FUNDAÇÃO DE ENSINO “EURÍPIDES SOARES DA ROCHA”
CENTRO UNIVERSITÁRIO EURÍPIDES DE MARÍLIA- UNIVEM
CURSO DE DIREITO

ALEXANDRE MORENO DE ANDRADE

ASPECTOS PENAIS E PROCESSUAIS PENAIS DAS CONDUTAS CRIMINOSAS NA INTERNET

MARÍLIA
2010

ALEXANDRE MORENO DE ANDRADE

ASPECTOS PENAIS E PROCESSUAIS PENAIS DAS CONDUTAS CRIMINOSAS NA INTERNET

Trabalho de Curso apresentado ao Curso de Direito da Fundação de Ensino "Eurípides Soares da Rocha", mantenedora do Centro Universitário Eurípides de Marília – UNIVEM, como requisito parcial para obtenção do grau de bacharel em Direito.

Orientador:
Profº. JAIRO JOSÉ GÊNOVA

MARÍLIA
2010

Andrade, Alexandre Moreno
Aspectos penais e processuais penais das condutas criminosas na internet / Alexandre Moreno de Andrade;
Orientador: Jairo José Gênova. Marilia, SP: [s.n.], 2010.
67 f.

Trabalho de Curso (Graduação em Direito) – Curso de Direito, Fundação de Ensino "Eurípides Soares da Rocha", mantenedora do Centro Universitário Eurípides de Marília – UNIVEM, Marília, 2010.

1. Crimes 2. Internet 3. Direito

CDD: 340.0285

FUNDAÇÃO DE ENSINO "EURÍPIDES SOARES DA ROCHA"
MANTENEDORA DO CENTRO UNIVERSITÁRIO EURÍPIDES DE MARÍLIA – UNIVEM
Curso de Direito

Alexandre Moreno de Andrade
RA: 37824-0

ASPECTOS PENAIS E PROCESSUAIS PENAIS DAS CONDUTAS CRIMINOSAS NA INTERNET

Banca examinadora do Trabalho de Conclusão de Curso apresentada ao Programa de Graduação em Direito da UNIVEM, F.E.E.S.R, para obtenção do Título de Bacharel em Direito.

Nota: 10,0 (dez)

ORIENTADOR(A): _____
Jairo José Gênova

1° EXAMINADOR(A): _____
José Henrique Ursulino

2° EXAMINADOR(A): Fabiana C. Ferrari
Fabiana Christina Ferrari

Marília, 01 de dezembro de 2010.

À Deus, por iluminar meu caminho, presente em todos os dias;

Aos verdadeiros amigos pelo incentivo;

À minha esposa Aline, pelo amor, apoio e carinho.

AGRADECIMENTOS

Agradeço todo o apoio e apreço recebido dos colegas e professores da UNIVEM.

Em particular, agradeço ao profº Jairo José Gênova pela dedicação e auxílio prestados durante a orientação, contribuindo de forma importante para a realização do presente trabalho.

Duas coisas são infinitas: o universo e a estupidez humana. Mas, no que respeita ao universo, ainda não adquiri a certeza absoluta.

Albert Einstein

O desenvolvimento técnico só vai deixar um único problema por resolver: a debilidade da natureza humana.

Karl Kraus

ANDRADE, Alexandre Moreno. **ASPECTOS PENAIS E PROCESSUAIS PENAIS DAS CONDUTAS CRIMINOSAS NA INTERNET.** 2010. 61 f. Trabalho de Curso (Bacharelado em Direito) – Centro Universitário Eurípides de Marília, Fundação de Ensino "Eurípides Soares da Rocha", Marília, 2010.

RESUMO

A presente monografia tem como objeto de estudo os problemas gerados na esfera jurídica pelas condutas criminosas praticadas na internet ou por meio desta. Demonstramos que com o surgimento e desenvolvimento da Tecnologia da Informação – TI, em particular a evolução em escala geométrica da Internet, a sociedade se viu repentinamente inserida em um mundo virtual sem fronteiras, onde o acesso à informação tornou-se instantâneo, levando-nos a um progresso sem precedentes em todas as áreas, sejam elas comerciais, científicas ou nas relações humanas. Porém como todo progresso da história humana, há quem vislumbre meios de se obter vantagens indevidas com essa evolução das TI's, utilizando-se para tanto de meios ilícitos, pois existe, devido à sensação de anonimato proporcionada pela Internet, a falsa impressão de que a rede mundial de computadores está imune às normas jurídicas e morais de nossa sociedade. Sendo assim, demonstrou-se que o grande desafio de nossos legisladores e dos operadores do direito é a difícil tarefa de acompanhar a evolução tecnológica e disponibilizar meios para que a lei pátria seja aplicada de forma eficiente no combate e punição dos crimes informáticos.

Palavras-chave: Tecnologia. Informação. Internet. Evolução. Lei.

SUMÁRIO

INTRODUÇÃO

Hoje, seja em sua vida privada ou na de governos e grandes corporações, todos vivem e usufruem das facilidades e da eficiência proporcionadas pela Tecnologia da Informação – TI, um complexo sistema formado por várias tecnologias as quais passam pelos sistemas de comunicações, transmissão de dados, softwares que facilitam o trabalho, a vida e o lazer dos indivíduos como um todo.

Mas talvez a ferramenta mais incrível criada pelo homem desde a antiguidade seja a INTERNET, ou como muitos a tem chamado recentemente, “a nuvem”, local onde pessoas em empresas podem, de forma virtual, se relacionar com outras pessoas ou até mesmo vender suas idéias e produtos.

Porém, como toda ferramenta criada pelo homem, a INTERNET vem de forma progressiva sendo utilizada para fins escusos, onde indivíduos buscam informações e suporte a fim de cometer atos ilícitos, os quais nos levam a identificação de vários tipos de crimes e nos evidencia a fragilidade de nosso sistema jurídico diante de um mecanismo que não conhece fronteiras e, tão pouco, a precariedade de nossas leis.

Assim, o objetivo do presente trabalho é abordar de forma geral os principais problemas enfrentados pelos operadores do Direito em face aos ilícitos praticados na Internet e por meio desta, utilizando-se, segundo as bases lógicas da investigação, o método hipotético-dedutivo proposto por Popper, que consiste no seguinte raciocínio: apresentação do problema, formulação de hipótese e teste da hipótese, onde verificar-se-á se nossas leis possuem mecanismos eficientes para coibir e punir crimes virtuais, em particular a pedofilia. Quanto à abordagem do problema a pesquisa é qualitativa, entendida como descrição e análise do objeto de estudo. Já quanto aos procedimentos técnicos é classificada como bibliográfica e documental (análise da jurisprudência, das Diretrizes do Comitê Gestor da Internet no Brasil, de projetos de leis em nossas casas legislativas, etc.).

Dentro do problema, deverão ser abordadas questões cruciais para o esclarecimento das mazelas jurídicas geradas pelo avanço tecnológico, ou seja:

- ✓ Nossas leis possuem mecanismos eficientes para coibir e punir crimes virtuais?
- ✓ Nossas leis evoluem na velocidade necessária para se combater a evolução dos crimes virtuais?
- ✓ É possível punir criminosos da internet com as leis que possuímos hoje?
- ✓ O mundo está preparado juridicamente para a evolução das TI’s?
- ✓ As ferramentas de investigação atuais são eficientes?

A fim de viabilizar as respostas a tais questionamentos o presente trabalho será dividido em três capítulos, sendo que o primeiro exporá em linguagem “simples” os conhecimentos técnicos necessários para a compreensão do funcionamento da Internet/informática, a fim de subsidiar o entendimento da relação Direito x Internet.

O Segundo capítulo irá abordar os principais aspectos penais que envolvem os crimes praticados por meio da Internet, as dificuldades em se aplicar a Lei pátria a alguns crimes específicos e se há necessidade ou não de Legislação específica para referidos crimes.

Por fim, o terceiro capítulo abordará os pontos mais importantes quanto aos aspectos processuais penais dos crimes informáticos, destacando-se o processo de investigação e obtenção da prova.

Abordaremos assim, a partir de agora, como acima exposto, em três capítulos, os principais problemas gerados na esfera jurídica penal e processual penal, em relação aos crimes informáticos, procurando expor seus aspectos mais importantes e relevantes.

CAPÍTULO I - O SURGIMENTO DA INTERNET

A INTERNET surgiu no ano de 1969, nos Estados Unidos da América, como alternativa ao sistema de comunicações existente até então, haja vista a necessidade de um sistema confiável no caso de uma guerra nuclear. Fica claro que esse sistema alternativo possuía, a princípio, finalidade militar, conforme esclarece Inellas (2009, pág. 02):

> *Outra denominação dada à pequena rede de computadores, que, como vimos, tinha ainda exclusiva finalidade militar, foi ARPAnet (Advanced Research Projects Agency Network), isto é, Agência Avançada de Desenvolvimento de Projetos para Trabalhos em Rede.*

A ARPAnet foi demonstrada publicamente, pela primeira vez, na Conferência Internacional de Comunicação entre Computadores no ano de 1972, surgindo em seguida a criação do correio eletrônico, bem como o protocolo TCP/IP, ainda utilizado.

Desta forma, em 1983, a rede foi dividida possibilitando o seu uso acadêmico, tendo como conseqüência o surgimento posterior de outras redes de computadores, porém todas dependiam da ARPAnet, o que veio a torná-la a rede das redes, passando assim a ser denominada de ARPA-INTERNET e, posteriormente, INTERNET.

Corrêa (2008, pág. 08) definiu a INTERNET da seguinte forma:

> *A Internet é um sistema global de computadores que possibilita a comunicação e a transferência de arquivos de uma máquina a qualquer outra máquina conectada na rede, possibilitando, assim, um intercâmbio de informações sem precedentes na história, de maneira rápida, eficiente e sem a limitação de fronteiras, culminando na criação de novos mecanismos de relacionamento.*

Com a evolução tecnológica, no ano de 1989 foi criada a World Wide Web (WWW), ou seja, a Rede Mundial de Computadores, a qual consagrou-se como um meio de comunicação e troca de dados rápido e eficiente, sendo utilizado por todos os segmentos sociais, de estudantes a cientistas.

Foi o surgimento da WWW que possibilitou a popularização da Internet, pois com sua combinação com os primeiros navegadores, denominados *browsers*, tornou-se possível aos usuários um acesso rápido e fácil à Internet, pois, de maneira interessante, passou a oferecer recursos que prendiam a atenção das pessoas, como imagens, vídeos e som.

Melhor define Corrêa (2008, pág. 11):

> *...a WWW é um conjunto de padrões e tecnologias que possibilitam a utilização da Internet por meio dos programas navegadores, que por*

> *sua vez tiram todas as vantagens desse conjunto de padrões e tecnologias pela utilização do hipertexto e suas relações com a multimídia, como som e imagem, proporcionando ao usuário maior facilidade na sua utilização, e também a obtenção de melhores resultados.*

1.1 A Internet no Brasil

A Fundação de Amparo à Pesquisa no Estado de São Paulo – FAPESP foi a responsável pela implantação do acesso a Internet no Brasil, quando no ano de 1988 passou a utilizar o sistema conhecido como Bitnet para "baixar" arquivos da Internet bem como utilizar-se do correio eletrônico.

Somente no ano de 1991, com a evolução da estrutura técnica, a FAPESP inicio o uso do protocolo IP, tornando-se assim a primeira instituição no país a realmente navegar na Internet, o que veio a torná-la, por conseqüência a administradora do domínio "br", bem como a responsável pela distribuição e alocação dos primeiros números Ip's do Brasil.

No ano seguinte deu-se um novo salto estrutural com a viabilização, por parte do Ministério da Ciência e Tecnologia, da implantação do primeiro backbone (tronco de rede) do país, o que viabilizou também a criação dos provedores de acesso privado, pois até então somente as instituições de ensino e pesquisa tinham acesso à rede.

Outro grande passo para a popularização da rede foi a invenção, em 1998, por um brasileiro, da internet via ondas de rádio, o que veio a facilitar em muito o acesso à rede por pessoas residentes em locais de difícil acesso, bem como a exigência de uma estrutura mais simples para sua implantação, uma vez não depender da rede de telefonia.

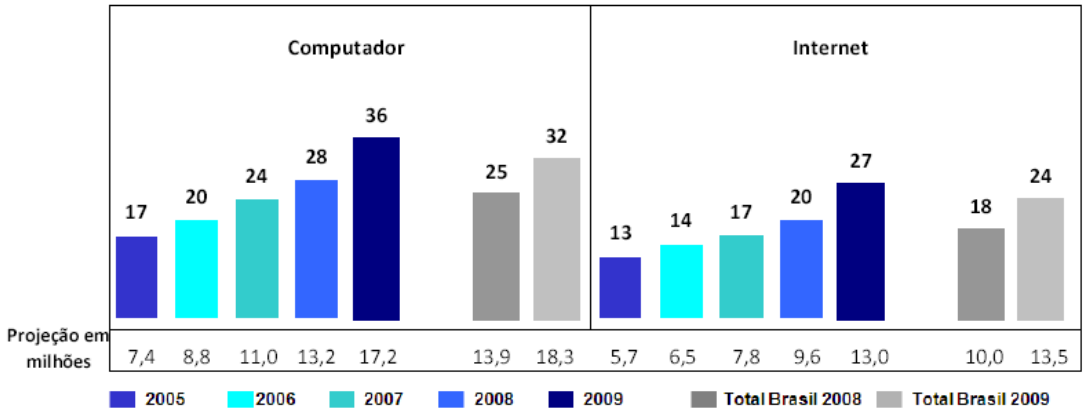
Observamos que a evolução do acesso à Internet no Brasil vem, desde sua implantação em 1988 crescendo de forma espantosa, como podemos ver na pesquisa realizada anualmente pelo Comitê Gestor da Internet no Brasil – CGI.br, por meio de seu Núcleo de Informação e Coordenação, onde os resultados demonstram o número de domicílios brasileiros detentores de algum tipo de Tecnologia da Informação – TIC's.

Vamos nos ater somente ao material de pesquisa referente a nosso tema de estudo, ou seja, a Internet, assim, temos como principal dado a expor o fato de, pela primeira vez, a utilização de banda larga para conexão à Internet tornar-se a mais utilizada no país, onde conforme a pesquisa, 66% dos domicílios com acesso a rede no Brasil utilizam-se do sistema de banda larga.

No gráfico a seguir podemos identificar de forma mais clara o desenvolvimento do

acesso ao computador e à Internet desde o ano de 2005, início da pesquisa, até o ano de 2009.

GRÁFICO 01 – Computador e Internet – Posse (%)



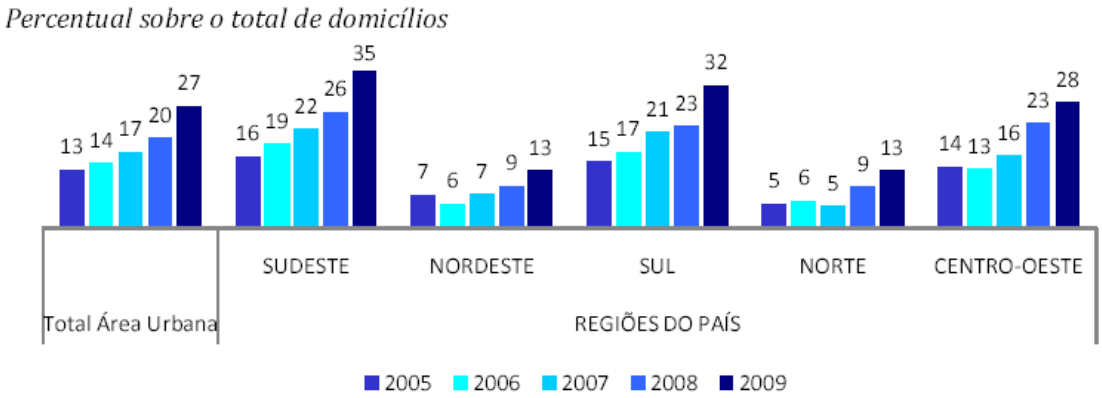
Base: TIC 2005: 8.540 entrevistados em área urbana. Projeção 44 milhões de domicílios em áreas urbanas.
TIC 2006: 10.510 entrevistados em área urbana. Projeção 45 milhões de domicílios em áreas urbanas.
TIC 2007: 17.000 entrevistados em área urbana. Projeção 46 milhões de domicílios em áreas urbanas.
TIC 2008: 16.940 entrevistados em área urbana / 3.080 entrevistados em área rural. Projeção 48 milhões de domicílios em áreas urbanas.
TIC 2009: 16.854 entrevistados em área urbana / 3.144 entrevistas em área rural. Projeção 49 milhões de domicílios em áreas urbanas.

Fonte: CGI.br

Analisando o gráfico observamos que tanto os domicílios que possuem um computador, quanto os que possuem acesso à Internet, mais que dobraram de percentual do ano de 2005 a 2009, sendo que o número de domicílios com acesso a Internet não vem acompanhando o crescimento do número de domicílios que possuem computador, depreendemos deste fato que o acesso aos provedores ainda é muito caro no país.

No gráfico abaixo veremos que a renda familiar influi diretamente no fato das famílias possuírem ou não acesso a Internet, pois fica demonstrado claramente que nas regiões do país com maior poder aquisitivo o percentual de domicílios com acesso é consideravelmente maior.

GRÁFICO 02 – Proporção dos domicílios com acesso à Internet (%)

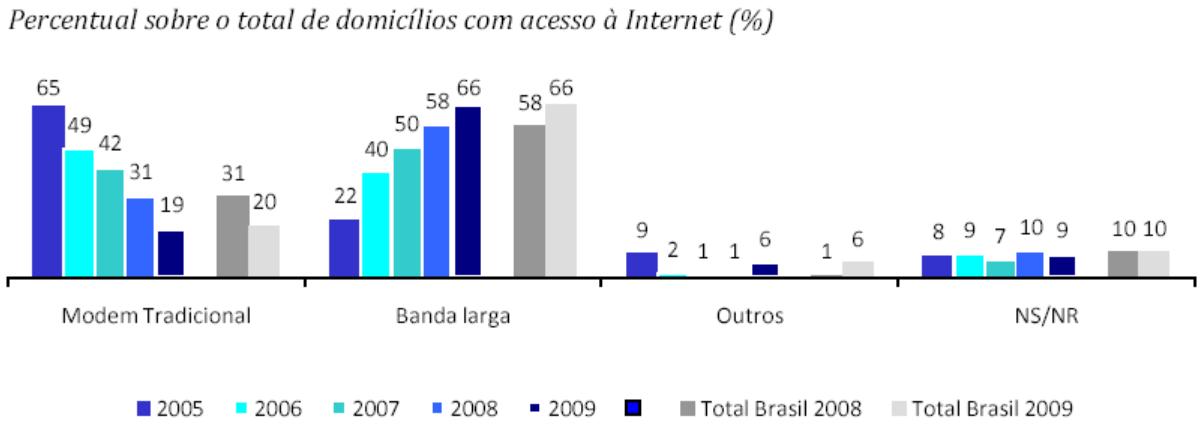


Base:
TIC 2005: 8.540 entrevistados em área urbana.
TIC 2006: 10.510 entrevistados em área urbana.
TIC 2007: 17.000 entrevistados em área urbana.
TIC 2008: 16.940 entrevistados em área urbana.
TIC 2009: 16.854 entrevistados em área urbana.

Fonte: CGI.br

No gráfico 03 vemos, como já citado, que apesar de ter ainda um alto custo no Brasil, e de eficiência questionada, a internet banda larga vem dominando a passos largos o número de domicílios com acesso á grande rede.

GRÁFICO 03 – Tipo de conexão para acesso à internet no domicílio (%)



Base:
TIC 2005: 1.830 entrevistados em área urbana.
TIC 2006: 1.523 entrevistados em área urbana.
TIC 2007: 2.875 entrevistados em área urbana.
TIC 2008: 3.389entrevistados em área urbana. 136 entrevistados em área rural.
TIC 2009: 4.572 entrevistados em área urbana. 198 entrevistados em área rural.

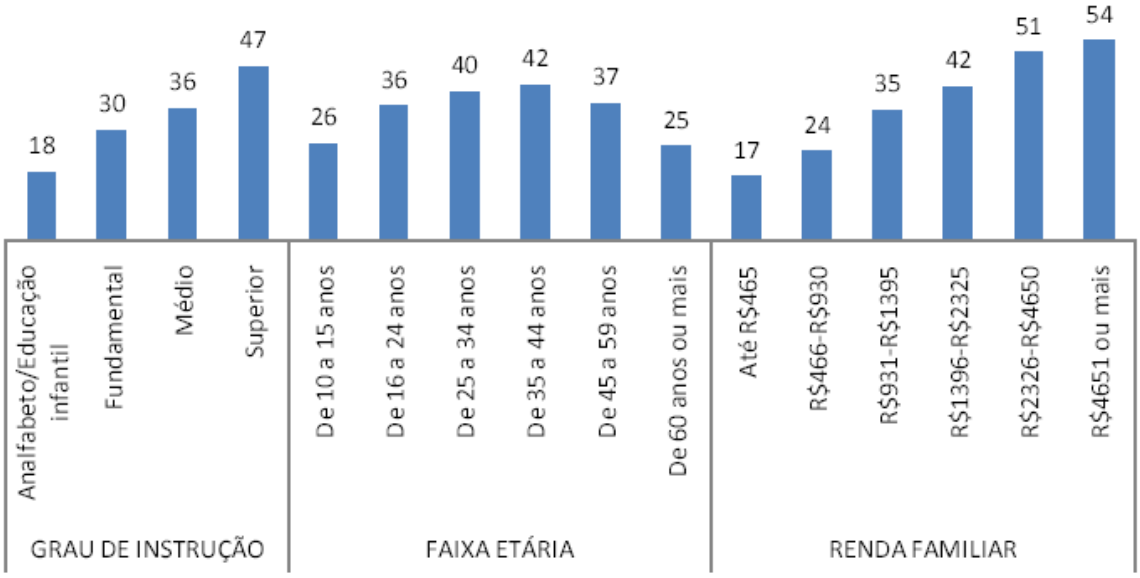
Fonte: CGI.br

Por fim, demonstra a pesquisa CGI.br que os problemas com segurança na Internet são freqüentes, mas sua identificação por parte dos usuários tem grande variação conforme grau de escolaridade, idade e renda familiar, o que torna essas pessoas vítimas potenciais das

mais variadas formas de ilícitos praticados por criminosos na Internet.

GRÁFICO 04 – Perfil dos Indivíduos que tiveram problemas de Segurança (%)

Percentual sobre o total de usuários de Internet



Base: 9.747 entrevistados que usaram a Internet nos últimos três meses (amostra principal + oversample *de usuários de Internet)*

Fonte: CGI.br

1.2 Comitê Gestor da Internet no Brasil – CGI.br

O CGI.br foi criado em 1995, pela Portaria Interministerial nº 147, de 31 de maio de 1995 e alterada pelo Decreto Presidencial nº 4.829, de 3 de setembro de 2003, para coordenar e integrar todas as iniciativas de serviços de Internet no país, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados. Conforme exposto no próprio site o CGI.br é,

> *Composto por membros do governo, do setor empresarial, do terceiro setor e da comunidade acadêmica, o CGI.br representa um modelo de governança na Internet pioneiro no que diz respeito à efetivação da participação da sociedade nas decisões envolvendo a implantação, administração e uso da rede. Com base nos princípios de multilateralidade, transparência e democracia, desde julho de 2004 o CGI.br elege democraticamente seus representantes da sociedade civil para participar das deliberações e debater prioridades para a internet, junto com o governo.*

Destacam-se dentre suas principais atribuições as atividades:

- ✓ a proposição de normas e procedimentos relativos à regulamentação das atividades na internet;
- ✓ a recomendação de padrões e procedimentos técnicos operacionais para a internet no Brasil;
- ✓ o estabelecimento de diretrizes estratégicas relacionadas ao uso e desenvolvimento da internet no Brasil;
- ✓ a promoção de estudos e padrões técnicos para a segurança das redes e serviços no país;
- ✓ a coordenação da atribuição de endereços internet (IPs) e do registro de nomes de domínios usando <.br>;
- ✓ a coleta, organização e disseminação de informações sobre os serviços internet, incluindo indicadores e estatísticas.

O CGI está dividido em diversos grupos de trabalho, cada qual focando uma área de atuação específica, sendo que para nós, o mais importante é o grupo de trabalho denominado CERT.br, (Centro de Estudos, Resposta e Tratamento de Incidentes na Internet) o qual tem a função de produzir documentos relativos à segurança nas redes ligadas à Internet no Brasil, emitir alertas de segurança para essas redes com relação à atividades maliciosas, bem como trabalhar pela conscientização dos usuários sobre problemas de segurança.

1.3 O que é o Protocolo TCP/IP

O protocolo TCP/IP tem a função de possibilitar a troca de informações entre redes de computadores, sendo que este protocolo atua em 04 etapas:

- ✓ A informação é empacotada em vários pacotes;
- ✓ Os pacotes são colocados em envelopes;
- ✓ Os envelopes são endereçados para um computador destino;
- ✓ O computador que recebe as informações faz a checagem de cada um dos pacotes e reconstrói a informação contida.

1.3.1 O IP

O IP (Internet Protocol) tem a seguinte definição no Wikipedia (2010):

> ***Protocolo de Internet*** *(em inglês: Internet Protocol, ou o acrónimo* ***IP****) é um protocolo de comunicação usado entre duas ou mais máquinas em rede para encaminhamento dos dados.*

É o Protocolo de Internet que possibilita a troca de informações por meio de envio de pacotes entre computadores de determinada rede, ou mesmo entre redes, o qual possibilita a identificação dos usuários destas redes, pois cada usuário conectado, durante seu período de conexão, possui um endereço IP único.

Ainda segundo o Wikipedia (2010) o endereço IP é precisamente definido como:

> *O* ***endereço IP*** *(Internet Protocol), de forma genérica, é um endereço que indica o local de um determinado equipamento (normalmente computadores) em uma rede privada ou pública.*

O endereço IP pode ser fixo ou dinâmico, sendo que o IP fixo normalmente é atribuído a um usuário de grande porte, como empresas por exemplo, assim este usuário sempre possuirá o mesmo número IP, estando ou não conectado à Internet, o que tem a vantagem, para fins de investigação, de facilitar a identificação de seu possuidor. Nada impede que um usuário doméstico possua um número IP fixo.

O IP dinâmico, hoje o mais usado pelos provedores de acesso, é atribuído no momento em que o usuário se conecta à Internet, sendo que ele possuirá este número único pelo tempo que permanecer conectado, quando este usuário efetuar nova conexão lhe será atribuído um novo número IP.

A forma dinâmica do IP tem como desvantagem dificultar a localização e a identificação exata do usuário que esteve conectado por determinado período de tempo.

O endereçamento IP não está adstrito somente aos computadores, pois este é atribuido a toda gama de aparelhos eletrônicos capazes de se conectar a uma rede, como por exemplo aparelhos celulares, video games de última geração, palm tops, etc, sendo que a atribuição do IP se dá no momento em que a conexão é estabelecida.

1.4 Mac Address

O Mac Address, ou endereço de Mac, é o modo mais eficaz para se identificar um equipamento, pois este número é único, tido como um verdadeiro DNA do aparelho. Vejamos a conceituação apresentada pelo Wikipedia (2010):

> *O* ***endereço MAC*** *(do inglês Media Access Control) é o endereço físico de 48 bits da estação, ou, mais especificamente, da interface de*

> *rede. O protocolo é responsável pelo controle de acesso de cada estação à rede Ethernet.*

O endereço de MAC é representado por 12 dígitos hexadecimais agrupados dois a dois, sendo estes separados por dois pontos. Exemplo:

00:00:5E:00:01:03

Ainda segundo a Wikipedia, o endereço é subdividido e representado da seguinte forma:

> *Os três primeiros octetos são destinados à identificação do fabricante, os 3 posteriores são fornecidos pelo fabricante. É um endereço único, i.e., não existem, em todo o mundo, duas placas com o mesmo endereço.*

Desta forma pode-se localizar e identificar um aparelho de maneira certa e absoluta por meio de seu endereço de MAC.

1.5 LOG de dados

Outro método utilizado para se identificar e registrar o acesso de usuários nas redes de computadores são os chamados Log's de acesso, os quais são assim definidos pela Wikipedia:

> *Em computação, **Log de dados** é o termo utilizado para descrever o processo de registro de eventos relevantes num sistema computacional. Esse registro pode ser utilizado para restabelecer o estado original de um sistema ou para que um administrador conheça o seu comportamento no passado. Um arquivo de log pode ser utilizado para auditoria e diagnóstico de problemas em sistemas computacionais.*

Fica clara a importância deste processo dentro das formas de investigação e da obtenção da prova dentro de nosso sistema legal, haja vista o Direito não evoluir na mesma velocidade da tecnologia, sendo em particular a Internet um campo novo e desconhecido para os operadores do Direito. Prossegue ainda a Wikipedia em sua definição:

> *Ademais, os logs possuem grande importância para o Direito da Tecnologia da Informação. A possibilidade de identificar a autoria de ações no ambiente virtual, permitindo a responsabilização dos autores, só é possível através da análise de logs. Os logs também*

podem ser entendidos como provas digitais.

Adiante veremos em nosso estudo a importância desses termos e processos até aqui expostos para os meios de persecução criminal.

1.6 Quem controla a Internet?

A Internet é administrada pela Internet Society, uma organização internacional sem fins lucrativos fundada em 1992 nos Estados Unidos, e por agentes governamentais, que fazem o acompanhamento e a devida promoção da Internet, regulamentando atividades, divulgando e expandindo informações, definindo padrões de funcionamento, e etc.

A Internet Society trabalha com foco no desenvolvimento, manutenção e evolução dos padrões da internet, gerenciamento dos processos necessários para o funcionamento da Internet e a construção de redes, harmonização das atividades internacionais para aumentar o desenvolvimento e disponibilidade da Internet, bem como a divulgação de informações relacionadas com a internet.

1.7 Como é feito o custeio da Internet

A internet é dividida basicamente da seguinte forma:

- ✓ Os provedores de backbone (redes capazes de transmitir grandes volumes de dados, constituídos por vários computadores), chamados de provedores classe A e B.
- ✓ Os provedores locais, chamados de provedores de classe C.
- ✓ Os usuários finais.

Backbone principal: detém toda estrutura da internet e está localizado nos Estados Unidos, sendo mantido por empresas;

Backbones secundários: mantidos por empresas privadas e públicas;

Provedores locais: pagam para acessar os backbones secundários;

Usuários finais: pagam para os provedores locais, pelo acesso a internet, sendo quem mantém de fato o sistema.

1.8 Como se conectar a Internet?

Há basicamente três alternativas:

1.8.1 Via provedores de acesso

Hoje, os provedores de acesso a internet são, em sua maioria, gerenciados por universidades, empresas de telefonia e empresas que se dedicam tão somente a fornecer acesso à internet.

Para utilizar os serviços de um provedor o usuário necessita de equipamentos básicos, como o “modem”, ou uma placa PCI de fax modem, efetuando o acesso por meio de uma linha telefônica, cabo ou via rádio, conforme a disponibilidade da provedora bem como da região em que está o usuário.

O provedor dará suporte necessário em todas as fases de conexão e acesso aos recursos da Rede, podendo ser definidos em três espécies principais, sendo estas o provedor de acesso, o provedor de informações e/ou provedor de conteúdo e o provedor de serviço.

Provedor de acesso: é instituição ligada à internet que obtêm conectividade IP e desta forma propicia aos usuários, sejam estes instituições ou indivíduos, o acesso a Internet;

Provedor de informação e/ou conteúdo: tem como objetivo a coleta, manutenção e organização de informações on-line, as quais são disponibilizadas para parte de seus assinantes que acessam a rede ou para toda internet;

Provedor de serviço: o mais importante para nosso estudo, tanto fornece o acesso a internet quanto trabalha na coleta, difusão e repasse de informações e conteúdo de dados no âmbito da internet.

1.8.2 Via redes locais

Nesta modalidade o acesso somente será possível via rede local de computadores de empresas, rede esta que deverá estar conectada a internet utilizando-se de uma linha dedicada de dados ADSL ou outra tecnologia adotada pela empresa.

A linha dedicada de dados ou ADSL, até pouco tempo, era inacessível para usuários domésticos devido ao seu alto custo, mas com a popularização da Internet bem como com o grande número de provedores existentes hoje, este custo vem caindo e os usuários domésticos tem tido acesso a este tipo de serviço.

1.8.3 Via banda larga

Este tipo de conexão para a internet atua exclusivamente para o tráfego de dados,

assim garante ao usuário grande velocidade nos aspectos de navegação na web, bem como no envio e recebimento de dados.

Os conteúdos mais acessados pelos usuários domésticos deste sistema são vídeos, jogos e músicas, bem como pesquisas e trabalhos acadêmicos.

Os equipamentos necessários para acesso à banda larga são uma placa de rede, um modem ADSL, uma linha telefônica que comporte este serviço, (podendo também ser via cabo ou rádio), e uma assinatura do serviço junto aos provedores de acesso a internet.

1.9 Quem são os criminosos que agem no mundo virtual?

Com o surgimento da Internet apareceram concomitantemente os estudiosos e os curiosos por este novíssimo mundo tecnológico. Assim, com a evolução dos computadores e da internet essas tecnologias passaram a ser usadas tanto de forma benéfica para a sociedade, propiciando acesso instantâneo à informação em qualquer parte do planeta, bem como também passou a ser explorada de forma imoral, antiética e muitas vezes criminosas, haja vista a liberdade e a enganosa sensação de anonimato proporcionada pelo mundo virtual.

Elencaremos as espécies mais conhecidas de usuários da grande rede:

1.9.1 Hackers

A princípio temos que destacar que há uma equivocada percepção do significado da palavra Hacker, e consequentemente do indivíduo assim rotulado por parte da sociedade como um todo. Por falta de conhecimento, a mídia, de forma geral, classificou os indivíduos que cometem crimes na internet, ou utilizando-se desta, como Hackers, porém esta nomenclatura não deve ser usada desta forma. Segundo a enciclopédia livre Wikipedia (2010) o termo Hacker define-se como:

> *Originalmente, e para certos programadores,* ***hackers*** *(singular:* ***hacker****) são indivíduos que elaboram e modificam software e hardware de computadores, seja desenvolvendo funcionalidades novas, seja adaptando as antigas.*
> *Originário do inglês, o termo hacker é utilizado no português. Os Hackers utilizam todo o seu conhecimento para melhorar softwares de forma legal. Eles geralmente são de classe média ou alta, com idade de 12 a 28 anos.*

Os Hackers são especilistas em Tecnologia da Informação e atuam geralmente na

área de segurança da informação, prestando serviços para empresas e governos. O termo Hacker pode ser tido como gênero, o qual é dividido em uma inúmera quantidade de espécies.

1.9.2 Crackers

São indivíduos que se utilizam de todo seu conhecimento em TI para cometer ilícitos por meio das redes de computadores, sendo definidos pelo Wikipedia como:

> *...quem pratica a quebra (ou* cracking*) de um sistema de segurança, de forma ilegal ou sem ética. Este termo foi criado em 1985 por hackers em defesa e contra o uso jornalístico do termo* hacker*. ...A verdadeira expressão para invasores de computadores é denominada Cracker e o termo designa programadores maliciosos e ciberpiratas que agem com o intuito de violar ilegal ou imoralmente sistemas cibernéticos.*

Os Crackers são especialistas em quebras de softwares, disponibilizando chaves de registro para que qualquer interessado possa utilizar-se de um software sem pagar pelo uso deste, causando desta forma grande prejuízo à empresa que detém os direitos sobre determinado produto.

Realizam ainda invasões a computadores de indivíduos e empresas a fim de causar danos a softwares, apropriar-se de informações visando obter alguma vantagem financeira ou simplesmente por “diversão”.

Existem inúmeras nomenclaturas específicas para casa especialidade técnica exercida por indivíduos que atuam na área informática, porém é inviável e desnecessário para nosso objetivo de estudo citar todos eles.

1.9.3 Criminosos leigos

O que temos que ter em mente é que não são somente esses especialistas em informática e principalmente em redes e Tecnologia da Informação os responsáveis por crimes cometidos na Internet ou utilizando-se desta.

Qualquer indivíduo com conhecimento básico em informática poderá acessar a Internet e divulgar informações sigilosas ou imagens de determinado indivíduo, cometendo desta forma um ilícito penal, como veremos adiante ao abordarmos os crimes de informática.

Há também casos frequentes de quadrilhas especializadas em furtos a bancos e empresas por meio da internet, onde Crackers são aliciados para viabilizar tais delitos por

meio de transferência de valores e informações pela própria Internet ou obtenção de senhas para posterior saque em caixas eletrônicos.

Existem também os crimes afeitos a oportunidade, praticados por indivíduos que valendo-se de sua ocupação profissional acessam computadores e redes de empresas, das quais são empregados, e cometem crimes contra seus empregadores.

Assim, como podemos constatar, o delinquente informático é de difícil identificação, não possuindo um perfil definido, podendo cometer crimes inerentes à informática, como violação de direitos autorais em softwares, crimes de furto, conforme acima citado ou mesmo de Pedofilia na Internet, onde indivíduos com conhecimentos básicos de acesso a Internet tentam assediar ou aliciar sexualmente crianças por meio de chats (salas de bate-papo) procurando obter satisfação sexual.

CAPÍTULO II - ASPECTOS PENAIS

2.1 A Informática e o Direito

Com o surgimento e a evolução das Tecnologias da Informação muito se tem falado sobre a possível aparição de um novo ramo do Direito, qual seja, o Direito Informático, sendo que como expõe Vasconcelos (2008, p. 29), *...há campo aberto para que o Direito Informático surja, com absoluta autonomia, possuindo princípios específicos e abrangendo o disciplinamento, com regras próprias*.

Hoje, o indivíduo que "navega" pela internet tem a falsa sensação de que está em um mundo onde tudo é permitido, regido por "leis próprias", leis essas que na verdade se tratam de códigos de conduta criados pelos próprios internautas, porém essa visão é equivocada, pois a sociedade possui sim um meio eficaz de vigiar e punir os transgressores do mundo virtual.

Assim, conforme pensamento de Daoun e Blum (2000, p. 119),

> *Partindo da premissa de que o Direito é a única forma de controle capaz de conter o avanço da criminalidade no mundo virtual, isto porque, de todos os sistemas de controle social, o Direito é o único que se reveste das características da coercitividade, sancionando as condutas havidas por ilícitas, quer sob a angulação penal, civil ou administrativa.*

Ainda não há um consenso sobre a nomenclatura a ser utilizada no que se refere ao ramo do Direito dedicado às condutas praticadas envolvendo a informática e a internet, sendo que alguns autores lhe atribuem a denominação de Direito Informático, ou Direito da Internet, ou ainda Direito Cybernético, todavia, a primeira denominação é claramente mais abrangente.

Nomenclaturas a parte, a grande discussão que se impõe é se há a necessidade de se implantar uma legislação específica para regular e punir essas "novas" condutas ou se a legislação existente, baseada em nossa Constituição Federal, Código Penal, sistema processual penal e leis esparsas são suficientes para coibir tais condutas.

Como bem disse Eric Schmidt (apud CORREA, 2008, p. V), ex-executivo da Sun Microsystems e atual presidente da Novel, *a Internet é a primeira coisa que a humanidade criou e não entende, a maior experiência de anarquia que jamais tivemos.*

Desta forma, é responsabilidade dos operadores do Direito indicar o caminho a ser tomado a fim de normatizar as condutas da grande rede, sem contudo, comprometer seu crescimento e inviabilizar suas formas de expressão e utilização.

Conforme expôs Corrêa (2008, p. 3),

> *O grande desafio para o Direito é a compreensão e o acompanhamento dessas inovações, garantindo assim a pacificação social, o desenvolvimento sustentável dessas novas relações, acima de tudo, a manutenção do próprio Estado Democrático de Direito. Aos operadores do Direito cabe a difícil tarefa de estudar e encontrar respostas, sensatas e inteligentes, para os novos desafios advindos desse novo paradigma, fazendo com que a pessoa humana e as novas tecnologias possam coexistir dentro de uma nova concepção de mundo.*

As mudanças, em termos de legislação, no Brasil vem se operando de forma lenta, pois há vários projetos de lei em discussão no Congresso Nacional, mas até a presente data muito pouco foi efetivamente votado, como veremos mais adiante.

Mas, pela postura que se vem adotando por parte de nossos legisladores, a tendência e consenso, é que não será criada uma legislação específica para os crimes informáticos, e sim deveremos ter uma atualização dos códigos e leis existentes, como por exemplo da recente alteração do ECA.

O motivo para tal postura é que a grande maioria dos crimes informáticos cometidos são facilmente enquadrados na tipologia de crimes previstos em nosso código penal e leis existentes, pois o que se muda em tais crimes, em sua grande maioria, é somente o meio de execução, assim não há motivos para se deixar de punir tal conduta.

2.2 Conceito de crime informático

Admitindo-se o surgimento desse novo ramo do Direito Informático temos que chegar a uma definição do que é, em essência, o crime informático, sendo que a princípio podemos citar Barret (1997, p. 44) apud Corrêa (2008) o qual expõe ser este *(...) a utilização de computadores para ajuda em atividades ilegais, subvertendo a segurança de sistemas, ou usando a Internet ou redes bancárias de maneira ilícita.*

Na mesma linha expõe Nigri (2001, p. 41) apud Inellas (2009), O crime informático, caracteriza-se, principalmente, por constituir um ato lesivo cometido através de um computador ou de um periférico com a intenção de se obter uma vantagem indevida.

Porém, as definições apresentadas não abordam o tema de forma completa e exata, deixando de citar o computador como alvo da conduta criminosa, bem como não levando em consideração que nem todas as condutas criminosas praticadas visam obter uma vantagem indevida, como por exemplo a invasão, pelos crackers, de sistemas considerados seguros, pelo

simples prazer de provar que são capazes.

Uma definição mais exata e completa, também citada por Inellas (2009, apud FERREIRA, p. 41, grifo nosso) expõe com clareza:

> *Se considerarmos, de acordo com a moderna doutrina penal, que* ***constitui crime da informática toda ação típica, anti-jurídica e culpável cometida contra ou pela utilização de processamento automático de dados ou sua transmissão****, conceito que pouco difere da definição da OECD e caracteriza os elementos necessários para a criminalização das condutas puníveis, poderemos estabelecer uma ampla gama de relações sociais e individuais, que comportam a utilização da informática e a possibilidade dos abusos que as deseja coibir através das normas penais (...)*

De acordo com as definições apresentadas, podemos classificar os crimes informáticos, conforme Costa (1997), como crimes virtuais puros, mistos e comuns, definido-os da seguinte forma:

> *Crimes virtuais puros. São aqueles em que o sujeito ativo visa especificamente ao sistema de informática, em todas as suas formas. Entendemos serem os elementos que compõem a informática o "software", o "hardware" (computador e periféricos), os dados e sistemas contidos no computador, os meios de armazenamento externo, tais como fitas, disquetes, etc.*

Nessa classificação os crimes são cometidos, em sua grande maioria por indivíduos com alto grau de conhecimento e domínio da informática como um todo, pois como citado, seu alvo principal é o ataque a softwares e hardwares, sendo que é aqui que podem surgir novas condutas não tipificadas nas leis existentes, como por exemplo a produção de vírus de computador.

Seguindo com a classificação de Costa (1997) temos os Crimes Virtuais Mistos, assim definidos: São todas aquelas ações em que o agente visa a um bem juridicamente protegido diverso da informática, porém, o sistema de informática é ferramenta imprescindível a sua consumação.

Nesta modalidade o uso da Informática, mais especificamente da Internet, é determinante para a obtenção do resultado desejado pelo delinqüente informático, sendo que este resultado não tem relação alguma com a informática/Internet, por exemplo, a invasão a um sistema de home banking a fim de efetuar transferências ilegais de fundos.

Por fim, temos os *Crimes Virtuais Comuns*, os quais são precisamente definidos por Costa (1997) como:

> *São todas aquelas condutas em que o agente se utiliza do sistema de*

> *informática como mera ferramenta a perpetração de crime comum, tipificável na lei penal, ou seja, a via eleita do sistema de informática não é essencial à consumação do delito, que poderia ser praticado por meio de outra ferramenta.*

Como exposto, nos Crimes Virtuais Comuns, o sistema de informática utilizado é somente uma ferramenta, a qual poderia ser substituída por qualquer outro meio, como nos crimes de estelionato (art. 171, CPB).

O conceito de crime informático apresentado, bem como sua classificação, apesar de ser só um dos muitos existentes na doutrina, facilitam em muito a identificação dos crimes de informática, e principalmente nos auxilia no enquadramento da conduta do agente ao tipo previsto na legislação vigente.

2.3 Princípios Constitucionais

Dando prosseguimento à discussão se há necessidade de legislação específica para regular as práticas delitivas ocorridas na Internet, ou se nossas antigas leis, principalmente nosso Código Penal que data de 1940, podem coibir os abusos praticados, temos que analisar alguns princípios de nossa Constituição Federal, onde as leis encontram suporte para sua existência e atuação.

A Constituição Federal de 1988 adotou o Estado Democrático de Direito, conforme seu Artigo 1º, tendo como princípio basilar o da Legalidade, a fim de assegurar a todos os indivíduos uma sociedade mais justa e igual.

A lei, segundo Silva (2007, p.121), é conceituada da seguinte forma:

> *Ato de decisão política por excelência, é por meio dela, enquanto emanada da atuação da vontade popular, que o poder estatal propicia ao viver social modos predeterminados de conduta, de maneira que os membros da sociedade saibam, de antemão, como guiar-se na realização de seus interesses.*

Assim, como exposto, a lei emana do povo, e desta forma todo indivíduo deve saber que qualquer conduta adotada fora dos padrões socialmente aceitáveis terá conseqüências diretas em sua vida.

O princípio da legalidade está previsto no artigo 5º, II da CF, segundo este *ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei*, ou seja, conforme pertinente afirmação de Silva (2007, p. 420):

> *É nesse sentido que se deve entender a assertiva de que o Estado, ou o*

> *Poder Público, ou os administradores não podem exigir qualquer ação, nem impor qualquer abstenção, nem mandar tampouco proibir nada aos administrados, senão em virtude de lei.*

Nos deparamos aqui com a legalidade penal, sendo esta uma garantia individual prevista no art. 5º, XXXIX da CF, para o qual *não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal*, ou seja, sem legislação prévia, não há que se falar em crime ou pena, e cabe, unicamente ao legislador, a tarefa de definir quais condutas serão tidas como crime e suas respectivas penas.

Atrelado a isto, temos o princípio da irretroatividade da lei penal, o qual está consubstanciado no artigo 5º, XL de nossa CF, o qual preceitua que *a lei penal não retroagirá, salvo para beneficiar o réu*, sendo que referidos princípios também estão previstos em nosso Código Penal.

O que vemos dos princípios até o momento citados é que necessitamos de um sistema que possua segurança jurídica a fim de que indivíduos respeitem as leis e venham a ter um convívio social equilibrado.

Desta forma, o que não podemos admitir é que um indivíduo possua um comportamento exemplar no meio social e, de forma equivocada, realize condutas inaceitáveis no mundo virtual, ou seja, a Internet, vindo a achar que só deverá respeitar as normas de condutas estabelecidas pelos próprios usuários.

Observamos nos preceitos constitucionais que qualquer crime poderá ser punido desde que haja lei anterior que o defina, assim, o que muitos criminosos que atuam no meio informático parecem desconhecer é que a maioria dos crimes por eles praticados, como veremos, são perfeitamente enquadrados na legislação existente.

Nossa Constituição Federal assegura em seu artigo 5º, XII *a inviolabilidade da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas,* tutelando, desta forma, a liberdade de manifestação do pensamento e o direito à intimidade.

Porém esta garantia individual não dá à pessoa o direito de praticar condutas delituosas valendo-se da norma constitucional, pois no mesmo inciso, na parte final, há a seguinte ressalva, *salvo, no último caso, por ordem judicial* (...), o que propicia ao estado a quebra de sigilo regulamentada pela lei 9.296/1996, levando a identificação do delinqüente e a sua possível punição.

Fica evidente, assim, a importância precípua em se observar e acatar o contido nos princípios constitucionais, pois são eles os regentes de todo nosso sistema de normas, como exposto por Mello (1994, p. 451) apud Capez (2005, p.8):

> *Violar um princípio é muito mais grave do que transgredir uma norma. A desatenção ao princípio implica ofensa não apenas a um específico mandamento obrigatório, mas a todo sistema de comandos. É a mais grave forma de ilegalidade ou inconstitucionalidade, conforme o escalão do princípio atingido, porque representa ingerência contra todo o sistema, subversão de valores fundamentais, contumélia irremissível a seu arcabouço lógico e corrosão de sua estrutura mestra.*

Referidos princípios deverão ser observados tanto no momento do surgimento da norma penal, por parte do legislador, bem como quando de sua aplicação por parte dos operadores do Direito. Neste sentido afirma Capez (2005, p. 9),

> *Os princípios constitucionais e as garantias individuais devem atuar como baliza para a correta interpretação e a justa aplicação das normas penais, não se podendo cogitar de uma aplicação meramente robotizada dos tipos incriminadores, ditada pela verificação rudimentar da adequação típica formal, descurando-se de qualquer interpretação ontológica do injusto.*

Toda a interpretação e aplicação das normas penais devem ter em conta o princípio genérico e regente do Direito Penal, ou seja, o princípio da dignidade humana, visando sempre à justa aplicação da norma penal, pois é deste princípio genérico que derivam seus princípios específicos, dentre eles o da legalidade, pois, novamente citando Capez (2005, p. 7), expõe-se com clareza,

> *Podemos, então, afirmar que do Estado Democrático de Direito parte o princípio da dignidade humana, orientando toda a formação do direito penal. Qualquer construção típica, cujo conteúdo contrariar e afrontar a dignidade humana, será materialmente inconstitucional, posto que atentatória ao próprio fundamento da existência de nosso Estado.*

Evidente está que as condutas praticadas na Internet devem estar, e por óbvio estão, sob a vigilância de nosso arcabouço de normas, em particular as de cunho penal, pois a Internet nada mais é do que uma ferramenta de facilitação do convívio social e como tal, mesmo que de natureza globalizada, ou seja, não reconhecendo as fronteiras físicas dos países, os indivíduos que dela se utilizam devem respeitar as leis internas de cada ente como país, pois, particularmente em nosso Estado, os operadores do Direito devem, em respeito aos princípios constitucionais, definir, interpretar e aplicar da melhor maneira possível a norma penal, coibindo assim condutas que possuem lesividade social.

2.4 Tipicidade

Não há como se falar de aplicabilidade da norma penal sem abordarmos, mesmo que de forma sucinta, a tipicidade, a qual é de suma importância, pois é por meio da análise do tipo penal e da adequação típica que saberemos se a norma poderá ser aplicada à conduta potencialmente lesiva.

Não devemos confundir o tipo penal com a tipicidade, pois o primeiro representa o modelo legal de comportamento e o segundo se refere à adequação da conduta humana ao tipo.

O tipo penal é definido por Santoro Filho (2001, p. 34) como sendo o modelo legal de comportamento, no qual estão inseridas determinadas características, que tornam a conduta relevante em matéria penal, ou seja, o legislador, ao legislar, insere no tipo condutas, as quais são representadas por verbos, caracterizando ação ou omissão, com a finalidade de proteger valores fundamentais da sociedade.

A tipicidade, como dito, nada mais é do que a adequação da conduta humana ao núcleo do tipo penal, a qual é melhor conceituada por Santoro Filho (2001, p. 36):

> *A tipicidade, deste modo, pode ser conceituada como a correspondência, a subsunção do comportamento humano (fato) ao tipo (previsão da lei penal), em todos os seus elementos.*

Desta maneira, analisando-se a conduta, seu resultado (exceto na tentativa), estando presente a relação de causalidade e a tipicidade, pode-se considerar o fato típico, e estando o mesmo em desacordo com o ordenamento jurídico, ou seja, sendo ele antijurídico, o fato concreto será considerado crime.

Tanto quanto os princípios constitucionais, o domínio destes conceitos também são de suma importância para a adequação das condutas praticados pelos indivíduos na Internet ao tipo penal, levando-nos a saber se a Lei penal em vigor é aplicável a essas condutas, ou se há necessidade de mudanças ou até a criação de lei penal específica.

2.5 A Analogia

Já comentamos no presente trabalho que as leis em vigência podem ser aplicadas a inúmeras condutas praticadas na internet, visando desta forma sua punição. Também foi exposto o fato de que existem algumas condutas, principalmente nos crimes informáticos puros, as quais não possuem previsão legal. Desta forma, temos que abordar o tema da

Analogia, pois sua aplicação, como veremos, não é admitida quando se tratar de norma penal incriminadora.

Pode se conceituar a Analogia, conforme Capez (2005, p. 34) da seguinte forma:

> *Consiste em aplicar-se a uma hipótese não regulada por lei disposição relativa a um caso semelhante. Na analogia, o fato não é regido por qualquer norma e, por essa razão, aplica-se uma de caso análogo.*

Seria simples para o operador do direito, aplicando a analogia, punir condutas que até então não são previstas em nosso ordenamento jurídico, porém, tal aplicação contraria o princípio da reserva legal, pois, não se pode permitir o uso da analogia a fim de se criar ilícitos penais, violando também o princípio da legalidade.

Neste sentido expõe Mirabete (2004, p. 47),

> *Diante do princípio da legalidade do crime e da pena, pelo qual não se pode impor sanção penal a fato não previsto em lei, é inadmissível o emprego da analogia para criar ilícitos penais ou estabelecer sanções criminais.*

Ou seja, jamais será possível a aplicação da analogia *in malam partem*, cabendo a aplicação desta somente em benefício do agente, pois neste caso não estaríamos ferindo nenhum princípio constitucional, até mesmo porque tal aplicação está prevista no artigo 4º da LICC, o qual prevê, *quando a lei for omissa, o juiz decidirá o caso de acordo com a analogia, os costumes e os princípios gerais do direito*, sendo esta uma forma de auto-integração da lei.

Temos que separar a analogia da interpretação analógica, pois, como já dito, na analogia não existe uma norma regulando a hipótese de forma expressa, enquanto que na interpretação analógica a norma existe, porém esta é genérica, devendo de tal modo ser a mesma interpretada. A interpretação analógica é aceita e amplamente aplicada.

Assim, apesar de possível a aplicação das leis existentes em nosso ordenamento jurídico às condutas praticadas na internet, não podem os operadores do direito aplicá-las de forma a violar os princípios constitucionais, sendo que desta forma, para algumas condutas, ainda necessitamos que o legislador atue de forma a sanar as lacunas existentes em nossa legislação.

2.6 Crimes Informáticos

Como vimos, até o presente ponto, os princípios constitucionais da reserva legal e da

legalidade deverão ser atentamente observados e respeitados no momento da aplicação da lei penal, porém isto não pode ser tomado como impedimento para a ação coercitiva do Estado perante as condutas praticadas na internet, pois, como já mencionado, na maioria das vezes a internet é utilizada somente como ferramenta de execução por parte dos agentes criminosos.

Desta forma, listaremos a seguir uma gama de condutas praticadas no meio virtual as quais constituem crime e são adequadamente previstas em nosso ordenamento jurídico.

2.6.1 Furto mediante fraude

Prevê o artigo 155, §4º, inciso II do Código Penal:

> *Subtrair, para si ou para outrem, coisa alheia móvel:*
> *(...)*
> *§4º A pena é de reclusão de 2 (dois) a 8 (oito) anos, e multa, se o crime é cometido:*
> *(...)*
> *II – com abuso de confiança, ou mediante fraude, escalada ou destreza;*
> *(...)*

O furto mediante fraude é a modalidade de furto mais praticada na internet, a qual se caracteriza por meio da transferência de fundos bancários, onde o criminoso se utiliza de um meio enganoso para iludir a vigilância da vítima, permitindo desta maneira acesso facilitado para subtração do objeto material.

No caso, o meio enganoso utilizado pelo criminoso, geralmente, trata-se de uma página falsa de um internet banking, onde o cliente iludido digita os números de sua conta corrente e senha a fim de acessar sua conta, mas tudo o que obtém é uma mensagem de erro, sendo que instantaneamente seus dados sigilosos são enviados para o criminoso, o qual fará uso dos mesmos para furtar valores da vítima.

Este crime se difere do estelionato, pois a vítima não entrega seus bens espontaneamente, haja vista a mesma nem saber que forneceu seus dados bancários ao criminoso.

2.6.2 Dano

Prevê o artigo 163, caput e §único, inc. III e IV do Código Penal:

> *Destruir, inutilizar ou deteriorar coisa alheia:*
> *(...)*

> *Parágrafo único. Se o crime é cometido:*
> *(...)*
> *III. contra o patrimônio da União, Estado, Município, empresa concessionária de serviços públicos ou sociedade de economia mista;*
> *IV. por motivo egoístico ou com prejuízo considerável para a vítima.*

Podemos citar como exemplo de crime de dano cometido por meio da internet a disseminação de vírus de computador com a intenção de causar prejuízo, destruição ou inutilização de dados e informações contidas nos computadores das vítimas.

Nesta modalidade de crime, o criminoso responde por disseminar o vírus e não por sua criação, invenção, pois não existe em nosso ordenamento jurídico previsão legal para tal conduta, assim só poderá ser punida a conduta de disseminar o vírus com a intenção de prejudicar outras pessoas, ressaltando-se que o número de vítimas é imensurável, pois o vírus de computador, como o biológico, se multiplica e se espalha pela rede de forma rápida e imprevisível.

2.6.3 Estelionato

Prevê o artigo 171, caput e §3º do Código Penal:

> *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:*
> *(...)*
> *§3º A pena aumenta-se de um terço, se o crime é cometido em detrimento de entidade de direito público ou de instituto de economia popular, assistência social ou beneficência.*

Um exemplo simples de crime de estelionato praticado pela Internet é a compra, pelo agente criminoso, de algum produto em uma loja virtual, utilizando-se de dados de um cartão de crédito de terceiro, pois desta forma a loja virtual, como vítima, estará entregando o produto de forma espontânea, ou seja, de forma voluntária, este entendimento é inclusive o defendido pelo STJ.

2.6.4 Crimes contra a honra

Prevê o artigo 138, caput e §1º do Código Penal:

> *Caluniar alguém, imputando-lhe falsamente fato definido como crime:*
> *(...)*

> *§1º Na mesma pena incorre quem, sabendo falsa a imputação, a propala ou divulga;*
> *(...)*

Prevê o artigo 139 do Código Penal, Difamar alguém, imputando-lhe fato ofensivo à sua reputação: (...).

Prevê o artigo 140, caput e §3º do Código Penal:

> *Injuriar alguém, ofendendo-lhe a dignidade ou o decoro:*
> *(...)*
> *§3º Se a injúria consiste na utilização de elementos referentes à raça, cor, etnia, religião, origem ou a condição de pessoa idosa ou portadora de deficiência:*
> *(...)*

Os crimes em tela atingem a honra objetiva e subjetiva da vítima, sendo que por honra objetiva endente-se a moral e a reputação da vítima e por honra subjetiva o sentimento da pessoa em relação a sua conduta moral e intelectual.

Os crimes de Calúnia e Difamação atingem a honra objetiva da vítima, enquanto que o crime de Injúria atinge a subjetiva.

Esses crimes são de fácil identificação na internet, pois eles se configuram por meio de veiculação, em páginas na internet, de fatos, crimes ou opiniões ofensivas, atribuídas a determinada pessoa, caracterizando desta forma um dos crimes acima expostos. Podemos citar como exemplo páginas de cunho racista e agressões de cunho étnico ou religioso.

2.6.5 Ameaça

Prevê o artigo 147 do Código Penal:

> *Ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave:*
> *(...)*

Crime este também de fácil caracterização, o crime de ameaça é cometido por meio da internet com a utilização de páginas criadas para ameaçar um indivíduo ou grupo de indivíduos, ou também por envio de mensagem de correio eletrônico (e-mail), ou seja, a internet é somente uma ferramenta de execução nesta modalidade de crime, como seria uma mensagem publicada em jornal ou o envio de uma simples carta ou telegrama.

2.6.6 Violação de correspondência

Prevê o artigo 151, caput e §1º, I do Código Penal:

> *Devassar indevidamente o conteúdo de correspondência fechada, dirigida a outrem:*
> *(...)*
> *§1º Na mesma pena incorre:*
> *I. quem se apossa indevidamente de correspondência alheia, embora não fechada e, no todo ou em parte, a sonega ou destrói;*
> *(...)*

A violação de correspondência na internet se dá mais precisamente com o uso do correio eletrônico (e-mail), onde a mensagem é interceptada ou acessada de forma indevida pelo criminoso informático.

Esta conduta se amolda ao inciso I do §1º do artigo 151 do CP, pois acessando indevidamente o computador da vítima, o criminoso, por meio do programa de correio eletrônico terá acesso a todas as mensagens enviadas e recebidas.

2.6.7 Incitação ao crime

Prevê o artigo 286 do Código Penal: Incitar, publicamente, a prática de crime: (...).

Nesta modalidade a internet é utilizada meramente como um simples meio de cometimento do crime em tela, haja vista ele se caracterizar, na internet, pelo envio de correspondência eletrônica ou a criação de uma página incitando usuários a cometerem delitos.

2.6.8 Apologia ao crime ou de criminoso

Prevê o artigo 287 do Código Penal: Fazer, publicamente, apologia de fato criminoso ou de autor de crime: (...).

Aqui, como no crime anterior, estamos diante de crime contra a paz pública, onde a internet, novamente, é utilizada somente como meio de atingir o objetivo danoso, configurando-se pela criação de página ou envio de correio eletrônico, fazendo, publicamente, apologia de fato criminoso ou autor de crime, como consta do caput do artigo em comento, destacando que a apologia deve ser de fato definido como crime, ou este não se configurará.

2.6.9 Induzimento, instigação ou auxílio ao suicídio

Prevê o artigo 122, caput do Código Penal: Induzir ou instigar alguém a suicidar-se ou prestar-lhe auxílio para que o faça: (...).

No caput do artigo, no verbo induzir, o agente incute na mente da vítima a idéia de autodestruição, enquanto que no verbo instigar o agente somente incentiva a vítima, haja vista esta já possuir em sua mente a idéia de autodestruição. Ainda no caput, onde se diz prestar-lhe auxílio, por tratar-se de crime material, não poderá ser praticada por meio da internet.

Assim vemos que somente será possível o agente ativo praticar o induzimento e a instigação nos crimes informáticos, onde podemos citar como exemplo, a troca de correio eletrônico do agente com a vítima, bem como a troca de mensagens por meio de programas de chat (bate-papo), como o MSN, ICQ, ou mesmo salas de bate-papo disponibilizadas em páginas da internet.

2.6.10 Favorecimento da prostituição

Prevê o artigo 228 do Código Penal:

> *Induzir ou atrair alguém à prostituição ou outra forma de exploração sexual, facilitá-la, impedir ou dificultar que alguém a abandone:*
> *(...)*

Observando-se os verbos contidos no caput vemos que o agente ativo somente poderá induzir ou atrair alguém a prostituição ou outra forma de exploração sexual ou ainda facilitá-la, não cabendo aqui, de nenhuma forma o impedimento ou o ato de dificultar que alguém a abandone, haja vista estes dois últimos verbos exigirem ação ou omissão material por parte do agente.

Existem vários exemplos para o crime em tela, sendo a criação de página contendo fotos de mulheres, ou envio dessas fotos por correio eletrônico, atingindo desta forma um universo ilimitado de usuários, visando induzir, atrair ou facilitar, que prostitutas ou mesmo usuários se prostituam, é um dos meios mais comuns e utilizados.

2.6.11 Rufianismo

Prevê o artigo 230 do Código Penal:

> *Tirar proveito da prostituição alheia, participando diretamente de seus lucros ou fazendo-se sustentar, no todo ou em parte, por quem a exerça:*
> *(...)*

Nesta modalidade, o crime é exercido utilizando a internet como mais uma ferramenta, onde o agente se utiliza de páginas onde oferece os serviços sexuais de mulheres e, diferentemente do crime de favorecimento, aqui existe a habitualidade e o agente obtém lucro direto por estes serviços.

2.6.12 Racismo

Prevê o artigo 20, §1º da Lei 7716/89:

> *Praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional.*
> *(...)*
> *§1º Fabricar, comercializar, distribuir ou veicular símbolos, emblemas, ornamentos, distintivos, propaganda que utilizem a cruz suástica ou gamada, para fins de divulgação do nazismo.*
> *(...)*

Estamos diante de outro crime onde o agente ativo utiliza a internet como opção de ferramenta para atingir seus objetivos. Podemos encontrar em uma rápida busca uma centena de páginas criadas com a finalidade de divulgar supostas ideologias que estimulam a discriminação a grupos raciais, como negros, ou étnicos, como os judeus.

Nestas páginas de internet esse grupos pregam a discriminação ou o preconceito contra determinados grupos sociais, sendo que os grupos mais conhecidos são os autodenominados seguidores do nazismo, os quais ainda se utilizam dos símbolos nazistas em suas páginas de internet, assim, além de cometerem os crimes previstos no caput do artigo em tela, também cometem os crimes previstos no §1º do mesmo artigo.

2.6.13 Crime contra a inviolabilidade dos segredos

Prevê o artigo 153, §1º do Código Penal:

> *(...)*
> *§1º Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou bancos de dados da Administração Pública;*
> *(...)*

Temos aqui um exemplo da tendência do legislador em não adotar um código informático próprio, mas sim atualizar as leis existentes, pois este §1º foi introduzido no artigo 153 do CP por meio da lei nº 9.983/2000.

Em regra, tal crime, como condição de procedibilidade exige a Representação do ofendido, porém, no que tange ao §1º, havendo prejuízo para a administração pública, a ação penal será incondicionada.

No caso específico do §1º, o crime poderá ser cometido por qualquer pessoa que venha a obter, de qualquer forma, informações sigilosas ou reservadas, contidas ou não em bancos de dados da administração pública, e venha a divulgá-las, sem justa causa, e de qualquer modo.

Assim, o agente que divulgar essas informações por meio da internet, seja utilizando-se de páginas, correio eletrônico, chat, ou qualquer outra forma, sem justa causa, atingindo um número indeterminado de pessoas, estará cometendo o crime em comento.

2.6.14 Crimes contra o consumidor

Prevêem os artigos do Código de Defesa do Consumidor (Lei 8078/90):

> *Art. 2º Consumidor é toda pessoa física ou jurídica que adquire ou utiliza produto ou serviço como destinatário final.*
> *(...)*
> *Art. 3º Fornecedor é toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, bem como os entes despersonalizados, que desenvolvem atividades de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de produtos ou prestação de serviços.*
> *§1º Produto é qualquer bem, móvel ou imóvel, material ou imaterial.*
> *§2º Serviço é qualquer atividade fornecida no mercado de consumo, mediante remuneração, inclusive as de natureza bancária, financeira, de crédito e securitária, salvo as decorrentes das relações de caráter trabalhista.*

Vemos nos supracitados artigos do CDC a clara definição do que seja consumidor, fornecedor, bem como de produto e serviço, sendo óbvio que tais definições são aplicáveis ao comércio eletrônico, ou seja, o comércio por meio da internet.

É cada vez mais comum pessoas efetuarem compras nas denominadas lojas virtuais, pois em sua maioria essas “lojas” não possuem um ambiente físico e em muitos casos também não possuem sequer estoque, o que torna seus preços mais competitivos em relação ao

mercado tradicional.

Mas o fato de não existirem fisicamente, mas só virtualmente, e por óbvio juridicamente, essas empresas tem cumprir as mesmas obrigações impostas ao modelo tradicional de comércio, estando assim sujeitas às penalidades do CDC.

Outro ponto importante a se salientar quanto à propaganda na internet, onde muitas empresas abusam do meio virtual e utilizam este como uma ferramenta para impor a todo momento suas ofertas de produtos aos usuários frequentadores de determinado site da internet.

O artigo 37 do CDC, proíbe toda forma de propaganda enganosa ou abusiva, seja ela praticada na televisão, jornais ou mesmo na internet, onde geralmente vemos a oferta de produtos que não existem, ou não possuem a qualidade divulgada pelo vendedor, por exemplo, condutas essas que podem vir a caracterizar inclusive o crime de estelionato.

2.6.15 Crimes eleitorais

Prevê o artigo 72 da Lei 9504/97:

> *Constituem crimes, puníveis com reclusão, de 5 (cinco) a 10 (dez) anos:*
> *I – obter acesso a sistema de tratamento automático de dados usado pelo serviço eleitoral, a fim de alterar a apuração ou a contagem de votos;*
> *II – desenvolver ou introduzir comando, instrução, ou programa de computador capaz de destruir, apagar, eliminar, alterar, gravar ou transmitir dado, instrução ou programa ou provocar qualquer outro resultado diverso do esperado em sistema de tratamento automático de dados usado pelo serviço eleitoral;*
> *(...)*

Na lei em comento, mais precisamente em seu artigo 72, visou o legislador coibir os crimes informáticos praticados contra o serviço eleitoral, onde em seu inciso I está previsto o crime de acesso ao sistema de dados da Justiça Eleitoral com o objetivo de fraudar a apuração ou a contagem de votos, ou seja, tenta-se coibir e punir a invasão dos sistemas informáticos da Justiça Eleitoral.

No inciso II vemos uma inovação, pois criminaliza o desenvolvimento ou introdução de comando, instrução ou programa de computador capaz de causar danos ou prejudicar o correto funcionamento do sistema informático do serviço eleitoral.

Como já dissemos aqui, nossa legislação comum não prevê a punição para quem

desenvolve ou cria programas denominados “vírus” de computador, mas neste inciso II claramente pune este tipo de conduta especificamente praticada contra o sistema de dados da Justiça Eleitoral.

2.6.16 Violação de direito autoral

Prevê o artigo 12 da Lei 9609/98:

> *Violar direitos de autor de programa de computador:*
> *(...)*
> *§1º 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:*
> *(...)*
> *§ 2º 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.*
> *§ 3º 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;*
> *(...)*

O artigo em tela visa proteger especificamente os direitos autorais em relação aos programas de computador, ou seja, tem a finalidade de combater a pirataria de software.

Neste caso a internet será utilizada como ferramenta a fim de se reproduzir ou comercializar programas de computador, visando desta forma a obtenção de lucro de forma direta ou indireta, sendo que a identificação da origem da violação do direito autoral torna-se quase impossível no âmbito da rede mundial de computadores.

2.6.17 Interceptação do fluxo de dados em tráfego por serviço de telecomunicações

Prevê o artigo 10 da Lei 9296/96:

> *Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo de justiça, sem autorização judicial ou com objetivos não autorizados em lei.*
> *(...)*

E no parágrafo único de seu artigo 1º está contido:

> *(...)*
> *Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática.*

Esta lei tem como objetivo regulamentar o inciso XII, do artigo 5º da CF, sendo que a princípio causou muita discussão no que tange a seu parágrafo único, pois esse foi considerado inconstitucional por alguns juristas e doutrinadores, haja vista que em sua parte final, o inciso XII, acima referido, só faz menção à autorização de interceptação por parte das comunicações telefônicas, dando a entender não serem possíveis nos demais casos.

Porém este entendimento, pelo menos de forma majoritária, já foi superado, e hoje a autorização judicial para quebra de dados telemáticos é amplamente utilizada.

Assim, fica claro que a interceptação, sem autorização judicial, de dados telemáticos, sejam eles obtidos por meio de chats (salas de bate-papo), MSN, correio eletrônico, ou qualquer meio utilizado para comunicação na internet deverá ser enquadrada como crime, independentemente da finalidade que esta possua.

2.6.18 Tráfico de drogas

Prevê o artigo 33 da Lei 11.343/2006:

> *Importar, exportar, remeter, preparar, produzir, fabricar, adquirir, vender, expor à venda, oferecer, ter em depósito, transportar, trazer consigo, guardar, prescrever, ministrar, entregar a consumo ou fornecer drogas, ainda que gratuitamente, sem autorização ou em desacordo com determinação legal ou regulamentar:*
> *(...)*
> *§ 1º Nas mesmas penas incorre quem:*
> *I - importa, exporta, remete, produz, fabrica, adquire, vende, expõe à venda, oferece, fornece, tem em depósito, transporta, traz consigo ou guarda, ainda que gratuitamente, sem autorização ou em desacordo com determinação legal ou regulamentar, matéria-prima, insumo ou produto químico destinado à preparação de drogas;*
> *(...)*
> *§ 2º Induzir, instigar ou auxiliar alguém ao uso indevido de droga:*
> *(...)*

Mais uma vez a internet, nesta modalidade de crime, será utilizada como ferramenta de execução do crime em tela, onde o agente ativo poderá criar uma página ou site na internet, ou utilizar-se de correio eletrônico ou mesmo sites de relacionamento, como ORKUT, FACEBOOK, etc, a fim de vender, oferecer, expor a venda, drogas ou matérias primas e insumos para a produção da mesma, ou ainda, utilizar das citadas ferramentas informáticas

para induzir ou instigar usuários da rede a usar indevidamente a droga.

2.6.19 Pornografia Infantil

Preceitua o artigo 241 do ECA:

> *Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente.*
> *(...)*

Com o advento da Lei 11.829/2008 houve a introdução no Estatuto da Infância e do Adolescente de alguns artigos visando o combate à cultura pedófila nos meios de comunicação, dos quais destacamos o artigo em tela bem como os demais que se seguem.

A referida Lei veio atender a grande necessidade de tipos específicos para as variadas formas de conduta praticadas na Internet, sendo esta um avanço legislativo considerável.

No artigo 241 vemos que a Internet poderá ser utilizada como meio de vender ou expor à venda, fotografia, vídeo ou outro registro que contenha conteúdo de cunho pedófilo envolvendo criança ou adolescente, podendo ser utilizado para tanto os conhecidos meios, como páginas, salas de bate-papo e comunidades virtuais restritas a membros cadastrados.

Prevê o artigo 241 –A do ECA:

> *Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:*
> *§1º Nas mesmas penas incorre quem:*
> *I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo;*
> *II – assegura por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo.*
> *§2º As condutas tipificadas nos incisos I e II do §1º deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo.*

Tal figura típica tem como principal objetivo atingir todos os meios de comunicação conhecidos, em especial a Internet, destacando-se em especial os incisos I e II, onde se introduziu a possibilidade de punir, como partícipe, pessoas ou empresas que fornecem meios para que o agente ativo armazene esse conteúdo pornográfico ligado a crianças e adolescentes

bem como possibilitam o acesso à Internet, como provedores de acesso e provedores de conteúdo, os quais após notificação judicial deverão retirar tais conteúdos do acesso público, sob pena de responderem pelo tipo penal em tela.

Prevê o artigo 241-B do ECA:

> *Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente.*
> *(...)*

Este artigo também introduz um novo tipo incriminador, pois tem como finalidade punir quem adquire, possui ou armazena o conteúdo indevido, sendo que anteriormente não havia previsão legal para esta conduta, a qual poderá ocorrer facilmente utilizando-se a internet como meio de execução, pois o indivíduo poderá adquirir tal fotografia, vídeo ou outra forma de registro de algum outro usuário da Internet e mantê-lo em seu computador para deleite pessoal.

Vejamos o artigo 241-C do ECA:

> *Simular a participação de criança ou adolescente em cena de sexo explícito ou pornográfica por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual:*
> *(...)*
> *Parágrafo único. Incorre nas mesmas penas quem vende, expõe á venda, disponibiliza, distribui, publica ou divulga por qualquer meio, adquire, possui ou armazena o material produzido na forma do caput deste artigo.*

Este crime poderá ser cometido tendo a Internet como meio de execução, conforme o contido no parágrafo único do dispositivo legal, onde o agente ativo divulga imagens modificadas, as quais simulam cenas de sexo contendo crianças e adolescentes, de forma indevida, utilizando-se para tanto de sites, comunidades e correio eletrônico, entre outros meios, conforme previsto no caput do artigo retro.

Preceitua o artigo 241-D do ECA:

> *Aliciar, assediar, instigar ou constranger, por qualquer meio de comunicação, criança, com o fim de com ela praticar ato libidinoso:*
> *(...)*

> *Parágrafo único. Nas mesmas penas incorre quem:*
> *I – facilita ou induz o acesso à criança de material contendo cena de sexo explícito ou pornográfica com o fim de com ela praticar ato libidinoso;*
> *II – pratica as condutas descritas no caput deste artigo com o fim de induzir criança a se exibir de forma pornográfica ou sexualmente explícita.*

Tal tipificação tem como alvo o agente que se utiliza da Internet, mais precisamente salas de bate-papo, sites, MSN ou softwares semelhantes, para relacionar-se com crianças a fim de levá-las a se expor ou a praticar algum ato libidinoso.

Destaca Nucci (2009, p. 269) o seguinte ponto: Note-se que não se exige o efetivo envolvimento sexual, pois se tal ocorrer, configura-se estupro ou atentado violento ao pudor, uma vez que a violência é presumida.

Observa-se que enquanto que no caput e no inciso I o agente tem como objetivo praticar ato libidinoso com a criança, no inciso II o agente tem como objetivo principal obter imagens, vídeos ou qualquer forma de registro contendo exposição pornográfica ou sexualmente explícita, geralmente obtida por meio de uma webcam.

Por fim citamos o artigo 241-E do ECA:

> *Para efeito dos crimes previstos nesta Lei, a expressão 'cena de sexo explícito ou pornográfica' compreende qualquer situação que envolva criança ou adolescente em atividades sexuais explícitas, reais ou simuladas, ou exibição dos órgãos genitais de uma criança ou adolescente para fins primordialmente sexuais.*

Importante citar este artigo, pois ele define corretamente a expressão utilizada nos artigos anteriores, facilitando desta forma a correta interpretação e aplicação da norma penal incriminadora.

Demonstramos até este ponto alguns dos principais crimes cometidos utilizando-se da Internet, seja ela como mera ferramenta de execução ou mesmo como meio imprescindível para a perpetração do crime.

Por óbvio este rol é meramente exemplificativo, não tendo-se a pretensão de se esgotar as possíveis aplicações da legislação existente às condutas praticada na rede mundial de computadores.

2.7 Projeto de Lei 84/1999

Sem dúvida o PLC 84/1999, o qual tramita na Câmara dos Deputados, estando

atualmente sendo analisado simultaneamente por três comissões, é o projeto mais completo e em estágio mais avançado de elaboração.

Este projeto, do deputado Luiz Piauhylino, tramita na Câmara dos Deputados há praticamente doze anos, o que demonstra a morosidade com que nossos legisladores atuam perante um tema de relevante importância para a sociedade.

Existem no Congresso Nacional mais de três dezenas de projetos de lei abordando condutas praticadas na internet, porém, o projeto em questão é atualmente o que supre da melhor maneira as lacunas existentes em nossa legislação.

A princípio o projeto apresentado visava à criação de uma lei esparsa, contemplando apenas conteúdo específico à área informática e de internet, porém, após a apresentação de vários substitutivos e sofrer também o apensamento de outros projetos de lei a mesma passou a ter o cunho de modificar o atual Código Penal de 1940, demonstrando assim, que o legislador não tem a intenção de criar um Código Penal Informático, e sim trabalhar na atualização das leis em vigor, como foi o caso da recente alteração/atualização do ECA.

Torna-se difícil tecer comentários específicos sobre cada novo artigo introduzido ou modificado do Código Penal, pois o projeto de lei vem sofrendo várias mudanças nas comissões pelas quais tem passado na Câmara e no Senado, sendo que o último parecer apresentado foi o do Senador Marcelo Crivella, o qual propôs alterações bem como a inclusão de novos tipos penais ao texto.

O último texto aprovado pela Câmara dos Deputados em 2003, criava os seguintes tipos penais, cometidos contra sistemas informáticos ou por meio deles:

- ✓ acesso indevido a meio eletrônico (art. 154-A);
- ✓ manipulação indevida de informação eletrônica (art. 154-B);
- ✓ conceitos legais de “meio eletrônico” e “sistema informatizado” (art. 154-C);
- ✓ pornografia infantil (art. 218-A);
- ✓ difusão de vírus eletrônico (art. 163, §3º);
- ✓ falsificação de telefone celular ou meio de acesso a sistema informático (art. 298-A).

No parecer do senador Crivella a criação do art. 218-A é suprimida, haja vista já ter sido contemplada pela alteração do Estatuto da Criança e do Adolescente.

Além da criação dos tipos acima citados, o texto prevê a alteração de tipos existentes em nosso CP, quais sejam:

1. acrescenta a palavra "telecomunicação" no tipo penal de atentado contra a segurança de serviço de utilidade pública (art. 265 do CP);

2. e no de interrupção ou perturbação de serviço telegráfico ou telefônico (art. 266 do CP);
3. estende a definição de dano do art. 163 do CP (crime de dano), por meio da equiparação à noção de "coisa" de elementos de informática como "dados", "informação" e "senha", sob a nova rubrica do dano eletrônico (acrescentando o §2º, incs. I e II) ;
4. equipara o cartão de crédito a documento particular no tipo falsificação de documento particular, acrescentando um parágrafo único ao art. 298 do CP, sob a rubrica de falsificação de cartão de crédito;
5. permite a interceptação do fluxo de comunicações em sistema de informática ou telemática, mesmo para crimes punidos apenas com detenção, por meio do acréscimo de um §2º. ao art. 2º. da Lei 9.296, de 24 de julho de 1996 (esta regula a interceptação das comunicações telefônica, informática e telemática).

Entendendo ainda estar incompleto o texto do projeto de lei, o Senador Crivella apresentou emenda contemplando mais dois novos tipos penais, sendo eles o de “Falsidade Informática” e “Sabotagem Informática”, assim redigidos:

> ***Art. 154-C***. *Introduzir, modificar, apagar ou suprimir dado ou sistema informatizado, ou, de qualquer forma, interferir no tratamento informático de dados, com o fim de obter, para si ou para outrem, vantagem indevida de qualquer natureza, induzindo a erro os usuários ou destinatários.*
> *Pena - detenção, de um a dois anos, e multa.*
> ***Parágrafo único***. *Nas mesmas incorre quem, com a mesma finalidade, cria, disponibiliza ou divulga comunicação eletrônica falsa.*
>
> ***Art. 154-D***. *Introduzir, modificar, apagar ou suprimir dado ou sistema informatizado, ou, de qualquer forma, interferir em sistema informatizado, com o fim de desorientar, embaraçar, dificultar ou obstar o funcionamento de um sistema informatizado ou de comunicação de dados à distância.*
> *Pena - detenção, de um a dois anos, e multa."*

Segundo Reinaldo Filho (2010), o artigo 154-C tem o objetivo de combater toda espécie de fraude informática, como por exemplo a criação de páginas falsas a fim de se obter dados de clientes de bancos, ou e-mails contendo programas denominados keylogger, os quais registram tudo que é digitado pela vítima em seu computador e após encaminha por e-mail para o agente criminoso sem o conhecimento da vítima.

Já o art. 154-D tem a função de evitar sabotagens ao funcionamento de computadores

e redes, onde, por exemplo, o agente criminoso pode enviar milhares de pacotes de dados para o computador vítima, tornando desta forma sua conexão lenta e ineficiente, impedindo assim que a vítima usufrua determinado serviço, este método é chamado de DoS (denial – of – service).

Outro ponto importante a ser abordado no projeto em questão é a imposição aos provedores de acesso para que mantenham a vigilância sobre os usuários conectados ao mesmo, devendo informar as autoridades qualquer suspeita de crime. Obviamente a redação do texto será suprimida ou alterada, como já solicitado pelo Senador Crivella, bem como pelo Senador Julio Semeghini, pois não se pode transferir para o particular a obrigação do estado neste sentido, devendo ainda ser respeitada a privacidade dos usuários, não sendo cabível este tipo de vigilância constante.

Ainda em relação aos provedores deverá ser incluído no texto, conforme o Senador Crivella, a obrigatoriedade de todos os provedores de internet armazenarem os registros de movimentação de seus usuários (logs) por um período mínimo de três (03) anos, medida esta imprescindível para viabilizar a investigação dos crimes praticados na internet.

Podemos observar que o projeto de lei em questão tem causado muitas discussões quanto à tipificação dos crimes informáticos, porém não há justificativa para que se leve quase doze anos para a elaboração de um texto de lei que venha a satisfazer os anseios sociais, haja vista a importância do tema abordado.

Na análise dos principais pontos do texto provisório vemos ainda que ele representa sim uma evolução legislativa face às leis em vigor, demonstrando que é possível se produzir as alterações necessárias em nosso Código Penal e leis esparsas já existentes a fim de coibir crimes praticados na internet, sendo que a alteração das leis parece ser o modelo adotado por nossos legisladores em prejuízo à uma lei específica para crimes informáticos.

CAPÍTULO III - ASPECTOS PROCESSUAIS PENAIS

Analisaremos neste capítulo quais são as principais dificuldades encontradas pelos operadores do direito para investigar, processar e consequentemente punir os criminosos que atuam no meio virtual ou se utilizam deste como ferramenta para perpetração de crimes.

Neste contexto daremos ênfase às principais ferramentas disponíveis hoje em nosso sistema processual bem como suas principais falhas, as quais prejudicam e por vezes inviabilizam a persecução criminal.

3.1 Investigação

Geralmente realizada na fase pré-processual, sendo esta atribuição da polícia judiciária, seja ela representada pela Polícia Civil dos Estados ou pela Polícia Federal, é de suma importância a fim de se combater os crimes informáticos, sendo que com o advento da Informática e a evolução em escala geométrica da Tecnologia da Informação, a metodologia de investigação criminal vem sendo alterada e atualizada com freqüência a fim de se acompanhar a evolução do criminoso virtual.

Com o intuito de tornar possível essa evolução a polícia judiciária vem criando núcleos especializados em combater o crime informático, adotando para tanto a atualização e capacitação de policiais em Tecnologia da Informação e gestão do conhecimento.

Como vimos no capítulo I o computador evoluiu, e evolui, rapidamente tornando-se uma ferramenta essencial no processo de gestão do conhecimento, tornando possível e comum a qualquer indivíduo ter acesso e processar uma quantidade considerável de volumes de dados.

Neste sentido de forma precisa dissertam Ferro Junior & Dantas (2006):

> *Em um exemplo mais recente e genérico, o complexo cultural da moderna TI possibilitou a interação humana virtual, face-a-face (com som e imagem), em um "ambiente de rede mundial" (Internet), capaz de unir e integrar indivíduos antes completamente separados pelas grandes distâncias da Terra. A efetividade e a rapidez das comunicações globais, fruto dos modernos sistemas de transporte aéreo e da telemática, forma fundamentais nesse processo, contribuindo para que a humanidade, antes dispersa e fragmentada, passasse a viver o fenômeno da chamada globalização ou transnacionalização. Isso atingiu também o crime, fazendo com que ele passasse a ter novas e múltiplas expressões e possibilidades.*

As duas principais dificuldades que encontraremos nesta fase de investigação serão ocasionadas pela citada globalização ou transnacionalização, pois como veremos adiante isto influirá diretamente nas questões de jurisdição e fixação da competência para se processar tais crimes, bem como a questão da prova em si e sua obtenção por parte dos investigadores, sendo este um árduo caminho, devido à lentidão dos mecanismos processuais disponíveis em nossa legislação.

Sobre essa lentidão processual temos o comentário de Ferro Junior & Dantas (2006):

> *Uma das características adversas deste novo cenário é o fato da legislação não disponibilizar instrumentos ágeis e velozes de acesso das organizações policiais à informação, em uma decorrência da aplicação de princípios jurídicos obsoletos, mormente em sua referência à competência jurisdicional e administrativa das polícias investigativas, tanto da União quanto dos entes federativos.*

Assim, todo o processo de investigação tem como principal finalidade a obtenção da prova, de forma lícita, possibilitando de maneira precisa a atuação dos mecanismos de persecução criminal.

3.1.1 Da Prova

Como já exposto, um dos principais obstáculos para o processamento e punição dos criminosos informáticos é a obtenção da prova, essa dificuldade está caracterizada não somente pelos meios técnicos, mas também pelo modelo processual vigente em nosso Estado.

Antes de abordar propriamente os meios de obtenção de prova e suas peculiaridades veremos o que é Prova, sua classificação e características.

A Prova é conceituada por Greco Filho (2006, p. 196) da seguinte forma:

> *No processo a prova é todo meio destinado a convencer o juiz a respeito da verdade de uma situação de fato. A palavra "prova" é originária do latim probatio, que por sua vez emana do verbo probare, com o significado de examinar, persuadir, demonstrar.*

Podemos extrair de tal conceito a certeza de que a finalidade da prova é o convencimento do juiz, sendo que a mesma está destinada ao magistrado, assim a prova deverá sempre ser obtida por meios idôneos, adequados e formalmente corretos.

Neste sentido o artigo 155 do Código de Processo Penal preceitua:

> *O juiz formará sua convicção pela livre apreciação da prova produzida em contraditório judicial, não podendo fundamentar sua decisão exclusivamente nos elementos informativos colhidos na*

> *investigação, ressalvadas as provas cautelares, não repetíveis e antecipadas.*
> *(...)*

Como depreende-se do caput do artigo o sistema processual penal brasileiro adotou o método misto de avaliação da prova, ou seja, a persuasão racional, onde o juiz deverá decidir a causa de acordo com seu livre convencimento, porém deverá fundamentá-lo nos autos, procurando desta forma persuadir as partes envolvidas bem como a comunidade. Este conceito encontra guarida em nossa Carta Magna, mais precisamente no artigo 93, IX.

Temos que observar que o referido artigo 155 faz uma ressalva quanto às provas produzidas em sede investigatória, assim devemos destacar que na investigação, mais precisamente na fase pré-processual, o inquérito policial é considerado sigiloso por natureza e não admite o contraditório, assim muitas das provas produzidas poderão ser contraditadas na fase processual, desta forma o magistrado não poderá tomá-las de forma única para a formação de seu livre convencimento, devendo para tanto, sempre que possível, confirmá-las em juízo.

As provas cautelares citadas no artigo são aquelas urgentes, as quais deverão ser produzidas de forma imediata sob pena de se perderem, enquanto que as não repetíveis são aqueles baseadas em exames periciais, e por fim as antecipadas, por exemplo a oitiva de uma testemunha, porém sendo possível sua repetição.

Tudo o que se deseja examinar, demonstrar, persuadir, auxiliar na formação do convencimento do juiz trata-se de objeto da prova, sendo que sobre o tema mais precisamente discorre Mirabete (2006, p. 250):

> *Objeto da prova é o que se deve demonstrar, ou seja, aquilo sobre o que o juiz deve adquirir o conhecimento necessário para resolver o litígio. Abrange, portanto, não só o fato criminoso e sua autoria, como todas as circunstâncias objetivas que possam influir na responsabilidade penal e na fixação da pena ou na imposição de medida de segurança.*

Quanto ao objeto, Mirabete (2006, p. 251) classifica a prova de duas maneiras, a **direta**, quando por si demonstra o fato, quando dá a certeza deles por testemunhas, documentos, etc., bem como a **indireta**, quando, comprovado um outro fato, se permite concluir o alegado diante de sua ligação com o primeiro, como na hipótese de um álibi, em que a presença comprovada do acusado em lugar diverso do crime permite concluir que não praticou o ilícito.

Seguindo com a classificação, Mirabete (2006, p. 251) ainda define que a prova, em

razão de seu **efeito** ou **valor** pode ser **plena**, completa, convincente (exigida, p. ex., para a condenação), ou **não plena**, uma probabilidade de procedência da alegação (suficiente para medidas preliminares, como arresto, sequestro, prisão preventiva, apreensão, etc).

Por fim, para Mirabete (2006, p. 252), as provas podem ser reais ou pessoais, sendo **reais** as provas que consistem em uma coisa ou bem exterior e distintas do indivíduo (a arma, o lugar do crime, o cadáver, as pegadas, as impressões digitais etc), e as **pessoais** as que exprimem o conhecimento subjetivo e pessoal atribuído a alguém: o interrogatório, os depoimentos, as conclusões dos peritos etc.

Outro ponto a se destacar, este de suma importância para nosso estudo, trata-se dos meios de prova. Nucci (2008, p. 342), de forma breve, utiliza-se da seguinte definição:

> *Meios de prova: são todos os recursos, diretos ou indiretos, utilizados para alcançar a verdade dos fatos no processo. (...) Os meios de prova podem ser lícitos – que são admitidos pelo ordenamento jurídico – ou ilícitos – contrários ao ordenamento.*

Por óbvio somente os meios lícitos poderão ser acatados pelo juiz, pois torna-se inadmissível qualquer prova obtida por meio ilícito ou mesmo imoral, antiético ou atentatório aos princípios constitucionais da dignidade da pessoa humana ou contrários aos bons costumes.

Os principais meios de prova estão elencados do Código de Processo Penal, disposto da seguinte forma:

- ✓ Do exame do corpo de delito, e das perícias em geral (artigos 158 a 184, CPC);
- ✓ Do interrogatório do acusado (artigos 185 a 196, CPC);
- ✓ Da confissão (artigos 197 a 200, CPC);
- ✓ Do ofendido (artigo 201 do CPC);
- ✓ Das testemunhas (artigos 202 a 225 do CPC);
- ✓ Do reconhecimento de pessoas e coisas (artigos 226 a 228 do CPC);
- ✓ Da acareação (artigos 229 e 230 do CPC);
- ✓ Dos documentos (artigos 231 a 238 do CPC);

O rol elencado não é taxativo, ou seja, não se excluirá nenhum outro meio de prova desde que, como já exposto, seja lícito e respeite os princípios constitucionais.

Quanto ao último meio de prova citado, dos documentos, cabe-nos fazer uma abordagem um pouco mais ampla devido ao surgimento do documento eletrônico, ou como também denominado, o cyberdocumento.

3.1.1.1 Documento eletrônico

Com o surgimento da informática e principalmente da internet o processo de transferência de dados e informações acelerou-se em uma velocidade espantosa, tornando muito mais eficiente a troca dessas informações e posteriormente a transferência de documentos, vindo a surgir então o documento eletrônico.

Existem inúmeros conceitos de *documento*, porém nenhum desses conceitos previu o surgimento do documento eletrônico, pois todos se fundam, ou fazem referência ao meio físico, palpável, o qual dá suporte ao registro da informação, porém isto não ocorre com o documento eletrônico, haja vista o meio eletrônico estar desvinculado de uma forma física rígida, como o papel por exemplo.

De acordo com Ferreira (1996, p. 605) podemos definir *documento* da seguinte forma:

> *1 Qualquer base de conhecimento, fixada naturalmente e disposta de maneira que se possa utilizar para consulta, estudo, prova etc. 2 Escritura destinada a comprovar um fato; declaração escrita, revestida de forma padronizada, sobre fato(s) ou acontecimento(s) de natureza jurídica.*

Vemos que tal conceito faz referência a *escritura* e *declaração escrita*, formas essas que limitam o conceito de *documento*. Marques (1967, P. 307) define documento como *a prova histórica real, visto que representa fatos e acontecimentos pretéritos em um objeto físico, servindo assim de instrumento de convicção.*

Tal definição também se prende ao modelo físico de conceito, não prevendo o surgimento de novas tecnologias.

Sobre tais conceitos de forma clara se manifesta Marques (2008, p. 123):

> *Partindo, então, dos conceitos construídos pelos doutrinadores supramencionados, verifica-se que há uma atribuição especial em procurar registrar o suporte físico como elemento marcante, chegando a ponto de alguns deles terem asseverado que o suporte utilizado para a materialização do documento garantirá o grau de fidelidade em relação ao que o autor quis representar.*

Desta forma verifica-se a necessidade de uma atualização no conceito de *documento*, a fim de que este possa de forma precisa abarcar a compreensão de documento eletrônico e suas infinitas formas de armazenamento e transmissão. Neste sentido discorre Marcacini (2002, p. 05) apud Marques (2008, p. 126):

> *a característica marcante do documento, é lícito dizer que, na medida em que a técnica evoluiu permitindo registro permanente dos fatos sem fixá-lo de modo inseparável em alguma coisa corpórea, tal registro também pode ser considerado documento. A tradicional definição de documento enquanto coisa é justificada pela impossibilidade, até então, de registrar fatos de outro modo, que não apegado de modo inseparável a algo tangível.*
> *Assim, renovando o conceito de documento – e até retornando à origem do vocábulo –* ***documento é o registro de um fato.*** *Se a técnica atual, mediante o uso da criptografia assimétrica, permite registro inalterável de um fato em meio eletrônico, a isto também podemos chamar de documento.*

Podemos ver que inquestionavelmente a informática vem mudando os conceitos jurídicos, até mesmo os considerados imutáveis até há pouco tempo, apesar de não termos ainda um conceito sedimentado de documento, os doutrinadores admitem e se esforçam na tentativa de definir um conceito que aborde e englobe todos os meios tecnológicos existentes, e até futuros, pois todos esses meios influenciarão de modo decisivo no elemento denominado prova e em sua obtenção.

3.1.2 Obtenção da prova

Como vimos no tópico retro são vários os meios de prova admitidos no direito pátrio, porém, em se tratando de crimes informáticos cometidos na internet, ou utilizando-se desta como ferramenta, o investigador dependerá a princípio da utilização da tecnologia, principalmente domínio do conhecimento técnico sobre o funcionamento da internet e redes de computadores, para identificar e localizar o delinqüente informático.

O fato criminoso poderá chegar ao conhecimento do investigador por meio de denúncia, da própria vítima ou mesmo de entidades civis como a SAFERNET, bem como pelo monitoramento da rede mundial de computadores, mais especificamente sites e usuários que atuam no Brasil.

A princípio, como veremos adiante, fatos contendo elementos de transnacionalidade ou interestadualidade, serão apurados no âmbito da Justiça Federal, bem como serão investigados pela Polícia Federal.

Dada a importância do tema, o Departamento de Polícia Federal criou um grupo especial de trabalho a fim de apurar os crimes cybernéticos, principalmente no que tange aos crimes de ódio e pornografia infantil na internet, este denominado GECOP, sediados em Brasília/DF.

O primeiro passo quando do recebimento de uma denúncia por parte do investigador será a identificação do local onde o acesso foi realizado por parte do agente criminoso, a fim de identificar a quem pertence à atribuição para instaurar o procedimento.

Existem ferramentas disponíveis na própria internet a fim de se iniciar o processo de identificação do responsável pela conduta criminosa, conhecidas como ferramentas de *WHOIS,* sendo no Brasil a mais utilizada o http://registro.br, poderá o investigador, por meio do endereço IP do agente criminoso, obter informações sobre qual provedor de acesso ou serviço está hospedando-o, dados cadastrais de tal provedor, podendo desta forma obter junto a referidos provedores a identificação do proprietário do site, ou identificação do usuário que acessou determinado serviço na rede, devendo o provedor informar a qualificação completa do mesmo, endereço e telefone, ou seja, todas as informações necessárias para se chegar ao agente criminoso.

Há entendimento jurisprudencial de que a Autoridade Policial não necessita de autorização judicial para requisitar às empresas provedoras de acesso ou serviços informações sobre os dados cadastrais de seus usuários, pois tais informações não estariam acobertadas pelo sigilo constitucional, estando a Autoridade Policial amparada pelo artigo 5º, IV da CF/88, bem como do artigo 6º, III do CPP.

Porém, mesmo com vários entendimentos jurisprudenciais neste sentido, algumas empresas se negam a fornecer tais informações, assim, deverá a Autoridade Policial, haja vista a necessidade de se chegar ao agente criminoso no menor tempo possível, a fim de se preservar as provas possivelmente contidas em seu computador, representar pela quebra de sigilo de dados e telemática em relação ao possuidor do registro IP em questão, alertando que um mesmo indivíduo poderá possuir vários acessos em datas, horários e time zones diferentes, registrando-se assim vários IP's diferentes, ou seja, um para cada acesso.

Deferida a quebra de sigilo o Juiz deverá impor um prazo, bem como pena de multa, para que a empresa cumpra com a solicitação da Autoridade Policial, mantendo o sigilo absoluto sobre tal investigação.

A provedora de acesso a internet obterá a informação do endereço IP do agente criminoso por meio dos log's de acesso e conexão mantidos pela própria empresa, porém ainda não há lei pátria que determine o período mínimo de manutenção dos referidos log's por parte destas empresas, assim, poderá ocorrer que tal informação já se perdera, levando o agente criminoso a permanecer impune.

Com relação aos log's, a fim de minimizar os prejuízos às investigações presentes e futuras, firmou-se um Termo de Compromisso de Integração onde os provedores, por

solicitação da Polícia Federal, bem como do Ministério Público Federal se comprometeram a preservar e armazenar, pelo prazo mínino de seis meses, todos os registros de logs de acesso e IP's originários dos usuários dos serviços de Internet.

Vale ressaltar que toda e qualquer representação pela quebra de sigilo em relação aos dados cadastrais e telemáticos de usuários da internet, seja acesso por meio telefônico ou mesmo ADSL, terá como suporte a Lei nº 9.296/96.

Neste ponto temos que ressaltar a dificuldade caso o provedor de acesso ou o usuário investigado estiver sediado no exterior, sendo que vem se adotando o procedimento no sentido de solicitar a cooperação policial internacional, por meio da INTERPOL, a fim de obter as informações necessárias bem como viabilizar a persecução penal.

O Brasil vem enfrentando dificuldades em aderir a tratados internacionais que visam o combate aos cybercrimes pois nossa legislação não contempla de forma específica todas as formas de crimes perpetrados no âmbito da grande rede mundial de computadores.

Temos em andamento no Congresso Nacional, como já abordado no tópico 2.7, um bom projeto de lei que atualizaria nosso antigo Código Penal, facilitando assim nossa adesão a tratados de cooperação internacional.

Outro passo importante para a obtenção da prova do crime informático é, após a confirmação dos dados cadastrais e comprovação de que referido IP foi utilizado por um usuário durante a prática de ato criminoso, a confirmação, por parte do investigador, se referidos dados fornecidos pela provedora de acesso realmente pertencem ao indivíduo apontado. Este passo é importante a fim de subsidiar a representação pelo Mandado de Busca e Apreensão, com o qual possivelmente se obterá a prova cabal em face do agente criminoso.

Porém, neste ponto pode surgir nova dificuldade, pois a diligência de confirmação dos dados do detentor do IP a ele atribuído pode levar o investigador a uma grande empresa ou mesmo a uma Lan House, o que em muitos casos torna impossível a identificação do usuário de referida máquina no momento do cometimento do ato criminoso.

Alguns passos importantes poderão ser executados pelo investigador a fim de se identificar o usuário de determinado terminal de computador nesses casos:

- ✓ Análise meticulosa dos log's fornecidos pela provedora, principalmente no que tange aos horários de acesso a Internet para cometimento do ilícito;
- ✓ Realização de oitiva dos responsáveis pela empresa a fim de identificar os possíveis usuários do computador no horário do delito;

- ✓ Verificar a existência de sistemas de controle de acesso aos computadores da empresa, ou seja, monitoramento eletrônico, de vídeo ou biométrico, facilitando desta forma a identificação do criminoso;
- ✓ Deve se ressaltar que os Estados de São Paulo e Mato Grosso do Sul possuem legislação específica quanto ao registro de usuários de computadores em relação a empresas denominadas Lan House ou similares, portanto nesses Estados tal registro é obrigatório e seus responsáveis responderão diretamente pelo descumprimento da lei.

Ao representar pelo Mandado de Busca e Apreensão a Autoridade Policial, ou até mesmo o representante do Ministério Público devem solicitar de forma específica a autorização para a apreensão de HD's, CD's, DVD's, máquinas fotográficas digitais ou qualquer meio potencial de armazenamento de arquivos ou imagens, bem como qualquer documentação que possa comprovar os fatos investigados e garantir o acesso dos investigadores ao conteúdo de quaisquer bancos de dados arrecadados na diligência de busca, devendo amparar tal autorização na Lei 9.034/95.

3.1.3 Prisão em Flagrante

Ainda abordando os aspectos inerentes à obtenção da prova não podemos deixar de abordar a questão da prisão em flagrante nos crimes informáticos, mais precisamente os cometidos pela Internet.

Nos crimes em tela a maioria dos agentes criminosos, bem como as demais pessoas, tem como certa a impossibilidade de serem surpreendidos no momento do cometimento do crime, e por este motivo, ou seja, a falsa certeza de impunidade, acabam por cometer atos criminosos de maneira reiterada e descuidada, vindo a facilitar sua identificação.

Obviamente que surpreender um indivíduo em situação flagrancial, na maioria desses crimes, é tarefa quase impossível, contudo com as mudanças legislativas que vem ocorrendo, bem como as que acreditamos estarem por ocorrer em um breve termo, o número de prisões em flagrante tem aumentado consideravelmente. Para perceber tal fato é só nos atentarmos para os noticiários e vermos as operações deflagradas pela Polícia Federal, como por exemplo a denominada "TAPETE PERSA", relacionada aos crimes de pornografia infantil por indivíduos denominados "pedófilos", onde foram presos onze indivíduos em oitos Estados.

Mas como chegar ao criminoso e efetuar sua prisão em flagrante? Esse é o grande

desafio do investigador, porém, no caso em comento, a mudança ocorrida no ECA, mais precisamente a introdução do artigo 241-B, o qual prevê que o armazenamento, ou seja, a posse de material com conteúdo pornográfico infantil por si só configura crime, vem possibilitando a prisão dos agentes criminosos.

Desta forma, durante o cumprimento do Mandado de Busca e Apreensão os investigadores, geralmente a Polícia, têm como integrante da equipe um perito especialista na área de informática e internet, o qual será o responsável em identificar, uma parcela que seja, do material com conteúdo criminoso o qual dará subsídio à prisão em flagrante do indivíduo.

Por fim, outro ponto importante a salientar é que o armazenamento do conteúdo ilícito não se dará somente nos meios físicos já citados, como HD, CD, DVD e etc, este também poderá ocorrer, e hoje já está difundido entre os Internautas, dentro da grande "NUVEM DA INTERNET", ou seja, tais arquivos poderão estar hospedados em um servidor ou mesmo uma máquina de terceira pessoa, onde somente o agente criminoso terá acesso por meio de um login e senha, desta forma, comprovada a propriedade do login e senha em relação ao agente criminoso, aspecto esse de difícil vinculação, mas não impossível, poderá também ser realizada a prisão em flagrante.

3.2 Provedores de Internet

Como já exposto anteriormente os provedores de Internet, sejam eles provedores de acesso, conteúdo ou serviços outros, são empresas prestadoras de serviços e respondem por seus atos como qualquer outra empresa.

Ocorre que a rede mundial de computadores possui aspectos únicos, levando desta forma essas prestadoras de serviços a ter problemas de cunho criminal e civil perante a sociedade, pois até pouco tempo não havia leis que regulamentassem a conduta de tais provedores, bem como o próprio entendimento jurisprudencial não ter uniformidade.

O que vinha ocorrendo até então era o fato de que indivíduos estavam se utilizando da internet para cometer crimes diversos, como por exemplo, os crimes contra honra, onde se divulgavam fotos de determinada pessoa ou expunham fatos não condizentes com a realidade, com o objetivo de denegrir imagem desta pessoa perante a sociedade.

Estes fatos vieram a gerar uma enormidade de ações penais e civis por danos morais contra as empresas provedoras de internet, onde alegava-se que tais provedoras teriam o dever de fiscalizar e coibir tais condutas criminosas.

Porém devido ao inimaginável fluxo de informações que circulam diariamente pelos

provedores tal tarefa torna-se impossível, vejamos precisa explanação de Correa (2008, p. 108) sobre este ponto:

> *Também, é impossível a fiscalização de todas as informações que entram e saem de um provedor, pois, além de servir seus usuários, também serve de "pista" para a Internet. Assim, um infindável número de informações, como e-mails, homepages, listas de discussões, chats, é atualizado instantaneamente por meio de procedimentos eletrônicos automáticos, sobre os quais o provedor não tem nenhum controle.*

Este entendimento vem se consolidando em nossos tribunais, pois não podemos responsabilizar quem não deu causa a tal fato, bem como é o entendimento de nossos legisladores, o que ficou claro com o advento da Lei 11.829/2008, mais precisamente a inclusão do §2º do Artigo 241-A, o qual prevê:

> *As condutas tipificadas nos incisos I e II do §1º deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo.*

Como vemos o legislador criou um mecanismo para garantir a retirada do conteúdo ilícito da Internet, tornando obrigatório aos provedores, depois de notificados, a exclusão do conteúdo, pois se não o fizerem também poderão responder pelo crime perpetrado, pois o provedor estaria conscientemente, de forma intencional, armazenando e veiculando conteúdo impróprio em seus servidores, crimes esses previstos no diploma legal em tela.

3.3 Da Competência

Sem dúvida, uma das maiores dificuldades existentes em relação aos crimes praticados na Internet é a definição quanto a quem pertence à atribuição de investigar, bem como a competência para processar e julgar tais crimes.

Sendo a Internet a personificação máxima da globalização, um usuário conectado no Brasil poderá praticar um crime tendo como vítima uma pessoa em outro país, em qualquer local do globo terrestre, desta forma, como se dará a fixação da competência?

Em respeito a normas e tratados internacionais, bem como à própria soberania dos Estados, o Brasil somente poderá investigar e punir condutas criminosas praticadas dentro de seu território, mesmo que seu resultado tenha se dado fora deste, observando-se assim o Princípio da Territorialidade.

Tal princípio está explícito no artigo 5º do Código Penal:

> ***Art. 5º*** *- Aplica-se a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido no território nacional.*
> *§ 1º - Para os efeitos penais, consideram-se como extensão do território nacional as embarcações e aeronaves brasileiras, de natureza pública ou a serviço do governo brasileiro onde quer que se encontrem, bem como as aeronaves e as embarcações brasileiras, mercantes ou de propriedade privada, que se achem, respectivamente, no espaço aéreo correspondente ou em alto-mar.*
> *§ 2º - É também aplicável a lei brasileira aos crimes praticados a bordo de aeronaves ou embarcações estrangeiras de propriedade privada, achando-se aquelas em pouso no território nacional ou em vôo no espaço aéreo correspondente, e estas em porto ou mar territorial do Brasil.*

O legislador adotou como regra a Teoria da Ubiguidade, considerando o lugar do crime sendo aquele em que se realizou qualquer parte do iter criminis, porém no caso dos crimes informáticos o iter criminis pode se desenrolar em locais diversos.

Assim, temos que diferenciar os delitos plurilocais dos crimes à distância, pois o primeiro se caracteriza por se desenvolverem em diferentes lugares, mas sempre dentro do território nacional, enquanto que o segundo se desenvolvem em diferentes países, ou seja, os atos executórios e o resultado se dão em países diferentes.

Desta forma, quando se tratarem de crimes plurilocais aplicaremos o artigo 6º do Código Penal, sendo que nos crimes à distância a competência será definida pela aplicação do artigo 70 e seus parágrafos, do CPP, o qual aduz:

> *Art. 70. A competência será, de regra, determinada pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução.*
> *§ 1º Se, iniciada a execução no território nacional, a infração se consumar fora dele, a competência será determinada pelo lugar em que tiver sido praticado, no Brasil, o último ato de execução.*
> *§ 2º Quando o último ato de execução for praticado fora do território nacional, será competente o juiz do lugar em que o crime, embora parcialmente, tenha produzido ou devia produzir seu resultado.*
> *§ 3º Quando incerto o limite territorial entre duas ou mais jurisdições, ou quando incerta a jurisdição por ter sido a infração consumada ou tentada nas divisas de duas ou mais jurisdições, a competência firmar-se-á pela prevenção.*

Fica claro que nos crimes à distância praticados no Brasil e que tenha seu resultado consumado em outro país, a competência pertencerá ao Juízo do local onde foi praticado o último ato de execução por parte do agente ativo, independentemente deste ser brasileiro ou

estrangeiro.

Mas ainda podemos nos deparar com outra circunstância, ou seja, aquela em que o agente ativo pratica os atos executórios em outro país e o resultado se consuma em território brasileiro.

Neste caso deveremos aplicar o preceito contido no artigo 88 do Código de Processo Penal:

> *Art. 88. No processo por crimes praticados fora do território brasileiro, será competente o juízo da Capital do Estado onde houver por último residido o acusado. Se este nunca tiver residido no Brasil, será competente o juízo da Capital da República.*

Assim, se praticado por brasileiro ou já residente no Brasil, o crime informático será processado pelo Juízo da Capital do Estado onde o agente por último residiu, em sendo este estrangeiro e nunca residido no Brasil, o mesmo será processado pelo Juízo da Capital da República.

Ainda deverão ser observados, quando da fixação da competência os casos especificamente previstos no artigo 7º do Código Penal, destacando-se o inciso I, alínea b de tal instituto:

> ***Art. 7º -*** *Ficam sujeitos à lei brasileira, embora cometidos no estrangeiro:*
> *I - os crimes:*
> *(...)*
> ***b) contra o patrimônio ou a fé pública da União, do Distrito Federal, de Estado, de Território, de Município, de empresa pública, sociedade de economia mista, autarquia ou fundação instituída pelo Poder Público;***
> *(...)*
> *II - os crimes:*
> *(...)*
> ***b) praticados por brasileiro;***
> *(...)*
> *§ 1º - Nos casos do inciso I, o agente é punido segundo a lei brasileira, ainda que absolvido ou condenado no estrangeiro.*
> *§ 2º - Nos casos do inciso II, a aplicação da lei brasileira depende do concurso das seguintes condições:*
> *a) entrar o agente no território nacional;*
> *b) ser o fato punível também no país em que foi praticado;*
> *c) estar o crime incluído entre aqueles pelos quais a lei brasileira autoriza a extradição;*
> *d) não ter sido o agente absolvido no estrangeiro ou não ter aí cumprido a pena;*
> *e) não ter sido o agente perdoado no estrangeiro ou, por outro motivo, não estar extinta a punibilidade, segundo a lei mais favorável.*

> *§ 3º - A lei brasileira aplica-se também ao crime cometido por estrangeiro contra brasileiro fora do Brasil, se, reunidas as condições previstas no parágrafo anterior:*
> *a) não foi pedida ou foi negada a extradição;*
> *b) houve requisição do Ministro da Justiça.*

Vemos que apesar da questão da extraterritorialidade ser complexa, a legislação nacional está suficientemente completa a fim de amparar as necessidades decorrentes dos crimes informáticos, podendo-se desta forma fixar com precisão a competência para processamento e julgamento de tais atos.

CONSIDERAÇÕES FINAIS

Objetivamos com o presente trabalho abordar de forma geral os principais problemas enfrentados pelos operadores do Direito em face aos ilícitos praticados na Internet e por meio desta, utilizando-se de métodos de pesquisa atuais procuramos responder aos questionamentos gerados pela rápida evolução tecnológica associada à morosidade do legislador brasileiro.

Ficou claramente demonstrado que nossas leis possuem mecanismos eficientes para coibir e punir crimes virtuais, porém essas leis não evoluem na velocidade necessária para se combater a evolução dos crimes virtuais, haja vista nosso sistema legislativo ser lento e excessivamente burocrático.

No que pese as dificuldades apresentadas pela evolução tecnológica, ainda é possível na quase totalidade dos casos, punir os criminosos da internet com as leis que possuímos hoje, haja vista as condutas praticadas se adequarem facilmente aos tipos penais existentes.

Como vemos, os países, de forma geral, não estão preparados juridicamente para a evolução das TI's, mais isso se dá mais pelo fato dos operadores do direito desconhecerem o funcionamento das Tecnologias da Informação, do que propriamente pelo fato de não existirem leis que coíbam tais condutas.

Como abordamos no terceiro capítulo, as ferramentas de investigação estão evoluindo rapidamente na tentativa de acompanhar o processo de evolução tecnológica, sendo que as técnicas de combate ao crime informático dependem muito mais do estudo da tecnologia por parte do investigador do que propriamente da criação de novas maneiras para se investigar.

Desta forma, em relação aos principais questionamentos abordados durante o presente trabalho, podemos afirmar que existem soluções satisfatórias em nosso sistema jurídico e investigativo atual para sanar os problemas encontrados, dando, desta forma, todo o suporte necessário para o efetivo combate às condutas criminosas na Internet.

REFERÊNCIAS

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**: promulgada em 5 de outubro de 1988. Vade Mecum. 7ª Ed. São Paulo: Saraiva, 2009. 70p.

_____. **Código Penal**. Vade Mecum. 7ª Ed. São Paulo: Saraiva, 2009. 563p.

_____. Lei nº 8.069, de 13 de julho de 1990. **Estatuto da Criança e do Adolescente**. Vade Mecum. 7ª Ed. São Paulo: Saraiva, 2009. 1063 p.

CAPEZ, Fernando. **Curso de direito penal, volume 1: parte geral (arts. 1º a 120).** 9ª ed. rev. e atual. – São Paulo: Saraiva. 2005.

CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. 4ª Ed. rev. e atualizada. São Paulo: Saraiva, 2008.

COSTA, Marco Aurélio Rodrigues da. **Crimes de Informática**. Jus Navigandi, Teresina, ano 1, n. 12, maio 1997. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=1826>. Acesso em: 24 maio 2010.

CRACKER. In: WIKIPÉDIA, a enciclopédia livre. Flórida: Wikimedia Foundation, 2010. Disponível em: <http://pt.wikipedia.org/w/index.php?title=Cracker&oldid=18567791>. Acesso em: 26 abr. 2010.

ENDEREÇO IP. In: WIKIPÉDIA, a enciclopédia livre. Flórida: Wikimedia Foundation, 2010. Disponível em: <http://pt.wikipedia.org/w/index.php?title=Endere%C3%A7o_IP&oldid=19678199>. Acesso em: 23 abr. 2010.

ENDEREÇO MAC. In: WIKIPÉDIA, a enciclopédia livre. Flórida: Wikimedia Foundation, 2010. Disponível em: <http://pt.wikipedia.org/w/index.php?title=Endere%C3%A7o_MAC&oldid=19388277>. Acesso em: 23 abr. 2010.

FERREIRA, Érica Lourenço de Lima. **Internet – macrocriminalidade e jurisdição internacional**. Curitiba: Juruá, 2008.

HACKER. In: WIKIPÉDIA, a enciclopédia livre. Flórida: Wikimedia Foundation, 2010. Disponível em: <http://pt.wikipedia.org/w/index.php?title=Hacker&oldid=19819765>. Acesso em: 23 abr. 2010.

INELLAS, Gabriel Cesar Zaccaria de. **CRIMES NA INTERNET**. 2ª Ed. Atualizada e ampliada. São Paulo: Editora Juarez de Oliveira, 2009. 69 p.

LOG DE DADOS. In: WIKIPÉDIA, a enciclopédia livre. Flórida: Wikimedia Foundation, 2010. Disponível em: <http://pt.wikipedia.org/w/index.php?title=Log_de_dados&oldid=19548526>. Acesso em: 23 abr. 2010.

LUCCA, Newton de e SIMÃO FILHO, Adalberto, (coordenadores) e outros. **Direito & Internet: aspectos jurídicos relevantes.** Bauru, SP: Edipro, 2000.

MARQUES, Antonio Terêncio G. L. **A prova documental na internet.** 1ª Ed. (ano 2005). / 3ª reimpr. / Curitiba: Juruá, 2008.

MIRABETE, Julio Fabbrini. **Manual de direito penal**. - 21 ed. – São Paulo: Atlas, 2004.

PINHEIRO, Reginaldo César. **Os cybercrimes na esfera jurídica brasileira**. **Jus Navigandi**, Teresina, ano 4, n. 44, ago. 2000. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=1830>. Acesso em: 24 maio 2010.

PROTOCOLO DE INTERNET. In: WIKIPÉDIA, a enciclopédia livre. Flórida: Wikimedia Foundation, 2010. Disponível em: <http://pt.wikipedia.org/w/index.php?title=Protocolo_de_Internet&oldid=19779574>. Acesso em: 23 abr. 2010.

REINALDO FILHO, Demócrito. ***O Projeto de Lei sobre Crimes Tecnológicos (PL 84/99) - Notas ao parecer do Senador Marcelo Crivella***. Boletim Jurídico, Uberaba/MG, a. 2, no 79. Disponível em: <http://www.boletimjuridico.com.br/ doutrina/texto.asp?id=280> Acesso em: 7 jun. 2010.

SANTORO FILHO, Antonio Carlos. **Teoria do tipo penal**. Leme, SP: Ed. de Direito. 2001.

SILVA, José Afonso. **Curso de direito constitucional positivo**. 28 ed. rev. e atual. São Paulo: Malheiros. 2007.

VASCONCELOS, Fernando Antonio de. Internet: responsabilidade do provedor pelos danos praticados. 1ª ed. (ano 2003), 6ª tir. / Curitiba: Juruá, 2008.

VIANNA, Tulio Lima. **HACKER: Um Estudo Criminológico da Subcultura Cyberpunk**. Disponível em: <www.mundojuridico.adv.br/cgi-bin/upload/texto274.doc>. Acesso em: 19 abr. 2010.