodrigues Barbosa
Bibliotecário-Documentalista
CRB-15/626

KILMARA BATISTA ESTRELA

CRIMES DIGITAIS

COMISSÃO EXAMINADORA

_____
(PRESIDENTE – ORIENTADOR)

_____
(2° MEMBRO)

_____
(3° MEMBRO)

Aprovada em_____ de _____de _____

SOUSA-PB
2003

Ao meu namorado, Sidney Alves, meu amor, pelo incentivo e apoio durante todo o curso.

RESUMO

Esta monografia tenta esclarecer todo o périplo que envolve o submundo da informática, de onde parte as ações que se transformam em crimes da Internet, um assunto extremamente atual. A Internet é uma "rede de computadores com abrangência mundial, interligando instituições governamentais, de educação e pesquisa, empresas de todos os segmentos de mercado, ONGs e pessoas físicas. Utilizada essencialmente como meio de comunicação e de provimento de informações, através dos serviços de rede" [1], proporcionando e viabilizando, assim, um hábil de útil intercâmbio de informações e culturas. De relativo fácil acesso, leva grandes benefícios e comodidades aos seus usuários, sendo observada como uma das maiores contribuições da tecnologia moderna às relações sociais, modificando-as, de certo modo. Todavia, com a popularização deste novo meio de interação, adveio um novo ambiente propenso a ser palco de ações delituosas, que demonstrou não ser seguro diante de criminosos que não mais usam arma de fogo e força física e sim, um aprendizado de anos. Estão dispostos apresentados neste trabalho três capítulos. No Capítulo I apresentamos o que vem a ser Internet, expondo o seu conceito, histórico, aspectos técnicos e a o anonimato exercido pelos seus usuários. No Capítulo II abordamos a natureza do crime, tendo como fundamento a teoria finalista, estabelecendo comentários sobre a estrutura deste: fato típico e seus elementos (conduta, resultado, nexo causal e tipicidade). Alguns artifícios técnicos utilizados pelos criminosos, que redundam nas invasões e interceptação de dados foram listados. Foram também abordados algumas modalidades de crime praticados pela Intenet como: a fraude, o adultério, a lavagem de dinheiro, a pirataria de software e a pedofilia. No Capítulo III foram discutidos os aspectos que permeiam a responsabilidade e repressão aos crimes praticados na Internet, a noção da criminalidade na Internet, sugestões para uma repressão eficaz, identificação do agente criminoso (*hacker)* nesse ambiente, e prevenção contra crimes digitais. Ficam demonstradas também algumas formas de se precaver dos ataques dos *hacker* e que atenção ao quesito segurança ainda é a melhor prevenção. Sugestões para a edificação de uma repressão eficiente foram apresentadas. Tendo como conclusão que urge, sobremaneira, uma necessidade em elaborar uma lei específica a fim de discriminar e controlar tais crimes, para fins de repressão às condutas criminosas praticadas através Internet.

Palavras-chave: Crime, Internet, Computador, Hacker, Anonimato.

---

[1] **Fonte: Revista Info**

SUMÁRIO

INTRODUÇÃO

O processo de globalização demandou uma série de mudanças no mundo, tanto no âmbito econômico, como no que tange às comunicações, reflexo também da interação política-social. Observada por esse prisma, a Internet[1] logo pode ser listada como um advento nas novas relações de interação exigidas e oferecidas pela globalização mundial. Todavia, esse novo meio de interação, também se constitui em um ambiente propício à ações criminosas, que, com tantas ferramentas, usado à serviço do crime pode trazer conseqüências danosas, micro e macro-socialmente, ou seja, pode prejudicar não tão somente o indivíduo, como também a coletividade.

Indubitavelmente, não podemos discutir toda essa tecnologia de ponta, seu meio, suas ferramentas, seus agentes e os crimes cometidos por estes, sem fazer uma observação meticulosa do que vem a ser o crime, seus elementos e todos os aspectos inerentes a este último.

O crime da Internet é entendido como uma conduta na qual um sistema de informática é o meio direto no cometimento do crime. Para Neil Barret os "crimes digitais" seriam: "(...) a utilização de computadores para ajuda em atividades ilegais, subvertendo a segurança de sistemas, ou usando a Internet ou redes bancárias de maneira ilícita". Assim sendo, estes crimes são os que têm como objetivo os dados contidos em computadores, cujo acesso será usado para ameaçar ou fraudar. Os agentes delituosos da Internet, conhecidos por *hackers*[2], têm como seu principal aliado o anonimato, que no caso é uma maneira de se tornar invisível às autoridades. O *hacker*, geralmente, é um individuo dotado de amplo conhecimento na área

---

[1] Rede de computadores com abrangência mundial, interligando instituições governamentais, de educação e pesquisa, empresas de todos os segmentos de mercado, ONGs e pessoas físicas. Utilizada essencialmente como meio de comunicação e de provimento de informações, através dos serviços de rede.

de informática e telefonia, utilizando-o para a prática de infrações no ambiente da Internet. Tecnicamente, é possível chegar a identificar os autores de certas ações, no entanto a dificuldade passa a ser a de enquadrar o indivíduo, já que ainda inexiste uma legislação específica para tal.

Urge, desse modo, através de prática legislativa, o advento de instrumentos legais capazes de tipificar condutas com mais especificidade, já que o assunto é de uma velocidade extrema, no que tange à criatividade e variáveis das mesmas.

[2] Pessoa com grande conhecimento técnico na área de telefonia, comunicações em rede e programação avançada que busca meios de invadir/acessar sistemas de informática de forma não autorizada, ilegal.

CAPÍTULO I:

DA INTERNET

1.1- CONCEITO

A Internet é uma gigantesca rede mundial de computadores, que inclui desde grandes computadores até micros de pequeno porte. Esses equipamentos são interligados através de linhas comuns de telefone, linhas de comunicação privadas, cabos submarinos(backbones[3]), canais de satélite e diversos outros meios de telecomunicação. Os computadores que compõem a Internet podem estar localizados, por exemplo, em universidades, empresas, cooperativas, prefeituras, e nas próprias residências. Fazendo um paralelo com a estrutura de estradas de rodagem, a Internet funciona como uma rodovia pela qual a informação contida em textos, som e imagem pode trafegar em alta velocidade entre qualquer computador conectado a essa rede.

As redes que formam a grande rede, a Internet, variam de tamanho e natureza, diferindo também nas instituições mantenedoras e a tecnologia utilizada. O que as une é a linguagem que usam para comunicar-se, ou seja, um protocolo de comunicação[4], o TCP/IP, um acrônimo para o termo Transmission Control Protocol/Internet Protocol Suite, ou seja, um conjunto de protocolos, onde dois dos mais importantes (o IP e o TCP) deram seus nomes à

---

[3] Linhas de fibra ótica com capacidade de transmissão extremamente alta - transportam grandes quantidades tráfego da Internet. Esses backbones são sustentados por agências governamentais e por corporações privadas. Estrutura de nível mais alto em uma rede composta por várias sub-redes.

[4] Conjunto formal de conversões e regras para iniciar, manter e fechar uma comunicação, que é a conexão. Este conjunto de regras é necessário a um ou mais elementos de processamento de dados de uma rede de computadores para que se comuniquem harmoniosamente. Existem vários tipos(CDDI, FDDI, PPP, SMB, xDSL, entre tantos), no entanto o adotado como padrão na internet foi o IP(Internet Procol)

arquitetura. Os protocolos TCP/IP podem ser utilizados sobre qualquer estrutura de rede, seja ela simples como uma ligação ponto-a-ponto ou uma rede de pacotes complexa.

1.2- HISTÓRICO

A Internet foi criada pelo governo americano, no fim da década de 1960, como uma rede do Departamento de Defesa dos Estados Unidos(DoD - Department of Defense), denominada ARPAnet (*Advanced Research Projects Agency Net*), durante a guerra fria, período em que os Estados Unidos e a extinta e então União Soviética travavam uma fantástica e assustadora corrida armamentística e tecnológica, e propositadamente planejada para funcionar de forma descentralizada. A inexistência de um centro de comando permitia que o sistema se mantivesse funcionando de modo independente, mesmo no caso de um ataque inimigo à sede do governo. Essa característica, aliada à velocidade de expansão da rede, dificultava o cálculo do número exato de usuários.

Segundo a filosofia da ARPAnet, um computador poderia conversar com qualquer outro computador na rede, enviando os dados através de um pacote do Protocolo TCP/IP (*Trasnmission Control Protoco l/ Internet Protocol*[5]). A arquitetura TCP/IP surgiu com a criação da própria ARPANET.

A ARPANET necessitava então de um modelo de protocolos que assegurasse tal funcionalidade esperada, mostrando-se confiável, flexível e de fácil implementação. É então desenvolvida a arquitetura TCP/IP, que se torna um padrão de *fato*.

---

[5] É importante salienter que o Internet Protocol da sigla "TCP/IP", embora seja assim denominado e conhecido, não quer dizer protocolo da INTERNET, mas sim protocolo de INTER-REDES. Foi adotado na INTERNET por suas facilidades de projeto, implementação e operação. Inicialmente era utilizado apenas pelos computadores provedores de acesso à INTERNET, mas pelas facilidades já citadas, passou a ser um padrão para outras redes de computadores.

Essa vocação de interagir eficazmente com quase todos os sistemas operacionais existentes, com outras redes, e com diferentes hardwares, impulsionou-o a ser utilizado em massa. Hoje, quando se menciona TCP/IP, vem imediata a associação com a *internet*, ocorrendo de modo idêntico o inverso: a *internet* está diretamente relacionada à arquitetura TCP/IP.

No decorrer da década de 1980 o projeto original foi desmembrado em um ramo militar e outro civil, voltado para pesquisa e desenvolvimento na área de redes de computadores. Este último, integrado por instituições de educação e pesquisa dos EUA além de algumas grandes empresas da área de informática, deu origem à rede que conhecemos atualmente por Internet.

As primeiras funções executadas com as tecnologias desenvolvidas pelo projeto foram as de correio-eletrônico, de transferência de arquivos e de acesso remoto a computadores, denominadas de serviços básicos da Internet.

Com o apoio financeiro da National Science Foundation, um grande número de instituições de educação e pesquisa dos EUA conectou-se à rede, disseminando o uso desses serviços na comunidade acadêmica americana e fazendo com que o número de computadores ligados à Internet nos EUA dobrasse a cada ano.

A rede brasileira foi implantada pelo governo federal através do Projeto da Rede Nacional de Pesquisa - RNP, criado em 1989 pelo MCT, com apoio de instituições governamentais de vários estados, entre as quais a Fundação de Amparo à Pesquisa do Estado de São Paulo – FAPESP.

A partir de 1995 a rede brasileira deixou de ser somente acadêmica, como já acontecera em 94 nos EUA, e empresas e indivíduos também passaram a usar os serviços da Internet. O Comitê Gestor da Internet Brasil é o responsável pela determinação de regras e

políticas para a porção brasileira da Internet e a Fapesp é responsável pelo registro de nomes de domínio .br.

1.3- ASPECTOS TÉCNICOS

Para se tornar usuário de uma rede de informação é preciso ter um computador, uma linha telefônica e um modem (aparelho que converte sinais[6], de telefone em linguagem de computador e vice-versa) ou um acesso por rádio freqüência[7] ou por satélite, sistema análogo às Televisões por assinatura. As informações - letras, formas gráficas, cores, luzes, sons etc.-- são transmitidas na forma de *bits*, as menores unidades da linguagem dos computadores, que trafegam por fibras ópticas. Segundo a Revista Info(2000), são três os tipos de computador usados pela Internet. Os computadores chamados servidores são grandes fornecedores de informações e programas, e em geral pertencem a instituições. O segundo tipo são os nódulos, grandes máquinas com papel semelhante ao dos servidores, mas que também ajudam a escoar o tráfego de informações da rede. Finalmente, os computadores do terceiro tipo são os computadores pessoais dos usuários, em maior número que os demais.

Uma das principais aplicações da Internet é o correio eletrônico, ou e-mail (abreviatura de electronic mail), mais rápido e barato que o correio comum. Todos os usuários da rede têm seu endereço eletrônico, uma espécie de caixa postal, cujo formato obedece a um padrão. Ele é composto de um nome escolhido pelo usuário, acrescido do caractere (arrôba) e

---

[6] Esses sinais vêm em forma de sons e são transmitidos pela linha telefônica da mesma forma como a voz. O modem receptor por sua vez converte esses sons em sinais digitais e os transfere para o micro, que os interpreta. Desse processo vem a palavra MODEM, que é a sigla de MOdulador / DEModulador. Um lado modula os sinais digitais em sinais analógicos, enquanto o outro lado "demodula" esses sinais analógicos novamente para sinais digitais.

[7] Conexão "user-servidor" através de redes "wireless" que utilizam ondas eletromagnéticas para transmitir e receber dados.

do nome do domínio[8] onde está o usuário, sempre terminado por três letras, que o identificam como militar (mil), educacional (edu), comercial (com), organizações (org) etc.

Os usuários da Internet também têm a sua disposição o mailing-list, um serviço de assinatura de artigos por temas de interesse. Os grupos organizam-se em categorias, identificadas por um grupo de letras, como sci, para ciência; rec, para lazer; soc, para sociedade; comp, para computadores etc.

A Internet conta também com programas para conversas entre até centenas de pessoas, simultaneamente, que usam a estrutura do serviço IRC[9], abreviatura do inglês Internet Relay Chat. Já com o Telnet[10], o usuário pode operar computadores à distância a partir de sua própria máquina. Existem ainda vários sistemas de "navegação", ou busca de informações, na rede. São eles o Gopher, o Wais e o WWW (abreviatura de World Wide Web[11], teia mundial), com recursos multimídia e uma facilidade de manipulação que permitiram popularizar os usos da Internet.

1.4- O ANONIMATO

Um dos problemas conseqüentes da popularização da Internet é o anonimato oferecido pelo serviço. Entre tantos motivos que dificultam a ação das autoridades no que tange à identificação do criminoso virtual, encontra-se esse fator, o que facilita o cadastro falso em provedores, usando dados falsos ou de outrem. Percebe-se essa prática de ocultação de

---

[8] Nome à esquerda do símbolo "@" num endereço eletrônico, ou a designação do endereço eletrônico de uma determinada máquina, empresa, instituição ou país.

[9] É um sistema que permite a interação de vários utilizadores ao mesmo tempo, divididos por grupos de discussão, conhecido também como canal oo sala. O contato é feito em tempo real (diálogo textual). Os utilizadores deste sistema podem entrar num grupo já existente ou criar o seu próprio grupo de discussão. É o tradicional "bate-papo" ou "chat".

[10] Protocolo/programa que permite a ligação de um computador a um outro, funcionando o primeiro como se fosse um terminal remoto do segundo. O computador que "trabalha" é o segundo enquanto que o primeiro apenas visualiza no seu monitor os resultados e envia os caracteres digitados (comandos) no seu teclado.

identidade quando, ao se buscar informações sobre um determinado acesso, depara-se com dados que não correspondem à realidade e dificulta mais ainda a tentativa de identificação, caso o usuário delinqüente não mais retorna ao "local" do crime, já que só dessa forma, excluída a cadastral, a identificação será concluída e, convenhamos, se a conduta foi executada intencionalmente, raramente haverá retorno em pouco espaço de tempo.

Se por um lado existem as dificuldades, identificar uma pessoa que se esconde atrás de um computador, na Internet, para praticar crimes não é impossível. Por padrão, a conexão à Rede só se dá através do protocolo TCP/IP(*Trasnmission Control Protocol/ Internet Protocol*). A arquitetura TCP/IP realiza a divisão de funções do sistema de comunicação em estruturas de camadas. Em TCP/IP as camadas são: Aplicação, Transporte, Inter-Rede, e Rede. São nas camadas de Rede e Inter-Rede que são atribuídas e implementadas funções importantes na conexão e uma, digamos, "ameaça", ao anonimato: o endereçamento de datagramas[12], que tem entre as informações de seu controle o endereço IP do destinatário e do emitente. Os protocolos desta camada possuem um esquema de identificação das máquinas interligadas, ou seja, conectadas na rede. Para identificar cada máquina e a própria rede onde estas estão situadas, é definido um identificador, o próprio endereço IP, que é independente de outras formas de endereçamento que possam existir nos níveis inferiores.

Saindo um pouco da tecnicidade, própria e inerente ao tema, percebe-se que com um pouco de boa vontade e um material humano de qualidade, pode-se identificar usuários mal intencionados na rede. Contudo, essa identificação, através do IP, é dificultada pelo simples fato, de o IP, que nada mais é, coloquialmente, do que uma "Carteira de Identidade" na rede não ser fixo na Internet como em outras espécies de rede, como por exemplo, na rede do meu banco. O IP, na "Net", (com exceção do acesso *wireless* e por banda larga, geralmente são Ips

---

[11] Recurso ou serviço oferecido na Internet que consiste num sistema distribuído de acesso a informações, as quais são apresentadas na forma de hipertexto, com elos entre documentos e outros objetos gráficos (menus, índices), localizados em pontos diversos da Rede.

fixos, ou sejam nunca mudam, ou mudam pouquíssimo) é atribuído aleatoriamente a cada conexão, IP Dinâmico, no entanto essa variação, pode-se dizer é pequena, por exemplo: os endereços IP são números de 32 bits, normalmente escritos como quatro octetos na forma decimal, como por exemplo 200.236.143.1. A primeira parte do endereço identifica uma rede específica na inter-rede, a segunda parte identifica um *host*[13] dentro desta rede. Este endereço, portanto, pode ser usado para nos referirmos tanto a redes quanto a um *host* individual. É através do endereço IP que os *hosts* conseguem enviar e receber mensagens pela rede, em uma arquitetura Internet TCP/IP. Essa variação costuma acontecer nos últimos algarismos, exatamente nos que identificariam o *user,* porém os primeiros permanecem, sendo possível identificar o *host*, que é o servidor de onde parte a conexão e a rede, que é o domínio.

Sendo assim, rastreando o IP do criminoso, chega-se ao seu provedor, onde, mediante a um mandado judicial, pode-se identificar, em uma análise mais detalhada a máquina(server)[14] de onde foram feitos os acessos, através dos arquivos de log's[15](espécie de registro detalhados de todos os acessos) e confrontar tais informações com o cadastro de clientes, chegando de fato ao user(usuário) que opera a máquina "client"[16](Os *logs* relativos a ataques recebidos pela rede, em geral, possuem as seguintes informações: data e horário em que ocorreu uma determinada atividade; endereço IP de origem da atividade e portas envolvidas. Dependendo do grau de refinamento da ferramenta que gerou o *log* ele também pode conter informações como: protocolo utilizado (TCP, UDP, ICMP, etc) e os dados completos que foram enviados para o computador ou rede. O problema é o tempo. A Constituição de 1988 limitou bastante o poder da polícia, procedimento feito para evitar que

---

[12] Bloco de informação preparado para trafegar numa rede de computadores, com um cabeçalho que identifica a sua origem e o seu destino

[13] Servidor

[14] Servidor. Um computador na Internet ou em outra rede qualquer, que oferece determinados serviços.

[15] Os *logs* são registros de atividades gerados por programas de computador. No caso de *logs* relativos a incidentes de segurança, eles normalmente são gerados por *firewalls* ou por sistemas de detecção de intrusão.

os abusos cometidos durante o período militar voltassem a ocorrer. Acontece que a obtenção de informações através dos provedores de acesso é algo difícil e demorado, geralmente não colaboram com a ação da polícia, vindo a "colaborar" mediante mandado judicial, o que pode onerar em tempo uma semana ou até mais. Essa demora só favorece ao *hacker*, já que há ataques que passam por dezenas de servidores, em provedores distintos, e os "rastros" do acesso indevido em cada um deles, "evaporam" em menos de uma semana, inviabilizando por completo a investigação[17].

Essa fusão de vários computadores em um ataque, usando até vários servidores, é uma iniciativa adotada há bastante tempo pelos *hackers*. Grandes ataques, nos quais servidores ou sites ficam fora do ar, são realizados assim. A diferença é que, até então, os computadores utilizados eram dos próprios agressores. Atualmente, qualquer incauto pode ser um dos culpados sem ter o menor conhecimento do que esteja acontecendo. Quando um grupo de *hackers* junta os próprios computadores tentar um ataque, buscam com isso fazer com que fiquem completamente anônimos. Pelo contrário, poderiam ser rastreados pela polícia ou pela própria empresa invadida. Estar anônimo na Internet não chega a ser uma tarefa das mais difíceis, porém, o menor deslize pode ser fatal para quem ataca. A identificação do criminoso digital é difícil, envolve muitos fatores e variáveis, todavia não é impraticável.

---

[16] No contexto Cliente/Servidor, um Cliente é um programa que pede um determinado serviço (por exemplo, a transferência de um arquivo) a um Servidor, outro programa. O Cliente e o Servidor geralmente estão em duas máquinas distintas, sendo esta a realidade para a maior parte das aplicações que usam este tipo de interação.

[17] Fonte: Hackers Expostos

CAPÍTULO II:

DO CRIME

Sobre o crime, é primordial traçar um esboço dos conceitos, fato típico, resultado e nexo causal, de modo objetivo.

A estrutura do crime, assim como seus requisitos, sofre profunda diferenciação de acordo com a teoria que se adote em relação à conduta, que é o primeiro elemento componente do fato típico. Assim, uma vez adotada a teoria clássica ou teoria finalista da ação, haverá grandes divergências acerca do significado dos temas que envolvem conduta, dolo, culpa e culpabilidade.

Para a teoria finalista, atualmente adotada, não se pode dissociar a ação da vontade do agente, já que a conduta é precedida de um raciocínio que o leva a realizá-la ou não. A conduta é o comportamento humano, voluntário e consciente (doloso ou culposo) dirigido à uma finalidade. Assim, o dolo e a culpa fazem parte da conduta, que é requisito do fato típico.

2.1- CONCEITO

Segundo Mirabete, do ponto de vista formal, o crime é toda conduta proibida por lei sob ameaça de pena; é fato típico e antijurídico. No aspecto analítico, a doutrina finalista moderna tem considerado o crime como conduta típica, antijurídica e culpável. Considera-se conduta típica a ação em sentido estrito ou a omissão, praticada com dolo ou culpa, que se amolda ao tipo penal. A conduta, todavia, só é antijurídica quando contraria o ordenamento jurídico por não está protegida pela lei penal com a exclusão de ilicitude. Culpável é a ação

típica quando reprovável, isto é, quando há imputabilidade do agente, potencial conhecimento da ilicitude e exigibilidade de conduta diversa.

No aspecto material, Damásio alude que o conceito de crime visa aos bens protegidos pela lei penal. Dessa forma, nada mais é que a violação de um bem penalmente protegido.

Define-se crime, também, como "fato típico e antijurídico", considerando-se a culpabilidade como condição para se impor uma pena.

O fato típico é o comportamento humano (ação ou omissão) que provoca um resultado (em regra), e é previsto como infração penal. A antijuridicidade é a relação da contrariedade entre o fato típico e ordenamento jurídico. Deixará de existir a ilicitude se o agente estiver amparado por uma causa excludente da mesma.

A culpabilidade, considerada como reprovação da ordem jurídica em face de está ligado o homem a um fato típico e antijurídico é, em suma, a contrariedade entre vontade do agente e a vontade da norma penal.

A punibilidade é mera conseqüência jurídica do delito, ou seja, a possibilidade de se impor pena ao agente do fato típico, antijurídico e culpável.

2.1.1 O CRIME NA INTERNET

A Internet é grande advento desse século, indubitavelmente. Todavia, junto com toda a sua utilização para tornar as nossas vidas mais fáceis, servindo-nos de uma mescla incalculável de informações, emergiu uma interação antes nunca vista entre todas as nações, uma espécie de "pós-globalização" ou o seu arremate final. Esse novo meio de comunicação e compartilhamento de culturas, é ambiente perfeito para crimes também nunca relatados, constituindo-se em um grande desafio não só para o Direito Penal, mas sim para todo o Direito Positivo e suas subdivisões clássicas (Direito Comercial, Civil, Internacional, etc),

surgindo novas áreas jurídicas que abrangem tais atividades, no estudo e na militância, como o Direito da Informática.

O crime na Internet é o recente fenômeno histórico-sócio-cultural caracterizado pela elevada incidência e ilícitos penais (delitos, crime e contravenções) que têm por objeto material ou meio de execução o objeto tecnológico informático(hardware, software, redes, etc.).

Para Feliciano, crime de informática é a conduta que atenta, imediatamente, contra o estado natural das coisas e recursos oferecidos por um sistema de processamento, armazenagem ou transmissão de dados, seja em sua forma, apenas compreendida pelos elementos que compõem um sistema de transmissão ou armazenamento de dados, seja na sua forma compreensível pelo homem.

Um crime relacionado à informática é todo aquele que atenta contra o estado natural dos dados e recursos dispostos por um sistema de processamento de dados, seja pela compilação, armazenamento ou transmissão de dados; o que outrora era executado com ações armadas, com contato visual, agora dispõe do anonimato oferecido pelas conexões na Internet, dispensando uma possível agressão física e não compondo, a distância física, um obstáculo à prática criminosa.

2.2- CLASSIFICAÇÃO

Em relação à classificação dos crimes na Internet, faz necessário afirmar que enquanto não entrarem em vigor leis específicas para enquadrar os crimes digitais, o Estado não contará com sustentáculos legislativos para esboçar nenhuma reação, através dos seus braços coercitivos, à essa novíssima modalidade de delinqüência.

Todavia, na maioria das vezes a Internet é apenas um instrumento de ação dos cybercriminosos. O autor Scarance Fernandes propugnou acerca da classificação, adequando-se de modo brilhante ao contexto de tais crimes.

2.2.1- Crimes digitais puros

São aqueles em que o sujeito ativo tem como alvo único o sistema de informática, em todas as suas formas; quando as ações físicas se materializam por atos de vandalismos contra a integridade física do sistema, pelo acesso indevido aos dados contidos no computador atacado, ou seja, correspondem aos novos tipos penais, surgidos com o uso progressivamente maior dos computadores e que deles necessitam para existirem.

2.2.2- Crimes digitais mistos

Nesses crimes a ferramenta do crime, como no furto de informações, o computador, através da Internet, é utilizado para a invasão de sistemas bancários e a transferência não autorizada de numerário. O objeto tecnológico é apenas o meio de execução.

Considera-se misto porque viola normas da lei penal comum e normas da lei penal de informática. Da lei penal comum, por exemplo, poder-se-ia aplicar o artigo 171 do Código Penal combinado com uma norma por mau uso de equipamento e meio de informática. Por esse fator não seria um delito comum apenas, pois incide na penal de informática, tendo assim claramente o concurso de normas (art. 70,CP).

2.2.3- Crimes digitais comuns

São crimes semelhantes aos cometidos em outros meios, como seriam os sites pedófilos, isto é, crimes que poderiam ser cometidos, com igual lesividade, mediante outro recurso que não o informático.

Insere-se aqui, como exemplo, o art. 171 do CP, o famoso 171, conhecido e imortalizado: o estelionato. Este que absorve todas as fraudes eletrônicas como: clonagem de cartão de crédito, desvio de dinheiro de contas correntes e outras situações em que a astúcia do meliante digital seja empregada de modo a conseguir benefício, em detrimento de outrem, que de modo honesto não obteria.

Destarte, entendemos ser a presente classificação, de Scarance Fernandes, eficaz na construção de uma legislação específica ou do recurso à interpretação progressiva para os ilícitos penais informáticos e para as condutas antijurídicas e culpáveis, em que o objeto material ou o meio de execução sejam o objeto tecnológico informático e não para praticar crimes.

2.3- HACKERS E SEUS CRIMES NA REDE

O meliante digital traz consigo peculiaridades que os diferem dos demais, tanto na utilização de fartos conhecimentos técnicos, como na operacionalidade da ação criminosa. Obviamente, nesta modalidade de crime as armas utilizadas são outras, como softwares específicos e conhecimento adquirido destilado no submundo da grande rede, inexistindo por completo qualquer possibilidade de contato físico coercitivo, pois todo o processo de "abordagem virtual", dá-se a uma distância presumidamente segura, isto para o invasor.

Dentre os delitos praticados pelos *hackers*, podemos citar os "passeios" em sistemas alheios, cujos podem causar não só estragos aos arquivos vitais da configuração da máquina invadida, como a própria subtração de dados valiosos, financeiramente, como é o caso de segredos empresariais e industriais e o banal furto de senhas e números de cartões de crédito, o que redunda, indubitavelmente, com outras práticas criminosas, como a compra de mercadorias usando esses dados de outrem e o próprio desvio de dinheiro para outras contas.

Segundo o dicionário Aurélio, *hacker*, substantivo de agente do v. to hack, 'dar golpes cortantes (para abrir caminho)'(do inglês) é um "indivíduo hábil em enganar os mecanismos de segurança de sistemas de computação e conseguir acesso não autorizado aos recursos destes, a partir de uma conexão remota em uma rede de computadores; violador de um sistema de computação". No entanto, engana-se quem definir *hacker* em tão poucas palavras. Aliás, faz-se mister afirmar que não existe definição alguma capaz de delimitar toda a subjetividade que envolve o comportamento desse "movimento". Vários são os tipos de indivíduos que se dedicam a essa prática: adolescentes querendo provar algo para si e para seu grupo, ou simplesmente tentando aprender; programadores testando novas possibilidades em software; especialistas em segurança testando falhas no sistema; delinqüentes cheios de má intenção, desejando, além de notoriedade no meio, vantagens financeiras; existem inúmeros perfis.

Para a legislação brasileira, qualquer que seja a qualidade ou intenção do violador, será ele um *hacker*, denominação primeira e genérica atribuída aos invasores de sistemas na Internet. Há dois anos, a empresa de aviação civil Varig teve seu site invadido: deletaram(apagaram) as informações sobre a corporação, e publicaram um pingüim lilás gigante com os dizeres *Brazil owned again* (o Brasil controla novamente, em inglês) em

verde e amarelo[18]. O responsável pela travessura eletrônica foi um grupo de *crackers* (Essa denominação é atribuída a uma parcela dos invasores, que teriam como objetivo danificar, roubar, fraudar dados pela Internet, seriam a escória do mundo *hacker,* enquanto que o próprio hacker, considerados a elite do submundo informático, seria um "Problem Solver", ou seja aquele que resolve problemas; segundo eles mesmos, o verdadeiro *Hacker* não costuma estragar nada, subtrair programas, ou sequer roubar informações em detrimento de outrem. O Hacker seria, acima de tudo, um intelectual informatizado. Contudo, ao que parece, o limiar entre essa divisão é muito tênue. O fato é que certa parte do "trabalho" dos *hackers* conseguiu quebrar algumas barreiras provocadas pelo monopolismo capitalista impostas pelas políticas adotadas pela indústria de tecnologia, como por exemplo o advento do mp3[19], do Dvix[20] e da quebra das proteções em DVD players domésticos - áreas comercias que dividirão o globo em regiões de reprodução, onde um DVD produzido em uma não poderia ser visto nos players de outra, o que, em tese, dificultaria a pirataria e o contrabando - , no entanto sugerindo outro debate específico da questão dos Direitos autorais.), como são conhecidos os vândalos on-line, chamado *tty0*. Por trás do nome impronunciável estão sete garotos de 15 e 16 anos que moram em São Paulo. De acordo com o instituto europeu Alldas, que monitora ataques virtuais, o tty0 é o sexto mais atuante do mundo. Não é o único brasileiro em destaque. Entre as dez gangues mais perigosas do planeta, o ranking inclui cinco brasileiras, inclusive o primeiro lugar, ocupado pelo Silver Lords, com mais de 1.000 invasões. Criado há alguns

[18] Essa prática é conhecida como "defacer", consiste em "desfigurar" a interface gráfica do site, trocando o conteúdo. É uma forma simples de ataque, mas que provoca grandes prejuízos.

[19] Padrão de arquivo de áudio compactado, coibido intensamente pelas gravadoras por facilitar a distribuição de obras fonográficas pirateadas. Paradoxalmente, torna-se a cada dia mais fácil encontra no mercado tocadores compatíveis com o formato, como DVD's domésticos, CD-players automotivos, etc.

[20] Padrão de arquivo de vídeo compactado, de alta qualidade, capaz de copiar dvd em cd comum e facilitar a pirataria(baixar custos). Pode ser visto no computador, mas já existem dvd's domésticos capazes de reproduzi-lo. Criado por hackers.

anos, esse grupo ficou famoso entre os ciberpiratas por promover uma espécie de vestibular on-line para aceitar novos integrantes[21].

O que torna o Brasil tão fértil em *hackers* é a impunidade. Se um hacker brasileiro entra em um computador só para ver o que há lá dentro e não altera as informações, não está cometendo um delito, pois não há lei que defina isso. Nos Estados Unidos poderia pegar dez anos de cadeia. No Brasil, o primeiro projeto de lei que define e tipifica os crimes digitais, cometidos por *hackers* que acessam com fins ilícitos uma rede ou um sistema de dados, foi apresentado ao Congresso Nacional, pelo Deputado Luiz Piauhylino, o Projeto de Lei nº 84, de 1999, onde prevê algumas modalidades de infrações pelo computador, bem como multas e penas.

O Brasil, atualmente, é uma das poucos países do mundo que ainda não dispõem de legislação específica no que tange aos crimes digitais, e a única na América Latina nesta situação. Por outro lado, foram criados delegacias e departamentos policiais de inteligência dedicados à investigação desse tipo de infração, mas os acusados ao serem presos são incluídos no rol dos crimes comuns, previsto na legislação penal brasileira. Indubitavelmente, trata-se de um avanço. Ínfimo, é verdade, todavia configurando uma iniciativa excelente, diante da desregulamentação a que nos referimos.

O Estado de São Paulo foi o primeiro a fornecer meios à polícia para que se investigasse essa nova modalidade de delito. O governador Geraldo Alckmin criou uma delegacia especializada no combate a crimes pela Internet. A nova divisão, que recebeu o nome de Delitos Praticados por Meios Eletrônicos, está ligada ao Departamento de Investigações sobre Crime Organizado(DEIC) e já apura desvios de dinheiro e de informações via rede, disseminação de vírus e ameaças por mensagens eletrônicas. Outra delegacia criada pela Secretaria de Segurança do Estado combate práticas de pirataria, como cópia irregular de

---

[21] **Fonte: Revista Geek**

discos e softwares. O Estado conta ainda com o Departamento de Telemática da Polícia Civil de São Paulo (Detel). [22]

Seguindo a iniciativa do vizinho estado, o Rio de Janeiro também disponibilizou recursos e hoje funciona na sede da Polícia Civil, no centro da capital, a Delegacia de Repressão aos Crimes de Informática. Rastrear as infrações é função de nove policiais que receberam treinamento intensivo de Internet. Nas primeiras semanas em que atuaram, cinco denúncias de crimes na Internet foram registradas na delegacia. Todos foram crimes contra a honra, difamações. Na maioria das vezes, os casos da Internet extrapolam os limites do Estado do Rio. Foi o que aconteceu com a cantora Sandy, da dupla com o irmão Júnior, que apareceu nua em fotomontagem de uma página da web. A denúncia chegou ao site do Centro Brasileiro de Defesa dos Direitos da Criança e do Adolescente. A diretora do centro, a advogada Cristina Leonardo, repassou a informação para seu homem de confiança na rede, o *hacker* Jorge Fernandes, que auxilia também a Polícia Federal. Identificado o nome e o endereço, na cidade de Olinda, em Pernambuco, do responsável pela fotomontagem, a Polícia Federal indiciou o acusado e determinou a retirada da foto.[23].

2.4- ARTIFÍCIOS TÉCNICOS UTILIZADOS PELOS CRIMINOSOS

São inúmeras as "artimanhas" praticadas pelos hackers para o êxito das suas intenções, geralmente auxiliados por algum programa, elaborado intencionalmente para fins ilícitos ou desviados das suas reais atribuições para tal. Nas linhas que seguem, estarão explicados os mais em voga, atualmente.

[22] **Fonte: Revista Info**
[23] **Fonte: Revista Info**

Vejamos um exemplo: usando o software IP SCANNER, que varre a rede em busca de endereçamentos IP's que possam levar a alguma porta sem proteção, o hacker invade e instala em sua presa um registrador de digitação. Ou seja, torna a máquina invadida um terminal do seu próprio computador, fazendo com que tudo que se digite ao teclado daquela, desde uma inocente epístola, até as senhas do cartão de crédito, seja enviado externamente. Nesse processo, pode ainda usar um outro software como o EVIDENCE ELIMINATOR, que camufla e apaga as suas próprias "pegadas" na rede, dificultando, praticamente, impossibilitando a sua localização e identificação. Toda essa empreitada, pode levar dias, semanas e até meses, pois os scanners saem testando aleatoriamente várias portas de máquinas diversas, em horários alternados.

Outra técnica consiste em usar um programa que altere o cabeçalho dos pacotes IP, que é quem identifica a máquina na rede, fazendo-se passar por outro terminal, simplesmente enganando o software que gerencia e administra a rede, no caso de uma rede local, para conseguir acesso. Daí a conseguir ler e subtrair ou até mesmo mudar arquivos vitais e valiosos é um pequeno passo.

O mais atual, digamos, que está na moda é o célebre ataque usando um falso site de Banco ou instituição financeira, um clone fiel. Bandidos cibernéticos registram endereço eletrônico parecido com o do banco e fazem uma página igual à da instituição. Na maioria dos casos nem se dão a esse trabalho. Daí enviam um e-mail à vítima com *subject*[24] atraente e chamativo, tipo: "Você ganhou uma viagem ao nordeste do Banco 'X' leia..." É apenas uma armadilha que conta com a distração de quem navega pela Internet. Ao entrar, o texto informa os detalhes da "sorte" obtida pelo incauto e o manda clicar em um *link*[25](que supostamente levaria ao site oficial do banco) para a confirmação de alguns dados. A vítima clica e é direcionado para um site idêntico, com visual clonado do original, onde encontra um

[24] Campo no programa de e-mail referente ao assunto da correspondência.

formulário com espaços para informações pessoais, entre elas a senha e o número da conta. Ao digitar a senha e os dados da conta e confirmar entrega-se o ouro aos bandidos, enviando os dados para alguma conta de e-mail.[26]

Outra tentativa de golpe similar à supradita, aconteceu recentemente quando um e-mail, supostamente provindo das Americanas.com informando que o destinatário fora sorteado com um prêmio de 100 mil reais em compras. Anexo à mensagem vem um link que aponta para um arquivo que, segundo recomendava o texto, deveria ser "baixado" e executado para o preenchimento dos dados pessoais do recebedor. O caso está ainda sob investigação, mas parece óbvio que é mais uma tentativa de subtração de dados ou ,no mínimo, de abrir uma porta para o exterior para uma futura invasão[27].

Porém, não é só no âmbito da rede que as investidas para uma invasão se dão. A engenharia social (O termo é utilizado para descrever um método de ataque, onde alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações.) também é usada pelos *hackers*. Os dois últimos exemplos supracitados também são obra desse subterfúgio. Na maioria dos casos, os especialistas de segurança concordam que as maiores ameaças não vêm do ataque de um pirata invasor, mas de alguém que está dentro da própria empresa, tanto no quesito ingenuidade como em uma insatisfação qualquer que poderá trazer uma vingança em forma de ataque ou cessão intencional de dados de segurança a outrem do meio externo. Segundo André Fucs, da Módulo, empresa que presta serviços de segurança de rede em São Paulo, uma tática comum é uma pessoa ligar para o funcionário da computação se apresentando como o presidente da empresa ou outro superior,

---

[25] Ponto no site que remete a navegação prá outro site
[26] **Fonte: Revista Info**
[27] Fonte: **Revista Info-Setembro**

e solicitar uma nova senha[28]. A equipe de segurança do centro de informações de redes do Brasil (NBSO) lançou uma nova versão, a nº 2, de sua Cartilha de Segurança[29] para Internet. Destinada ao público em geral, o documento procura sanar dúvidas comuns sobre segurança de computadores e redes, explicar o significado de termos da Internet e servir como um guia de procedimentos para os usuários aumentarem sua segurança online.

2.5- ALGUNS CRIMES PRATICADOS NA Internet

2.5.1- Fraude

O caput do artigo 171, do Código Penal diz:

> "Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualque routro meio fraudulento:
>
> Pena – reclusão de um a cinco anos."

A seqüência de atos que estimulam alguém a erro, no intuito de que esta se comporte como se estivesse em plena lucidez da realidade é nomeada fraude. O agente da fraude delineia e executa uma série de acontecimentos, produzindo uma ação na vítima, que sem todo esse percurso ela não faria.

A fraude é elemento constitutivo e característico do estelionato, sendo eventualmente exigido em outros tipos penais, às vezes como integrante do tipo básico (arts. 175, 215, 236 do Código Penal) e outras como qualificadora (arts. 227, §2º, 228, §2º do Código Penal).

---

[28] Fonte **Revista Geek**
[29] Fonte: **http://www.nbso.nic.br/docs/cartilha/.**

Como exemplo temos a clonagem de cartão de crédito, o desvio de numerário de contas bancárias, o uso indevido de cartões de crédito em compras pela Internet, o acesso à Internet por meio de provedores de acesso usando senhas falsas, de outrem, etc.

2.5.2- Corrupção de Menores

O crime de corrupção de menores, rogado no artigo 218 do Código Penal, comina pena de reclusão de um a quatro anos, à conduta de corromper ou facilitar a corrupção de pessoa maior de 14 anos e menor de 18 anos, com ela praticando ato de libidinagem ou induzindo-a a praticá-lo ou presenciá-lo; trata-se de um crime contra os costumes.

Todavia, se um interlocutor induzir pessoa maior de 14 anos e menor de 18 anos à prática ou assistência de ato libidinoso, pela Internet, desafia a norma repressiva do supracitado artigo(218). A corrupção inicia-se, amiúde, em salas de bate-papo(*Chat*) e mais raramente por e-mail. A consumação do crime dar-se-á, sempre, com o ato de libidinagem real, praticado ou presenciado pelo aliciado.

Segundo Mirabete, o ato de libidinagem é o que provoca a libido, é o ato concupiscente, obsceno, capaz de suscitar no menor o senso dos prazeres carnais e inspirar viciosos costumes da vida real.

A identificação dos aliciadores far-se-á por infiltração policial (contatos mantidos por agentes, que, nos próprios *chats* simulam interesse em participar das redes de aliciamento), programas de rastreamento de IP, pois o *chat* também gera *logs* e posterior consulta ao cadastro de provedores.

2.5.3- Lavagem de Dinheiro

Sob uma intricada teia de transações é executada a lavagem de dinheiro, cujo o objetivo principal de montar tão eficiente labirinto monetário é despistar as autoridades, da real origem do numerário.

A Lei nº 9.613/98 tipificou, no ordenamento pátrio, os crimes de lavagem de bens, direitos e valores, criando para a fiscalização do sistema financeiro e de molde a prevínir as operações de branqueamento.

O Conselho de Atividades Financeiras(COAF), formado por servidores públicos de reputação ilibada, provenientes dos quadros discriminados no artigo 16 da supracitada lei, é criado, no âmbito do Ministério da Fazenda, com a finalidade de disciplinar, aplicar penas administrativas, receber, examinar e identificar as ocorrências suspeitas de atividades ilícitas previstas nesta lei, sem prejuízo da competência de outros órgãos e entidades.

A responsabilidade de evitar a lavagem de dinheiro é do Estado, pois esse numerário passivo de lavagem escapa incólume da tributação e da verificação de sua procedencia e deveria ser rastreado e confiscado, de modo a conter e diminuir a evasão de divisas ilegais para o exterior, diligenciando junto às autoridades naciuonais dos países receptores e firmando tratados multilaterais a respeito do tema.

2.5.4- Pirataria de *Software*

Software, segundo o Dicionário Aurélio, seria: "Em um sistema computacional, o conjunto dos componentes que não fazem parte do equipamento fisico propriamente dito e que incluem as instruções e programas (e os dados a eles associados) empregados durante a utilização do sistema."

A Lei nº 9.609/98 trata da propriedade intelectual dos programas de computador e também delega sobre a pirataria de software. Segundo o seu artigo 12, "violar os direitos de autor de programa de computador", produzindo cópias ilegais, estará sujeito a detenção de 6 meses a dois anos mais uma multa que a ABES(Associação Brasileira de Software) avalia em duas mil vezes o valor do software original. Todavia, se a prática tem fins comerciais a pena aumenta para 1 a 4 anos de reclusão mais a multa.

A Internet favorece essa prática, a pirataria de software duas frentes que merecem destaque: a da distribuição(venda) e do *crackamento*[30] de *keys*[31].

Já foi explicada a oferta do anonimato pela rede, pois bem, valendo-se desse artifício, "piratas" anunciam e vendem suas "mercadorias" com grande desenvoltura, seja por e-mail ou por *sites* próprios, geralmente hospedados em servidores fora do país. O procedimento é o seguinte: o "pirata" manda uma lista de programas disponíveis para cópia por e-mail, geralmente em arquivo .doc, do Microsoft Word, o comprador em potencial lê o arquivo e se gostar de alguma "oferta" manda um e-mail com endereço e telefone e, obviamente, as suas escolhas. Feito isso, há uma confirmação por telefone e é só esperar o "material" bater à porta através do Sedex (á cobrar), serviço dos Correios. Às vezes, só vendem com pagamento adiantado, feito em contas correntes, notadamente usando um "laranja", identidade de outra pessoa.

Já o crackamento acontece da seguinte forma: o programa original vem com uma senha para ser inserida durante o programa de instalação ou depois desta para registrar o *software*, uma tentativa de burlar a pirataria. Para divulgação são distribuídas cópias originais de demonstração, onde ficam ativas durante 30 dias e depois caso não seja digitada a senha de registro, é automaticamente desabilitada. Na Internet, encontra-se até em *sites* gratuitos

---

[30] Referente a *Cracker*, quebrar.
[31] "Chave", tipo de senha que vem com o programa original.

arquivos que ao serem rodados desbloqueiam o programa, quando não se encontram os números à venda.

2.5.5- Pedofilia

Nenhum ato protagonizado por *hackers* na Internet chegou perto de comover a sociedade, gerando repulsa e asco, como um praticado, na imensa maioria das vezes, pelo usuário comum: a troca de fotos eróticas envolvendo crianças e adolescente e publicação de *sites* com conteúdo pedófilo.

A pedofilia consiste na perversão sexual, em que o adulto experimenta sentimentos eróticos em relação a crianças e, para fins legais, adolescentes. É uma manifestação particular de crono-inversão("consiste no amor pelo sexo oposto com grande diferença de idade, conforme Hélio Gomes). A veiculação de imagens de pedofilia pela Internet é alarmante, desde a década de 90, que deflagrou forte repressão criminal no Brasil, com base na absoluta desativação dos sites hospedados em provedores nacionais.

O direito das crianças e dos adolescentes é amparado no ECA, o Estatuto da Criança e do Adolescente, em sua Lei nº 8.069/90, onde reputa como criança, em seu artigo 2º, os indivíduos que têm até doze anos de idade incompletos e adolescente entre doze e dezoito anos.

O Estatuto da Criança e do Adolescente prevê várias condutas imputáveis, como exemplo, destacamos a do artigo 241, que alude à pedofilia.

> "Art.241. Fotografar ou publicar cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
>
> Pena – reclusão de um a quatro anos."

Obviamente, àquele que publica ou deixa esses arquivos, contendo material pedófilo, à disposição de qualquer usuário na Internet, é perfeitamente suscetível de pena, ao ser denunciado tendo como base o artigo supradito. Não obstante, àquele usuário que remete por e-mail, um arquivo que contenha foto de criança ou adolescente na prática de sexo, não estará cometendo a mesma transgressão, por não está publicando, no sentido de tornar público, e sim, remetendo a um outro dado usuário, promovendo assim, conduta atípica.

Esse tipo de prática no Brasil, impulsionou uma visceral reação por parte de toda a sociedade, resultando na criação de organismos não governamentais para combater os abusos, o que funciona à base de pesquisa e posterior denúncia às autoridades.

CAPÍTULO III:

DA RESPONSABILIDADE E REPRESSÃO

3.1 RESPONSABILIDADE PELOS CRIMES PRATICADOS NA INTERNET

Como em outros países, o Brasil é palco que constantes debates acerca a quem se atribuir a responsabilidade dos crimes perpetrados pela Internet. Na maioria dos casos onde se imputa a responsabilidade a alguém, os provedores de acesso são feitos de "bode expiatório", por através deles transitar os agentes da ação delituosa.

Certamente pelo descompasso cronológico, a atual Constituição Federal data de 1988 e a Internet só começava a engatinhar em 1995, não existe nenhuma lei que estabeleça responsabilidade aos provedores de serviço por ator perpetrados por seus associados, nem permite que as informações inerentes ao cadastro, ao próprio trânsito de conexões e acesso sejam visualizadas ou fiscalizadas. A Constituição Federal desfila toda a sua obsolescência, em relação ao tema, quando ordena:

> "Art. 5º (...)".
>
> "XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal".

PAESANI, como alguns estudiosos que antagonizam a elaboração de uma lei específica sobre a matéria, consolidam que:

> "Não é com uma histérica caça às bruxas que se protegem os menores ou se garante a segurança e o desenvolvimento da comunicação na rede. O instrumento viável é um só: a vigilância dos pais e educadores. Esta orientação deveria se destinar também a outras áreas das novas técnicas e alegam que se não é correto deixar uma criança sozinha diante de um televisor, também não deve ser deixada só diante de um computador". (PAESANI, L. M. 2000: 90)

Entende-se que a imputação da responsabilidade unicamente ao provedor de acesso é um equívoco, já que a responsabilidade dos arquivos armazenados e distribuídos pela rede é exclusivamente do usuário, que no caso é o autor. Sugere-se então, que na legislação porvir delineie responsabilidades ao provedor no que tange ao controle do conteúdo que transita em seus cabos, reconhecendo, diante mão, a dificuldade de total fiscalização frente ao enorme volume de dados, para que essa prestação de serviços não ofereça brechas a certos modos de crime. E que caso se suspeite de alguma atividade suspeita em determinado provedor, seja desburocratizado o acesso às informações por parte da polícia ou que se apresse, por parte do Poder Judiciário a emissão de ordens judiciais, quando a investigação envolver crimes digitais, dado ao fator tempo.

3.2- SUGESTÕES PARA UMA REPRESSÃO EFICAZ

O que se poderia evidenciar, em relação à repressão, seria uma política, por parte do governo federal, de incentivos à atividade policial, especializando o corpo de investigadores, a exemplo de alguns estados que, por iniciativa própria de seus governadores, criaram organismos especializados no trato de vias digitais no cometimento do crime.

Sob o aspecto legislativo, espera-se que se torne lei, o Projeto de Lei nº 84/99 de autoria do Deputado Luiz Piauhylino Monteiro, da bancada de Pernambuco, onde se busca classificar as condutas que podem redundar em crime na Internet e na área de informática, atribuindo penalidades as mesmas, regulamentando esse âmbito novo no Direito brasileiro

Atribuí-se no supracitado projeto vários responsáveis por regulamentar e fiscalizar todo o processo de tramitação de dados, em todos os ambientes, sejam privados ou estatais, claramente embasado e adaptado das legislações inglesa e norte-americana, que notoriamente já têm uma vasta experiência no trato dessa questão.

A iniciativa do Poder Legislativo é louvável, pois a necessidade de uma legislação específica no que tange à Internet é de caráter urgentíssimo, pois determinadas condutas se encontram no vácuo da legislação penal vigente, passando intactas à punibilidade, prejudicando o trabalho policial na tipificação e enquadramento dos criminosos, causando com isso grandes prejuízos, sem que se tenha um sustentáculo legal para repressão à altura.

3.3- PREVENÇÃO CONTRA CRIMES DIGITAIS

A área de segurança na Internet aparece como sendo um dos mercados mais promissores, tanto no segmento de serviços como no desenvolvimento de novos softwares de segurança, atingindo um público que vai desde o usuário corporativo, como as grandes empresas, ao usuário doméstico.

Os especialistas nesse novo segmento são profissionais qualificados e, não raro, *hackers* que mudaram de lado e migraram para o serviço, que traz lucros vultosos à quem trabalha com eficiência. Por qual motivo seria tão oneroso manter a segurança de uma rede empresarial? Pelo simples risco de também ter prejuízos financeiros enormes ocasionados por uma invasão. O FBI e o Computer Security Institute, gestor de segurança dos EUA, estimam que entre 1997 e 1999, teve-se um prejuízo de 360 milhões de dólares em conseqüência dos crimes computacionais[32]. Segundo o delegado da Polícia Civil de São Paulo, Dr. Mauro Marcelo de Lima e Silva, que investiga crimes digitais, o número de ataques bem sucedidos é

---

[32] **Fonte: Revista Info**

muito maior do que aparece nas estatísticas, tanto no Brasil como no exterior. Isso porque as empresas associam esse tipo de acontecimento a uma propaganda negativa, preferindo assumir os prejuízos em âmbito interno.

A prevenção contra esses ataques, além de anti-vírus, o usuário doméstico precisa de proteção extra para o acesso à Internet. Uma prevenção que se populariza a cada dia é o uso do *firewall*, um sistema simples e lógico, instalado no computador, cuja função principal é interligar duas ou mais redes e proteger essa conexão. Normalmente um *firewall* se ocupa de dois objetivos: a interligação entre a rede interna da empresa com a rede Internet e o gerenciamento do que pode e o que não pode trafegar entre elas. Para o usuário doméstico esse tipo de proteção é instalada por software e aumentará consideravelmente a segurança de quem trafega pela Internet. Essa necessidade do usuário comum não requer o mesmo grau de investimento exigido pelas necessidades de uma corporação, que são bem distintas(Para o uso pessoal existem boas alternativas, algumas pagas, como o Norton Internet Security, e outras gratuitas, como o Zone Alarm).

Um usuário doméstico leigo poderia perguntar: "mas quem ia querer invadir meu computador e por qual motivo?". Incontáveis são os *hackers* que passam a noite "scanneando", buscando, uma porta TCP/IP aberta por "n" motivos. Exemplificando alguns: utilizar a máquina em alguma atividade ilícita, para esconder sua real identidade e localização; utilizar o computador para lançar ataques contra outros; furtar números de cartões de crédito e senhas bancárias; furtar a senha da conta do provedor do invadido, para acessar a Internet se fazendo passar pelo mesmo; furtar dados pessoais, como CPF, ect., ou simplesmente para destruir tudo que tiver ao alcance, como os dados vitais do sistema operacional da máquina invadida. Esse mesmo usuário doméstico fica ainda mais exposto ao ataque externo quando a sua conexão à Internet é concebida através de redes *wireless*, por rádio-frequência, ou por banda larga, pois os IP´s atribuídos geralmente são fixos, ou variam

pouquíssimas vezes, o que facilita as investidas dos *hackers*, que se sentem atraídos ainda pelo alto *bandwidth*[33] agregado às conexões por banda larga. Com uma maior "largura de banda" eles podem aglutinar mais poder de ataque atacando esse usuário e usando sua máquina e seu acesso, banda larga, para outras invasões mais complicadas e ousadas. Outro fator a se preocupar, nesses dois tipos de acesso, é o fato da conexão está ativa o tempo todo. Ou seja, o usuário liga o computador para digitar um texto, brincar inocentemente em um jogo e estará conectado à rede o tempo que passar nessa situação. O que pode atenuar esse risco é desligar o cabo da conexão enquanto não usa a Internet. O *firewall* aparece como sendo essencial, também nesse caso.

O *firewall* profissional, que é usado em empresas, é uma combinação de hardware e software, que atuará basicamente em dois níveis: Segurança. Protegendo a rede corporativa interna do mundo externo, usuários mal-intencionados que usam a Internet; Economia e administração de acesso. Antes de a empresa pensar em aumentar o link de Internet, convém estudar o uso dele. Com o uso de uma solução adequada em *firewall*, a empresa passa a obter instrumentos de administração, medição e avaliação de uso racional do link, permitindo, portanto restringir ou autorizar a navegação, de forma a otimizar os recursos da rede e da Internet. É bom lembrar que não existem apenas *hackers* externos.

Esse controle que o *firewall* leva à mãos do administrador da rede acaba por promover uma disciplina interna que redunda na otimização da banda de acesso à rede Internet, permitindo maior uso com menor custo, gerando, obviamente, economia; uma ou mais máquinas da rede só retiram e-mails e não navegam(restringe assim o entretenimento no horário de trabalho); navegação em horários e/ou sites pré-autorizados; possibilidade de verificação dos sites mais acessados pelos usuários e detalhes de acesso por usuário; lista negra (sites proibidos) e lista branca (sites autorizados).

---

[33] Largura de Banda. Termo que designa a quantidade de informação passível de ser transmitida por unidade de

Outro software que guarda uma certa semelhança com o *firewall*, é uma novidade no Brasil. Trata-se da versão 3.0 do sistema de detecção de intrusões e análise de eventos em redes ManHunt, da *softhouse*(empresa de software) Symantec, que combina detecção de anomalias de protocolo(principais brechas para ataques externos), de negação de serviço e identificação de ataques. Segundo a empresa, o ManHunt 3.0 pode ser programado para rastrear a invasão até a sua origem, reforçar o cumprimento das políticas de segurança, iniciar uma resposta personalizada e enviar notificações para os administradores em tempo real. O sensor do sistema, diz a Symantec, controla e identifica a violação de protocolos, como o TCP/IP .

Fora desse circuito de softwares que, literalmente, seguram os *hackers*, o simples procedimento de ficar atento e desconfiar de tudo, já previne muito. Por exemplo, recomenda-se amplamente, por todo tipo de mídia, que nunca devemos executar um arquivo anexado proveniente de alguém que não conhecemos. O cuidado de submeter qualquer arquivo anexado, vindo de onde vier, por um software anti-vírus também é de extrema importância para integridade dos dados gravados em um computador.

Existem softwares que previnem, ou tentam prevenir, praticamente todos esses tipos de "vermes" digitais. Para tal é conveniente o usuário se informar e ficar atento, mas como "prevenir é melhor que remediar", não custa muito adotar o procedimento de *back-up*[34] como rotina cotidiana, seja em casa ou na empresa, pois caso haja algum dano aos arquivos, existirão cópias para reposição.

tempo, num determinado meio de comunicação (fio, onda radio, fibra óptica, etc.).

CONCLUSÃO

A Internet e as facilidades trazidas pela evolução tecnológica na área de informática são indispensáveis aos anseios da vida moderna. O novo ambiente proporcionado pela "grande rede", para realização de crimes, aparece como sendo fruto da vulnerabilidade que coexiste com todo o tráfego de informações.

A preocupação e o debate que existem em torno da questão de segurança na Internet, relaciona-se, incestuosamente, com a ausência de legislação específica, o que quase sempre redunda na impunidade aos criminosos. Há também a falta de estrutura das polícias, o que já prejudica a reunião de provas até em crimes "reais e concretos", o que dirá nos "digitais e subjetivos", e falta de qualificação específica dos agentes de investigação, urgindo também maiores investimentos nessa infra-estrutura.

As leis que atualmente vigem, estão completamente desatualizadas, pois foram elaboradas fora desse contexto, mesmo porque não havia essa popularização da Intenet à época, nem a suspeita de que redes poderiam ser veículos para a realização de crimes, tendo o computador como instrumento e a "WEB", como ambiente para tal.

Uma nova especialidade no Direito está advindo, junto com o advento da Internet, o que atesta que multidisciplinaridade é útil sobremaneira em todos os ramos de atuação e será explorada tanto nas academias, como nos tribunais.

Assim sendo, urge, sobremaneira, a criação de uma legislação específica atual e que puna de modo exemplar condutas distorcidas nesse âmbito, criando mecanismos que, além de coercitivos, acompanhem a própria dinâmica da Internet e que se adaptem e prevejam o porvir criminoso, o que evolui na mesma velocidade do seu próprio ambiente, a *web*.

BIBLIOGRAFIA

BERGONSO, Carlos Alberto. **Minidicionário de Informática**, Erechim-RS: Edelbra, 2001

CAPEZ, Fernando. **Direito Penal** – Parte Geral. São Paulo: Edições Paloma. Série Doutrina. 7 ed. 2001.

CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet,** São Paulo: Saraiva, 2000.

ESTATUTO DA CRIANÇA E DO ADOLESCENTE. IBM Brasil. Brasília 13 de julho 1990.

GONÇALVES, Victor Eduardo Rios. **Direito Penal: Parte Geral, Volume** 7. São Paulo: Saraiva, 2000.

GRECO, Marco Aurélio; MARTINS, Ives Gandra da Silva. **Direito e Internet**: relações jurídicas na sociedade informatizada. São Paulo: Revista dos Tribunais, 2001.

MCCLURE, Stuart. **Hackers Expostos.** São Paulo: Makron Books do Brasil, 1999.

MIRABETE, Júlio Fabbrini. **Código Penal Interpretado.** São Paulo: Atlas, 1999.

PAESANI, Liliana Minardi. **Direito e Internet**. São Paulo: Atlas, 2000.

REVISTA JURÍDICA - Consulex. Ano VI, n. 129, 31 de maio de 2002.

REVISTA INFO – Editora Abril. Ano 15, nº 173, agosto de 2000.

REVISTA GEEK – Editora Digerati. Ano II, nº 10, junho de 2001.

TAROUCO, Liane Margarida Rockenbach. **Evolução do gerenciamento de Redes**. In Sociedade Brasileira para Interconexão de Sistemas Abertos, Ed., Gerenciamento de Redes - Uma abordagem de sistemas abertos. São Paulo: Makron Books do Brasil, 1993.

TAMIS, Instituto. **Popularização da Internet: introdução ao uso de correio eletrônico e web.** Documento nº RNP/REF/0186, versão final. São Paulo: outubro de 1997.

ANEXOS

ANEXO 1

LEI DE SOFTWARE
LEI Nº 9.609, DE 19 DE FEVEREIRO DE 1998.

Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências.

O PRESIDENTE DA REPÚBLICA
Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei

Capítulo I
DISPOSIÇÕES PRELIMINARES

Art. 1º Programa de computador é a expressão de um conjunto organizado de instruções em linguagem natural ou codificada, contida em suporte físico de qualquer natureza, de emprego necessário em máquinas automáticas de tratamento da informação, dispositivos, instrumentos ou equipamentos periféricos, baseados em técnica digital ou análoga, para fazê-los funcionar de modo e para fins determinados.

Capítulo II
DA PROTEÇÃO AOS DIREITOS DE AUTOR E DO REGISTRO

Art. 2º O regime de proteção à propriedade intelectual de programa de computador é o conferido às obras literárias pela legislação de direitos autorais e conexos vigentes no País, observado o disposto nesta Lei.

§ 1º Não se aplicam ao programa de computador as disposições relativas aos direitos morais, ressalvados, a qualquer tempo, o direito do autor de reivindicar a paternidade do programa de computador e o direito do autor de opor-se a alterações não-autorizadas, quando estas impliquem deformação, mutilação ou outra modificação do programa de computador, que prejudiquem a sua honra ou a sua reputação.

§ 2º Fica assegurada a tutela dos direitos relativos a programa de computador pelo prazo de cinqüenta anos, contados a partir de 1º de janeiro do ano subseqüente ao da sua publicação ou, na ausência desta, da sua criação.

§ 3º A proteção aos direitos de que trata esta Lei independe de registro.

§ 4º Os direitos atribuídos por esta Lei ficam assegurados aos estrangeiros domiciliados no exterior, desde que o país de origem do programa conceda, aos brasileiros e estrangeiros domiciliados no Brasil, direitos equivalentes.

§ 5º Inclui-se dentre os direitos assegurados por esta Lei e pela legislação de direitos autorais e conexos vigentes no País aquele direito exclusivo de autorizar ou proibir o aluguel comercial, não sendo esse direito exaurível pela venda, licença ou outra forma de transferência da cópia do programa.

§ 6º O disposto no parágrafo anterior não se aplica aos casos em que o programa em si não seja objeto essencial do aluguel.

Art. 3º Os programas de computador poderão, a critério do titular, ser registrados em órgão ou entidade a ser designado por ato do Poder Executivo, por iniciativa do Ministério responsável pela política de ciência e tecnologia.

§ 1° O pedido de registro estabelecido neste artigo deverá conter, pelo menos, as seguintes informações:

I - os dados referentes ao autor do programa de computador e ao titular, se distinto do autor, sejam pessoas físicas ou jurídicas;

II - a identificação e descrição funcional do programa de computador;

III - os trechos do programa e outros dados que se considerar suficientes para identificá-lo e caracterizar sua originalidade, ressalvando-se os direitos de terceiros e a responsabilidade do Governo.

§ 2° As informações referidas no inciso III do parágrafo anterior são de caráter sigiloso, não podendo ser reveladas, salvo por ordem judicial ou a requerimento do próprio titular.

Art. 4° Salvo estipulação em contrário, pertencerão exclusivamente ao empregador, contratante de serviços ou órgão público, os direitos relativos ao programa de computador, desenvolvido e elaborado durante a vigência de contrato ou de vínculo estatutário, expressamente destinado à pesquisa e desenvolvimento, ou em que a atividade do empregado, contratado de serviço ou servidor seja prevista, ou ainda, que decorra da própria natureza dos encargos concernentes a esses vínculos.

§ 1° Ressalvado ajuste em contrário, a compensação do trabalho ou serviço prestado limitar-se-á à remuneração ou ao salário convencionado.

§ 2° Pertencerão, com exclusividade, ao empregado, contratado de serviço ou servidor os direitos concernentes a programa de computador gerado sem relação com o contrato de trabalho, prestação de serviços ou vínculo estatutário, e sem a utilização de recursos, informações tecnológicas, segredos industriais e de negócios, materiais, instalações ou equipamentos do empregador, da empresa ou entidade com a qual o empregador mantenha contrato de prestação de serviços ou assemelhados, do contratante de serviços ou órgão público.

§ 3° O tratamento previsto neste artigo será aplicado nos casos em que o programa de computador for desenvolvido por bolsistas, estagiários e assemelhados.

Art. 5° Os direitos sobre as derivações autorizadas pelo titular dos direitos de programa de computador, inclusive sua exploração econômica, pertencerão à pessoa autorizada que as fizer, salvo estipulação contratual em contrário.

Art. 6° Não constituem ofensa aos direitos do titular de programa de computador:

I - a reprodução, em um só exemplar, de cópia legitimamente adquirida, desde que se destine à cópia de salvaguarda ou armazenamento eletrônico, hipótese em que o exemplar original servirá de salvaguarda;

II - a citação parcial do programa, para fins didáticos, desde que identificados o programa e o titular dos direitos respectivos;

III - a ocorrência de semelhança de programa a outro, preexistente, quando se der por força das características funcionais de sua aplicação, da observância de preceitos normativos e técnicos, ou de limitação de forma alternativa para a sua expressão;

IV - a integração de um programa, mantendo-se suas características essenciais, a um sistema aplicativo ou operacional, tecnicamente indispensável às necessidades do usuário, desde que para o uso exclusivo de quem a promoveu.

Capítulo III
DAS GARANTIAS AOS USUÁRIOS DE PROGRAMA DE COMPUTADOR

Art. 7° O contrato de licença de uso de programa de computador, o documento fiscal correspondente, os suportes físicos do programa ou as respectivas embalagens deverão

consignar, de forma facilmente legível pelo usuário, o prazo de validade técnica da versão comercializada.

Art. 8° Aquele que comercializar programa de computador, quer seja titular dos direitos do programa, quer seja titular dos direitos de comercialização, fica obrigado, no território nacional, durante o prazo de validade técnica da respectiva versão, a assegurar aos respectivos usuários a prestação de serviços técnicos complementares relativos ao adequado funcionamento do programa, consideradas as suas especificações.

Parágrafo único. A obrigação persistirá no caso de retirada de circulação comercial do programa de computador durante o prazo de validade, salvo justa indenização de eventuais prejuízos causados a terceiros.

Capítulo IV
DOS CONTRATOS DE LICENÇA DE USO, DE COMERCIALIZAÇÃO E DE TRANSFERÊNCIA DE TECNOLOGIA.

Art. 9° O uso de programa de computador no País será objeto de contrato de licença.

Parágrafo único. Na hipótese de eventual inexistência do contrato referido no caput deste artigo, o documento fiscal relativo à aquisição ou licenciamento de cópia servirá para comprovação da regularidade do seu uso.

Art. 10° Os atos e contratos de licença de direitos de comercialização referentes a programas de computador de origem externa deverão fixar, quanto aos tributos e encargos exigíveis, a responsabilidade pelos respectivos pagamentos e estabelecerão a remuneração do titular dos direitos de programa de computador residente ou domiciliado no exterior.

§ 1° Serão nulas as cláusulas que:

I - limitem a produção, a distribuição ou a comercialização, em violação às disposições normativas em vigor;

II - eximam qualquer dos contratantes das responsabilidades por eventuais ações de terceiros, decorrentes de vícios, defeitos ou violação de direitos de autor.

§ 2° O remetente do correspondente valor em moeda estrangeira, em pagamento da remuneração da que se trata, conservará em seu poder, pelo prazo de cinco anos, todos os documentos necessários à comprovação da licitude das remessas e da sua conformidade ao caput deste artigo.

Art. 11° Nos casos de transferência de tecnologia de programa de computador, o Instituto Nacional da Propriedade Industrial fará o registro dos respectivos contratos, para que produzam efeitos em relação a terceiros.

Parágrafo único. Para o registro de que trata este artigo, é obrigatória a entrega, por parte do fornecedor ao receptor de tecnologia, da documentação completa, em especial do código-fonte comentado, memorial descritivo, especificações funcionais internas, diagramas, fluxogramas e outros dados técnicos necessários à absorção da tecnologia.

Capítulo V
DAS INFRAÇÕES E DAS PENALIDADES

Art. 12° Violar direitos de autor de programa de computador:

Pena - Detenção de seis meses a dois anos ou multa.

§ 1° Se a violação consistir na reprodução, por qualquer meio, de programa de computador, no todo ou em parte, para fins de comércio, sem autorização expressa do autor ou de quem o represente:

Pena - Reclusão de um a quatro anos e multa.

§ 2° Na mesma pena do parágrafo anterior incorre quem vende, expõe à venda, introduz no País, adquire, oculta ou tem em depósito, para fins de comércio, original ou cópia de programa de computador, produzido com violação de direito autoral.

§ 3° Nos crimes previstos neste artigo, somente se procede mediante queixa, salvo:

I - quando praticados em prejuízo de entidade de direito público, autarquia, empresa pública, sociedade de economia mista ou fundação instituída pelo poder público;

II - quando, em decorrência de ato delituoso, resultar sonegação fiscal, perda de arrecadação tributária ou prática de quaisquer dos crimes contra a ordem tributária ou contra as relações de consumo.

§ 4° No caso do inciso II do parágrafo anterior, a exigibilidade do tributo, ou contribuição social e qualquer acessório, processar-se-á independentemente de representação.

Art. 13° A ação penal e as diligências preliminares de busca e apreensão, nos casos de violação de direito de autor de programa de computador, serão precedidas de vistoria, podendo o juiz ordenar a apreensão das cópias produzidas ou comercializadas com violação de direito de autor, suas versões e derivações, em poder do infrator ou de quem as esteja expondo, mantendo em depósito, reproduzindo ou comercializando.

Art. 14° Independentemente da ação penal, o prejudicado poderá intentar ação para proibir ao infrator a prática do ato incriminado, com cominação de pena pecuniária para o caso de transgressão do preceito.

§ 1° A ação de abstenção de prática de ato poderá ser cumulada com a de perdas e danos pelos prejuízos decorrentes da infração.

§ 2° Independentemente de ação cautelar preparatória, o juiz poderá conceder medida liminar proibindo ao infrator a prática do ato incriminado, nos termos deste artigo.

§ 3° Nos procedimentos cíveis, as medidas cautelares de busca e apreensão observarão o disposto no artigo anterior.

§ 4° Na hipótese de serem apresentadas, em juízo, para a defesa dos interesses de qualquer das partes, informações que se caracterizem como confidenciais, deverá o juiz determinar que o processo prossiga em segredo de justiça, vedado o uso de tais informações também à outra parte para outras finalidades.

§ 5° Será responsabilizado por perdas e danos aquele que requerer e promover as medidas previstas neste e nos arts. 12 e 13, agindo de má-fé ou por espírito de emulação, capricho ou erro grosseiro, nos termos dos arts. 16 17 e 18 do Código de Processo Civil.

Capítulo VI
DISPOSIÇÕES FINAIS

Art. 15° Esta Lei entra em vigor na data de sua publicação.

Art. 16° Fica revogada a Lei n° 7.646, de 18 de dezembro de 1987.

Brasília, 16 de fevereiro de 1998; 177° da Independência e 110° da República
FERNANDO HENRIQUE CARDOSO
José Israel Vargas

ANEXO 2

PROJETO DE LEI Nº 84, DE 1999.
(do Sr. Luiz Piauhylino)

Dispõe sobre os crimes cometidos na área de informática, suas penalidades e outras providências.

O Congresso Nacional Decreta:

Capítulo I
POR REDES DE DOS PRINCÍPIOS QUE REGULAM A PRESTAÇÃO DE SERVIÇO COMPUTADORES

Art 1°. O acesso o processamento e a disseminação de informações através das redes de computadores deve estar a serviço do cidadão e da sociedade, respeitados os critérios de garantia dos direitos individuais e coletivos e de privacidade e segurança de pessoas físicas e jurídicas e da garantia de acesso às informações disseminadas pelos serviços da rede.

Art 2°. É livre a estruturação e o funcionamento das redes de computadores e seus serviços, ressalvadas as disposições especificas reguladas em lei.

Capítulo II
DO USO DE INFORMAÇÕES DISPONÍVEIS EM COMPUTADORES OU REDES DE COMPUTADORES

Art 3°. Para fins desta lei, entende-se por informações privadas aquela relativa a pessoa física ou jurídica identificada ou identificável.

Parágrafo Único: É identificável a pessoa cuja individuação não envolva custos ou prazos desproporcionados.

Art. 4°. Ninguém será obrigado a fornecer informações sobre sua pessoa ou de terceiros, salvo nos casos previstos em lei.

Art.5°. A coleta, o processamento e a distribuição, com finalidades comerciais, de informações privadas ficam sujeitas à prévia aquiescência da pessoa a que se referem, que poderá ser tornada sem efeito a qualquer momento, ressalvando-se o pagamento de indenizações a terceiros, quando couberem.

§1°. A toda pessoa cadastrada dar-se-á conhecimento das informações privadas armazenadas e das respectivas fontes.

§ 2°. Fica assegurado o direito a retificação de qualquer informação privada incorreta.

§ 3°. Salvo por disposição legal ou determinação judicial em contrário, nenhuma informação privada será mantida à revelia da pessoa a que se refere ou além do tempo previsto para a sua validade.

§4°. Qualquer pessoa, física ou jurídica, tem o direto de interpelar o proprietário de rede de computadores ou provedor de serviço para saber se mantém informações a seu respeito, e o respeito do teor.

Art.6°. Os serviços de informações ou de acesso a bancos de dados não distribuirão informações privadas referentes, direta ou indiretamente, a origem racial, opinião política,

filosófica, religiosa ou de orientação sexual, e de filiação a qualquer entidade, pública ou privada, salvo autorização expressa do interessado.

Art.7°. O acesso de terceiros, não autorizados pelos respectivos interessados, a informações privadas mantidas em redes de computadores dependerá de prévia autorização judicial.

Capítulo III
DOS CRIMES DE INFORMÁTICA

Seção I
Dano a dado ou programa de computador

Art. 8°. Apagar, destruir, modificar ou de qualquer forma inutilizar, total ou parcialmente, dado ou programa de computador, de forma indevida ou não autorizada.

Pena: detenção de um a três anos e multa.

Parágrafo único. Se o crime é cometido:

I - contra o interesse da União, Estado, Distrito Federal, município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos,

II - com considerável prejuízo para a vítima;

III - com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;

IV - com abuso de confiança;

V - por motivo fútil;

VI - com o uso indevido de senha ou processo de identificação de terceiro ou

VII - com a utilização de qualquer outro meio fraudulento;

Pena: detenção, de dois a quatro anos e multa.

Seção II
Acesso indevido ou não autorizado

Art. 9°. Obter acesso, indevido ou não autorizado, a computador ou rede de computadores

Pena: detenção, de seis meses a um ano e multa.

§ 1° Na mesma pana incorre quem, sem autorização ou indevidamente, obtém, mantém ou fornece a terceiro qualquer meio de identificação ou acesso a computador ou rede de computadores.

§ 2°se o crime é cometido;

I - Com acesso a computador ou rede de computadores da união, estado, distrito federal, município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;

II - Com considerável prejuízo para a vítima;

III - Com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;

IV - Com abuso de confiança;

V - Por motivo fútil;

VI - Com o uso indevido de senha ou processo de identificação de terceiro; ou.

VII- Com a utilização de qualquer outro meio fraudulento.

Pena: detenção, de um a dois anos e multa.

Seção III
Alteração de senha ou mecanismo
de acesso a programa de computador ou dados

Art. 10°. Apagar, destruir, alterar ou de qualquer forma inutilizar, senha ou qualquer outro mecanismo de acesso a computador, programa de computador ou dados, de forma indevida ou não autorizada.

Pena: Detenção de um a dois anos e multa,

Seção IV
Obtenção indevida ou não
autorizada de dado ou instrução de computador

Art. 11°. Obter, manter ou fornecer, sem autorização ou indevidamente, dado ou instrução de computador.

Pena: detenção, de três meses a um ano e multa.

Parágrafo único. Se o crime é cometido:

I - com acesso a computador ou rede de computadores da União, Estado, Distrito federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos,

II - com considerável prejuízo para a vítima;

III - com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;

IV - com abuso de confiança;

V - por motivo fútil;

VI - com o uso indevido de senha ou processo de identificação de terceiro; ou.

VII - com a utilização de qualquer outro meio fraudulento.

Penas detenção, de um a dois anos e multa.

Seção V
Violação de segredo armazenado em computador,
meio magnético, de natureza magnética, óptica ou similar.

Art. 12°. Obter segredos; de indústria ou comércio, ou informações pessoais armazenadas em computador, rede de computadores, meio eletrônico de natureza magnética, óptica ou similar,de forma indevida ou não autorizada.

Pena: detenção, de um a três anos e multa.

Seção VI
Criação, desenvolvimento ou inserção em computador de
dados ou programa de computador com fins nocivos.

Art. 13°. Criar, desenvolver ou inserir, dado ou programa em computador ou rede de computadores, de forma indevida ou não autorizada, com a finalidade de apagar, destruir, inutilizar ou modificar dado ou programa de computador ou de qualquer forma dificultar ou impossibilitar, total ou parcialmente, a utilização de computador ou rede de computadores.

Pena: reclusão, de um a quatro anos e multa.

Parágrafo único: se o crime é cometido:

I - Contra o interesse da União, estado, distrito federal, município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;

II - Com considerável prejuízo para a vítima;

III- Com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;

IV- Com abuso de confiança;

V - Por motivo fútil;

VI- Com o uso indevido de senha ou processo de identificação de terceiro ou

VII- Com a utilização de qualquer outro meio fraudulento

Pena: reclusão, de dois a seis anos e multa.

Seção VII
Veiculação de pornografia através de rede de computadores

Art. 14°. Oferecer serviço ou informação de caráter pornográfico em rede de computadores, sem exibir, previamente de forma facilmente visível e destacada aviso sobre sua natureza, indicando o seu conteúdo e a inadequação para criança ou adolescentes

Pena: detenção de um a três anos e multa.

Capítulo IV
DAS DISPOSIÇÕES FINAIS

Art. 15°. Se qualquer dos crimes previstos nesta lei é praticado no exercício de atividade profissional ou funcional, a pena é aumentada de um sexto até a metade.

Art 16°. Nos crimes definidos nesta lei somente se procede mediante representação do ofendido, salvo se cometidos contra o interesse da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta, empresa concessionária de serviços públicos, fundações instituídas ou mantidas pelo poder público, serviços sociais autônomos, instituições financeiras ou empresas que explorem ramo de atividade controlada pelo poder público, casos em que a ação é pública incondicionada.

Art 17°. Esta lei regula os crimes relativos à informática sem prejuízo das demais cominações previstas em outros diplomas legais.

Art 18°. Esta lei entra em vigor 30 (trinta) dias a contar da data de sua publicação.

ANEXO 3

PROJETO DE LEI Nº 1.713, DE 1996.

CÂMARA DOS DEPUTADOS
(Do Sr. Cássio Cunha Lima)

Dispõe sobre o acesso, a responsabilidade e os crimes cometidos nas redes integradas de computadores e dá outras providências.

(As Comissões de Ciência e Tecnologia, Comunicação e Informática; e de Constituição e Justiça e de Redação)
O Congresso Nacional decreta:

Capítulo I
DOS PRINCÍPIOS QUE REGULAM A PRESTAÇÃO DE SERVIÇO POR REDES INTEGRADAS DE COMPUTADORES

Art. 1º O acesso, o tratamento e a disseminação de informações através das redes integradas de computadores devem estar a serviço do cidadão e da sociedade, respeitados os critérios de garantia dos direitos individuais e coletivos, da privacidade das informações pessoais e da garantia de acesso às informações disseminadas pelos serviços da rede.

Art. 2º Considera-se, para efeitos desta lei:

a) Rede integrada de computadores - qualquer sistema ou conjunto de sistemas, destinado à interligação de computadores ou demais equipamentos de tratamento eletrônico, opto-eletrônico ou ótico de dados, com o fim de oferecer em caráter público ou privado informações e serviços a usuários que conectem seus equipamentos ao sistema.

b) Administrador de rede integrada de computadores - entidade responsável pelo funcionamento de rede de computadores. ou de parte de uma rede de computadores e pela continuidade dos respectivos serviços de rede

c) Infra-estrutura de rede - conjunto dos recursos ou serviços de telecomunicações ou de conexão de outra natureza que viabilizem o funcionamento de rede de computadores.

d) Serviços de rede - serviços essenciais ao funcionamento de rede integrada de computadores, providos pelo administrador de rede, inclusive serviços de controle de acesso, segurança das informações, controle do tráfego de informações e catalogação de usuários e provedores de serviços de valor adicionado.

e) Serviços de valor adicionado - serviços oferecidos aos usuários da rede integrada de computadores que criam novas utilidades específicas, ou novas atividades relacionadas com o uso da rede.

f) Serviço de informação - serviço de valor adicionado caracterizado pela disseminação de informações, limitada ou não, através de rede integrada de computadores.

g) Serviço de acesso a bases de dados - serviço de valor adicionado caracterizado pela coleta, armazenamento e disponibilidade para consulta de informações em bases de dados.

h) Transferência eletrônica de fundos (TEF) - serviço de valor adicionado caracterizado pelo intercâmbio de ordens de crédito ou débito entre usuários de uma rede integrada de computadores, ou por operações cuja finalidade e efeito sejam a transferência de fundos de um patrimônio a outro sem movimentação efetiva de moeda, através de instruções eletrônicas.

i) Base de dados - coleção de informações, armazenada em meio eletrônico, opto-eletrônico ou ótico, que permita a busca das mesmas por procedimentos manuais ou automatizados de qualquer natureza.

j) Provedor de serviços - entidade responsável pela oferta de serviços de valor adicionado.

l) Provedor de informações - entidade responsável pela oferta de serviços de informações ou de acesso a bases de dados.

m) Usuário de rede - pessoa física ou jurídica que utiliza os serviços oferecidos pela rede integrada de computadores ou pelos provedores de serviços ou de informações através dessa rede, ou que possa, legitimamente, receber ou ter acesso a informações transportadas pela rede de computadores.

n) Controle de acesso à rede - conjunto de procedimentos de segurança estabelecidos pelo administrador da rede, a serem executados pelo usuário para ter acesso aos serviços da rede.

Art. 3° É livre a estruturação e o funcionamento de redes integradas de computadores e seus serviços, nos termos desta Lei, ressalvadas as disposições específicas aplicáveis à sua infra-estrutura.

Capítulo II
DO CONTROLE DE ACESSO ÀS REDES DE COMPUTADORES

Art. 4° Toda rede de computadores cujo acesso é oferecido ao público, ou a uma comunidade restrita, gratuitamente ou mediante remuneração de qualquer natureza deverá ter um administrador de rede legalmente constituído.

Art. 5° O administrador de rede é responsável pelos serviços de rede e pela segurança do controle de acesso, nos termos contratuais estabelecidos com o usuário, respeitando as disposições da Lei n° 8.078, de 11 de setembro de 1990, que "dispõe sobre a proteção do consumidor e dá outras providências".

Art. 6° O usuário deverá empenhar-se em preservar a segurança e o segredo de suas senhas, cartões, chaves ou outras formas de acesso à rede de computadores.

Art. 7° Os provedores de serviços de valor adicionado poderão estabelecer procedimentos adicionais de controle de acesso a seus serviços, bases de dados ou informações.

Capítulo III
DA SEGURANÇA DOS SERVIÇOS E DAS INFORMAÇÕES NAS REDES DE COMPUTADORES

Art. 8° O administrador da rede e o provedor de cada serviço são solidariamente responsáveis, nos termos de suas atribuições específicas, pela segurança, integridade e sigilo das informações armazenadas em bases de dados ou disponíveis à consulta ou manuseio por usuários da rede.

Art. 9°. O provedor de informações está sujeito às determinações e limitações estabelecidas na legislação vigente para a atividade de agência de notícias.

Art.10°. As disposições relativas aos serviços de transferência eletrônica de fundos serão regulamentadas por disposição específica, atendidos os direitos e obrigações estabelecidos nesta Lei.

Capítulo IV
DO USO DE INFORMAÇÕES DISPONÍVEIS EM REDES DE COMPUTADORES OU BASES DE DADOS

Art.11°. São consideradas pessoais as informações que permitam, sob qualquer forma, direta ou indiretamente, a identificação de pessoas físicas às quais elas se refiram ou se apliquem.

Art.12°. Ninguém será obrigado a fornecer informações e dados sobre sua pessoa ou a de terceiros, salvo nos casos previstos em lei.

Art.13°. A coleta, o processamento e a distribuição, com finalidades comerciais, de informações pessoais ficam sujeitas à prévia aquiescência da pessoa a que se referem.

§ 1° A toda pessoa cadastrada dar-se-á conhecimento das informações pessoais armazenadas e das respectivas fontes.

§ 2° É assegurado ao indivíduo o direito de retificar qualquer informação pessoal que julgar incorreta.

§ 3° Salvo por disposição legal ou determinação judicial em contrário, nenhuma informação pessoal será conservada à revelia da pessoa a que se refere ou além do tempo previsto para a sua validade.

§ 4° Qualquer pessoa, identificando-se, tem o direito de interpelar o prestador de serviço de informação ou de acesso a bases de dados para saber se estes dispõem de informações pessoais a seu respeito.

Art.14°. É proibida a coleta de dados por meios fraudulentos, desleais ou ilícitos.

Art.15°. Os serviços de informação ou de acesso a bases de dados não distribuirão informações pessoais que revelem, direta ou indiretamente, as origens raciais, as opiniões políticas, filosóficas, religiosas ou sexuais e a filiação a qualquer entidade, salvo autorização expressa do interessado.

Art.16°. Nenhuma decisão administrativa ou judicial poderá basear-se, para a definição do perfil do acusado ou da parte, apenas em dados obtidos mediante o cruzamento de informações automatizadas.

Art.17°. Somente por ordem judicial e observado os procedimentos e a legislação cabíveis. Poderia haver cruzamento de informações automatizadas com vistas à obtenção de dados sigilosos.

Capítulo V
DOS CRIMES DE INFORMÁTICA COMETIDOS EM DECORRÊNCIA DA UTILIZAÇÃO DE COMPUTADOR OU EQUIPAMENTO DE INFORMÁTICA EM REDES INTEGRADAS

Art.18°. Obter acesso, indevidamente, a um sistema de computador ou a uma rede integrada de computadores:

Pena - detenção, de 3 (três) meses a 6 (seis) meses, ou multa.

§1° Se o acesso se faz por uso indevido de senha ou de processo de identificação magnética de terceiro:

Pena - detenção, de 1 (um) a 2 (dois) anos, e multa.

§ 2° Se, além disso, resulta prejuízo econômico para o titular:

Pena - detenção, de 1 (um) a 3 (três) anos, e multa.

§ 3° Se o acesso tem por escopo causar dano a outrem ou obter vantagem indevida.

Pena - detenção, de 2 (dois) a 4 (quatro) anos, e multa.

§ 4° Se o sistema ou rede integrada de computadores pertence a pessoa jurídica de direito público interno, autarquias, empresas públicas, sociedades de economia mista, fundações instituídas ou mantidas pelo Poder Público e serviços sociais autônomos, a pena é agravada em um terço.

Art. 19. Apropriar-se indevidamente de informações, de que tem a posse ou a detenção em rede integrada de computadores:

Pena - reclusão, de 1 (um) a 3 (três) anos, e multa.

Art. 20. Obter segredos empresariais ou informações de caráter confidencial em sistema ou em rede integrada de computadores, com o intuito de causar danos financeiros ou obter vantagem econômica para si ou para outrem:

Pena - reclusão, de 1 (um) a 4 (quatro) anos, e multa.

Parágrafo único. Aumentam-se em um terço as penas se as informações são copiadas ou transferidas a outrem.

Art. 21. Apropriar-se indevidamente de valores, de que tem a posse ou a detenção, através da manipulação de qualquer sistema de processamento de dados, obtendo assim vantagem econômica para si ou para outrem:

Pena - reclusão, de 1 (um) a 5 (cinco) anos, e multa.

Art. 22. Obstruir o funcionamento de rede integrada de computadores ou provocar-lhe distúrbios:

Pena - detenção, de 1 (um) a 2 (dois) anos, e multa.

Parágrafo único. Se resulta obstrução permanente ou distúrbio grave:

Pena - reclusão, de 4 (quatro) a 6 (seis) anos, e multa.

Art. 23. Obter acesso a sistema ou a rede integrada de computadores, com o intuito de disseminar informações fraudulentas:

Pena - reclusão, de 1 (um) a 5 (cinco) anos, e multa.

Art. 24. Falsificar, alterar ou apagar documentos através de sistema ou rede integrada de computadores e seus periféricos:

Pena - reclusão, de 1 (um) a 5 (cinco) anos, e multa.

§ 1° Nas mesmas penas incorre quem, sabendo ser falso, utiliza-se de documento obtido através de sistema ou rede integrada de computadores.

§ 2° Considera-se documento o dado constante no sistema de computador e suporte físico como disquete, disco compacto, cd-rom ou qualquer outro aparelho usado para o armazenamento de informação, por meio mecânico, ótico ou eletrônico.

Art. 25. Interceptar indevidamente a comunicação entre computadores durante a transmissão de dados:

Pena - detenção, de 6 (seis) meses a 1 (um) ano, e multa.

Parágrafo único. A pena é agravada em um terço se a interceptação invade a privacidade do usuário.

Art. 26. Obter, de forma não autorizada, informações confidenciais ou pessoais do indivíduo em sistema ou rede integrada de computadores:

Pena - detenção, de 6 (seis) meses a 1 (um) ano, e multa.

Parágrafo único. Se resulta prejuízo econômico, a pena é aumentada até a metade.

Art. 27. Deixar de informar ou de retificar dados pessoais contidos em rede integrada de computadores, quando requerido pelo interessado:

Pena - detenção de 3 (três) a 9 (nove) meses, e multa

Parágrafo único. Na mesma pena incorre quem:

I - Transfere dados pessoais contidos em um sistema de computador, sem a permissão do interessado, a pessoa não autorizada com finalidade diversa daquela à qual a informação foi obtida;

II - Transfere, sem a permissão do interessado, dados pessoais para fora do país

Art. 28. Obter acesso a sistemas de dados ou rede integrada de computadores de instituições financeiras com o objetivo de transferir, para si ou para outrem dinheiro, fundos, créditos e aplicações de terceiro:

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

Art. 29. Obter acesso ilícito a sistema de computador ou a rede integrada de computadores, com o intuito de apropriar-se de informações confidenciais ligadas à segurança nacional:

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

Parágrafo único. Se, além do acesso, as informações são copiadas, vendidas ou transferidas para outrem, a pena é agravada em um terço.

Capítulo VI
DAS DISPOSIÇÕES FINAIS

Art. 30. Se os crimes cometidos nesta Lei são praticados como meio para a realização de outros, a pena é aumentada de um sexto até a metade.

Art. 31. Os administradores de redes integradas de computadores, os provedores de serviços e de informações que, no exercício da função, provocam desvio nas finalidades estabelecidas para o funcionamento da rede, incorrem na pena de reclusão de 1 (um) a 2 (dois) anos, e multa.

Art. 32. Nos crimes definidos nesta Lei somente se procede mediante representação do ofendido, salvo nos casos do § 4°, do art. 18 e do Art. 29, em que a ação é pública incondicionada.

Art. 33. Aplica-se subsidiariamente a legislação penal em vigor.

Art. 34. Esta lei entra em vigor 30 (trinta) dias a contar da data de sua publicação.

Art. 35. Revogam-se as disposições em contrário.