INSTITUTO VALE DO CRICARÉ

FACULDADE VALE DO CRICARÉ

CURSO DE DIREITO

CRIMES DE INFORMÁTICA

SÃO MATEUS – ES

2007

MARTA FERNANDES BERNARDO

CRIMES DE INFORMÁTICA

Trabalho apresentado ao Curso de Direito, como pré-requisito para a obtenção do título de bacharel em Direito, da Faculdade Vale do Cricaré.
Prof. Orientador: Samuel Davi Garcia Mendonça

SÃO MATEUS

2007

MARTA FERNANDES BERNARDO

CRIMES DE INFORMÁTICA

Banca examinadora:

Prof. Samuel Davi Garcia Mendonça

_____

Profª.

Prof.

AGRADECIMENTOS

Agradeço, primeiro de tudo a Deus, por ter me permitido chegar até aqui.

A todos os professores que ensinam como coração, em especial ao professor Samuel Davi Garcia Mendonça, à professora Renata Zanette, pela orientação fornecida e à coordenadora Jackeline por manter a faculdade coesa.

Aos colegas, pelo companheirismo.

Aos meus pais, que sempre me incentivaram em todos os sentidos e principalmente a continuar estudando.

E ao meu querido filho, pela compreensão por tantas ausências.

“nesse concubinato do homem com a máquina, onde alguma vez se instala um amor doentio, a máquina não é humanizada, mas o homem é mecanizado.”

Stanciu

RESUMO

O objetivo deste trabalho é iniciar uma discussão sobre a nova modalidade de crimes surgidos nos últimos tempos, os crimes de informática, contribuir para o avanço jurídico do ordenamento pátrio, colaborando com o estudo de uma proposta para suprir a legislação pátria com lei até então inexistente sobre o assunto, evitando que os *ciber* criminosos continuem impunes, e alimentar o debate sobre o novo ramo de direito emergente, o Direito Informático.

SUMÁRIO

1. INTRODUÇÃO

Com o avanço da tecnologia e da informática ocorrido nos últimos trinta anos, o uso do computador se disseminou por órgãos públicos, empresas privadas, universidades e escolas, tendo se popularizado a ponto de estar presente em grande parte dos lares deste país. E com os computadores surgiu um novo tipo de crime, o crime de informática.

A escolha do tema deu-se devido ao fato de que uma das preocupações do homem moderno é com os rumos das novas tecnologias, com os crimes surgidos com o uso do computador e com a utilização da rede mundial de computadores, a *World Wide Web*, mais conhecida como *internet*, por estar se tornando palco para o cometimento de crimes das mais diversas naturezas, sem haver, em contrapartida, legislação que tipifique tais condutas.

Considerando-se que o ordenamento jurídico penal nacional se alicerça no princípio da reserva legal, consubstanciado no Art. 1°, *caput*, do Código Penal: “Não há crime sem lei anterior que o defina. Nem pena sem prévia cominação legal”, o legislador se vê na posição de ter que correr contra o tempo para não deixar impunes criminosos que a cada instante ligam seus computadores para o cometimento de crimes, que acontecem não mais em escala pessoal, mas atingindo enormes proporções, por meio da *Internet.*

Na escolha do tema, foi considerada a existência de um hiato no ramo do direito penal, entre estes novos crimes cometidos com o uso do computador, que ainda não foram positivados, e a lei penal vigente.

Os criminosos, que são oportunistas, mudaram seu *modus operandi*, pois não mais precisam ir ao local do crime, passando a cometer crimes utilizando-se da *Internet* como instrumento para sua prática.

A *Internet* não é um meio novo para a execução de velhos crimes contidos no Código Penal. Ela é muito mais que isto. Isto ficará claro no decorrer do trabalho.

Muitos crimes podem ser adequados à legislação em vigor, especialmente à Lei 2.848/40, isto é, ao Código Penal Brasileiro. Porém, muitas ações decorrentes do avanço tecnológico não se enquadram a qualquer tipo penal, não sendo possível haver a subsunção de tais condutas ilícitas executadas por meio da *Internet*, à norma positivada. São condutas novas, inexistentes há até pouco tempo atrás.

Algumas leis a respeito do tema já foram elaboradas, tais como a Lei de Proteção ao *Software,* Lei 7.646/87, a Lei de Proteção a Propriedade Intelectual, Lei n° 9.609/98, a Lei sobre a Interceptação Ilegítima, Lei 9.296/96, a Lei do Direito Autoral, n° 5.988/73 em seu artigo 2°, bem como o art. 2, inciso I, da Lei 8.137/90, cujos conteúdos encontram-se nos apensos ao final deste trabalho.

Vários projetos de lei sobre o tema tramitam no Congresso Nacional, tais como o Projeto de Lei 3.279/76, da Câmara dos Deputados, o Projeto de Lei 96/77, do Senado Federal, o Projeto de Lei 4.125/89 da Câmara, o Projeto de Lei 579/91, da Câmara, o Projeto de Lei 152/91 do Senado, o Projeto de Lei 4.102/93, do Senado, o Projeto de Lei 75/89.

Ocorre que a maioria dos Projetos de Lei que tramitam na Câmara dos Deputados é arquivada quando seus autores não são reeleitos, por força do art. 105 do Regimento Interno daquela casa, o que em feito com que os atos ilícitos praticados por meio da rede de computadores fiquem, muitas vezes, sem regulamentação.

Diante da inexistência de legislação específica em vigor a respeito dos crimes cibernéticos, faz-se necessária pesquisa nesta área do direito penal, a fim de que haja um avanço jurídico no ordenamento pátrio, com a elaboração de uma proposta de projeto de alteração à Lei 2.848/40, o Código Penal Brasileiro, objetivando preencher a lacuna existente em nossa legislação, positivando os crimes que por enquanto não podem punir os agentes, ante a inexistência de lei, e assim, trazer conseqüências sociais e individuais e fazer jus aos anseios de justiça da população.

Com este trabalho tentarei responder a como poderiam os crimes de informática se enquadrar em nossa legislação? Como seriam definidos? Em que titulação e capitulação seriam situados? Como têm sido tipificados os crimes cometidos pela rede mundial de computadores? Como dar-lhes uma caracterização específica e abrangente?

A escolha do tema deveu-se ainda à intenção de se vislumbrar meios de evitar ou coibir os crimes cometidos por meio de sistemas de informática e pela *Internet.*

Durante a pesquisa não me aterei na discussão da questão dos direitos autorais, bem como da pedofilia por meio da internet, por entender que os mesmos já se encontram abrangidos pela norma, o primeiro pela Lei

5.988/73, e o segundo pela Lei 10.764/03, que alterou o art. 241 da Lei 8.069/90, o ECRIAD.

Também não estabelecerei uma única forma de expressão tal como “crime informático”, “crime de informática” “crime de computador” ou “crime cibernético”, bem como não fixarei uma só terminologia para o “direito de informática” ou “direito informático”, tendo em vista os termos ainda estarem sendo discutidos e ainda não existir unanimidade a respeito. Assim, farei uso das expressões, livremente.

1 CRIMES DE INFORMÁTICA

1.1 Definição

A Organização para a Cooperação Econômica e Desenvolvimento (OECD) define crime informático como qualquer conduta ilegal, não ética, ou não autorizada, que envolva processamento automático de dados e/ou a transmissão de dados (apud REIS, 1997, p.12).

Para Marco Aurélio de Oliveira Costa em seu livro "O Direito e a *Internet*", a expressão crimes de informática, entendida como tal, é toda a ação típica, antijurídica culpável contra ou pela utilização de processamento automático e/ou eletrônico de dados ou sua transmissão. Segundo este autor, nos crimes de informática, a ação típica se realiza contra ou pela utilização de processamento automático de dados ou a sua transmissão. Ou seja, a utilização de um sistema de informática para atentar contra um bem ou interesse juridicamente protegido, pertença ele à ordem econômica, a integridade corporal, à liberdade individual, à privacidade, à honra, ao patrimônio público ou privado, à Administração Pública, etc.

Crime de informática, segundo Sergio Marcos Roque (apud Penteado, p. 309) poderia ser assim definido:

> É a conduta definida em lei como crime em que o computador tiver sido utilizado como instrumento para a sua perpetração ou consistir em seu objeto material. Ao primeiro chamaremos de crime de informática impróprio ou comum, e ao segundo, de próprio ou autêntico.

Assim, poderíamos entender que há duas categorias de crimes de informática: os que são praticados por meio do uso do computador e os perpetrados contra os dados ou sistemas de informática.

Quando o computador for utilizado apenas como instrumento para a realização do crime, será considerado **um crime de informática comum** [grifo nosso], mas quando a ação do criminoso se dirigir contra os dados contidos no sistema, será definido como **crime de informática autêntico** [grifo nosso], porque nesse caso, o computador é essencial para a existência do delito.

Para John Teber (apud Penteado, p.317), o crime de computador só poderia ser assim definido quando o computador for essencial para o crime.

Como exemplos de crimes de informática comuns poderiam ser citados: o furto mediante fraude, o estelionato, diversos tipos de falso, crimes contra os costumes, violação contra a liberdade individual, enfim, os crimes tradicionais, diferenciados apenas pela opção de utilização do computador como meio para sua perpetração.

Quanto aos crimes de informática autênticos podem ser citados: os crimes de dano, os de interceptação ilegítima, os de acesso ilegítimo e os de reprodução ilegítima, que podem se apresentar como figuras de crimes complexos ou isoladamente.

O dano informático tem amplitude maior que o tipificado no art. 163 do Código Penal, pois o agente pode ter como objetivo não só a destruição da coisa, como obter vantagem para si ou para terceiros. Consiste em danificação na alteração, a supressão ou destruição de dados informáticos de modo a produzir dano ao usuário ou a terceiros.

O dano causado tanto pode referir-se à parte física do equipamento quanto ao software ou a dados, se o dano reduzir ou suprimir sua utilização bem como seu valor.

Interceptação ilegítima é o ato destinado a captar informações contidas num sistema automatizado de dados, através de dispositivos eletromagnéticos, acústicos, mecânicos ou outros.

Não há na lei penal brasileira a figura típica do acesso ilegítimo a redes ou sistemas informáticos ou telemáticos, entretanto, para a maioria das hipóteses em que o cesso for o instrumento, poderá a conduta ser enquadrada em alguma das figuras existentes em nosso Código Penal de crimes contra o patrimônio ou contra a pessoa. Apenas quando se tratar de crime autônomo de simples acesso não autorizado é que não há possibilidade de punição, visto não existir tal tipo em nossa legislação até o momento.

1.2 Classificação dos Crimes

A classificação dos crimes por meio da informática é importante para a melhor compreensão do assunto.

Ulrich Sieber, citado por Sandra Galveas (1997, p.62) divide os crimes por computador em três grupos:

1- Os crimes econômicos;

1.1 Fraude por manipulação de dados em sistemas de processamento de dados;

1.2 Espionagem de dados e pirataria de programas;

1.3 Sabotagem informática;

1.4 Furto de serviço ou furto de tempo;

1.5 Acesso não autorizado a sistemas;

1.6 Uso de computador para crimes empresariais.

2- Ofensas contra Direitos Individuais;

2.1Uso incorreto de informação;

2.2 Obtenção ilegal de dados e arquivo de informações;

2.3 Revelação ilegal e mau uso de informação;

2.4A dificuldade de se distinguir entre obtenção, arquivamento ou revelação de informação.

3- Ofensas contra interesses supra-individuais.

3.1 Ofensas contra interesses estaduais e políticos;

3.2 Crimes contra a integridade humana.

Já Marc Jeager, citado por Ivette Senice em seu livro: Os crimes de Informática (apud Sandra Gouvea, 1997, p.65), propõe outra classificação:

1. As fraudes propriamente ditas, subdivididas em:

1.1 Fraudes no nível do *hardware*;

1.2 Fraudes no nível do input;

1.3 Fraudes no nível do tratamento;

1.4 Fraudes no nível do *output;*

2. Atentados à vida privada.

O Carlos M. Romeo Casabona, (apud Reis, 1997, p.31), na Espanha, forneceu a seguinte classificação:

- Manipulação de entrada de dados *(input);*

- Manipulação no programa;

- Manipulação na saída de dados (*output);*

- Manipulação à distância.

João Marcelo de Araújo Junior (apud Sandra Gouvea, 1997, p. 66) propõe a seguinte classificação, baseada na natureza do dano:

1. Prejuízos econômicos diretos;

2. Prejuízos econômicos indiretos;

3. Prejuízos intangíveis.

As condutas que atentam contra os sistemas de informática são geralmente as seguintes:

- Acesso não autorizado;

- Interceptação não autorizada;

- Uso não autorizado a sistemas de informática;
- Inserção – inserção de valores ou dados falsos;
- Alteração – alterar dados ou informações;
- Supressão- apagar informações ou dados;
- Furto – furto de informação, de dados ou de valores;
- Dano a dado ou programa de computador;
- Fraude por manipulação de computador.

A partir da evolução da tecnologia a doutrina passou a se questionar sobre qual o tratamento que deve ser dado a um arquivo eletromagnético. Caminha-se no sentido de se decidir que os arquivos eletromagnéticos são considerados documentos. As informações contidas em um computador constituem bem de enorme valor.

1.3 Sujeito Ativo

Nos dias de hoje está ocorrendo uma verdadeira democratização dos crimes praticados por meio da informática. O criminoso do computador de hoje é o homem comum, pode não saber nada, ou apenas o suficiente para a prática do crime pretendido. De acordo com as diferentes motivações, estes criminosos podem ser classificados em quatro categorias básicas: o criminoso

tradicional ou o criminoso profissional; o funcionário criminoso ou o profissional criminoso; o terrorista virtual e o brincalhão criminoso.

As estatísticas mostram que a maioria dos crimes de informática são praticados por funcionários de empresas públicas ou privadas. Em pesquisa feita pela *Price Waterhouse*, revelou que funcionários estariam envolvidos em 82% dos ataques aos sistemas de informática no setor privado. 58% destes ataques são efetuados por funcionários que possuem autorização, e 24% por funcionários não autorizados.

As motivações podem ser de diversas naturezas, tais como: adquirir ganhos financeiros, necessidade de aceitação ou respeito, idealismo, curiosidade, busca de emoção, anarquia, aprendizado, ignorância, espionagem industrial, espionagem nacional, vingança,

Pesquisas demonstraram que na maioria dos casos a motivação é o desejo de vingança, por terem sido despedidos ou por insatisfação com o salário ou com a chefia.

2 A INFORMAÇÃO COMO BEM JURÍDICO A SER TUTELADO

Por ser um fenômeno recente, ainda não se tem a consciência de que a informação contida nos sistemas de informática é um bem jurídico e como tal, deve ser protegido por lei. Assim, a informação transforma-se em uma nova matéria-prima, pertencente ao gênero especial dos bens imateriais.

O art. 155, caput do CP diz: “Subtrair para si ou para outrem, coisa alheia móvel: Pena – reclusão de1(um) a 4(quatro) anos,e multa”, e o § 3°, esclarece: “Equipara-se à coisa móvel a energia elétrica ou qualquer outra que tenha valor econômico”.

A informação pode ser tratada como “coisa alheia móvel”? Nos termos do art. 155, coisa é toda substância corpórea, material, ainda que não tangível, susceptível de apreensão e que tem um valor qualquer. Ficam pois, excluídas como objeto material do furto, as coisas incorpóreas ou imateriais, de cuja existência só dá testemunho a inteligência humana.

Para o Direito Penal, móvel é tudo quanto é suscetível de remoção, ou por ser dotado de movimento próprio, suscetível de remoção, ou por ser dotado de movimento próprio – os semoventes – ou por ação do homem. A idéia de coisa móvel para o Direito Civil é diferente do Direito Penal.

A informação ou dado se enquadra nestes conceitos? Se ela estiver em um disco rígido, dá-se o nome de furto? Houve o furto do disco, ou das informações? E se não houvesse furto do disco, mas uma transferência de

dados, os dados originais continuariam no mesmo lugar. Onde houve remoção?

A informação que está num meio magnético nada tem a ver com a produção de energia elétrica ou outra qualquer. Ela tem um valor próprio, só se torna impulso elétrico para fins de processamento.

Assim, a informação ainda hoje não tem lugar em nenhum titulo ou capítulo do Código Penal brasileiro, ela está desprotegida, desamparada, dentro dos ordenamentos penais conhecidos, inclusive o nosso.

O caput do art. 171 do Código Penal diz que: “Obter para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil,ou qualquer outro meio fraudulento. Pena-reclusão, de 1(um) a 5(cinco) anos, e multa.”

Na fraude por manipulação de um computador contra um sistema de processamento de dados, o sujeito passivo não foi induzido, nem sabe se houve erro e tampouco o sujeito passivo foi mantido em erro.

Portanto, na ocorrência da subsunção das novas condutas às normas vigentes, os fatos não estão sendo devidamente acolhidos pela legislação existente. O que está havendo é uma adaptação, muitas vezes inadequada ou imprecisa. Isto sem mencionar os casos em que não existe regulamentação alguma de modo a adequar fato à norma em vigor.

3 A INTERNET

Durante a Guerra Fria, pesquisadores de uma instituição militar americana começaram a imaginar um sistema imune a bombardeios, que fosse capaz de interligar muitos computadores, permitindo o intercâmbio entre eles. A primeira versão deste sistema chamou-se *Advanced Reserarch Projects Agency - ARPAnet*, e sua característica principal foi não possuir um comando central, a fim de que em caso de destruição de um ou mais computadores, todos os outros equipamentos ligados ao sistema continuassem operando. Assim, foi desenvolvido um sistema de comunicação aparentemente anárquico e sem controle, mas por isso mesmo seguro, não possuindo dono e nenhuma base física isolada.

Décadas mais tarde, surgiu o nome *Internet*, quando a tecnologia anteriormente desenvolvida serviu para ligar universidades americanas entre si, e depois institutos de pesquisa em outros países. Mas a idéia central continuou a mesma: uma espécie de associação mundial de computadores, todos interligados por meio de um conjunto de regras padronizadas que especificam o formato, a sincronização e a verificação de erros em comunicação de dados. Esse conjunto de regras recebeu a denominação de protocolo.

A *Internet* nada mais é do que um meio de comunicação que depende de outro meio de comunicação. Ela pode trafegar por meio de uma linha telefônica, de um sinal de rádio, de um cabo de televisão, etc. Não se limita aos serviços acessados pelo uso da sigla inicial *www*, as páginas assim iniciadas são apenas um dos inúmeros serviços e procedimentos possíveis via *Internet*.

É popularmente conhecida como rede de acesso público irrestrito. É uma rede pública.

Já na década de noventa, com a invenção da *World Wide Web(rede mundial)*, um enorme pacote de informações em formato de texto ou mídia (imagens e arquivos de áudio e vídeo), organizadas de forma a que o usuário possa navegar na rede, a partir de seqüências associativas, os *links,* entre blocos vinculados, dando início à exploração comercial do serviço. Ao se digitar o nome de um *site,* na verdade o que se está é digitando um número, que, para facilitar a memorização é escondido por um endereço alfabético, o chamado número *IP.*

Os *sites*, que são coleções de páginas a respeito de determinado assunto, constituem como as informações na *Web* são geralmente agrupadas. Os *sites* podem ser acessados por intermédio de programas de navegação (*browsers*), como o *Internet Explorer*, o *Netscape*, ou o *Mozila Firefox*. O endereço que digitamos nestes programas de navegação para acessar algum *site* é chamado de URL, ou Localizador Uniforme de Recursos. O termo site é usado para identificar o local onde ficam armazenadas as informações acessadas, isto é, as páginas da *Internet.*

Os endereços da *Web* seguem uma estrutura ordenada, composta por domínios. O endereço eletrônico é composto de três partes, ou **domínios:** os "**nomes de domínio**", como por exemplo: *hotmail, google*, tam; os "**domínios de nível superior**", por exemplo: .com., org., .gov, etc, ou os "**domínios de países**", indicativo do país de origem, tal como: .br, .de, .den, ou fr. *Sites*

sediados nos Estados Unidos não possuem a extensão final, pois como foi o país de origem da *Internet*, não se pensou necessária tal informação.

Os URLs digitados na navegação necessitam ser traduzidos para um endereço numérico, denominado "**endereço *IP***"*[grifo nosso]*. As comunicações entre os computadores conectados à rede são feitas por intermédio de regras chamadas de protocolos. ***IP*** diz respeito a esses **protocolos na *Internet.***[grifo nosso]. Cada *site* ou página que acessamos está hospedado em um computador permanentemente ligado à rede, chamado de servidor, o qual é identificado apenas pelo endereço numérico *IP*.

A tradução dos nomes de domínio para um endereço *IP* é feita por um computador chamado servidor DNS.

Para que haja a navegação, é necessária uma conexão com a rede. A conexão é feita através de um *modem*, ligado a uma linha telefônica ou a um cabo. As concessionárias de telefone comercializam linhas especiais para a internet, conhecidas como "banda larga." A conexão com a *Internet* depende ainda da assinatura de um provedor de acesso como UOL, Globo, IG, Terra, etc.

A regulamentação estatal da atividade desses provedores é mínima, dificultando as investigações e contribuindo para a impunidade de alguns crimes cibernéticos.

Está surgindo um Código de Conduta ou Código de Auto Regulação da Internet, que visa prevenir a utilização ilícita ou potencialmente ofensiva da rede por meio da divulgação de uma correta cultura e da responsabilidade de todos os sujeitos ativos da rede *Internet.*

Quando o usuário faz a conexão à rede, recebe um número – o *IP*. Esse número, durante o tempo de conexão, pertence exclusivamente ao usuário. A identificação do *IP* é o passo mais importante na investigação do crime cibernético, juntamente com a hora exata da conexão e o fuso horário do sistema.

Como já foi dito, a *Internet* é um conjunto de redes interligadas, de abrangência mundial. Através da *Internet* estão disponíveis serviços como correio eletrônico, transferência de arquivos, acesso remoto a computadores, acesso as bases de dados e diversos tipos de serviços de informação.

Quando foi projetada, inicialmente, o objetivo da I*nternet* era permitir diversas possibilidades de conectividade entre as partes que estivessem interagindo. Portanto, a interoperabilidade e não a segurança, foi enfatizada. As propriedades intrínsecas da *Internet* representam a principal fonte de sua vulnerabilidade e falhas e ataques. A *Internet* conecta centenas de redes regionais e redes de provedores de serviços regionais espalhadas pelo mundo inteiro. Seu enorme tamanho afeta sua confiabilidade e abre uma porta para problemas como roteamentos incorretos, falhas de transmissão, adulteração de dados e falhas de componentes físicos (tais como os roteadores) em um número infinito de pontos.

A *Internet* é organizada na forma de espinhas dorsais que são estruturas de rede capazes de manipular grandes volumes de informações constituídas basicamente por roteadores de tráfego interligados por circuitos de alta velocidade.

Interligadas às espinhas dorsais de âmbito nacional, há espinhas dorsais de abrangência regional, estadual ou metropolitana, que possibilitam a interiorização da *Internet* no país.

Conectados às espinhas dorsais, estão os provedores de acesso ou de informações que são os efetivos prestadores de serviços aos usuários finais da Internet, que os acessam tipicamente através do serviço telefônico. Existem no país espinhas dorsais *Internet* independentes, de âmbito nacional ou não, sob a responsabilidade de diversas entidades. É facultada aos provedores de acesso ou de informações a escolha da espinha dorsal à qual se conectará, assim como será de livre escolha do usuário final o provedor de acesso ou de informações através do qual terá acesso à *Internet*.

A medida que mais redes são conectas, ameaças podem atacar a rede de computadores. As ameaças mais comuns são: ameaças à rede corporativa, ameaças aos servidores da internet, ameaças à transmissão de dados, ameaças à disponibilidade dos serviços, ameaças de repudiação (negar que a transação tenha ocorrido).

3.1 A Internet e a Privacidade x Liberdade de Acesso

Dispõe o art. 5° - X da Constituição Federal de 1988:

“São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito de indenização pelo dano material ou moral decorrente de sua violação.”

Assim, resguarda-se a vida privada e a intimidade da pessoa, assegurando-se sua inviolabilidade.

Tal dispositivo visa proteger a personalidade humana contra intromissões alheias ou indesejáveis, e, face aos novos meios de comunicação, principalmente a internet, o homem encontra-se permanentemente exposto, tendo encontrado dificuldades em delimitar a esfera de sua privacidade. O conceito de privacidade passou a significar o direito de dispor com exclusividade sobre as próprias informações.

Porém, o direito à privacidade constitui um limite natural ao direito à informação. Assim, é necessário que haja consentimento da pessoa para a divulgação de informação a seu respeito, pois é dela a tutela de sua privacidade.

Dispõe o art. 220 da Constituição Federal:

"A manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo não sofrerão qualquer restrição, observado o disposto nesta Constituição."

Portanto, deve-se ter liberdade de escolha entre os vários fornecedores, e de seleção de serviços na busca da informação.

Existe uma grande discussão em curso, vez que uma das principais características da internet é o anonimato, e qualquer tentativa de limitar a possibilidade deste anonimato, viola um dos princípios da internet, isto é, o de ser um espaço de liberdade total.

3.2 Convenção sobre a Cibercriminalidade

Aberta à assinatura de todos os países, foi adotada pelo Conselho da Europa, em 2001, obrigando os Estados a tipificarem as seguintes condutas:

1- Infrações contra a confidencialidade, integridade e disponibilidade dos dados e sistemas informáticos;

a) acesso doloso e ilegal a um sistema de informática;

b) interceptação ilegal de dados ou comunicações telemáticas;

c) atentado à integridade dos dados;

d) atentado à integridade de um sistema;

e) produção, comercialização, obtenção ou posse de aplicativos ou códigos de acesso que permitam a prática dos crimes mencionados;

2 - Infrações informáticas:

a) falsidade de dados;

b) estelionatos eletrônicos.

2- Infrações relativas ao conteúdo:

a)pornografia infantil (produção, oferta, procura, transmissão e posse de fotografias ou imagens realistas de menores ou de pessoa que aparecem com menores, em comportamento sexual explícito;

b) racismo e xenofobia (difusão de imagens, idéias ou teorias que preconizem ou incentive, o ódio, a discriminação ou a violência contra uma pessoa ou grupo de pessoas, em razão

de raça, religião, cor ascendência, origem nacional ou étnica, injúria e ameaça qualificadas pela motivação racista ou xenófoba, negação, aprovação ou justificação do genocídio ou outros crimes contara a humanidade.

3- Atentado à propriedade intelectual e aos direitos que lhe são conexos.

3.3 *Virus, Worms, Spywares*, Cavalos de Tróia e Outros

Hoje em dia, há registros de 100 mil tipos diferentes de vírus. Há ainda as pragas, como os *worms, spywares*, e cavalos de tróia.

Os danos causados por programas de computador que carregam vírus, *worms* ou *logic bombs* representam um grande perigo.

Vírus é um programa ou parte de um programa de computador, malwares, normalmente maliciosos ou programas destrutivos criados para danificar ou destruir arquivos armazenados no disco rígido, principalmente os essenciais para o funcionamento do sistema, tornando o sistema inoperante ou impedindo totalmente seu funcionamento. Os vírus podem se espalhar nos computadores ligados a uma rede ou através de discos infectados. Sua principal característica é o poder de disseminação, pois são capazes de se replicar indefinidamente. O vírus se propaga infectando, isto é, inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos de um

computador. Ele depende do programa ou arquivo hospedeiro para que possa se tornar ativo e dar continuidade ao processo de infecção.

Worm é um programa capaz de se propagar automaticamente através de rede, enviando cópias de si mesmo de computador para computador. Diferentemente do vírus, não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser executado para se propagar. Sua propagação se dá através da exploração de vulnerabilidades existentes ou falhas na configuração de softwares instalados nos computadores. Como os vírus, são construídos de forma semelhante para se infiltrar em programas legítimos. Degradam sensivelmente o desempenho de redes e podem lotar o disco rígido, devido à grande quantidade de cópias de si mesmo que costumam propagar. Causam transtornos para os que recebem estas cópias. Eles prejudicam o acesso aos serviços de rede.

As bombas-lógicas são programadas para destruir ou modificar dados em um tempo futuro, requerem um conhecimento especializado.

Alguns estudiosos entendem que vírus, *worms* e bombas-lógicas constituem modificações ilegítimas de dados, e portanto, se inserem na rubrica de alteração de dado. Outros os consideram como sabotagem.

Spywares são programas espiões, geralmente usados com fins comerciais. São instalados quando o usuário recebe algum e-mail, baixa algum tipo de arquivo, ou navega pela *Internet*. Uma vez executados, passam a monitorar as páginas acessadas e o que é digitado pelo usuário. As conseqüências de um programa espião incluem a lentidão no acesso à

Internet, a mudança de página inicial do *browser* e a proliferação das janelas conhecidas como: *pop-ups*.

Em muitos casos, as mensagens contidas nos *pop-ups windows* apresentam *links*, que podem redirecionar o usuário para uma página fraudulenta ou induzi-lo a instalar algum *software* malicioso para, por exemplo, furtar senhas bancárias ou números de cartões de crédito.

Bot (robô) é um programa capaz de se propagar automaticamente, explorando vulnerabilidades existentes ou falhas na configuração de *softwares.* Dispõe de mecanismos de comunicação com o invasor, permitindo que o *bot* seja controlado remotamente. Normalmente o *bot* se conecta a um servidor e entra em um canal ou sala determinada. Aguarda as instruções do invasor, monitorando as mensagens. O invasor, ao se conectar ao mesmo servidor e entrar no mesmo canal, envia mensagens que são interpretadas pelo *bot,* que, seguindo as instruções, executa as ações.

Um fenômeno recente tem sido a proliferação das redes de computadores infectados, os *botnets*. São redes formadas por computadores infectados por *bots.* Elas são criadas para furtar dados, enviar *spams,* trocar programas piratas e obter vantagens financeiras. Isto se dá com o recebimento de um *e-mail* falso, supostamente remetido por uma instituição financeira, ou órgão governamental. O *e-mail* contendo arquivos maliciosos anexados ou acessados entram em ação quando o usuário seleciona um determinado *link*. Aberto o arquivo, um robô(*bot*), é instalado no computador do usuário. Através da Internet, o robô conecta o computador a uma rede (*botnets*), controlada por um *cracker*. Este indivíduo pode remotamente controlar as máquinas dos usuários

vinculados à rede, obtendo dados como senhas e números de cartões e furtando arquivos pessoais e dados internos do sistema. Há casos destas operações se realizarem automaticamente, sem a necessidade de intervenção do *cracker*.

Cavalo de tróia ou *trojan horse*, são programas aparentemente inofensivos que contêm códigos maliciosos capazes de ter acesso e copiar todos os arquivos armazenados no computador, de destruir dados armazenados, formatando o disco rígido do computador, de enviar informações sigilosas, de furtar senhas e outras informações sensíveis, permitir que o atacante tenha total controle sobre o computador.

O cavalo de tróia distingue-se de um vírus ou de um *worm* por não infectar outros arquivos, e nem propagar cópias de si mesmo automaticamente. Normalmente é um único arquivo que necessita ser executado. Geralmente é anexado a um e-mail ou está disponível em algum site na internet.

Normalmente o cavalo de tróia procura instalar, sem que o usuário perceba, programas que realizam uma série de atividades maliciosas.

3.4 Segurança de Computadores

Um computador é seguro se ele atende a três requisitos básicos relacionados aos recursos de que dispõe:

- confidencialidade: diz que a informação só está disponível para aqueles devidamente autorizados;

- integridade: diz que a informação não é destruída ou corrompida e o sistema tem um desempenho correto;

- disponibilidade: diz que os recursos/serviços do sistema estão disponíveis sempre que forem necessários;

As senhas servem para autenticar o usuário, é utilizada no processo de verificação da identidade do usuário, assegurando que este é quem diz ser.

Criptografia: É a ciência e arte de escrever mensagens em forma cifrada ou em código. É parte de um campo de estudos que trata das comunicações secretas, usadas, para:

- Autenticar a identidade de usuários;

-Autenticar e proteger o sigilo de comunicações pessoais e de transações comerciais e bancários;

-Proteger a integridade de transferências eletrônicas de fundos.

Certificado Digital: É um arquivo eletrônico que contém dados de uma pessoa ou instituição, utilizados para comprovar a sua identidade.

3.5 A Responsabilidade dos Provedores

A legislação brasileira sobre a responsabilidade dos provedores no enfrentamento de crimes cibernéticos é deficiente, uma vez que não há uma definição clara dos deveres das empresas que mantém serviços de acesso e hospedagem de páginas.

Em países como a Holanda, Suécia, Austrália ou Canadá, os governos estão exigindo que os provedores informem à polícia tão logo tomem conhecimento de crimes cometidos no uso dos serviços da *Internet* e preservem as evidencias, por um prazo determinado por lei.

A identificação de um criminoso cibernético depende, da identificação do endereço *IP* do computador por ele utilizado. Um provedor, normalmente, controla uma enorme quantidade de endereços de IPs, os quais são atribuídos ao assinantes, durante o período de conexão.

Os números de *IP* são normalmente dinâmicos, isto é, cada vez que um usuário faz a conexão à rede, seu computador é aleatoriamente vinculado a um endereço de *IP,* disponibilizado pelo provedor. O computador do usuário retém o endereço de *IP* durante a conexão, impedindo que o mesmo protocolo seja atribuído a outro assinante, no mesmo período. Mas quando, o usuário encerra a conexão, o protocolo se torna, novamente disponível para ser atribuído a outro assinante no mesmo período.

Ao se receber a notícia de um crime cibernético a primeira coisa a fazer é providenciar a identificação do meio usado. Foi cometido em um *website*? Por um *e-mail*? Programa de troca de arquivos eletrônicos? Arquivos ou mensagem ofensivas trocadas em programas de mensagem instantânea (tipo MSN ou

ICQ)? Em salas de bate-papo? Em grupos de discussão? Em comunidades virtuais como o *Orkut*? Uma das mais importantes evidências a se coletar é o número de *IP*. O *IP* deve estar acompanhado da data, hora exata da conexão ou comunicação e o fuso horário do sistema.

Sendo assim, os provedores de acesso e também os de hospedagem deve manter um banco de dados eletrônico, contendo uma lista de cada endereço de *IP* utilizado, juntamente com a correspondente data, hora e região de conexão.

É imprescindível que os provedores assumam a responsabilidade de informar corretamente os consumidores de seus serviços acerca dos mecanismos de proteção contra ações danosas, mantenham dados cadastrais informados por seus assinantes de acesso e proporcionem a educação necessária ao uso responsável da *internet*.

Autoridades reguladoras de alguns estados vêm celebrando “Termos de Compromisso” com os provedores, os quais se obrigam a preservar os dados dos usuários pelo prazo mínimo de seus meses e a informar ao tomar conhecimento de algum crime em suas páginas.

3.6 Programas de Trocas de Mensagens

Os maiores riscos relacionados ao uso de programas como o ICQ ou MSN *Messanger,* AOL *Instant Messenger, Yahoo Messenger,* etc., estão no

conteúdo dos próprios diálogos travados. Alguém pode se utilizar de técnicas persuasivas para obter informações sensíveis dos usuários.

3.7 Sites de Relacionamento

Em sites de relacionamento como o *ORKUT,* deve-se estar atento e avaliar com cuidado as informações que se colocará disponível, principalmente aquelas que poderão ser vistas por todos, nas comunidades em que se participa, pois que as informações podem ser mal utilizadas.

3.8 Validade dos Atos Jurídicos realizados pela *Internet.*

Se no início a Internet surgiu como um meio de comunicação, hoje ela se apresenta também como um meio de comércio, surgindo as empresas distas “ponto.com”.

Para que um ato jurídico seja válido são necessários: agente capaz; objeto lícito, possível, determinado ou determinável; forma prescrita e não defesa em lei.

Os negócios jurídicos realizados pela Internet não são proibidos por lei, e, inexistindo forma prescrita em lei, serão eles considerados válidos, até prova

em contrário. Todos os meios de prova para validar os negócios jurídicos realizados pela Internet são válidos.

Atualmente, as transações comerciais pela *Internet* valem-se de meios idôneos para identificação de onde partiu o pedido de uma compra. Trata-se do *IP*, que identifica a máquina de onde partiu o pedido da transação. A cada pedido realizado por meio eletrônico, a máquina que o recebe identifica o *IP* de quem realizou a transação e, desta forma, tem-se por consumada a relação entre consumidor e fornecedor.

Para a verificação do ônus da prova, deve ser sempre em favor do consumidor. O fornecedor deverá então, principalmente quando a transação tiver ocorrido por meio de compra por cartão de crédito, manter os dados relativos à transação. A melhor prova, é ainda, a pericial, com o fim de identificar os registros de *IP* para a validação de possível discussão.

4 LEGISLAÇÃO EXISTENTE NO BRASIL HOJE

A legislação, no Brasil, acerca do tema é esparsa, constante de leis diversas, surgidas a partir do ano de 1990, ainda incipientes diante do desenvolvimento tecnológico, da universalização do uso do computador e da *Internet* e ao se levar em consideração a diversidade de crimes que vêm surgindo desde então. Para conhecimento do leitor, segue em anexo uma compilação da legislação pertinente, analisada abaixo.

Em 1973 surgia a Lei dos Direitos Autorais que veio regulamentar os aspectos relativos à autoria e à proteção dos direitos dos autores pertinentes à publicação, transmissão ou emissão, retransmissão, reprodução ou contrafação de suas obras.

Em 1987 foi publicada a lei 7.646, que dispunha sobre a proteção da propriedade intelectual sobre programas de computador e sua comercialização no país, logo revogada pela Lei 9.609,de 1998.

No ano 2000, a Lei 9983/00, que veio para alterar alguns dispositivos do Código Penal e incluir outros, regulou alguns novos tipos penais especificamente relacionados à sistemas de informática, localizados nos crimes contra a Administração Pública, o art. 313-A do Código Penal, sancionou a seguinte conduta:

“Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizado ou bancos de dados da Administração Pública, com o fim de obter vantagem indevida para si ou para outrem ou para causar dano”;

Já o art. 313-B, também incluído descreveu:

“Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente”, sendo a pena aumentada caso haja dano para a Administração Pública.

Ainda acrescido pela mesma lei, foi positivado, no Título Dos Crimes contra a Inviolabilidade de Segredos, no art. 153, § 1°-A :

“Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública”.

Foi ainda, incluído pela mesma lei, o Art. 325 ao Código Penal, que versa:

“Revelar fato de que tem ciência em razão do cargo e que deva permanecer em segredo, ou facilitar-lhe a revelação, ou ainda que permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública, bem como se utiliza, indevidamente, do acesso restrito".

Com a Lei 10.764/03, o Estatuto da Criança e do Adolescente também sofreu alteração em seu Art. 241, sobre a possibilidade do crime ocorrer de pornografia infantil ser praticado pela rede mundial de computadores. Previu a responsabilidade criminal de quem assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens produzidas e ainda a quem assegura, por qualquer meio, o acesso, na rede mundial de computadores ou

internet, das fotografias, cenas ou imagens produzidas com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente.

Além destes crimes, previstos em nossa legislação, o que ocorre, muitas vezes é a **subsunção** [grifo nosso] de condutas ilícitas, utilizando-se a legislação existente, como por exemplo o crime de dano previsto no art. 163 do Código Penal, ou o de Furto, previsto no art. 155, ou o crime de injúria, art. 140 ou ainda os crimes de racismo, previstos no art. 20 e § 2°, da Lei 7.716/89, etc., desconsiderando-se o meio por meio do qual a conduta foi praticada, considerando-se o resultado obtido.

5 PREVENÇÕES/RECOMENDAÇÕES

Uma das preocupações iniciais deste trabalho era evitar ou coibir os crimes cometidos por meio de sistemas de informática e pela internet. Evitar por completo é como querer acabar com completo com o cometimento de crimes na seio das sociedades, o que não deixará de ocorrer nem no futuro longínquo, tendo em vista a popularidade do uso dos computadores pelos quatros cantos do país e em todos os recantos do mundo.

Por este motivo, procurei buscar saídas, soluções para que cada usuário de computador, consciente, possa se utilizar a fim de se proteger de ataques danosos à sua vida, à sua família, à sua honra, a seus bens. Abaixo segue lista não conclusiva das ações que podem ser intentadas com este propósito:

- Manter o os programas de proteção periodicamente atualizados;

- Programar o antivírus para verificar os arquivos do *HD(disco rígido)*, os obtidos pela *Internet*, os flexíveis,e unidades removíveis como cd, *DVDs* e *pen-drives*;

- Desabilitar no leitor de *e-mail* a auto-execução de arquivos e nem no caso de arquivos comprimidos, o formato executável;

- As senhas de preferência devem conter no mínimo oito caracteres, contendo letras, números e símbolos;

- Alterar as senhas com freqüência, utilizando-se uma senha para cada serviço;

- Nunca abrir *e-mails* enviados por estranhos, principalmente aqueles anexados com programas ou arquivos com extensão: *.exe, .src, .bat, e pif;*

- Não clicar em *links* que apareçam no conteúdo de um *e-mail*;

- Desconfiar sempre de arquivos anexados à mensagens,mesmo que tenham sido enviados por pessoas ou instituições conhecidas;

- Instalação de *firewall* pessoal, e de filtros *anti-spam;*

- Desativar a execução de programas Java na configuração de seu browser, o que não costuma comprometer a exibição da página;

- Bloquear pop-ups windows;

- Ao realizar transações comerciais via *web*, certificar-se da procedência do *site,* e se estes *sites* são realmente das instituições que dizem ser;

- Somente acessar *sites* de instituições financeiras e de comércio eletrônico, digitando o endereço diretamente no *browser* e não clicando em um *link* existente em uma pagina ou em um *e-mail*;

- Fazer periodicamente cópias de segurança, ou *backups* de dados importantes;

- Utilizar pelo menos uma ferramenta anti-*spyware* e mantê-la sempre atualizada;

- Ao realizar transações comerciais ou bancárias, certificar-se que o site faz uso de conexões seguras;

- Não acessar sites de comércio eletrônico ou *Internet Banking* através de computadores de terceiros;

- Utilizar criptografia sempre que precisar enviar um e-mail com informações sensíveis (que contenham senhas, números de cartão de crédito);

- Evitar disponibilizar dados pessoais ou de sua família ou fornecer dados sobre seu cotidiano em blogs e sites de redes de relacionamentos.

6. ATUALIDADES

A justiça brasileira condenou pela primeira vez uma pessoa por crimes na *Internet.* O hacker Guilherme Amorim de Oliveira Alves, de 19 anos, foi sentenciado a passar seis anos e quatro meses na prisão por invadir entre outros sites, as páginas dos quatro maiores bancos do país (Caixa, Banco do Brasil, Itaú e Bradesco).

A sentença saiu no dia 31 de dezembro passado, quando Alves completava quase um ano detido na Penitenciária de Segurança Máxima de Campo Grande, onde continua preso. Alves agiu em São Paulo, no Rio, em Niterói e no Mato Grosso do Sul.

Segundo as acusações contra o jovem, só o Banco do Brasil apurou em um período inferior a um mês, cento e oito transações fraudulentas em contas correntes.

A sentença foi dada pela juíza Janete Lima Miguel. Outro acusado, o policia militar Evanancy Soares de Alcântara, foi sentenciado a quatro anos,oito meses e vinte dias. Ele teria recebido créditos de Alves pra recarregar seu celular.

Alves era o cérebro da quadrilha. Começou em Corumbá, copiando espelhos de site de grandes bancos. As retiradas não foram muito significativas. Os saques começaram a ser notados em 2002. O objetivo era retirar de uma só vez, de vários bancos, um total de R$150.000,00(cento e cinqüenta milhões.

7. DIREITO INFORMÁTICO

Em alguns países já se reconheceu a necessidade da criação de um ramo específico do direito para lidar com o assunto da informática na ciência jurídica, tratando-se do Direito Informático. Parte da doutrina alega tratar-se de um ramo do direito público, outra parte da doutrina defendo-o como pertencente ao ramo do direito privado, ou mesmo do direito administrativo. Há ainda quem defenda a necessidade deste direito dever ser concebido como um direito internacional, capaz de poder ver aplicadas suas normas a todos os países do mundo.

O objeto imediato do direito informático seria a informação jurídica eletronicamente processada e os seus objetos mediatos, a informática e a telemática, integrando ainda o seu âmbito as decisões judiciais sobre matérias informáticas. O objeto do direito informático seria os aspectos jurídicos de memorização e tratamento de informações e o da telemática o transporte de informações. A informação, por sua vez, é um bem imaterial.

O direito informático seria um direito interdisciplinar, mas autônomo.

Almeida Filho em seu livro Direito da Informática (2005, p. 85) define Direito Eletrônico como:

> O conjunto de normas e conceitos doutrinários, destinados ao estudo e normatização de toda e qualquer relação onde a informática seja o fator primário, gerando direitos e deveres secundários. É ainda, o estudo abrangente, com o auxílio de todas as normas codificadas de direito, a regular as relações dos mais diversos meios de comunicação, dentre eles os próprios da informática.

Hoje, no Brasil,o estudo do Direito da Informática vem sendo valorizado, e ainda há muito o que ser debatido e discutido.

09. PRINCIPIOS NORTEADORES DA PROPOSTA

Na elaboração da proposta de projeto de alteração ao Código Penal, de inclusão dos crimes de informática, tentarei observar os princípios da proporcionalidade da pena, da culpabilidade, da lesividade, bem como da teoria da tipicidade.

O princípio da proporcionalidade determina que a pena não pode ser superior ao grau de responsabilidade pela prática do fato, significando que a pena deve ser medida pela culpabilidade do autor, tendo em vista que a culpabilidade é a medida da pena. “Exige-se uma proporção entre o desvalor da ação praticada pelo agente e a sanção a ser a ele infligida, e,num aspecto prevencionista, um equilíbrio entre a prevenção geral e a prevenção especial para o comportamento do agente” (Mirabete, 2001, p. 57).

Significa dizer que o legislador deverá analisando minuciosamente o fato para melhor enquadrá-lo à tipificação da norma, sopesando o crime praticado, para não haver excesso.

Com o advento da teoria da tipicidade, o princípio da reserva legal ganhou muito de técnica. Típico é o fato que se amolda à conduta criminosa descrita pelo legislador. É necessário que o tipo (conjunto de elementos descritivo do crime contido na lei penal) tenha sido definido antes da prática delituosa, como o requer o princípio da anterioridade da lei.

Ao levar em consideração o princípio da culpabilidade, vale a pena observar que a pena só pode ser imposta a quem, agindo com dolo ou culpa, e

merecendo juízo de reprovação, cometeu um fato típico e antijurídico. É um fenômeno individual, pois o juízo de reprovabilidade ou culpabilidade, do juiz, recairá sobre o sujeito imputável, que podendo agir de maneira diversa, tinha condições de alcançar o conhecimento da ilicitude do fato. A culpabilidade é também um fenômeno social, pois a correlação de forças sociais de um determinado momento histórico é que determina quem deve ser considerado culpado ou inocente. Este princípio, que serve de fundamento e medida da pena, não se coaduna com a responsabilidade penal objetiva, i.e., aplicação de pena sem dolo, culpa e culpabilidade.

Pelo princípio da lesividade, o direito penal só deve ser aplicado quando a conduta lesiona um bem jurídico tutelado, não sendo suficiente que seja imoral ou pecaminosa. Este princípio pode ser extraído do art. 98, I da Constituição Federal, ao disciplinar as infrações penais de menor potencial ofensivo.

Nos crimes cometidos por meio da Internet, a lesividade sofreu grande alteração. O que anteriormente era cometido pelo criminoso contra um indivíduo de cada vez pela proximidade física entre ambos, por meio da Internet é possível se lesar indeterminada quantidade de pessoas quase que simultaneamente, estando infrator e vítima a centenas de quilômetros distantes.

8. PROPOSTA DE PROJETO DE LEI

Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal e dá outras providências.

O CONGRESSO NACIONAL decreta:

Art. 1º São acrescidos à Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, com os seguintes dispositivos:

Art. 2º Esta Lei dispõe sobre os crimes de informática, e dá outras providências.

Art. 3º Os dados de informática ou a informação ou a base de dados contida nos sistemas de informática reputam-se, para os efeitos legais, bens imateriais.

Art.4°Equipara-se à coisa:

I - o dado, a informação ou a base de dados presente em meio eletrônico ou sistema informatizado;

II - a senha ou qualquer meio de identificação que permita o acesso a meio eletrônico ou sistema informatizado.

"Disposições comuns"

"Art. 141 .....

V- Se o crime é cometido por meio da *Internet.*

"Ameaça pela *Internet*" (AC)

Art. 147-A – Ameaçar alguém, grupo de pessoas ou comunidades por meio da *Internet.* (AC)

Pena – detenção, de 1 (um) a 6(seis) meses,ou multa. (AC)

"Inviolabilidade dos sistemas informatizados (AC)

"Art. 151-A Acessar, indevidamente ou sem autorização, meio eletrônico ou sistema informatizado:

"Pena - detenção, de três meses a um ano, e multa. " (AC)

"Art. 151-B Acessar, indevidamente ou sem autorização, meio eletrônico ou sistema informatizado obtendo informações, dados, arquivos, pastas, processamentos ou outros, a fim de obter vantagem ilícita para si ou para outrem em prejuízo alheio.

"Art. 151-C Acessar, indevidamente ou sem autorização, meio eletrônico ou sistema informatizado alterando informações, dados, arquivos, pastas, processamentos ou outros, para obter vantagem para si ou para outrem."(AC)

"§ 1º Nas mesmas penas incorre quem fornece ou facilita a terceiro meio indevido ou não autorizado de acesso a meio eletrônico ou sistema informatizado." (AC)

"§ 2º Somente se procede mediante representação, salvo se o crime é cometido contra a União, Estado, Município, empresa concessionária de serviços públicos ou sociedade de economia mista." (AC)

"Art. 153-A Divulgar alguém, pela internet, conteúdo de documento particular ou confidencial de pessoa física ou jurídica, obtido por acesso indevido ou sem autorização, cuja divulgação possa produzir dano a outrem."(AC)

"Pena - detenção, de um a dois anos, e multa. " (AC)

"§ 1º Somente se procede mediante representação."(AC)

"§ 2° Se da divulgação acarretar dano a outrem, a pena será acrescida de um a dois terços, sem prejuízo da reparação dos danos.(AC)

"Art. 155 - .....

§ 4°

V- Se o furto é cometido por meio da internet, ou por acesso a banco eletrônico. (AC)

VI – Se o furto é cometido por meio da internet ou por acesso a banco eletrônico e subtração atingir diversas pessoas. (AC)

"Dano Informático" (AC)

Art. 163-A – Danificar, alterar, suprimir ou destruir informação, dados informáticos, software, processador, sistema informatizado, ou similar." (AC)

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

§ 1° Se o objetivo do dano for obter vantagem para si ou para terceiros.(AC)

Pena – A pena será acrescida de um a dois terços, e multa. (AC)

"Art. 171 - .....

§ 2°.....

VII – Se a obtenção para si ou para outrem de vantagem ilícita em prejuízo alheio, mediante artifício, ardil ou qualquer outro meio fraudulento se der por meio da *Internet.*(AC)

"Difusão de vírus eletrônico. (AC)

"Art.267- Difundir programas maliciosos ou destrutivos, em sistemas de informática ou por meio da internet, com a finalidade de destruir, inutilizar, danificar, modificar, dificultar funcionamento adquirir ou furtar dados não autorizados. (AC)

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

"Difusão qualificada (AC)

§ 1° A pena aumenta-se de um terço, se o crime é praticado com a finalidade: (AC)

I - de obter para si ou para outrem, vantagem indevida; (AC)

II - por vingança; (AC)

III - por espionagem industrial; (AC)

IV – por motivo fútil. (AC).

"Art. 286.....

"§ 1° A pena aumenta-se de um terço a metade, se a incitação ao crime for praticada por meio da internet. (AC)

"Art. 286-A Ofensas contra interesses estaduais e políticos. "(AC)

Pena – detenção de 3(três) a 6(seis) meses ou multa. (AC)

"Art. 287- .....

§ 1° A pena aumenta-se de um terço ate a metade, se a apologia ao crime for praticada por meio da internet. (AC)

""Art. 298.....

Falsificação de cartão de crédito(AC)

"Parágrafo único. Equipara-se a documento particular o cartão de crédito ou débito."(AC)

"Pena - Reclusão de 1 a 5 anos, e multa. (AC)

"Falsificação de telefone celular ou meio de acesso a sistema eletrônico. (AC)

"Art. 298 A. Criar ou copiar, indevidamente ou sem autorização, ou falsificar código, seqüência alfanumérica, cartão inteligente, transmissor ou receptor de radio freqüência ou de telefonia celular ou qualquer instrumento que permita o acesso a meio eletrônico ou sistema informatizado. (AC)

"Pena - reclusão, de um a cinco anos, e multa."

9. CONCLUSÃO:

Segundo Muraro, citado por Blum (2001, p.215), “...a revolução tecnológica, sempre mais acentuadamente, ganha um dinamismo próprio, desprovido de diretrizes morais, conduzido por um “cientificismo” ao qual são estranhas e mesmo desprezíveis quaisquer preocupações éticas, metafísicas, humanísticas. Torna-se cega e desordenada, subtraindo-se ao controle até mesmo dos sábios, que a desencadeiam.“

O Direito não é estático. É ele um fenômeno tão mutante e dinâmico quanto as próprias relações humanas. É o direito é parte integrante das ciências sociais aplicadas, e como tal, não pode ficar alheio às inovações na sociedade, em especial as trazidas pela informática e pela *Internet*.

A *Internet* é um desafio para o Direito. O controle da *Internet* é difuso e cooperativo, para não dizer anárquico. Mas, mesmo tendo a *Internet* nascido e crescido livre não significa que ela deva viver sem regramentos, a própria sociedade está começando a entender que ela deve ser regulada.

A tendência do crime é acompanhar as oportunidades. Se as oportunidades existirem em sistemas de computador, os criminosos as encontrarão. A gama de delitos que podem ser perpetrados pela *Internet* é quase infinita.

É preciso preservar a liberdade, mas também é preciso inibir os abusos.

Neste trabalho, busquei mostrar os meios de se evitar ataques de ciber criminosos bem como fazer uma proposta de projeto de lei que alterasse o Código Penal Brasileiro, inserindo novos artigos que incluíssem a tipificação

dos crimes de informática surgidos até os dias de hoje. Mas percebo agora que isto é pouco.

Com o surgimento de um novo ramo do direito, ainda em gestação, o Direito Informático, entendo agora, ao concluir este trabalho, que faz-se necessária uma lei própria, para os crimes de informática em nosso ordenamento, tendo em vista sua especificidade e caráter técnico, e para evitar que o Código Penal transforme-se numa colcha de retalhos.

Considerando-se que hoje uma gama enorme das atividades humanas estão sendo executadas pela *Internet,* desde estudos, pesquisas, consultas, passando por atos de comércio, como compras, vendas, transações, negociações comerciais, contratos internacionais, transferências de valores, aplicações de valores, chegando-se a conversas, bate-papos, e a até, quem diria, namoros etc, uma lei específica que trate do assunto, é que conseguiria ter tal amplitude.

Em vista da abrangência cada vez maior de eventos possíveis no que concerne à informática e a *Internet*, faz-se necessário um estudo aprofundado e minucioso de todo o universo das ocorrências, com a criação de uma lei específica para estes crimes, para que estes delitos possam um a um ser positivados, a fim de que quando alguém sair lesado em transações cibernéticas, possa recorrer, e chegando-se ao infrator, este possa ser devidamente penalizado na extensão de seu delito e na medida de sua culpabilidade.

REFERÊNCIAS BIBLIOGRÁFICAS

ALMEIDA FILHO, José Carlos de Araújo; CASTRO, Aldemario Araújo. **Manual de Informática Jurídica e Direito da Informática**. 1. ed. Rio de Janeiro : Forense, 2005.

BERNSTEIN,Terry. et al. **Segurança na Internet**. Rio de Janeiro : Campus, 1997 (tradução de Insight Serviços de Informática).

BLUM, Renato M. S. Opice (coord.) et al. **Direito Eletrônico** : a internet e os tribunais. Bauru, SP : Edipro, 2001.

BRASIL. Procuradoria da República no Estado de São Paulo. Comitê Gestor da Internet. **Manual Prático de Investigação** : crimes cibernéticos. São Paulo, 2006.

COSTA, Marco Aurélio de Oliveira. **O Direito e a Internet.** Disponível na Internet via www.url:http://www.jus.com.br/doutrina/crinfo2.html. Acessado em 06.04.07

DA REDAÇÃO. Advogados alertam para punições de crimes cometidos pela internet. **Correio Braziliense.** Disponível no site: www.denunciar.org.br/twiki/bin/view/SaferNet/Noticia2006810213524 . Acessado em 12 mar. 2007.

FINKELSTEIN, Maria Eugênia Reis. **Aspectos Jurídicos do Comércio Eletrônico**. Porto Alegre : Síntese, 2004.

GOUVEA, Sandra. **O Direito na Era Digital**: crimes praticados por meio da informática. Rio de Janeiro : Mauad, 1997.

Internet. Disponível: http://pt.wikipedia.org/wiki/Imagem:Internet-users-public-access-xi-unctad.jpg. [Acessado em 15 mar. 2007].

ORRICO JUNIOR, Hugo. **Pirataria de Software**. São Paulo : Ed.do Autor, 2001.

PAESANI, Liliana Mainardi. **Direito e Internet**. 3.ed. São Paulo : Atlas, 2006.

PAESANI, Liliana Mainardi. **Direito de Informática** : comercialização e desenvolvimento internacional do software. 2 ed. São Paulo : Atlas, 1999

PENTEADO, J. de Camargo. **Justiça Penal 7**: Justiça Criminal Moderna. [s.l.] : Revista dos Tribunais, [19--].

PIMENTEL, Alexandre Freire. **O Direito Cibernético:** um Enfoque Teórico e Logico-Aplicativo. Rio de Janeiro : Renovar, 2000.

REINALDO FILHO, Demócrito Ramos. **Questões técnicas dificultam condenações por crimes cometidos pela internet**. Revista Juristas

REIS, Maria Helena Junqueira. **Computer Crimes** : a criminalidade na era dos computadores. Belo Horizonte : Del Rey, 1996.

ROSA, Fabrízio. **Crimes de Informática**. 2. ed. Campinas : Bookseller, 2005.

SÃO PAULO, O Estado de. **Em MS estudante de 19 anos é primeiro hacker a ser condenado à prisão no Brasil**. Disponível: www2.uol.com.br/aprendiz/guiadeempregos/nova/noticias/geo60104.htm#1. Acessado em 12 mar. 2007.

Segurança e vírus. Câmara dos Deputados debaterá crimes cometidos na internet. Disponível: wnews.uol.com.br/site/noticias/materia.php?id_secao=4tid_conteudo=6483. Acessado em 14 mar. 2007.

VASCONCELOS, Márcio José Accioli de. **Pânico na Internet**. São Paulo : Chantal, 1999

www.stj.gov.br/SCON/jurisprudencia/toc.jsp?tipo_visualizacao=RESUMO&livre=crimes+pela+internet&b=ACOR. Acessado em 22 abr. 2007.

www.planalto.gov.br/ccivil_03/Leis/L5988.htm. [Acessado em17 mai. 2007]

GLOSSÁRIO

Botnets: rede de computadores infectadas;

Browser: páginas de busca;

Cookies: são muito utilizados para rastrear e manter as preferências de um usuário ao navegar pela internet;

Cracker: é o hacker malicioso, possui grande conhecimento técnico e o utiliza para praticar crimes.

Firewall: dispositivos constituídos pela combinação de software e hardware utilizados para dividir e controlar o acesso entre redes de computadores, dificultam a invasão de crackers. O firewall pessoal, é um software utilizado para proteger um computador contra acessos não autorizados vindos da internet;

Hacker: pessoa com grande capacidade técnica sobre os sistemas de informática, não comete crimes, é um pesquisador.

IDS(Intrusion Detection System): são sistemas de detecção de intrusão;

Logs: 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 e que possuem as informações de data, horário, endereço de IP e portas envolvidas;

Pheaker: é o hacker ou cracker da telefonia. Especializado em fraudes nos sistemas telefônicos;

Phishing ou phishing scam: fraude que se dá através do envio de mensagem não solicitada, que se passa por comunicação de uma instituição conhecida, e que procura induzir o acesso à páginas falsificadas, projetadas para furtar dados pessoais e financeiros dos usuários;

Pop-ups windows: pequenas janelas que aparecem automaticamente e sem permissão, sobrepondo a janela de browsers, após um usuário acessar um site. Tem sido amplamente utilizados para apresentar mensagens com propaganda, e, por isso, têm sido classificados como pop-ups spam;

Scam: ou golpe, é qualquer esquema ou ação enganosa e/ou fraudulenta para obter vantagens financeiras;

Spam: envio indiscriminado de e-mails não solicitados, que geralmente são enviados para um grande número de pessoas, qualquer que seja a finalidade, como a divulgação de cursos, produtos ou serviços. Normalmente utilizam-se bancos de dados específicos, como advogados,engenheiros, etc.; bancos de dados, na maioria das vezes, obtidos ilegalmente e depois comercializados;

Spywares: programas espiões;

Vírus: programas maliciosos criados para danificar arquivos armazenados no disco rígido, principalmente os essenciais para o funcionamento do sistema, tornando o sistema inoperante ou impedindo totalmente seu funcionamento.

WWW: *World Wide Web* ou rede mundial.