FACULDADE DE CIÊNCIAS E EDUCAÇÃO DE RUBIATABA - FACER
CURSO DE DIREITO

ANDRÉIA MENDES PARREIRA MACIEL

CRIMES DE INFORMÁTICA E A LEGISLAÇÃO BRASILEIRA

Associação Educativa Evangélica
BIBLIOTECA

RUBIATABA - GO

FACER - FACULDADE DE CIÊNCIAS E EDUCAÇÃO DE RUBIATABA
CURSO DE DIREITO

ANDRÉIA MENDES PARREIRA MACIEL

CRIMES DE INFORMÁTICA E A LEGISLAÇÃO BRASILEIRA

Monografia apresentada a FACER – Faculdade de Ciências e Educação de Rubiataba, como requisito para obtenção do grau de Bacharel em Direito sob a orientação do professor Eduardo Barbosa Lima.

RUBIATABA - GO

2008

ANDRÉIA MENDES PARREIRA MACIEL

CRIMES DE INFORMÁTICA E A LEGISLAÇÃO BRASILEIRA

COMISSÃO JULGADORA
MONOGRAFIA PARA OBTENÇÃO DO BACHARELADO DE DIREITO PELA FACULDADE DE CIÊNCIAS E EDUCAÇÃO DE RUBIATABA

RESULTADO_____

Orientador _____
Eduardo Barbosa Lima
Especialista em Direito Penal

1° Examinador _____
Geruza Silva de Oliveira
Mestre em Sociologia

2° Examinador _____
Eliane de Fátima Rodrigues
Mestre em Ciências Ambientais e Saúde

Rubiataba, 2008

Dedico este trabalho Minha Mãe Fátima que esteve sempre do meu lado e batalhou comigo para que eu pudesse concluir o curso, aos meus irmãos que sempre me apoiaram e aos meus amigos que nunca me abandonaram durante essa jornada. A Deus que esteve comigo em todos os momentos da minha vida, desde o inicio me dando sabedoria e força para superar os obstáculos e enfrentar os desafios.

RESUMO: O acelerado crescimento da informática nas últimas décadas trouxe consigo grandes benefícios para a sociedade em geral. Juntamente com esses avanços vieram novos tipos de crimes bem como a repaginação em ambiente de rede de crimes antigos praticados de outras formas, são os crimes de informática. As novas tecnologias fazem parte da vida da sociedade moderna, ela precisa de computador em casa, no trabalho, nas escolas e outras áreas de atividade humana. Pensando nisso alguns países também estão tentando acompanhar esta evolução, apresentando e discutindo leis para coibir esses crimes, mas não é uma tarefa fácil, por existir muitas dificuldades em alguns aspectos legais. É necessário se adequar e criar mecanismos para enfrentar os crimes de informática para poder sobreviver a um futuro globalizado.
Palavras-Chave: desenvolvimento; direito; crimes; tecnologias.

ABSTRACT: The accelerated growth of information technology in recent decades has brought major benefits to society in general. Along with these advances come new types of crimes and also crimes old charged in other ways, are the crimes of information technology. Modern society can no longer live without technology, they need computer at home, work, schools and other activities. Other countries are also trying to monitor these developments, presenting and discussing laws to curb such crimes, but is not an easy task because there are many difficulty in some aspects. We have to adapt and create mechanisms for addressing the crimes of information technology can survive in a globalized future.

Keywords: development; law; technology.

INTRODUÇÃO

A era da informática trouxe muitas facilidades que foram alcançadas pelo uso do computador destacando-se a internet. Assim juntamente com e-mail e trabalho on-line, nasceram os crimes de informática, delitos que são praticados contra o sistema de informática ou por meio deste, onde abrange o computador com seus acessórios e a internet.

Estas que são altamente lesivas, encontram-se previstas na legislação penal e legislação extravagante, onde a internet ou outro ambiente eletrônico é somente o meio de execução, estando à tipificação perfeita ao ato proferido.

O que se percebe é que surgiram novos crimes e também novas maneiras de cometer antigos crimes. São crimes que podem ter sua consecução no meio cibernético: Plágio, calúnia pirataria de software, pedofilia, racismo, ameaça, lavagem de dinheiro e outros.

Então, estamos diante de condutas que, utilizando-se da internet para sua consumação, ferem direitos de terceiros, considerando em uma acepção ampla que engloba aquilo que perturba preceitos éticos e morais, bem como bens e direitos juridicamente tutelados.

Cada país está adaptando suas legislações para abrangerem os crimes digitais, porém ainda há lacunas na legislação, muitos projetos de lei foram apresentados, alguns se encontram em tramitação, outros foram engavetados e alguns aprovados. A prática reiterada destes crimes reflete a carência de normas regulamentadoras, onde os indivíduos que usam a informática e as vítimas dessas condutas ficam desprotegidos.

Os crimes de informática têm atraído a atenção de muitos doutrinadores que impõe uma interpretação evolutiva da legislação em consonância com o contexto em que a norma será aplicada. Sendo que o frenético surgimento de novas tecnologias exige ao interprete e ao aplicador do direito, conhecimentos mais específicos na área de informática.

Trata-se de uma tarefa árdua, pois diante do estudo do tema percebe-se a escassez de doutrinas, o que torna ainda mais interessante a abordagem do tema e seu estudo, pois abri-se a oportunidade de explorar um assunto que é novo e que esta à frente de nossos olhos, a vista de toda a sociedade.

Percebe-se, frente ao que foi exposto que não pode, o Legislativo, omitir-se na regulamentação das relações celebradas por meio da Internet, nos mais diversos fins, para os quais a mesma vem sendo utilizada. A inexistência de leis extravagantes, inevitavelmente aumenta a incidência de lides, em face das imprecisões que ainda cercam a matéria.

Com a normatização das operações em tela, atribuir-se-ia maior segurança às mesmas, fator que propiciaria a captação de novos investimentos para o setor. Além disso, os profissionais do direito não teriam que utilizar criatividade e princípios gerais do direito para defender os interesses de seus constituintes, nas causas que versam sobre a rede mundial de computadores. Urge-se assim, breve iniciativa das autoridades competentes a fim de que sejam elaborados e discutidos novos projetos de lei voltados à regência das operações via Internet, este inovador e fantástico veículo de informações.

No objetivo geral procuramos conhecer condutas típicas e atípicas, os novos tipos penais e os crimes já conhecidos e que utilizam a informática como meio para execução, bem como identificar a importância da reflexão com relação às novas condutas criminosas.

Inclui-se no nosso objetivo específico analisar a realidade dos crimes mostrando os delitos que surgiram com a explosão da tecnologia da informação bem como verificar as indicações legislativas do país.

Para tanto, usaremos como método de trabalho o dedutivo, em que se parte de um conhecimento geral para um particular, onde o nosso tema, referindo-se ao enquadramento do direito na era digital, ficará circunscrita a sua relação com o Direito Penal. A pesquisa será baseada em dados bibliográficos que enfoquem o tema de forma geral e de forma específica, principalmente, artigos em revistas especializadas, livros, internet e jornais.

O presente estudo justifica-se porque atualmente a nossa legislação possui uma lacuna quando se trata de processar e julgar crimes de informática. Existem países que

regularam a matéria como os Estados Unidos e Portugal. No Brasil existe a lei que altera a Lei nº 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente, visando aprimorar o combate à produção, venda e distribuição de pornografia infantil criminalizando a obtenção e a posse de tal material bem como outras condutas relacionadas à pedofilia na Internet. Existem vários projetos de lei em discussão na Câmara dos Deputados sendo que o mais polêmico é Substitutivo aos projetos de lei 137/2000 e 76/2000, do Senado, e 89/2003, da Câmara

O Direito Criminal da Informática deve se desenvolver rapidamente, de modo a serem sistematizadas normas que atinjam os crimes tipificados na prática e que são cometidos com a utilização de computadores e sistemas para que assim proporcionem mais proteção e contribuam na produção de provas.

1 A NATUREZA JURÍDICA EM INTERFACE COM AS NOVAS TECNOLOGIAS

1.1 O Computador e a internet

O Computador é geralmente conceituado como equipamento ou dispositivo capaz de armazenar e manipular, lógica e matematicamente, quantidades numéricas representadas fisicamente. Uma máquina que consiste em um equipamento de entrada e saída que manipula informações sob diversas formas, podendo comunicar e arquivar dados digitais ou analógicos.

A história do computador tem seu início há muito tempo atrás, quando foi criado, há aproximadamente 4.000 a.C. um aparelho muito simples formado por uma placa de argila onde se escreviam algarismos que auxiliavam nos cálculos. Esse aparelho era chamado de ábaco, antepassado mais remoto da máquina de calcular. Então no ano de 1642, Blaise Pascal, francês de 18 anos, inventou a primeira máquina de somar da história, o que serviu para que o alemão Gottfried Wilhelm von Leibniz aperfeiçoasse a idéia e criasse uma maquina de multiplicar e dividir.

Os primeiros computadores começaram a aparecer durante a década de 40, ainda utilizando válvulas. O computador mais famoso daquela época foi o ENIAC (Electronic Numerical Integrator Analyzer and Computer), construído em 1946, pelas necessidades militares e foi utilizado para montar tabelas de calculo das trajetórias dos projeteis. Em 1951 surgiram os primeiros computadores em série, e com a explosão tecnológica hoje tem se os PC (computadores pessoais) e notebooks.

A Internet é uma rede de comunicação mundial, com a finalidade de compartilhar informações e serviços, onde estão interligados milhões de computadores, que pode ser conectada por satélites, linhas telefônicas, fibra ótica ou por ligações por microondas.

No início a Internet permitia apenas três serviços básicos: o correio eletrônico (e-

mail), conexão remota por login e transferência de arquivos. O correio eletrônico é o serviço de mensagens, é o recurso mais antigo da internet. Já a conexão remota por login, permite acessar programas e aplicações disponíveis em outro computador. E a transferência de arquivos se constitui em outro recurso básico da Internet que pode ser utilizada na transmissão de documentos, imagens, sons ou software.

A internet surgiu com o projeto ARPANET[1], da agencia de projetos avançados (ARPA) do departamento de defesa norte-americano que confiou em 1969 à Rand Corporation a elaboração de um sistema de telecomunicações que garantisse que um ataque nuclear Russo não interrompesse a corrente de comando dos Estados Unidos. A solução foi a criação de redes locais (LAN), posicionadas em locais estratégicos, coligados por meio de redes de comunicações geográficas (WAN), pois na eventualidade de uma cidade vir a ser destruída por ataque nuclear essa rede garantiria a comunicação entre as cidades coligadas.

A expansão da internet ocorreu em 1973, quando Vinton Cerf registrou o protocolo TCP/ IP Protocolo de Controle da Transmissão / Protocolo Internet. Trata-se de um código consente aos diversos NetWorks incompatíveis, para programas e sistemas comunicarem entre si:

> WWW nasceu no ano de 1989 no Laboratório Europeu de Física de altas energias, com sede em genebra, sob o comando de T. Berners – Lee R. Cailliau. É composto por hipertextos, ou seja, documentos cujo texto, imagem e sons são evidenciados de forma particular e podem ser relacionados com outros documentos. (PAESANI, 2003, p. 33)

A Internet chegou ao Brasil em 1988 por iniciativa da comunidade acadêmica de São Paulo e Rio de Janeiro. Em 1989 foi criada, pelo Ministério de Ciência e Tecnologia, a Rede Nacional de Pesquisas (RNP), uma instituição com os objetivos de iniciar e coordenar a disponibilização de serviços de acesso à Internet no Brasil. Com a RNP, veio a interligação inicial de 11estados a partir de Pontos de Presença (POP) em suas capitais.

A exploração comercial da Internet no Brasil foi iniciada em dezembro de 1994 a

[1] ARPANET, acrônimo em inglês de Advanced Research Projects Agency Network do Departamento de Defesa dos Estados Unidos da América, foi a primeira rede operacional de computadores à base de comutação de

partir de um projeto-piloto da Embratel, permitindo o acesso à Internet através de linhas discadas. Posteriormente, em abril de 1995, o acesso passou a ser permitido através de linhas dedicadas via RENPAC (Rede Nacional de Pacotes) ou linhas E1.

Existem na rede os troncos principais, chamados de *BACKBONES* (em português: espinhas dorsais), que são responsáveis pelas principais rotas de tráfego. No Brasil, estes backbones são representados pela Embratel e pela RNP, além de outras entidades privadas que também prestam este tipo de serviço.

1.2 Internet e seu funcionamento

Ligados aos *backbones*, estão os provedores de acesso, como a *Progressnet*, que permitem que o usuário em sua própria casa ou no trabalho, acesse a Internet. Os provedores possuem linhas telefônicas que, ao receber uma ligação de um usuário doméstico, conecta-o à Internet e enquanto durar essa conexão ele está vinculado ao provedor.

A partir de então, o usuário transfere e recebe dados da rede, utilizando os diversos serviços da Internet. Tudo que se precisa é usar uma linha telefônica particular, conectando-a ao computador pelo aparelho chamado modem. Com esse equipamento, e um programa básico de comunicação, pode-se entrar em contato via telefone-computador com a provedora de acesso à Internet.

No momento em que o usuário envia um e-mail ou acessa algum site, o modem converte os sinais digitais do computador em sinais analógicos e os envia para o provedor que realiza o serviço inverso:

> As comunicações entre os computadores na internet adotam um **protocolo** específico: o TCP/IP (*Transmission Control Protocol/Internet Protocol*). Esse protocolo divide a mensagem em pequenos blocos de informações denominados de pacotes onde são definidos o destino da informação e a forma de reconstituir a mensagem original. Nesse sentido, computadores diferentes, funcionando de maneiras diferentes, podem estabelecer comunicações entre si: é o conceito de arquitetura aberta, consagrado na

internet. (CASTRO, 2008)

O provedor encaminha os vários pacotes da mensagem para o ponto mais próximo do computador de destino. Esse procedimento é realizado por máquinas conhecidas como **roteadores**, que lê o endereço de destino dos pacotes e os envia. Conforme os pacotes gerados vão sendo enviados pela Internet os roteadores que se encontram ao longo do caminho certificam o endereço marcado pelo IP e conforme o tráfego da rede naquele momento escolhem a melhor rota a ser percorrida pelos pacotes até o seu destino final. Como o tráfego muda a todo instante, os pacotes podem percorrer caminhos diferentes para chegarem ao seu destino.

Portanto, a utilização da internet (navegação, comunicação por correio eletrônico, etc) pressupõe a existência dos seguintes componentes: a) microcomputador (do usuário); b) linha telefônica; c) modem; d) provedor de acesso à internet (*Internet Service Provider*); e) *software* de correio eletrônico, navegação, etc; f) protocolo TCP/IP (normalmente o *software* necessário já vem instalado no equipamento adquirido); g) computadores dos provedores (roteadores e outros, permanentemente ligados com os outros provedores); h) conexões (utilizando diversos meios, tais como linhas telefônicas, cabos de fibra ótica, satélites, cabos submarinos, ondas de rádio, rede elétrica, etc).

1.3 A informática e o Direito

O ser humano em sua evolução viu a necessidade de obter e repassar certos tipos de informações para uma melhor vida em sociedade. Por causa desta necessidade ele foi aperfeiçoando desde a invenção da escrita até a invenção da atual internet. A internet, por sua vez, apresentou ao mundo uma nova evolução da sociedade, trazendo a todos a informação imediata.

Sabe-se claramente que o ser humano ao criar a internet tinha em mente que tal ferramenta deveria ser usada para o meio de comunicação e até comércio da sociedade. Mas ao nos depararmos com a realidade notamos que não é só isso que esta acontecendo.

Com o grande avanço da globalização há um maior número de internautas na rede, há também um grande número de transações, que desperta o interesse de pessoas de má fé, que adentram a internet em alguns sistemas sem autorização para fazer operações fraudulentas, também chamadas operações piratas. Pode-se invadir sistemas, furtar informações sigilosas e causar sérios danos irreparáveis.

Hoje a internet é vista como meio de comunicação que interliga milhões de computadores no mundo inteiro e permite o acesso a uma quantidade de informações praticamente inesgotáveis, anulando a distância de lugar e tempo. O avanço da tecnologia na área da informática provocou uma revolução nas relações sociais, as facilidades alcançadas pelo uso do computador e a internet transformaram a vida moderna. É a Era da Informática.

A rede passou a ser tão importante em nossa sociedade que a mídia sempre a tem em pauta, o que deu origem a revistas especializadas e encartes próprios nos principais jornais e revistas. Tal importância apenas demonstra que é impossível ficar alheio a essa nova corrente, especialmente no presente momento onde assistimos ao fenômeno da globalização e o acesso às informações sobre o que está ocorrendo é primordial.

Essas inovações atingem o direito em todas as áreas, encontramos na rede objetos para compra e venda, troca, leilões, etc. O comércio eletrônico cresce a cada dia e tem como conseqüência um aumento de consumidores, mas não é só comercio, serviços também são oferecidos e podem ser contratados na internet. Estamos na época dos contratos virtuais.

O ensino à distância revolucionou o sistema educacional, diversos cursos de extensão são oferecidos pelas instituições brasileiras. As matérias são enviadas por transferência de arquivos, contato por e-mail entre aluno e professor ou encontro em salas virtuais.

Tantas novidades na área da tecnologia propiciaram o aparecimento de novos tipos de crimes ou novas formas de praticar os já conhecidos tipos penais. O grande problema da justiça para desvendar esses crimes é o fato de serem crimes sem suspeitos, e com poucas pistas.

Para se ter noção de que tipo de informações está sendo tratada, na atualidade

aproximadamente oito milhões de brasileiros acessam a internet. Dentro de dois anos esse número pode chegar a quinze milhões e pesquisas do Instituto de Peritos em Tecnologias Digitais e Telecomunicações (IPDI) revelam que os prejuízos causados pelos crimes on-line, atingiram uma média de um valor superior a 100 milhões de reais. Os benefícios da modernidade e celeridade alcançados com a rede mundial, trazem na mesma proporção, a prática de ilícitos penais que vêm confundindo não só as vitimas como também os responsáveis pela persecução penal.

1.4 Informática como disciplina jurídica

1.4.1 A informação como bem jurídico

O progresso tecnológico transformou a informação em mercadoria, que sob a forma de impulsos magnéticos faz uma coleta de dados, ou seja, a informação transformou-se em uma nova matéria prima que pertence ao gênero dos bens imateriais. Na medida em que a tecnologia avança permite-se uma incrível rapidez na sua circulação e a informação que pode ser guardada, manipulada ou até subtraída ilicitamente, passa a ter uma relevância jurídica antes não reconhecida.

No passado a informação circulava lentamente, não alterava o curso normal da vida do homem e era recebida por uma pequena parcela da sociedade. Hoje a informação é vista como forma de mensagem e existem detentores que são os possuidores dos bancos de dados, gestores dos sistemas eletrônicos, ou seja, todos os que conhecem e fazem uso dos sistemas informáticos. Para Frosini (1984, p. 397 apud ROHRMANN, 2005)

Direito de Informática se ocupa do exame dos problemas jurídicos, que assumem caráter de ordem geral, como é a qualificação de um novo princípio constitucional, até o reconhecimento de um novo Direito Humano, que é uma figura do antigo Direito Natural. Foi assim reconhecido nos acordos de Helsinki de 1975(...) e como reforço desta posição é suficiente pensar na 'liberdade de Informática', que consiste no direito de se informar sobre a própria identidade informativa, construída na memória magnética de um banco de dados pessoais.

Os atos ilícitos relacionados ao uso da informática bem como sua difusão e circulação, têm atraído a atenção de muitos doutrinadores que impõe uma interpretação evolutiva da legislação em consonância com o contexto em que a norma será aplicada. Sendo que o frenético surgimento de novas tecnologias exige ao interprete e ao aplicador do direito, conhecimentos mais específicos na área de informática.

1.5 Natureza Jurídica e definição de conceitos básicos da Informática

1.5.1 Hardware

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

Para a unidade de hardware existem varias denominações que o próprio legislador usa para indicar o computador sendo várias expressões como: elaborador eletrônico, sistema informático, tratamento automático etc. Muito embora sejam usadas na linguagem comum existe uma diferença entre as expressões em seu uso técnico.

Quanto à natureza jurídica do hardware considerado em sua unidade, pertence como produto industrial à categoria dos bens materiais que se submetem às normas usuais. Mas se ocorrer alguma inovação técnica no hardware, que satisfaça aos requisitos da patenteabilidade, pode ser protegida mediante o depósito do pedido de patente de invenção,

ou então pode ser requerido o depósito do pedido de registro do modelo industrial. Sendo assim é perfeitamente aplicável ao hardware o conjunto de regras e institutos elaborados em matéria de disciplina de concorrência entre empresas, e de tutela de segredos científicos e industriais.

1.5.2 Software

Mostrando o quanto os sistemas operacionais revolucionaram o campo da computação, Torres (1998, p. 342-343) relata como era realizada a operação do computador antes do advento dos sistemas operacionais, ficando claro o quanto era complicado ser utilizado por pessoas leigas.

O sistema operacional é o conjunto de programas, que gerenciam recursos, processadores, armazenamento, dispositivos de entrada e saída e dados da máquina e seus periféricos. Sem o sistema operacional, um usuário para interagir com o computador deveria conhecer profundamente diversos detalhes sobre o hardware do equipamento, o que tornaria o seu trabalho lento e com grandes possibilidades de erros. O sistema operacional tem por objetivo funcionar como uma interface entre o usuário e o computador, tornando sua utilização mais simples, rápida e segura.

Dentre suas funções básicas podem ser citadas:

> Definição da interface com o usuário, apresentando uma máquina mais adequada e tornando a comunicação mais natural e inteligível; Compartilhamento de hardware e software entre usuários, de modo que o sistema seja utilizado de maneira mais eficiente, trazendo maior benefício na execução de trabalhos mais complexos; Gerenciamento dos dispositivos de entrada e saída. (TORRES, 1998, p. 342-343)

Existem vários tipos de sistemas operacionais que se diferem pelos serviços que eles proporcionam aos usuários e principalmente o modo pelo qual executam tais tarefas. Os tipos de sistemas operacionais e sua evolução estão relacionados diretamente com a evolução do

hardware e das aplicações por ele suportadas. Muitos termos inicialmente introduzidos para definir conceitos e técnicas foram substituídos por outros, na tentativa de refletir uma nova maneira de interação ou processamento.

A proteção jurídica do software possui importância científica e também econômica. É imprescindível que se adotem medidas jurídicas diretamente relacionadas ao direito autoral para a organização de sua tutela legal. Vale dizer que o programa de computador caracteriza-se por dois aspectos: um aspecto material, quando ele é incorporado em alguns suportes, tais como cartões magnéticos, discos, circuitos integrados, etc. e o aspecto imaterial, pois resulta de trabalho de criação. Como um bem imaterial onde para sua produção concorrem subsídios tecnológicos sofisticados e complexos, os programas de computador precisam de investimentos que sustentem o desenvolvimento de pesquisas que estimulem a criatividade dos especialistas em computação.

Para o desenvolvimento de um software, geralmente, requer-se a utilização de material humano altamente qualificado, por um longo espaço de tempo, tornando-se assim um negócio altamente dispendioso. Cada passo pode representar escolhas e iniciativas humanas e dados os custos envolvidos na elaboração do software e como costuma ser fácil copiar determinados programas, é justo a proteção legal do software.

É importante lembrar que no Brasil, a Lei n° 9.609 de Fevereiro de 1998 capitulo I, art. 1°, dispõe sobre a proteção da propriedade intelectual de programa de computador bem como a sua comercialização no Brasil, no define software como:

> Programa de computador é a expressão de um conjunto organizado de instruções em linguagem natural ou codificada, contida em suporte físico de qualquer natureza, de emprego necessário em máquinas automáticas de tratamento da informação, dispositivos, instrumentos ou equipamentos periféricos, baseados em técnica digital ou análoga, para fazê-los funcionar de modo e para fins determinados.(PAESINI, 2005, p. 27)

1.5.3 Sistema Informático

O sistema informático é o conjunto de elementos (hardware e software) composto de uma unidade central de elaboração de dados, uma unidade periférica e um software e que são essenciais para o funcionamento de um computador.

O sistema informático ideal foi definido por Borruso (1978 apud ROHRMANN, 2005, p. 26) como:

> um complexo unitário de máquinas com funções diferenciadas, com extraordinária capacidade de memorizar qualquer tipo de dado e, portanto, de incorporar o pensamento passado ou presente, capacidade de operar em velocidade vertiginosa, cálculos, pesquisas (...) e realidades complexas que por dimensão e quantidade escapam da possibilidade de um controle humano e que, por conseqüência, se transforma numa inteligência artificial operativamente superior às próprias faculdades do homem que a criou.

2 CRIMES DE INFORMÁTICA EM SEUS ASPECTOS PROCESSUAIS

2.1 Das Provas

Para identificar a autoria da conduta ilícita nos delitos informáticos na maioria das vezes existirá enorme dificuldade, pois diferente do mundo "real", no mundo virtual não tem como fazer a identificação e autenticação dessa identidade visualmente ou pela simples análise de documentos e elementos identificadores.

Quando alguém está conectado na rede, são necessários dois elementos identificadores: o endereço da máquina que envia as informações à Internet e o endereço da máquina que recebe tais dados. Esses endereços são chamados de *IP — Internet Protocol*, sendo representados por números, que, segundo LESSIG, não revelam nada sobre o usuário da Internet e muito pouco sobre os dados que estão sendo transmitidos.

A prova na informática é umas das questões mais polêmicas, há dificuldade em aplicar o direito nessas situações, especialmente em se consolidar provas capazes de iniciar um inquérito policial e quem sabe oferecer denúncia.

O problema começa na fase investigatória que é onde se deve apurar a existência do crime bem como o meio, sua localização, o objeto e os resultados. Os problemas processuais continuam já que é possível identificar a maquina utilizada, mas dificilmente determinará quem praticou a conduta delituosa, pois na maioria dos casos um único computador é utilizado por várias pessoas.

2.2 Prova originárias da informática no Direito Brasileiro

Na investigação deve-se identificar quem de fato usou o computador para a prática

do delito, pois sem essa apuração fica impossível oferecer denúncia e não cabe acusação formulada em face do proprietário da maquina sem existir provas de que o mesmo foi autor do crime, *in verbis:*

> O art.5º LVI da Constituição Federal estabelece:"São inadmissíveis, no processo, as provas obtidas por meios ilícitos". O art. 332 do Código de Processo Civil reza: "Todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste código, são hábeis para provar a verdade dos fatos, em que se funda a ação ou a defesa".

Ao interpretar se a lei de uma forma genérica, pode se ver que ela não exclui a prova de informática. Na legislação civil, a prova de atos jurídicos é a forma escrita, então o jurista poderá aceitar elementos informáticos desde que tenha o mesmo alcance do previsto no Código Civil:

> A informação registrada tem a materialidade idêntica à informação escrita. Basta transcreve-la no papel para que possa ser lida. Assim, o fax poderá constituir um *começo de prova escrita* sempre que se possa estabelecer fielmente sua origem. É necessário ressaltar que,se a *assinatura* for da essência do ato, não poderá ser comparada à *chave do acesso magnético* nem poderá ser juridicamente fundada. (PAESANI, 2005, p. 32).

Com a falta de legislação específica a jurisprudência assume um papel importante, pois existem situações confusas conforme o valor que se dê a prova.

Consoante os direitos processuais brasileiros, civil e penal, dispomos de, grosso modo, meios para que sejam provadas as alegações em juízo, são eles:

> a) Confissão - quando o confidente admite como verdadeiro um fato contrário ao seu interesse e favorável ao adversário (artigo 348 do Código de Processo Civil). Isso no juízo civil, porque no juízo criminal, caso a infração não deixe vestígios, será indispensável o exame de corpo de delito, não podendo supri-lo a confissão do acusado (artigo 158 do Código de Processo Penal). Ademais, sua validade não é absoluta, haja vista que o valor da confissão se aferirá pelos critérios adotados para os outros elementos de prova, e para a sua apreciação o juiz deverá confrontá-la com as demais provas do processo, verificando se entre ela e estas existe compatibilidade ou

> concordância (artigo 197 do Código de Processo Penal); qual seja, no juízo criminal ela somente se prestará para a condenação do réu se existirem outras provas.b) A prova documental - é admitida como prova no direito brasileiro, mas, por exemplo, o e-mail poderia ser considerado como um documento? A resposta é não. Primeiro porque é da essência de um documento que o mesmo seja assinado (ressalvadas as hipóteses legais relativas a telegramas, radiogramas, livros comerciais e outras); segundo porque onde lhe falta a intrínseca materialidade de quaisquer documentos, sobra sua implícita e etérea essência. Isso nos leva a concluir que a sua capacidade de prova estará sempre comprometida, podendo ser acrescida da necessidade de outros meios de prova em relação a seu conteúdo, tais quais a prova pericial, a testemunhal. Isto vale para qualquer outro documento eletrônico, imagem, texto, som, etc.c) A prova pericial - consiste em exame, vistoria ou avaliação. Todavia o juiz não está adstrito ao laudo pericial, podendo formar a sua convicção com outros elementos ou fatos provados nos autos. A perícia é o mais eloqüente e adequado meio de se fazer a prova judicial no campo da informática, desde que observadas as formalidades de procedimentos cautelares próprios.d) A inspeção judicial - ocorre quando o juiz, de ofício ou o requerimento da parte, inspeciona pessoas ou coisas, a fim de se esclarecer sobre fato que interesse à decisão da causa (artigo 440 do CPC). É uma prova difícil pois sistemas de informática não são nem pessoa nem coisa. Mas é possível inspecionar o hardware, por exemplo. Sempre que um fato não for provado documentalmente, por confissão ou por perícia, é admissível a prova testemunhal.

2.3 Investigação

A finalidade da investigação é oferecer subsídios para que o autor da ação penal possa ingressar em juízo e a Autoridade Policial deve buscar identificar a autoria da infração:

> O artigo 6º do CPP enumera as diligências a serem efetuadas, sendo importante salientar que o rol lá exposto não é taxativo, mas ao contrário, exemplificativo, cabendo ao Delegado de Polícia determinar outras diligências adequadas ao caso concreto. Em se tratando de crime de informática, a investigação não é muito diferente da dos crimes comuns, acrescentando-se apenas, os instrumentos investigatórios advindos com o computador e a internet. Desta forma, a Autoridade Policial pode se orientar pelos critérios enumerados no dispositivo legal acima citado, ouvindo ofendido, indiciado, testemunhas etc. (CASTRO, 2003, p. 105).

2.4 Competência

Para estabelecer a competência para o processo e o julgamento dos crimes de informática é preciso verificar a incidência da lei brasileira. Se o Brasil competente deve ser aplicada as regras do CPP (Código de Processo Penal) onde a competência é determinada pelo lugar onde consuma a infração.

Daí a importância de se identificar o local da consumação do delito, tarefa muitas vezes difícil nos crimes de informática. Quando for possível localizar a máquina utilizada pelo agente na execução do crime, está resolvida a questão da competência.

O problema surge quando é impossível descobrir o lugar em que se consumou o crime. No caso de uma pessoa usar um *notebook* para a prática de um delito ela poderia estar em qualquer lugar e, com o auxílio de uma linha telefônica, então quando não se conhece o local da consumação deve-se aplicar a regra subsidiária para a fixação da competência, o domicilio ou residência do réu. E se ele possuir mais de uma residência firma-se a competência pela prevenção e se o agente for desconhecido será competente o juiz que tomar conhecimento do caso:

> Estabelecida a competência em razão do local, passamos à analise da competência em razão da matéria. Os crimes de informática poderão ser objeto de julgamento no Juizado Especial Criminal ou perante o juiz de direito. Há de ser respeitada a competência pela prerrogativa de função (artigo 84 CPP) e as regras de conexão e continência (arts.76/82 CPP). Caso haja conexão de um crime de informática de menor potencial ofensivo e outro de maior gravidade, entendemos que os processos de julgamento devem ser separados. O primeiro deve ser julgado no JEC e o segundo na Vara Criminal. Impõe-se a separação em razão da competência do Juizado Especial ser constitucional e, portanto, absoluta. O JEC não pode julgar uma infração de maior gravidade, sendo possível assim exercer a *vis atractiva* e ao mesmo tempo uma infração de menor potencial ofensivo não pode ser julgada no JEC. Outro caminho não há, senão o desmembramento.
> (CASTRO, 2003, p. 108).

O ciberespaço é um ambiente altamente criativo, informativo, bastante lucrativo, mas não harmonioso. Através da Internet pode se obter acesso a um sistema num determinando

país, manipular dados em outro e obter resultados em um terceiro país. Nos países em que existem leis específicas para o caso, temas como o da extraterritorialidade, jurisdição e competência são amplamente discutidos.

Então a grande dificuldade está em definir a competência para o processo e julgamento dos crimes da informática que estejam envolvendo muitos países. Pois, muitas vezes o que é considerado crime em um lugar pode não ser em outro, o que por si só já dificulta a forma de disciplinar a matéria:

> Talvez seria ideal a criação de um Estatuto Internacional definindo crimes de informática, impondo regras para a Internet e para o uso das redes de telecomunicações internacionais, que pudesse questionar os países signatários punindo os que contrariassem as regras impostas. Seria um Estatuto com tipos penais internacionais, que poderiam também complementar as legislações penais específicas dos países membros. (SILVA, 2008)

3 PRINCIPAIS TIPOS DE CRIMES DE INFORMÁTICA

3.1 Os Crimes de Informática

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

O crime de informática é aquele praticado contra o sistema de informática ou através deste, é uma conduta lesiva e dolosa. Em principio é um crime de meio, pois se utiliza de um meio, o virtual. Não é um crime de fim, isso quer dizer que o meio de materialização da conduta criminosa é que é virtual e não o crime. A maioria dos crimes acontece também no mundo real, sendo a internet apenas um facilitador. A sensação de anonimato e o alcance global desse meio de comunicação fazem com que o número de infrações cresça e com ela a preocupação de diminuir tais condutas.

Os tais "crimes de informática" são classificados de diversas formas. Destacamos as duas mais utilizadas. Existiriam os crimes de informática próprios e os impróprios. Os primeiros são aqueles que somente podem ser efetivados por intermédio de computadores ou sistemas de informática, sendo impraticável a realização da conduta por outros meios. Já os qualificados como impróprios admitem a prática por diversos meios, inclusive os meios informáticos.

Segundo Costa, (2008) existem diferentes classificações quanto ao seu objetivo material, a saber:

> Crime de Informática Puro: São os crimes em que o sujeito ativo os objetiva atingir o sistema de informática, em todas as suas formas. Entende se 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. As ações físicas se materializam, portanto, é crime de informática puro toda e qualquer conduta ilícita que tenha por único objetivo o sistema de computador, seja pelo atentado físico ou técnico do equipamento e seus componentes, inclusive dados e sistemas. Crime de Informática Misto: São ações em que o agente tem em vista um bem juridicamente protegido distinto da informática, sendo o sistema de informática ferramenta indispensável para a consumação da conduta criminosa. Nesse caso o agente tem por objetivo realizar operações de transferência ilícita de valores de outrem, utilizando o computador para alcançar o resultado dessa vantagem ilegal, sendo o computador ferramenta indispensável. Crime de Informática Comum São condutas onde o agente usa o sistema de informática como uma ferramenta para realizar um crime comum, tipificável na lei penal. Sendo assim, o sistema de informática não é essencial para a realização do crime, que poderia ser praticado usando outro instrumento. Como exemplo temos os casos de estelionato, e as mais amplas formas de fraude.

3.2 Tipos de sujeitos ativos

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

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

> jovens, normalmente de 24 a 33 anos, às vezes até menores, de 12 a 16 anos, tomando o computador como um "game" para invadir sistemas; estudantes ou operadores de computação; inteligentes, normalmente com QI acima da média; sexo masculino e de cor branca; bem vestidos, educados, de fino trato; aventureiros, audaciosos; trabalham além da jornada de trabalho, competentes; mudam constantemente de emprego; começam com crimes pequenos, como pirataria; são bons vizinhos, são pessoas acima de qualquer suspeita; são réus primários (MEDEIROS, 2008).

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

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

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

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

3.3 Extorsões e Fraudes

A internet hoje em dia, é um dos maiores veículos de comércio moderno, fazendo parte da vida de muitas pessoas no mundo. A internet vem se tornando parte do comércio mundial e acaba envolvendo varias relações comerciais como: compras *on-line*, pagamentos via internet *banking*, pagamentos com cartões de créditos e vários outros, que também são os principais casos de fraudes e extorsões no universo digital.

Hoje em dia as fraudes via internet alcançaram um número assustador, acontece que indivíduos enganam possíveis compradores via internet, que acabam caindo em golpes. Esses golpes atualmente, ocorrem em grande parte, através de transferência de grandes valores entre contas correntes, em questão de minutos. Outra forma bem conhecida entre os internautas é a propaganda de anúncios de produtos inexistentes, que geralmente são recebidos em forma de *e-mail*, e assim, com o dinheiro em conta não enviam o produto ao comprador. As queixas mais freqüentes, no entanto, são casos de planos de pirâmides e marketing de *multilevel*, ofertas de cartões de crédito, oportunidades de negócios mirabolantes, entre outros. Assim, vale o bom senso e a cautela antes de realizar qualquer negócio via Internet.

Isso tudo ocorre, devido aos grandes gênios, que criam esses fantásticos programas de computador, muito sofisticados, e que inibem qualquer tipo de pista dessas ações fraudulentas.

A partir daí começam os abusos de lavagem eletrônica de dinheiro do crime organizado e até mesmo o tráfico de drogas por meio eletrônico.

3.4 Pirataria de Softwares

Os softwares, ou programas de computador foram uma das maiores criações humanas dos últimos tempos, a invenção desses programas, propulsou o desenvolvimento tecnológico mundial.

As grandes empresas existentes, trabalham com softwares de última geração, que armazenam cada vez mais, uma maior número de dados e informações, que as vezes são confidenciais. Esses softwares são programas caríssimos e sendo roubados e revendidos, podem gerar cada vez mais a pirataria.

A lei do software prevê punições cíveis e criminais para os crimes de violação dos direitos autorais de programas de computador. Do ponto de vista civil, quem violar direitos autorais responde por perdas e danos, ou aplicar uma pena pecuniária pela transgressão do preceito.

Na esfera criminal, a pena sobre crimes de violação de direitos autorais de softwares, ou programas de computador, pode ser de 6 meses, a 2 anos de detenção, ou até mesmo 4 anos de reclusão juntamente com o pagamento de uma indenização extremamente absurda.

No Brasil e demais países latino-americanos, para termos um parâmetro dessa realidade, a pirataria é responsável por um rombo de mais de 1,1 bilhões de dólares. A taxa de pirataria é superior a 80% dos programas vendidos, perdendo apenas para os países asiáticos.

3.5 Pedofilia

Dos crimes praticados através da Internet a pedofilia é sem sombra de dúvidas o que causa maior repúdio e revolta na sociedade. É inaceitável o constrangimento ao qual as crianças e adolescentes são submetidos para saciar o prazer doentio e repugnante de pessoas imorais. A pedofilia tira da criança o que ela tem de mais valioso, sua inocência infantil. Uma

conduta tão grave como esta merece uma severa reprimenda por parte da sociedade, seja pelo Poder Público, ao processar e julgar os criminosos, seja pela participação individual de todo cidadão, ao denunciar os envolvidos nesta prática e apontar os *sites* de divulgação.

A pedofilia consiste num distúrbio de conduta sexual, no qual o indivíduo adulto sente desejo compulsivo por crianças ou pré-adolescente, podendo ter caráter homossexual ou heterossexual. Na maior parte dos casos trata-se de homens, muitos deles casados, que se sentem incapazes de obter satisfação sexual com uma pessoa adulta.

O Estatuto da Criança e do Adolescente, Lei 8.069/90, cuida dos direitos das crianças e dos adolescentes. Criança, para o estatuto, é a pessoa até doze anos de idade incompletos e adolescente aquela entre doze e dezoito anos (artigo 2° da Lei 8.069/90).

A Lei 8.069/90 possui vários tipos penais, dentre eles encontramos o referente à pedofilia. *In verbis*: "art. 241- Fotografar ou publicar cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: Pena – reclusão de um a quatro anos".

Publicar é tornar público, divulgar. Quem insere fotos de criança ou adolescentes em cena de sexo na Internet está publicando e, assim, cometendo a infração. O crime pode ser praticado através de *sites, home pages*, muitas delas destinadas à pornografia. É importante salientar que não importa o número de internautas que acessam a página, ainda que ninguém conheça o seu conteúdo, as imagens estarão à disposição de todos, configurando a infração. Por outro lado, quem envia um *e-mail* com uma foto anexada não está tornando público e sim enviando à determinada pessoa, destarte, a conduta é, infelizmente, atípica.

Como a lei protege o menor, há quem sustente que só existirá crime quando a vítima for conhecida e identificada. Ousamos discordar. Ainda que desconhecida, a criança ou adolescente que tevê sua foto divulgada está protegida pelo ECA. Desta forma, a identificação pode facilitar a persecução penal, mas sua ausência não tem o condão de impedir o processo.

Na pedofilia, como nos outros crimes praticados através da Internet, não é difícil identificar a máquina, posto que todo computador possui um número, o problema é saber quem utilizou o computador para divulgar as fotos de crianças e adolescentes. Em se tratando de empresas, estabelecimentos de ensino, cafés e outros locais em que o uso é feito por

diversas pessoas, a investigação pode ser infrutífera.

Embora a pena abstratamente cominada admita a suspensão condicional do processo, entendemos ser impossível a concessão do benefício (art. 89 da Lei 9.099/95), pelas seguintes razões: A conduta social de quem divulga fotos de crianças e adolescentes em cena de sexo é extremamente reprovável, causando repúdio e revolta na sociedade. Os motivos que levam o agente à prática do crime são imorais e repugnantes. Acrescente-se que as conseqüências deste tipo de infração podem ser gravíssimas, o agente que divulga as fotos de um menor, além de expor sua privacidade, provoca lhe traumas irreparáveis. Observe-se, que muitas vezes tais fotos são divulgadas a outros menores, o que gera um distúrbio em seu amadurecimento sexual. As circunstancias do fato são desprezíveis, o agente utiliza as crianças para satisfazer sua lascívia. Assim, quem comete tal conduta é indigno, depravado e pervertido.

4 DA REGULAMENTAÇÃO

4.1 A regulamentação penal da informática

Chamamos de Direito da Informática o conjunto de normas que estão designadas a regular a prevenção, a repressão e a punição aos fatos que atentem contra o uso, exploração, segurança, transmissão e sigilo de dados armazenados e de sistemas manipulados por computadores.

Para se ter uma idéia da importância da existência da regulação penal da informática, na Suíça as seguradoras perdem anualmente cerca de 6 milhões de francos, somente através de delitos de informática. Na França, em 1998, 700 milhões de francos foram perdidos em crimes realizados através da informática, valor este superior aos prejuízos com assaltos bancários no mesmo ano. Tais perdas não se dão apenas em países desenvolvidos. Os mesmos crimes são cometidos no Brasil.

Por outra, já é uma instituição mundial a inoculação, em todos os tipos de computadores, por vírus, principalmente nos sistemas bancários, que geram incalculáveis prejuízos e, no Brasil, mais especificamente, estes destruidores de dados, arquivos e informações, até o momento caminham impunes, por falta de legislação especifica.

4.2 O Problema na Tipificação das Condutas Virtuais

Para se aplicar à devida sanção penal, deve se ter fixo um sujeito infrator, um dos elementos intrínsecos da ação. O direito penal não pode alcançar pessoas abstratas, virtuais. Não podemos, na sanha de condenar, aplicar a sanção penal àquele que pela sua conduta não concorreu de qualquer modo para a caracterização do evento criminoso.

Diante deste fato é que os crimes perpetrados neste ambiente se caracterizam pela ausência física do agente ativo, por isso, ficaram usualmente definidos como sendo crimes virtuais, ou seja, os delitos praticados por meio da internet são denominados de crimes virtuais, devido à ausência física de seus autores.

Não basta, para a aplicação da sanção penal, o conhecimento superficial sobre a identidade do acusado, não se trata de homonímia, mas da comprovação de que aquele que se figura como imputado realmente praticou o que lhe é imputado. Tendo como norte o caráter virtual deste meio, as transações e ingressos na internet são realizados por meios de chaves, códigos formulados através da criptografia.

O grande problema na tipificação das condutas "anti-sociais" perpetradas no ciberespaço é que não existe atualmente uma legislação infraconstitucional definindo os crimes cometidos no ambiente virtual, o que torna mais difícil de estar se fazendo justiça, tendo em vista a "astronômica" lacuna legislativa existente no ambiente supracitado.

Inobstante, de pronto surge uma possibilidade de regulação advinda da Lei de Introdução do Código Civil, que preceitua em seu art. 4° que: "quando a lei for omissa, o juiz decidirá o caso de acordo com a analogia, os costumes e os princípios gerais do direito".

Infelizmente, não é tão fácil assim, pois a legislação infraconstitucional deve estar pautada nos ditames da Constituição Federal, sendo assim deve ser respeitado o princípio da legalidade esculpido no art. 5°, XXXIX da CF/88, preceituando que: "Não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal". O mesmo preceito está disposto no art.1° do Código Penal Brasileiro.

É nesta nova realidade que assistimos o surgimento de um "ambiente anárquico", no qual o delinqüente utiliza o computador doméstico ou não, como meio de praticar uma gama de delitos, fazendo com que, o que deveria facilitar a vida das pessoas, através dos novos meios de comunicação, a internet, está trazendo um verdadeiro transtorno para o convívio pacífico no ambiente social e virtual.

4.3 Legislação Brasileira

4.3.1 O direito penal de informática vigente no Brasil

Naturalmente, considerando as dimensões do País e as suas carências, já é imenso o caldo de cultura para a prática de atos ilícitos em detrimento de bens informáticos ou destinados à violação de interesses e de dados armazenados ou protegidos em meio digital.

Conseqüentemente, é força convir que o Código Penal de 1940 — pensado conforme a doutrina da década de trinta — não se presta *in totum* a regular relações da era digital, num País que almeja inserir-se na cena global da sociedade da informação. Essa sociedade que é produto da revolução tecnológica, advinda com o desenvolvimento e a popularização do computador.

4.3.2 A lei dos direitos autorais

Uma questão controvertida aos doutrinadores e estudiosos do direito no campo dos direitos autorais é a proteção legal a todo e qualquer tipo de criação intelectual veiculada através da rede mundial de computadores - Internet.

A facilidade em disponibilizar, pela Internet, conteúdos, informações, bases de dados ou qualquer outro tipo de criação intelectual se entrelaça, igualmente, com a simplicidade na produção e edição de cópias de tais criações, em detrimento ao direito de seus autores:

> entretanto mais especificamente na disciplina de direitos autorais, torna-se necessário salientar que nos termos da lei dos direitos autorais, Lei n° 9.610, de 19-2-1998, o objeto é constituído por obras do engenho de caráter criativo que pertence à ciência, à literatura, à musica, às artes figurativas, à fotografia, à arquitetura, ao teatro, à cinematografia, ao rádio, à televisão, ao programa de computador etc. qualquer que seja a forma expressa.(PAESANI, 2003, p. 62)

A lei 9.610/98 veio dar proteção legal a toda e qualquer criação intelectual, ensejando indenizações aos seus autores e titulares, seja no campo moral, seja no campo patrimonial, independentemente do meio que a suporta (eletrônico ou tangível), quando dispõe, em seu artigo 7º, inciso XIII, que "são obras intelectuais protegidas as criações do espírito, expressas por qualquer meio ou fixadas em qualquer suporte, tangível ou intangível, conhecido ou que se invente no futuro, tais como as coletâneas ou compilações, antologias, enciclopédias, dicionários, bases de dados e outras obras, que, por sua seleção, organização ou disposição de conteúdo, constituem uma criação intelectual."

Assim, o meio eletrônico está inserido na proteção legal vigente, sendo perfeitamente cabível a reivindicação dos direitos autorais violados através desse meio.

A proteção conferida pela legislação vigente abrange aquelas obras explicitamente referidas no texto do artigo 7º, da Lei 9.610/98, porém a estas não se limita, podendo ser ampliada a qualquer tipo de criação de espírito humano, que constitua uma obra intelectual.

4.3.3 O Código Penal e o direito de informática

O Código Penal Brasileiro tutela a matéria relacionada ao direito do autor no Título III, que trata "Dos Crimes contra a Propriedade Imaterial", mais especificamente no Capítulo I que diz respeito aos "crimes contra a propriedade intelectual", a saber *in verbis:*

> Violação de direito autoral : Art. 184 – Violar direito autoral: Pena – detenção, de 3 (três) meses a 1 (um) ano, ou multa. 1º Se a violação consistir em reprodução, por qualquer meio, com intuito de lucro, de obra intelectual, no todo ou em parte, sem autorização expressa do autor ou de quem o represente, ou consistir na reprodução de fonograma ou videofonograma, sem a autorização do produtor ou de quem o represente: Pena- reclusão, de 1(um) a 4(quatro) anos, e multa de Cr$ 10.000,00 (dez mil cruzeiros) a Cr$ 50.000,00(cinqüenta mil cruzeiros). 2º Na mesma pena do parágrafo anterior incorre quem vende, expõe à venda, aluga, introduz no País, adquire, oculta, empresta, troca ou tem em propósito, com intuito de lucro, original ou cópia de obra intelectual, fonograma ou videofonograma, produzidos ou reproduzidos com violação de direito autoral. 3º Em caso de condenação, ao prolatar a sentença, o juiz determinará a destruição da

produção ou reprodução criminosa.

No que se refere a estes dispositivos, há muitas críticas a respeito, entendendo que não existe uma previsão específica de cada tipo penal, deixando o crime de violação ao direito autoral bastante genérico (diz-se que é uma norma penal em branco). Desta forma, o que se tem de fazer é dar uma interpretação extensiva a estes artigos, tentando, com isso, aplicar a sanção penal disposta.

4.3.4 A lei de software

A Lei 9.609/98 dispõe sobre a proteção da propriedade intelectual dos softwares de programas de computador e sua comercialização no país. Em seu artigo 1°, define o conceito de programa:

> Programa de computador é a expressão de um conjunto organizado de instruções em linguagem natural ou codificada, contida em suporte físico de qualquer natureza, de emprego necessário em máquinas automáticas de tratamento de informação, dispositivos, instrumentos ou equipamentos periféricos, baseados em técnicas digital ou análoga, para fazê-los funcionar de modo e fins determinados. (PAESINI, 2005, p. 40)

Conforme a supracitada lei, o uso regular do software dar-se-á através do contrato de licença. Não existindo referido contrato, sua regularização fiscal dar-se-á através do documento fiscal relativo à aquisição ou licenciamento da cópia.

Outra novidade introduzida pela nova lei foi à possibilidade do titular do software autorizar ou proibir o aluguel comercial, não sendo este direito exaurível pela venda, licença ou outra forma de transferência da cópia, exceção feita ao software cujo objeto em si não seja essencialmente o aluguel.

Relativamente à questão da pirataria, podemos dizer que a nova lei considera crime de sonegação fiscal todo aquele que piratear ou usar cópia não autorizada. Dessa forma, a lei

confere poderes à Receita Federal para investigar a origem das cópias de programas utilizados nos microcomputadores.

Em relação à tutela penal, a lei do software trata dos crimes e das penalidades em seu Capítulo V, artigo 12, ao prever *in verbis*:

> a pena de detenção de seis meses a dois anos ou multa a quem violar direitos de autor de programa de computador, reproduzindo para fins de comércio, sem autorização expressa do autor ou de quem o represente; e pena de reclusão de um a quatro anos e multa a quem tem o intuito de vender, expor à venda ou tem em depósito, para fins de comércio, original ou cópia de programa de computador, produzido com violação de direito autoral.

Deve-se aplicar com rigor as normas existentes a coibir a violação dos direitos dos autores de software, bem como, incentivar a edição de legislação que possa acompanhar a evolução dos programas e das técnicas de vilipendio dos direitos intelectuais.

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

4.4 Projetos de lei

Por só poder existir em sociedade, o homem faz com que das relações nasça a necessidade de normas de organização de conduta social; normas que delimitem a atividade das pessoas. O ciberespaço tem sido visto como uma nova forma de sociedade, uma sociedade virtual e, por isso inatingível pelas leis do mundo real, mas não se pode dar ouvidos aos mais

afoitos que defendem ser a rede de computadores uma terra sem lei.

Diante dessa realidade, surgiu a preocupação de se buscar meios eficazes de controlar as ações dos usuários via Internet, evitando e punindo manobras que coloquem em perigo ou lesionem bens jurídicos. Como se tem visto e com infeliz freqüência, o mecanismo que se entende o mais adequado é o regulamentação das condutas via Direito Penal.

São muitos os Projetos de Lei que tramitam com descrições de condutas que devem ser punidas. O legislador, como sempre, apressa-se em criar leis, para dirimir problemas sociais, sem, contudo se preocupar com a necessidade da criação. Por outro lado, essa pressa leva à publicações de leis com conteúdos inconstitucionais, desprovidas da técnica necessária para uma perfeita compreensão e aplicação da norma e, por vezes, completamente desnecessárias.

Na verdade, todo ambiente social, de uma maneira ou de outra, cria suas próprias regras paralelamente ao seu desenvolvimento. Nesta área não poderia ser diferente. Mas a verdade é que, incorre em grave erro aquele que afirma a ausência de leis que regulem as ações praticadas com a utilização do computador.

Com isso, verifica-se também, a existência de projetos que buscam regulamentar a competência para julgamento desses crimes. Apenas para ilustrar, podemos citar o Projeto de Emenda à Constituição 407/2005, que está aguardando designação de relator na Comissão de Constituição e Justiça e de Cidadania, que pretende atribuir à Justiça Federal o processamento de crimes praticados no âmbito da Internet ou em ambientes similares, disseminados em escala mundial, atribuindo aos Juízes Federais a competência para julgar e processar o crime virtual, e demais ilícitos praticados pela Internet.

Altera, ainda, o artigo 109 da nova Constituição Federal. Outra tentativa de regulamentar o assunto é o Projeto de Lei nº 4144/2004, que corre apensado ao Projeto de Lei n.º403/2001 que visa alterar a Lei nº 8.069, de 13 de julho de 1990, a Lei nº 9.296, de 24 de julho de 1996, e o Decreto-Lei nº 2.848, de 7 de dezembro de 1940, e dá outras providências. O projeto tipifica os crimes informáticos, incluindo os crimes de sabotagem, falsidade e fraude informática; autoriza as autoridades a interceptarem dados dos provedores e prevê pena de reclusão para quem armazena, em meio eletrônico, material pornográfico, envolvendo

criança e adolescente.

Foi enviado às Comissões de Seguridade Social e Família; Ciência e Tecnologia, Comunicação e Informática e Constituição e Justiça e de Cidadania. O Projeto de Lei n.°403 dispõe sobre o acesso a informações da Internet, e dá outras providências. Podemos citar, ainda, o Projeto de Lei n°1. 713, de 1996 que procura regular acesso, tratamento e disseminação de informações através da internet. Este projeto está apensado ao Projeto de Lei n.° 1070, de 1995 que dispõe sobre crimes oriundos da divulgação de material pornográfico através de computadores.

Dentre os vários Projetos de Lei o 879/2000 que muda o Código Penal e cria o chamado projeto de "*cybercrime*". Esse Projeto de lei foi proposto em 1999 e, sem guardar muita semelhança com o projeto original, prevê a alteração do Código Penal, criando os crimes contra a inviolabilidade dos sistemas informatizados, o acesso indevido a meio eletrônico, a manipulação indevida de informação eletrônica, difusão de vírus eletrônico, a pornografia infantil. Conceitua o que deve ser entendido por meio eletrônico e sistema informatizado, além de outras alterações e acréscimos.

É importante ter em linha de consideração que o Direito Penal atua quando for absolutamente necessário. O uso excessivo de leis penais, como remédio às mazelas sociais, leva o Direito Penal à uma situação de descrédito, numa função meramente simbólica e negativa. Por outro lado, deve-se observar, também, e isso decorre do princípio da fragmentariedade, que os bens jurídicos só devem ser defendidos penalmente, ante certas formas de agressão que se apresentem intoleráveis socialmente.(MIRABETE, 2001)

A eficácia de qualquer lei está condicionada, de certa forma e não somente, à obediência à esses princípios. Quando se fala em crime informático, tendo em vista ser mais abrangente, o mais importante é estabelecer qual o bem jurídico atingido com a ação do agente. É a natureza desse bem jurídico que irá determinar a existência ou não de tipo penal para punir a conduta. A natureza desses objetos materiais que se encontram no mundo virtual não muda por estarem grafados em *bits* e não em átomos.

As coisas do mundo material podem ser grafadas em *bits*, mudando sua estrutura material para a forma virtual, mas isto não faz com que elas deixem de ser reais, mas precisam

ser atualizadas para que possam ser usadas no mundo real. Assim, não se pode ignorar que nosso Código Penal, de 1940, nos delitos de forma livre, pode, na grande maioria dos casos, solucionar os problemas relativos à criminalidade informática, basta para a sua utilização que na tipificação da conduta, o aplicador do Direito ignore a estrutura material do bem jurídico lesionado, mas considere exclusivamente as natureza do seu conteúdo.

4.5 O projeto de lei n.76 de 2000

O projeto 76/00, em seu artigo primeiro, define e tipifica os crimes de uso indevido da informática. Dentre estes crimes destacam-se a destruição de dados e de sistemas (artigo 1°, 1°, I), apropriação de dados alheios (artigo 1°, 1°, II), a supressão de dados (artigo 1°, 1°, IV), a divulgação de informações sobre a intimidade das pessoas sem que haja consentimento prévio (art. 1°, 3°, II). Para tais crimes, a pena prevista é detenção de um a seis meses, acrescida de multa.

Destacam-se, ainda, os crimes praticados contra a moral pública e a opção sexual (art.1°, 6°). Dentre estes crimes estão a corrupção de menores e a divulgação de material pornográfico. Em relação a esta divulgação o legislador deveria restringi-la somente se se tratar de pornografia infantil, de ofensa à privacidade, ou se não houver aviso prévio sobre a inadequação do conteúdo para crianças e adolescentes.

Conforme o artigo 1° da supracitada lei, os crimes de uso indevido da informática podem ser: 1) contra a inviolabilidade de dados; 2) contra a propriedade e o patrimônio; 3) contra a honra e a vida privada; 4) contra a vida e a integridade física das pessoas; 5) contra o patrimônio fiscal; 6) contra a moral pública e a opção sexual; e 7) contra a segurança nacional.

As normas do projeto de lei 76/00, devido ao fato de serem muito específicas, podem se tornar obsoletas em um curto período de tempo, uma vez que as mudanças no campo da informática ocorrem com extrema rapidez.

4.6 O projeto de lei n. 84 de 1999

O projeto trata dos crimes de informática em geral, definindo-os e prevendo as respectivas penas. Dentre os crimes elencados no projeto estão a destruição, o apagamento e a modificação de dados sem que haja devida autorização, a obtenção de acesso indevido a computadores, a criação ou introdução de programa em computador, de forma indevida, com o objetivo de destruir, apagar ou modificar outro programa de computador.

Quanto aos direitos individuais, o referido Projeto inova ao prever punição para a veiculação de pornografia em redes de computadores, sem prévio aviso aos usuários sobre a natureza da informação disponibilizada.

Os projetos supracitados têm características mais próximas do que almejam os doutrinadores brasileiros, embora, ainda esteja distante, não da perfeição jurídica, do mínimo que atenda ao presente tecnológico, de modo a proteger o sistema, o computador, seus periféricos, e também o uso adequado.

Apesar de não preencher totalmente as necessidades da área de informática, são os mais completos, e tem nos especialistas tanto da informática como do Direito, ferrenhos defensores da sua aprovação. Todavia, a normatização dos crimes de informática deve ser mais ampla, abrangendo um maior leque de condutas.

Vê-se, pois, que os projetos são abrangentes e inovadores. Apesar dos avanços, em termos de projeto, já que a legislação brasileira é pobre sobre o tema, é importante que os crimes de informática sejam normatizados ao abrigo do conhecimento técnico de condutas ilícitas, evitando-se, assim, as lacunas ocasionadas pela generalidade dos seus núcleos.

4.7 Projeto de Lei n.3773 de 2008

O Projeto de Lei 3773/08 altera a Lei nº 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente, a mesma já havia sido aprovado no Senado em julho e foi sancionado pelo do Presidente da República, prevendo punições mais rigorosas e criminaliza atos como armazenar e adquirir pornografia infantil, por exemplo, que não eram previstos na legislação anterior.

Então os artigos 240 e 241 da Lei nº 8.069 , de 13 de julho de 1990, passam a vigorar com uma nova redação. Com a Lei 11.829/08 quem "produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente", deverá enfrentar pena de reclusão, de quatro a oito anos, e multa.

Também será punido "quem agencia, facilita, recruta, coage, ou de qualquer modo intermedeia", a participação de criança ou adolescente nessas cenas.

A pena será aumentada 1/3 (um terço) se o agente comete o crime:

> I - no exercício de cargo ou função pública ou a pretexto de exercê-la; II - prevalecendo-se de relações domésticas, de coabitação ou de hospitalidade; ou III - prevalecendo-se de relações de parentesco consangüíneo ou afim até o terceiro grau, ou por adoção, de tutor, curador, preceptor, empregador da vítima ou de quem, a qualquer outro título, tenha autoridade sobre ela, ou com seu consentimento.

Além disso, quem "vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente", será apenado com: Reclusão, de quatro a oito anos, e multa.

A Lei 11.829/2008 é um avanço bastante considerável onde a sociedade fica mais rigorosa na punição desse tipo de crime, mas as entidades cobram uma ação coordenada para enfrentar o problema.

Rocha (apud QUEIROZ, 2008) entende que, no futuro, a certificação digital poderá contribuir para reduzir a presença de menores em sites de relacionamento de adultos ou em outros endereços, cujos conteúdos são de caráter erótico ou mesmo pornográfico.

Entendemos que a Lei somente não resolve. Mas já é um passo muito importante, pois contribui no conjunto de ações que devem ser adotadas para enfrentar o problema de maneira mais eficaz.

4.8 Projeto de Lei Substitutivo ao PL da Câmara nº 89, de 2003, e Projetos de Lei do Senado nº 137, de 2000, e nº 76, de 2000

Crimes como pedofilia, clonagem de cartões de crédito, envio de vírus, interceptação de senhas, dentre outros, agora serão tipificados no Código Penal Brasileiro e os infratores podem ser penalizados com multas e detenções que variam de um a seis anos de reclusão. Para tanto basta o presidente Luiz Inácio Lula da Silva sancionar o projeto de lei aprovado esta semana no Congresso que fixa novos tipos e crimes praticados com uso da informática.

Com a sanção presidencial, passam a ser crimes contra a segurança dos sistemas informatizados: a prática de pedofilia; a violação de sistemas de segurança particulares e públicos; obter e transferir dispositivos protegidos; divulgação, utilização e comercialização de informações pessoais .

O projeto ainda obriga o responsável pelo provimento de acesso a rede a manter em ambiente controlado e de segurança, pelo prazo de 3 (três) anos, os dados dos usuários e fornecê-los à Polícia mediante prévia requisição judicial; preservar imediatamente, após requisição judicial, outras informações requisitadas em curso de investigação; informar, de maneira sigilosa, à autoridade competente, denúncia que tenha recebido e que contenha indícios da prática de crime sujeito a acionamento penal .

Desde sua primeira versão, em junho de 2006 recebeu várias críticas, mas a aglutinação de diversos projetos que tratavam do tema acabou produzindo o texto consensual,

que mesmo não sendo perfeito para o momento é o possível. O Substitutivo aos projetos de lei 137/2000 e 76/2000, do Senado, e 89/2003, da Câmara. Estes projetos tratavam de crimes na Internet, portanto, são tipificados os crimes de invasão de sistemas e redes, criação e propagação de vírus, acesso e divulgação indevida de dados, pedofilia e phishing.

O senador Eduardo Azeredo juntou estes projetos e os tornou uma única lei onde modifica em alguns tópicos do Código Penal. Este projeto aprovado segue para Câmara dos Deputados e passará também por outras comissões, tendo também que ser votada em plenário.

4.8.1 O que significa o substitutivo

O substitutivo é quando unifica vários projetos legislativos, nesse caso, Projeto de Lei da Câmara 89/2003 e os Projetos de Lei do Senado 137/2000 e 76/2000. Este substitutivo altera as seguintes leis:

> Código Penal (Decreto-Lei 2.848), Código Penal Militar (Decreto-Lei 1.001), Código Processual Penal (Decreto-Lei 3.689), Código do Consumidor (Lei 8.078), Lei que regulamenta a interceptação telefônica (Lei 9.296), Lei que dispõe sobre infrações de repercussão interestadual ou internacional (Lei 10.446)

4.8.2 Alterações no Código Penal

O substitutivo acrescenta os seguintes tipos de crimes ao Código Penal:

> Dano por difusão de vírus eletrônico ou digital ou similar; Acesso indevido a rede de computadores, dispositivo de comunicação ou sistema informatizado; Obtenção, manutenção, transporte ou fornecimento indevido de informação eletrônica ou digital ou similar; Violação ou divulgação indevida de informações depositadas em banco de dados; Difusão maliciosa de código; Falsificação de telefone celular ou meio de acesso a rede de computadores, dispositivo de comunicação ou sistema informatizado. Além

de alterar crimes já tipificados no CP, como: Furto; Atentado contra a segurança de serviço de utilidade pública; Interrupção ou perturbação de serviço telegráfico ou telefônico; Falsificação de documento particular; Crimes contra a honra (título I capítulo V do Código Penal); Sonegação de papel ou objeto de valor probatório.

4.8.3Alterações no Código Penal Militar

Acrescenta também os seguintes tipos de crimes ao Código Penal Militar:

Dano por difusão de vírus eletrônico ou digital ou similar; Acesso indevido a rede de computadores, dispositivo de comunicação ou sistema informatizado; Obtenção, manutenção, transporte ou fornecimento indevido de informação eletrônica ou digital ou similar; Violação, divulgação de informações depositadas em banco de dados; Difusão maliciosa de código. E ainda altera crimes já tipificados no CPM, como: Furto qualificado; Crimes contra o patrimônio (título V do Código Penal Militar); Inutilização, sonegação ou descaminho de material probante.

4.8.4 Alteração no Código Processual Penal

Permite a prisão preventiva em caso de crime de informática, modificando essa matéria no CPP.

4.8.5 Alteração no Código do Consumidor

Os fornecedores de produtos e serviços ficam responsáveis em informar o consumidor quais são os riscos e medidas de segurança digital.

4.8.6 Alteração na Lei que regulamenta a interceptação telefônica

Com alteração que foi proposta pelo substitutivo será permitido a interceptação do fluxo de comunicações em rede de computadores, dispositivo de comunicação ou sistema informatizado.

4.8.7 Alteração na Lei que dispõe sobre infrações de repercussão interestadual ou internacional.

Em vigor a nova Lei permitirá a atuação da Polícia Federal em crimes de informática.

4.8.8 Tópicos próprios do Projeto de Lei

Além dessas alterações supracitadas, o substitutivo define tópicos próprios nos artigos 20 a 23, onde se encontram as obrigações dos usuários de redes de computadores e dos provedores de acesso. Umas destas obrigações são o registro, a identificação e a autenticação dos usuários. (BITTENCOURT, 2008).

O PLS é formado de 26 artigos sendo:

> Artigo 1º - Apresenta a LEI; Artigos 2º ao 11º - Altera o Código Penal; Artigos 12º ao 17º - Altera o Código Penal Militar; Artigo 18º - Altera a Lei que regulamenta a interceptação telefônica (Lei 9.296); Artigo 19º - Altera o Código Processual Penal; Artigos 20º ao 23º - Estabelece artigos de lei próprios; Artigo 24º - Altera a Lei que dispõe sobre infrações de repercussão interestadual ou internacional (Lei 10.446); Artigo 25º - Altera o Código do Consumidor; Artigo 26º - Dispõe sobre o prazo de entrada em vigor da lei.

Esse projeto tem gerado muitas polêmicas e não restam dúvidas de que no Brasil ou no exterior, regular crimes virtuais é uma tarefa bastante difícil. Sabe-se da necessidade de que sejam estabelecidas leis o mais rápido possível para que diminua a impunidade nos delitos, tornando menos vulnerável o processo de investigação. Também para que os usuários possa navegar com mais conforto, agilidade e acima de tudo com maior segurança.

Um dos pontos mais polêmicos é a exigência de que os provedores mantenham cadastro completo e validem o acesso dos internautas com base nos seus dados pessoais a cada conexão à web. Além disso, os provedores serão obrigados a manter os registros de acesso (logs e endereço IP) por no mínimo três anos. A pena prevista para o provedor que permitir o acesso sem identificação é de detenção, de um a dois anos, e multa. Além disso, o provedor que não mantiver os registros de acesso por três anos está sujeito de dois a seis meses de prisão.

Os críticos da proposta alegam que a exigência de cadastro e identificação representa um risco à liberdade civil dos usuários além de tornar o acesso à rede mais burocrático. Já os defensores acreditam que essa medida deve assegurar a identificação e a punição dos criminosos virtuais.

Outro ponto polêmico do projeto é o chamado "acesso indevido" (ARAS, 2008), que prevê punição de dois a quatro anos de prisão tanto para quem praticar tal crime quanto para quem fornecer os meios para que ele seja praticado, ou seja, o provedor de acesso.

A crítica a este ponto reside na falta de especificidade da legislação, que deixa aberto à interpretação dos juízes o que seria o chamado "acesso indevido". Além disso, a pena é considerada elevada e incompatível com a natureza do crime.

É necessário lembrar que a internet não criou novos bens jurídicos já tuteláveis pelo Direito Penal como patrimônio, intimidade e a honra. Depara-se então com um novo cenário onde a adoção de sistemas possibilitou a prática de certos atos lesivos que não existiam no mundo presencial, daí a necessidade urgente da aprovação de projetos, tipificando condutas penais específicos.

CONCLUSÃO

Como o Direito é uma Ciência Social, pode se concluir que sempre passa por enormes mudanças de acordo com desenvolvendo das sociedade. Então, à medida que surgem novos meios de comunicação, que se avança em termos de tecnologias, o Direito não deve ser excluído e nem se excluir desse processo, ao contrário, deve buscar acompanhar esses avanços para disciplinar as condutas que vem surgindo junto com novas tecnologias.

Os conceitos reunidos mostram polêmica e controvérsia, em razão de sua natureza e da complexidade do tema. Observando estas questões, entendemos que estes crimes devem ser observados sob a ótica do objeto material, do bem jurídico a ser protegido. Portanto acreditamos serem crimes de informática todos aqueles em que o agente se utiliza dos meios tecnológicos como instrumento ou fim do delito.

Através deste conceito foi permitido que esses crimes fossem divididos em três categorias: puros, mistos e comuns. E essa classificação permite que o legislador crie normas próprias para coibir tais práticas delitivas, aperfeiçoando as normas existentes abrangendo o universo deste tipo de crime.

Buscou se a forma como são aplicadas as normas penais existentes à certas condutas, mostrando ser possível a utilização de tais normas vigentes a estes delitos, mas sabendo que não é o bastante e percebendo as deficiências e que as já existentes não suportam os tipos criminais desta natureza.

O que se percebe também é que nem sempre ocorre o uso da lei penal vigente a estes delitos, muitas vezes o que ocorre é o desconhecimento dos aplicadores do direito, ficando o delinqüente informático à impunidade.

Por outro lado, pelos vários delitos descritos ao longo deste trabalho percebemos a imensa preocupação do Brasil e de outros países com o crescimento de métodos sofisticados delitivos perpetrados através de vias informáticas.

Foi possível constatar ao longo deste trabalho que o crescimento de forma incontida à expansão da corrida ao domínio da informática, por este motivo deve se incentivar os procedimentos de pesquisa, aquisição de tecnologia, e também que seja propiciado o estudo jurídico do direito voltado à informática. Temos certeza que o Poder Judiciário saberá enfrentar todas as barreiras com muita sabedoria e eqüidade, fazendo solucionar os conflitos informáticos e prevalecer a Justiça.

REFERÊNCIAS BIBLIOGRÁFICAS

ARAS, Vladimir. **Informática jurídica**. Disponível em: <http://www.informatica-juridica.com/trabajos/artigo_crimesinformticos.asp>. Acesso em: 10 jun. 2008.

BITTENCOURT, Gustavo. **Analise substitutivo do pls 76/2000.** Disponível em: <http://www.gustavobittencourt.com/2006/11/anlise-do-substitutivo-do-pls-762000.html>. Acesso em: 20 out. 2008.

CASTRO, Aldemário Araújo. **Crimes de informática**. Disponível em: <http://www.aldemario.adv.br/crimesinformpublic.htm>. Acesso em: 12 jul. 2008

_____. **Informática jurídica e o direito de informatica. Disponível em:** <http://www.aldemario.adv.br/infojur/conteudo4texto.htm>. Acesso em 15 jul.2008.

CASTRO, Carla Rodrigues de Araújo. **Crimes de informática e seus aspectos processuais**. Rio de Janeiro: Lúmen Júris, 2003.

_____ **Pedofilia**. Disponível em:<http://www.buscalegis.ufsc.br/arquivos/m2-pedofiliaI.html>. Acesso em: 9 ago. 2008.

COSTA, Marco Aurélio Rodrigues. **Crimes de informática.** Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=182>. Acesso em: 22 ago. 2008.

DAOUN, Alexandre Jean. Os novos crimes de Informática, **Revista Eletrônica Jus**

Navigandi, n.37, 2008. Disponível em: <http://www.jus.com.br/doutrina/texto.asp?id=1827>. Acesso em: 21 out. 2008.

MEDEIROS, Willian Ricardo. Disponível na Internet via WWW. URL: http://www.buscalegis.ufsc.br/arquivos/tecnicas_e_golpe_crimes_de_iformatica_enquadramento_penal.html.

MIRABETE, Julio Fabbrini. **Manual de direito penal**. São Paulo: Atlas, 2001.

PAESANI, Liliana Minardi. **Direito e internet**: liberdade de informação, privacidade e responsabilidade civil. 2. ed. São Paulo: Atlas, 2003.

_____. **Direito de informática**: comercialização e desenvolvimento internacional do software. 5. ed. São Paulo: Atlas, 2005.

ROCHA, N. **Movimento "Internet Segura" cobra mais ação no combate à pedofilia**. Disponível em: <http://www.convergenciadigital.com.br/cgi/cgilua>. Acesso em: 15 ago. 2008.

ROHRMANN, Carlos Alberto. **Curso de direito virtual**. Belo Horizonte: Del Rey, 2005.

SILVA, Remy Gama. **Crimes da Informática.** Disponível em: <http://www.cesarkallas.net/arquivos/livros/E-books%20de%20Direito/00715%20-%20Crimes%20da%20Inform%E1tica.pdf>. Acesso em: 17 ago. 2008.