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

JÚLIA MÁRCIA LOURENÇO DE ALMEIDA MARTINS

O AJUSTAMENTO DA NORMA PENAL PERANTE OS CRIMES DIGITAIS

SOUSA - PB
2006

JÚLIA MÁRCIA LOURENÇO DE ALMEIDA MARTINS

O AJUSTAMENTO DA NORMA PENAL PERANTE OS CRIMES DIGITAIS

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

Orientador: Professor Esp. Admilson Leite de Almeida Júnior.

SOUSA - PB
2006

JÚLIA MÁRCIA LOURENÇO DE ALMEIDA MARTINS

O AJUSTAMENTO DA NORMA PENAL PERANTE OS CRIMES DIGITAIS

Trabalho de Conclusão de Curso apresentado em, _____

BANCA EXAMINADORA

_____

Professor(a) Esp. Admilson Leite de Almeida Júnior

Orientador(a)

_____

Examinador (a)

_____

Examinador (a)

Sousa - PB

Novembro-2006

Dedicatória:

Dedico este trabalho, primeiramente a Deus, responsável pela minha existência, por ter guiado meus sonhos e por proporcionar a vitória de ter chegado até aqui. Ao meu namorado, Eraldo, pelo amor e pela paciência que teve comigo nessa caminhada, principalmente pelo colo oferecido nos momentos mais sensíveis. A Luciana, minha irmã espiritual pelas palavras de carinho e pelo constante incentivo que me deu durante todos esses anos, me fazendo acreditar que sou capaz. A meus familiares, em especial, a minha avó que me proporciona o amor de mãe, pelo apoio material que me deste para concretizar a vitória de mais uma batalha.

Agradecimentos:

Agradeço, de uma maneira muito especial, ao meu orientador Admilson Leite de Almeida Júnior. pela colaboração e incentivo na feitura desse trabalho e a minha especial amiga Zenite Nóbrega, pelo carinho e pela confiança que, constantemente, depositas em mim.

RESUMO

A pesquisa abordará o tema do ajustamento normativo em face dos crimes digitais, passando pelo histórico da Internet e sua popularidade no Brasil. Logo em seguida, tratar-se-á dos Princípios norteadores das relações jurídico-penais, mais precisamente do Princípio da Reserva Legal, por ser este o mais diretamente afetado quando se pretende enquadrar figuras típicas ainda não contempladas pela lei em vigor. É realizado também um enfoque sobre a classificação da nova modalidade delituosa e seus reflexos no ordenamento jurídico, assim como um direcionamento voltado à necessária tipificação dos que não estão enquadrados no Direito pátrio em defesa do não uso da analogia. O ponto principal da pesquisa consiste na atitude de ajustar o ordenamento a um fato novo, fato este que carece de uma urgente proteção por violar bens considerados vitais para a sociedade atual. Por isso, aponta-se a necessidade da aprovação do Projeto de Lei nº84/99, que versará sobre os crimes cometidos no espaço digital. Mostrará, por fim, o posicionamento da jurisprudência assente no que tange ao enquadramento penal dos crimes de informática. Para isso será adotada a técnica da documentação indireta, através de pesquisas bibliográficas e publicações em geral.

Palavras-chave: internet. crimes digitais. ajustamento penal.

ABSTRACT

The research will approach the subject of the normative adjustment in face of the digital crimes, passing for the description of the Internet and its popularity in Brazil. Immediately afterwards, one will be about the Principles Constitutional norteadores of the legal-criminal relations, more necessarily of the Principle of the Legal Reserve, for being this more directly affected when it is intended to fit typical figures not yet contemplated by the law in vigor. In special way when it is treated to apply the law the cases not contemplated for this, but that they need the state defense, before the materiality of its harmful effect to the social seio. An approach on the classification of the new delictual modality, the new goods is also carried through ranks in evidence for the use of the Internet and its consequences in the legal system, as well as an aiming come back to the necessary tipificação of that they are not fit in the native Right in defense of not the use of the analogy. The main point of the research consists of the attitude to adjust the order to a new fact, fact this that lacks of a urgent protection for violating goods considered vital for the current society. Therefore, it is pointed necessity of the approval of the Project of Law nº84/99 that it is in transaction in the National Congress and that will turn on the crimes committed in the digital space. It will show, finally, the main on crimes to Computer science and that they are part of the current scene of crime, as well as the positioning of the jurisprudence seats in what it refers to to the criminal framing of the computer science crimes. For this the technique of the indirect documentation will be adopted, through bibliographical research and publications in general.

Word-key: Internet. Digital crimes. Criminal adjustment.

SUMÁRIO

INTRODUÇAO

A Internet se mostra como uma das melhores expressões da modernidade. Torna-se um instrumento capaz de alterar as relações sociais no âmbito político, econômico e social. Inevitavelmente a mudança no seio social gerada em decorrência desse instrumento tecnológico, proporciona uma reação jurídica sobre o tema. Novos conceitos são postos a analise da ciência jurídica e o ajustamento do Direito Positivo aos fatos advindos da disposição da Informática é a necessária e imediata resposta que o ordenamento pátrio oferece diante da nova realidade.

Porém para que o reajuste do sistema normativo atual aconteça de maneira fiel às aspirações sociais, diante da inevitável dependência da sociedade dos recursos tecnológicos, se faz necessário o conhecimento pormenorizado do conceito, histórico e desenvolvimento da Internet. O primeiro capitulo desse trabalho tratará, de maneira nítida, sobre os aspectos particulares da imensa rede que é a Internet, suas principais características, seu funcionamento e sua conseqüente regulamentação no Brasil, de maneira que proporcione ao legislador e ao aplicador do Direito, uma visão ampla e técnica do meio digital, tão necessária quando se trata da tipificação de condutas perante novos conceitos. Ver-se, pois, que se faz necessária a classificação dos crimes já expostos no Direito Penal pátrio, na qual apenas se utilizam das ferramentas proporcionadas pela Internet para praticar delitos já tipificados na lei em vigor, denominados como crimes digitais impuros, daqueles que carecem de uma proteção especifica e ligada ao próprio recurso tecnológico , sendo imprescindível para a configuração

do crime a existência do sistema de dados. considerados como crimes digitais puros.

Dentre os Princípios resguardados pela Constituição Federal de 1988, um deles merece destaque no que tange ao ajustamento do ordenamento jurídico pátrio diante dos fatos prejudiciais ao equilíbrio social e que sejam operados através da Internet: o Princípio da Reserva Legal. De acordo com esse Princípio, que mais se configura uma garantia individual, nenhum ato humano pode ser considerado crime sem que exista uma lei, em sentido estrito, que o determine. Isso significa que alguns crimes perpetrados através da Internet, e que violam bens ainda não amparados no ordenamento jurídico atual, não estão sujeitos aos efeitos coercitivos da lei e é sobre essa ótica que o segundo capítulo abordará a problemática. Diante disso, cabe aos construtores da lei a tarefa de verificar fatos que carecem de uma regulamentação especifica, como também de uma repressão eficaz, em observância aos Princípios Constitucionais já consagrados, a exemplo do já citado Princípio da Reserva Legal.

Diante da função normativa de aproximar a realidade do Direito, surge a necessidade da tipificação de condutas penais ligadas aos crimes digitais. Razão pela qual o terceiro capitulo apontará alguns dos principais crimes digitais cometidos nos dias de hoje , que encontram subsidio legal , quais sejam aqueles que apenas utilizam o sistema de dados para a consumação da ação delituosa, mas que ainda necessitam de uma integração conceitual diante de bens jurídicos inéditos apresentados pelo impacto tecnológico na sociedade. E abordado também a aplicação integrativa das leis atuais perante a necessária resposta que o Poder Judiciário deverá fornecer diante de lides que envolvam crimes realizados através das ferramentas proporcionadas pela Internet, e seus reflexos jurídicos,

tendo em vista o impedimento do uso da analogia em se tratando de normas incriminadoras ou agravantes.

A urgência inerente ao tema, no que tange à atualização das leis brasileiras diante de crimes cometidos pelos recursos digitais, se traduz na necessária votação do Projeto de Lei nº 84/99 de autoria do Deputado Luiz Piauhylino, em que pretende proteger o usuário da Internet, tipificando agressões ao normal funcionamento do sistema de dados.

O tema do presente trabalho é justamente o aprimoramento da legislação brasileira em face das novas modalidades de delitos, cometidos pelos recursos que o desenvolvimento tecnológico oferece à sociedade atual. A ausência de uma legislação especifica para delitos dessa espécie vem gerando divergências doutrinárias e jurisprudenciais quanto ao alcance das leis em vigor diante dos crimes digitais. A questão é atual e importante por gerar na comunidade usuária da Internet e nos demais membros da coletividade uma insegurança, pelo fato do Código Penal em vigor e as demais leis extravagantes não acompanharem o avanço da conduta delitiva, indubitavelmente presente nos dias de hoje.

Os métodos procedimentais adotados foram o histórico e o analítico-sintético, na qual se buscou analisar posições doutrinárias e jurisprudenciais, ressaltando as divergências existentes quanto ao tema, assim como foi utilizado o método dedutivo de abordagem, eis que se partindo de considerações gerais, enunciados, princípios e análise doutrinária e jurisprudencial, buscou-se soluções aos problemas suscitados no decorrer do texto, empregou-se também, a técnica da documentação indireta realizando levantamento de dados através da pesquisa bibliográfica de publicações como livros, publicações avulsas, teses, etc.

O objetivo do presente trabalho é fornecer subsídios científicos para os aplicadores do Direito e profissionais da área, através de uma pesquisa que busca sanar possíveis dúvidas decorrentes da aplicação da legislação atual em face das peculiaridades decorrentes dos crimes digitais, em virtude da ausência de lei que o tipifique sob os moldes que o sistema de dados exige.

CAPITULO 1 ASPECTOS TÉCNICOS DOS CRIMES DIGITAIS

Quando se estiver diante de situações peculiares, deve-se assim tratá-las, usando a isonomia material de que desigual deve ser tratado por desigual, de fato, se qualificar. Os crimes digitais, que se mostram essencialmente inovadores, fazem parte de uma espécie de delito que surpreende o direito positivo exigindo uma abordagem cuidadosa e detalhada sobre seus aspectos particulares, pois, para que a ciência jurídica acompanhe o ajustamento desse novo fato social ao ordenamento pátrio, faz-se necessário o conhecimento pormenorizado dos seus elementos. Convém ainda, antes de conhecer o uso maléfico da Internet, enquanto imensa rede que liga milhões de pessoas em fração de segundos, conhecer a história e o desenvolvimento desta para, enfim, visualizar nitidamente os crimes cometidos neste espaço.

1.1 Conceito e histórico dos crimes digitais

O que hoje se conhece por Internet, nasceu no final de década de 1960 pelo Departamento de Defesa dos Estados Unidos, denominado ARPANET (*Advanced Research Projects Agency Net – Agência de Projetos de Desenvolvimento Avançado)*, com a específica função de resistir a ataques militares como também proporcionar pontos estratégicos para o governo americano. O objetivo desse projeto era criar uma rede interligada que mantivesse a comunicação das bases militares à medida que não deixasse vulnerável ao ataque soviético um único centro de comando, proporcionando, desta forma, maior segurança. Essa finalidade retratava o período histórico pelo

qual esse país atravessava, o período da Guerra Fria, quando acontecia uma assustadora corrida armamentista através do aprimoramento tecnológico.

A idéia de comunicação entre os computadores favoreceu a criação de um sistema descentralizado de comando, uma vez que não existiria mais um centro estático que dominasse as informações, mas uma rede interligada que "conversasse" com outros computadores através de uma linguagem própria constituída por um pacote denominado TCP/IP (*Trasnmission Control Protocol / Internet Protocol)*. A utilização desse sistema de interconexão e comunicação juntamente com o sucesso obtido pelo pacote TCP/IP, pela sua fácil implementação numa variedade de plataformas nos diferentes *hardwares* de computador, despertou a iniciativa das Universidades Americanas no projeto, causando o que posteriormente adveio: o desmembramento em um ramo militar e outro civil. Este último voltado especificamente para pesquisa e desenvolvimento na área de redes de computadores. Com isso, instituições de ensino e pesquisa dos Estados Unidos, além de grandes empresas da área de informática, deram origem à imensa rede, hoje denominada Internet.

Desenvolvida por civis, a Internet vem, de uma forma avassaladora, ampliando o quadro de suas funções. Algumas são classificadas como "serviços básicos da internet", como por exemplo, as de correio-eletrônico, de transferência de arquivos e de acesso remoto a computadores. O desenvolvimento e a acessibilidade a esse recurso tecnológico deve-se também à contribuição da Física e da Eletrônica, áreas do conhecimento que, paralelamente ao avanço da rede , vêm progredindo em termo de pesquisa.

Pode-se conceituar a Internet como um novíssimo meio de comunicação, marcado pela utilização comum de um protocolo capaz de permitir o acesso de

qualquer computador a outros, interligados através de linhas comuns de telefone, denominada *modem,* linhas de comunicação privada, linhas de transmissão de fibra ótica, canais de satélite e diversos outros meios de conexão. A Internet seria, portanto, uma vasta coleção de grandes e pequenos computadores interligados em redes que se estendem pelo mundo inteiro.

Como expressão maior da globalização, a Internet torna-se símbolo da pós-modernidade, cuja riqueza se traduz na informação, entendida aqui com a imediata transmissão de dados. Esta rede se apresenta como o paraíso da informação que, como um bem de grandioso valor na sociedade atual, atrai inevitavelmente o crime, pois como bem diz Corrêa (2000, p. 42); "onde há riqueza há crime". Mais ainda, quando se apresenta diante da fragilidade que esta riqueza, enquanto sistema integrado de dados, ainda representa, por não estar, de todo, regulamentada. No lugar de metralhadoras e armas, delinqüentes desse meio agora usam uma rede de computadores e sofisticados programas que proporcionam a mais ampla liberdade nesta grande aldeia mundial, surgindo os crimes denominados crimes digitais ou crimes informáticos.

Entende-se por crime digital qualquer ação em que o computador seja o instrumento ou objeto do delito ou então qualquer crime ligado ao tratamento automático de dados. Vale ressaltar que os crimes se classificam em crimes digitais puros e impuros. Estes se caracterizam pelo fato de serem também cometidos fora do ambiente "virtual" que a internet proporciona, ou seja, é o fato típico e antijurídico que se caracteriza mesmo não existindo o recurso da rede, é independente deste e o utiliza apenas como meio para sua execução, estando tais crimes já tipificados pela nossa legislação penal, como por exemplo, o crime de estelionato (Art. 171, CP). Já os crimes digitais puros são aqueles em que o

objeto do delito, ou seja, o bem tido como prejudicado, é o próprio sistema de dados, o que significa que só podem ser concebidos em face deste, sendo tais fatos nocivos ao sistema como um todo. Ao contrário dos crimes digitais impuros, os crimes digitais propriamente ditos, não encontram resguardo legal pelo ordenamento jurídico atual.

O meliante digital detém características proporcionadas justamente pelo avançado meio em que se desenvolve como também pela fragilidade da evolutiva transmissão de dados, peculiaridades estas que o difere dos demais, tanto na utilização de ricos conhecimentos técnicos, como na operacionalidade da ação criminosa. Dentre as vantagens que essa nova espécie de delinqüente possui, está o anonimato, visto que se constitui uma tarefa difícil identificar, com a nitidez exigida pela legislação penal na imputação de um crime, aquele que está por trás de um computador e necessariamente onde este se localiza, já que se trata de um problema de ordem mundial, pela proporção que a rede se estendeu. É inegável que o anonimato está para o criminoso com uma forte garantia da eficácia de sua ação; em contrapartida, para as autoridades responsáveis pela sua detenção se apresenta como um dos maiores obstáculos.

Embora seja uma tarefa difícil, a necessária identificação do autor do delito não se configura impossível, pois, por padrão, a conexão (primeiro passo do indivíduo ao ingressar na rede) só se dá através do protocolo TCP/IP (*Transmission Control Protocol / Internet Protocol)* e essa arquitetura, que mantém a comunicação entre os computadores, realiza a divisão das funções do sistema de comunicação em estruturas de camadas. Em TCP/IP, tais camadas são: Aplicação, Transporte, Inter-Rede e Rede. São nessas últimas camadas que o anonimato pode ser ameaçado, já que são atribuídas a elas funções

importantíssimas na conexão, como o endereçamento de *datagramas*, que possui entre as informações de seu controle o endereço IP do destinatário e do emitente. Os protocolos desta camada possuem um esquema de identificação do diálogo das máquinas que estejam interligadas, melhor dizendo, nas máquinas que estejam conectadas na rede. É escolhido um identificador para detectar cada máquina e a própria rede onde esteja situada, ou seja, o próprio IP, que é independente de qualquer outro endereçamento que possa existir nessa conexão, nos níveis inferiores. Embora ainda haja dificuldade para as autoridades responsáveis reprimirem os delitos dessa natureza, pelo fato do IP na Internet não ser fixo, utilizando-se racionalmente e privilegiadamente o tempo, sem delongas, por exemplo, na expedição de uma ordem judicial que possa autorizar o provedor a rastrear de onde foram feitos os acessos, através dos arquivos de log's (espécie de registro detalhado de todos os acessos); há a possibilidade de obter uma investigação criminal eficaz nessa área.

A medida que se aprimora a rede mundial, com investimentos cada vez mais intensos, o criminoso se especializa no espaço virtual de maneira assustadora, chegando a proporcionar os próprios ditames para o avanço, pois são, ao contrário dos criminosos conhecidos na doutrina tradicional, cidadãos que tiveram a oportunidade de se aprimorar, geralmente jovens de 15 a 25 anos, de classe média ou alta, detentores de amplos conhecimentos na área de informática. São os famosos *hackers e crackers* que, muitas vezes, influenciam o avanço do sistema pela influência reversa aos que precisam deter conhecimentos mais "avançados" para obstar ou ao menos prevenir a ação maléfica na rede. Tendo por núcleo de sua denominação o verbo *hack* (no sentido de golpear), os *hackers* são sujeitos aptos a invadir sistemas, atuam por emulação, desafiando

seus próprios conhecimentos técnicos e a segurança de sistemas informatizados de grandes companhias e organizações governamentais. No início da cultura cibernética, eram tidos como heróis da revolução informática porque teriam contribuído para o desenvolvimento da indústria do *software* e para o aperfeiçoamento dos computadores pessoais e de segurança dos sistemas informáticos. Os *crackers*[1], por sua vez, são os "*hackers aéticos*". Invadem sistemas para adulterar programas e dados, furtar informações e valores, enfim, prejudicar pessoas através do sistema interligado que a Internet proporciona. Praticam fraudes eletrônicas e derrubam redes informatizadas, causando prejuízos a vários usuários e à coletividade. Enquanto os *harckers* têm a intenção de desafiar seus próprios conhecimentos, estes objetivam precipuamente prejudicar o regular processamento de dados.

1.2 O surgimento da Internet e sua regulamentação no Brasil

No Brasil, o surgimento da Internet deu-se no meio acadêmico. Em 1988, Oscar Sala, professor da Universidade de São Paulo (USP) e conselheiro da Fundação de Amparo à Pesquisa no Estado de São Paulo (Fapesp), desenvolveu a idéia de estabelecer contatos com Instituições de outros países para compartilhar dados por meio de computadores. O primeiro passo já teria sido dado. Foram necessários, porém, sete anos para que os ministérios das Comunicações e Tecnologia autorizassem o uso comercial da Internet no país, pois somente em 1995, teve início a abertura da Internet sob a modalidade

[1] Parte lógica do computador, aquela que você não pode ver nem tocar, mas opera constantemente.

comercial, a partir de um projeto piloto da Embratel que permitia o acesso à rede através de linhas discadas.

Há quem afirme, no entanto, que a história da Internet no Brasil, confunde-se com a própria história da Rede Nacional de Pesquisa (RNP), razão pela qual não se pode deixar de tratar dessa Instituição. A Rede Nacional de Pesquisa (RNP) foi criada no ano de 1989, através do incentivo da comunidade acadêmica de São Paulo e do Rio de Janeiro, com o precípuo escopo de coordenar e disponibilizar serviços de acesso à Internet no Brasil. Construindo, assim, uma infra-estrutura da rede Internet no âmbito acadêmico, por isso, dizer-se que o surgimento da Internet no país foi implementado para o uso nesse meio. A Rede Nacional de Pesquisa, como era inicialmente denominada, tinha também a função de inseminar o uso de redes no país, ou seja, na sociedade civil como um todo. Em paralelo à implantação estrutural da Internet no país, a Rede Nacional de Pesquisa dedicou-se a tarefas múltiplas, tais como divulgar os serviços oferecidos pela Internet no meio acadêmico através de seminários, montagens de repositórios e treinamentos, estimulando a consciência acerca de sua importância estratégica para o país e tornando-se referência em aplicação de tecnologias associadas à internet.

Em 1995, o Ministério da Ciência e Tecnologia (MCT) juntamente com o Ministério das Comunicações constituíram um órgão responsável pela regulamentação e desenvolvimento da Internet em nosso país; o Comitê Gestor Internet. Esse importante órgão foi criado pela Portaria Interministerial nº. 147 de 31 de maio de 1995, alterada pelo Decreto Ministerial nº. 4.829 de 03 de dezembro de 2003, para coordenar e integrar todas as iniciativas de serviço de Internet no país: movendo a qualidade técnica, a inovação e inseminação dos

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

Dentre as principais atribuições do Comitê Gestor Internet do Brasil, pode-se destacar os seguintes: a propositura de normas e procedimentos relativos à regulamentação da Internet; a recomendação de padrões e procedimentos técnicos operacionais para a Internet no Brasil; a promoção de estudos e padrões técnicos para a segurança das redes e serviços no país e a coordenação da atribuição de endereços de Internet (IPs) e do registro de nomes de domínio (designação de endereço eletrônico) usando o sufixo ".br" .

No entanto, o Comitê Gestor da Internet frise-se, carece de maior expressão e poder de regulamentação, pois como se percebe, atêm-se a normatização técnica e administrativa da Rede, embora forneça subsídios informativos quanto a temas de relevância jurídico-legal, tendo em vista o amálgama formado pelos temas jurídicos e técnicos quando nos referimos à Internet, ou seja, quando tratamos de sua regulamentação. Exemplo desta benéfica contribuição por parte do Comitê é o fornecimento, de forma gratuita, da "Cartilha de Segurança Jurídica"; das "Recomendações para Desenvolvimento e Operação da Internet/BR" e das "Recomendações para evitar invasões".

Todo o usuário que queira abordar a questão da regulamentação da Internet no Brasil seja enfocando a Internet como um todo, preocupado com os crimes que possam ser cometidos com o uso da rede, seja visando ao comércio eletrônico e a necessidade de propiciar segurança e fidelidade nas transações comerciais, contratos, assinaturas e similares, deve, primeiramente, estudar as "Recomendações para Desenvolvimento e Operação da Internet no Brasil", que possui, dentre outras, as seguintes orientações: a necessidade da adoção de meios de acesso (telefonia, cabos e outras tecnologias que permitam a identificação inequívoca da origem de ataques à segurança da rede, seus serviços e usuários), além da brilhante recomendação da adoção pelos respectivos provedores, de práticas de cadastramento e recadastramento das contas dos usuários de forma a obter dados cadastrais completos que permitam obter a identificação de pessoa natural ou jurídica que utiliza a Internet.

No que se refere aos bens jurídicos lesados pela violação do sistema e sua normal funcionalidade,verifica-se pouca regulamentação quanto ao âmbito penal, encontrando-se alguns tipos em normas esparsas como, por exemplo, no Art. 10 da Lei Federal nº. 9.296/96, que considera crime punível com reclusão de 2 a 4 anos e multa, "realizar interceptação de comunicações telefônicas ou telemática, ou quebrar segredo de Justiça , sem autorização judicial ou com objetivos não autorizados em lei " , além de algumas adaptações do Código Penal vigente, como no Art. 313-B , introduzido pela Lei nº. 9.983/ 2000 que tipificou o crime de modificação ou alteração não autorizada do sistema de informações. Já quanto aos direitos autorais, o legislador teve uma visão futurista e, antevendo o desenvolvimento da era digital, inseriu no texto da Lei nº. 9.610/98, a devida proteção aos direitos autorais das obras quando considera, de uma forma

brilhante, que obras possam ser armazenadas, inseridas e disseminadas nesse meio imaterial, conferindo eficácia à proteção aos direitos autorais, inclusive, independentemente do registro.

Tais tipificações não resolvem o problema da criminalidade na Internet, do ponto de vista do direito objetivo, mas revelam a preocupação do legislador infraconstitucional de proteger os bens informáticos e de assegurar, na esfera penal, a proteção de dados e interesse da Administração Pública e do Estado Democrático, bem como a privacidade "telemática" dos indivíduos. Entretanto o reconhecimento da lesividade de condutas que surgem à proporção em que a Internet se populariza e à noção da intervenção mínima, impõem que outros bens jurídicos, além dos listados, sejam pinçados e postos sob a tutela penal. Por isso mesmo, está em tramitação no Congresso Nacional o PLC, Projeto de Lei da Câmara dos Deputados nº. 84/89, de autoria do Deputado Luiz Piauhylino (PSDB-PE), que pretende inserir no rol dos novos tipos penais, o crime de dano a dado ou programa de computador, acesso indevido ou não autorizado, alteração de senha ou acesso a computador ou dados, violação de segredo industrial, comercial ou pessoal em computador, criação ou inserção de vírus, oferta de pornografia em rede sem aviso de conteúdo, e publicação de pedofilia, cominando-se penas que variam entre um e quatro anos.

1.3 O funcionamento da Word Wide Web

Urge fazer uma importantíssima distinção entre a Internet, enquanto grande rede que interliga computadores através de uma linguagem própria (TCP/IP) e o recurso da World Wide Web, enquanto integrador de informações, dentro do qual

a grande maioria das informações disponíveis na Internet podem ser acessadas, de formas simples e consistente em diferentes plataformas. Fazendo um comparativo factual e hipotético, pode-se dizer que a Internet seria a avenida e os diferentes transportes nas quais as pessoas utilizam para se deslocar seria o recurso da World Wide Web.

Para conceituar a World Wide Web, torna-se necessário o conhecimento do que seja "hipertexto", já que ambos, muitas vezes, em sua praticidade, se confundem. A idéia do hipertexto foi desenvolvida pelo visionário Ted Nelson em meados dos anos 70, constituindo um documento que possui palavras em seu bojo as quais, quando selecionadas pelo usuário, conduzem-no para outro documento, relacionado àquele vocábulo que lhe serviu de "atalho". A idéia daquele pensador era, diante da grande rede que é a internet, conectar toda a informação mundial em um sistema gigante de "hipertexto" (palavra que etimologicamente significa grande texto) fazendo sua relação dentro de uma base de dados única.

Assim, pode-se visualizar a World Wide Web, como uma convergência de concepções ou idéias relativas à grande Rede, utilizando-se de um padrão universal que permite e intensifica o acesso de qualquer computador ligado à Internet ao hipertexto, procurando, assim, interligar toda a informação dispersa nela. Corrêa (2000, p. 11) conceitua a "WWW" como;

> 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 de 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.

No que tange aos benefícios que a WWW proporcionou à Internet, destaca-se com muita propriedade a simplicidade que seu funcionamento emprestou para a expansão da rede e a sua conseqüente acessibilidade. Essa operacionalidade simplificada pode ser entendida facilmente através da análise dos três importantes componentes desse sistema de hipertexto, quais sejam: a utilização de uma inferface amigável, a habilidade de incorporar uma vasta gama de tecnologias e tipos de documentos na transferência e a importantíssima capacidade de permitir a leitura universal, o que significa que qualquer pessoa que acesse uma página , de qualquer lugar, utilizando qualquer tipo de computador, poderá lê o mesmo documento que simultaneamente, outra pessoa, em qualquer parte do mundo estiver acessando.

O sistema WWW permite a estadia de um documento em um determinado local (identificado por um endereçamento eletrônico único, denominado URL) para que todos possam acessá-lo. Tal sistema percorre quatro fases, que obedecem ao protocolo de transferência de hipertexto HTTP, "hypertext transfer protocol", que são os caminhos que a informação segue dentro da rede de maneira a se tornar acessível a qualquer aparelho ligado à Internet: a conexão, fase na qual navegador tenta relacionar-se com o servidor endereçado; o requerimento, em que o navegador especifica o tipo de servidor selecionado; a terceira fase seria a resposta, quando acontece a transação de informações entre o navegador e o servidor e, por ultimo, o fechamento que caracteriza o término da conexão com o servidor.

No inicio da utilização da Web, colocava-se documentos apenas em texto, porém devido ao surgimento da linguagem construída e utilizada pela World Wide Web, qual seja o HTML, desenvolveu na Internet uma comunicabilidade fácil e

atrativa. Seu funcionamento é bastante simples, operando numa série de códigos escritos em formato texto, também conhecido como formato ASCII[2]. São códigos traduzidos pelos programas navegadores, tais como o *Internet Explorer,* em formatos específicos na tela, onde o usuário possa interagir. Dessa forma, a linguagem utilizada é capaz de produzir sons, imagens, listas, formas, mapas e muito mais. A revolução na linguagem de comunicação entre o usuário e a rede resultou justamente no surgimento de uma interface interativa, fazendo da Internet, sobretudo através da WWW, algo mais simples e claro. O que faz da linguagem HTLM importante para o desenvolvimento da Internet é a interpretação de seus códigos pelos navegadores, com o aparecimento de alguns itens em sublinhado, criando os famosos *links,* ou seja, dispositivo que dirige a navegação intuitiva na Web, materializando a idéia de hipertexto e, conseqüentemente, atraindo investimentos na rede, pelo espaço rico em multimídia, enquanto apresentação de informações de maneira multissensorial e integrada sendo, portanto, favorável ao comércio e as demais transações comerciais.

[2] ASCII (American Standard Code for Information Interchange); padrão muito usado em todo o mundo, no qual números, letras maiúsculas e minúsculas, alguns sinais de pontuação, alguns símbolos e códigos de controle correspondem a números de 0 a 127.

CAPÍTULO 2 O PRINCÍPIO DA RESERVA LEGAL PERANTE OS CRIMES VIRTUAIS

Cada caminho, cada norma, cada regra contém um juízo de valor prévio e necessário, o que legitima a referida conduta na qual se impõe. O ordenamento jurídico é revestido de valores ditados por princípios de Direito Natural além de estabelecer critérios de acordo com a conjuntura que o justifica enquanto expressão de poder. No que se refere ao trabalho em tela, tem-se, prioritariamente, que ater-se à visão do Estado Democrático de Direito, na qual há garantias, conquistadas gradativamente durante a história moderna e princípios específicos norteadores do direito penal, perpassando pelo ramo constitucional quais sejam: o Principio da Legalidade, e seus sub-ramos; Princípio da Reserva Legal e da Anterioridade da Lei. No que tange aos fatos advindos do inevitável progresso tecnológico, resta o adequado reajuste das normas, disciplinando a proteção dos novos valores, sem perder de vista tais princípios que o orientam.

2.1 O Princípio da Reserva Legal na legislação brasileira

No patamar mais elevado da "pirâmide", dentro do qual, para efeito de estudo pretende-se enquadrar o ordenamento jurídico pátrio, encontram-se as determinações da Constituição Federal de 1988. No cume desse sistema normativo está, justamente, o princípio que representa a decisão política fundamental, que consiste na incursão do ordenamento brasileiro numa espécie de "status" de garantia, ou seja, enquadra-se o ordenamento e os sub-princípios que orientam o poder estatal como um todo, num sistema denominado Estado Democrático de Direito. Tal sistema tem como corolário o respeito às garantias

dos cidadãos que, pela sua fundamentação, outorga os poderes para que se instituam as leis, de maneira que esse elemento humano detenha a garantia de conviver num Estado onde não haja arbítrio e tirania por quem detém o poder, mas que este se legitime em função destas garantias.

O Princípio da Legalidade surgiu expressamente e primordialmente, na "Magna Carta", imposta pelos barões ingleses ao rei João Sem Terra, no ano de 1215. Seu artigo 39 previa que nenhum homem livre poderia ser submetido a pena não prevista em lei local, surgindo a essencial idéia da reserva legal. Posteriormente, no direito moderno, já sob a influência do Iluminismo, esse Princípio ganhou força com a finalidade de combater a insegurança dos cidadãos, gerada pelo arbítrio dos julgadores. A teoria da separação dos poderes, preconizada por *Montesquieu* contribuiu para a estruturação desse sistema, à medida que defendia a vedação da usurpação, pelo Judiciário de função própria do Legislativo, não permitindo que considerasse criminosas condutas assim não contempladas pelo legislador. De fato, a partir da separação funcional dos Poderes, ao legislador passou a competir a função de selecionar, dentre o imenso rol de comportamentos humanos, os mais perniciosos ao corpo social e, assim, defini-los como crimes e conseqüentemente cominar-lhe a correspondente sanção penal. Por outro lado, ao juiz coube a tarefa de aplicar aos casos concretos, estrita e rigorosamente, apenas o que estivesse estabelecido nas regras penais objetivas. A partir dessa idéia de proclamação das liberdades públicas, o princípio da legalidade veio a ser respaldado nos mais importantes diplomas consagradores da igualdade entre os homens, tal como o *Bill of Rigths,* firmado na Filadélfia, em 1774; a Constituição dos Estados Unidos da América, a Declaração Universal dos Direitos do Homem, durante a Revolução Francesa em

1789, dentre outros grandes diplomas dos direitos humanos. No Brasil, louvavelmente, o princípio foi acolhido em todas as Cartas Constitucionais, desde a Constituição Imperial datada de 1824 até a nossa atual Constituição Federal de 1988.

O respectivo trabalho tem a específica função de tratar do Principio Constitucional da Liberdade, que está no rol das classificadas "garantias constitucionais", ou seja, direitos invioláveis em que o Estado tem o duplo dever: o positivo, de proporcionar a praticidade daqueles direitos primordiais e o negativo, que seria a abstenção do Estado perante esses, através da não intervenção, o que significa que ele age em defesa dos direitos quando limita a extensão do poder. Tal princípio se traduz na liberdade do particular agir livremente dentro do contexto social, pois está permitido para o cidadão tudo o que a lei não considera nocivo, e conseqüentemente, não tipificado como crime. Ou seja, vale aqui o brocardo que para o particular "tudo o que não for proibido, é permitido". Essa expressão popular nada mais é que a tradução simplificada de um dos princípios mais importantes da legislação brasileira; o Princípio da Legalidade.

O Princípio da Legalidade nasceu do anseio de estabelecer na sociedade humana regras permanentes e válidas, que fossem obras da razão e que pudessem abrigar os indivíduos de uma conduta arbitrária e imprevisível da parte dos governantes. Tinha-se em vista alcançar um estado geral de confiança e certeza na ação dos titulares do poder, evitando-se assim a dúvida, a intranqüilidade, a desconfiança e a suspeição, tão usuais onde o poder é absoluto e acha dotado de uma vontade pessoal soberana ou se reputa absoluto e onde, enfim, as regras de convivência não foram previamente elaboradas nem reconhecidas. Esse precioso Princípio encontra na sua própria descrição, duas

subdivisões explícitas de dois outros princípios de igual relevância para o Estado Democrático de Direito, quais sejam o Princípio da Reserva Legal e o Princípio da Anterioridade da Lei. O artigo 5º da Constituição Federal de 1988 estatui no seu inciso XXXIX que *"não há crime sem lei anterior que a defina, nem pena sem prévia cominação legal"*.

Ao consagrar que não há crime nem pena a ser cominada, isto é, que não há agressão a bem jurídico tutelado pelo ordenamento penal brasileiro como também que não há a aplicação de seu conseqüente preceito secundário que é a sanção, sem a respectiva lei que o determine em letras precisas, impessoais e evidentes e que o crime também não iria se configurar sem que antes existisse uma lei em vigor que o determinasse, estar-se-ia diante dos respectivos princípios: Princípio da Reserva Legal, por reservar a lei em sentido estrito a definição dos fatos típicos, e da Anterioridade, pela garantia de que o fato apenas será considerado crime se já existir a lei que o classifique antes do cometimento da ação, ou seja, sem a instabilidade de uma posterior condenação por lei subseqüente à realização do fato. Faz-se aqui a necessária e polêmica distinção entre o Principio da Legalidade e seu ramo específico que é o Princípio da Reserva Legal; ao primeiro se considera abrangência mais significativa que ao segundo, uma vez que por ele fica certo que qualquer comando jurídico impondo comportamentos forçados há de provir de espécies normativas devidamente elaboradas conforme as regras do processo legislativo constitucional. Por outro lado, o Princípio da Reserva Legal se dá de maneira mais restrita e prática, por incidir somente sobre os campos materiais especificados pela Constituição Federal. Se todos os comportamentos humanos sejam direta ou reflexamente,

estão sujeitos ao princípio da Legalidade, somente alguns são submetidos ao Princípio da Reserva da Lei.

Constitucionalmente assegurado, o principio da reserva legal deixa a cargo exclusivo do Poder Legislativo a apreciação valorativa do que seja crime, materialmente considerado, ou seja, será legítimo aquele órgão quando se tratar da tipificação dos delitos, de maneira que o processo legislativo atenda aos ditames da própria Carta Magna, decorrendo de obra elaborada perante o "devido processo constitucional" e, aqui, se poderia ressaltar a competência especifica e indelegável da União para legislar sobre matéria penal, o que significa que somente o Congresso Nacional tem a possibilidade ou legitimidade para legislar sobre as condutas que avançam a legislação atual e desrespeitam bens ainda não protegidos pelo Direito Positivo, embora estejam enquadrados na realidade social, tais como os crimes cometidos na era digital.

No âmbito penal, este princípio se reveste de uma garantia fundamental. A figura típica é apresentada unicamente pela lei em seu sentido estrito, o que afasta a possibilidade de incriminação ou agravação da pena através de normas subalternas a esta, como por exemplo, a Medida Provisória. Desta forma, exerce função assecuratória do primado da liberdade, a partir do momento em que somente se pune alguém pelos requisitos desta lei, ou seja, que o fato seja típico e antijurídico, deixando os membros da coletividade protegidos contra toda e qualquer espécie de invasão arbitrária do Estado em seu direito de liberdade. Assim, o Princípio da Reserva Legal possui uma regra, segundo a qual ninguém poderá ser punido pelo poder estatal, nem sofrer qualquer violação em seu direito de liberdade e uma exceção, pela qual os indivíduos somente serão punidos se, e somente se, vierem a praticar condutas previamente definidas em lei como

indesejáveis. Pode-se, portanto, sintetizar o princípio da Reserva Legal, no campo penal, como o mais importante de seus princípios por corresponder a uma aspiração básica e fundamental do homem: a de ter uma mínima proteção contra qualquer forma de tirania e arbítrio dos detentores do exercício do poder, capaz de lhe garantir a convivência em sociedade, sem o risco de ter sua liberdade cerceada pelo Estado, a não ser nas hipóteses previamente estabelecidas pelas regras gerais, abstratas e impessoais.

Diante do acatamento dos Princípios mencionados, e tendo em vista que a incidência do Direito é uma necessidade inafastável para a harmonização das relações jurídicas ciberespaciais, faz-se necessária a edição de novas leis para a proteção dos bens jurídicos, postos em evidência diante das novas formas de invadir direitos de outrem, por meio dos mecanismos proporcionados pelos recursos digitais. Por isso, embora repudiando o exagero de certas tipificações, não há como negar a interação entre o Direito Penal e a Internet, pois o ciberespaço e suas culturas não estão fora do mundo "real" e, estando nesse mundo, invariavelmente, acabarão por sujeitar-se ao Direito, para regulamentação de possíveis abusos contra essa mesma comunidade digital bem como prevenir e inibir ações ilícitas e ilegítimas dos membros da sociedade informatizada contra bens jurídicos valiosos para toda pessoa ou organização humana.

2.2 A tipificação de condutas penais e a atuação do legislador

A partir do momento em que o homem passou a viver em sociedade, surgiu a necessidade de um respeito mútuo para com o direito de seu semelhante. Faz-se assim, necessária a taxação de condutas que seriam

danosas e prejudiciais ao próprio homem, que feria direito alheio e não poderia ser admitida na coletividade sob o risco de desorganizá-la. Dava-se início, então, a tipificação do ilícito, conduta (omissiva ou comissiva) contrária ao Direito, à moral e aos bons costumes, e a taxação dessas condutas pelo Poder Legislativo, de acordo com a teoria da Tripartição dos Poderes, defendida de maneira sublime pelo filósofo *Montesquieu,* que mais apropriadamente seria a tripartição das funções estatais de um Estado dotado de soberania que é, indiscutivelmente, uma. Ou seja, a esse poder, confere a função precípua de elaborar as normas necessárias ao convívio social. Alexandre de Morais expõe, de maneira brilhante, as razões históricas e filosóficas da função legiferante por parte do Poder Legislativo (69: 2003);

> Importante salientarmos as razões pelas quais, em defesa do Princípio da Legalidade, o Parlamento detém o monopólio da atividade legislativa, de maneira a assegurar o primado da lei como fonte máxima do Direito; por tratar-se de sede institucional dos debates políticos; por configurar-se em uma caixa de ressonância para efeito de informação e mobilização da opinião púbica e por constituir um órgão que, em tese, devido a sua composição heterogênea e a seu processo de funcionamento, torna a lei não uma mera expressão de sentimentos, mas a vontade resultante da síntese de posições antagônicas e pluralista da sociedade.

A função do legislador consiste na absorção dos fatos contrários à idéia de Justiça e equilíbrio e os combate através de normas coercitivas, de diretrizes obrigatórias que relevam bens resguardados pela coletividade como um todo. O Direito Penal constitui-se o resultado de escolhas políticas influenciadas pelo tipo de Estado em que a sociedade está organizada. O direito de punir é uma manifestação necessária do poder de supremacia do Estado nas relações com os cidadãos, principalmente na relação indivíduo-autoridade. A situação histórica, os

valores aos quais a sociedade atual adere, portanto, condiciona o conceito de crime e conseqüentemente, o conceito de bem jurídico e sua importância para o Direito Penal. A visão constitucional defendida hoje por inúmeros doutrinadores em todo o mundo nada mais é que o desenvolvimento da visão positivista, que reconhece a criação do conceito de bem jurídico penal a partir das normas jurídicas hierarquicamente superiores às demais, aquelas decorrentes da Constituição Federal.

Porém, é o próprio legislador penal o responsável para determinar a proteção penal, observado o limite do Direito Penal, por meio de critérios político-criminais e não dogmático-constitucionais. A resposta à questão formulada sobre o conceito de bem jurídico que deverá ser protegido pelo legislador, somente poderá ser dada por intermédio da visão social do bem jurídico e não de sua visão exclusivamente positivista. Tendo em vista o paradigma de bens, genericamente considerados pela Constituição Federal somada à necessidade da inserção de novos conceitos oriundos da tecnologia indiscutivelmente inserida na nossa realidade, cabe ao legislador infraconstitucional a sensibilidade de perceber aqueles que estão diretamente ligados a uma violação, sob uma nova postura, em relação àqueles bens. E o que acontece com as novas espécies de delitos, denominados "crimes digitais", pois na medida em que surgem meios eletrônicos e novos recursos, novos bens também hão de ser amparados pela legislação, exigindo do legislador um aprimoramento nessa área, visto que não há como dispor e impor sobre condutas penais sem adentrar e conhecer o seu conteúdo. O resultado dessa especialização legislativa será necessariamente a nítida diferenciação entre atos lícitos, ou seja, atos permitidos pelo ordenamento, e

ilícitos, contrários aos bens adotados pelo Estado Democrático de Direito, dentro da nova conjuntura social proporcionada pela tecnologia.

O ato ilícito gera efeitos não queridos pelo autor (sanção) que pode abranger tanto a esfera civil como a penal, como ainda a extrapenal ou ambas. Civilmente, o ilícito é o que ordinariamente chamamos de ato ilícito. Dentro do Direito Penal, o ilícito penal caracteriza o crime, que tem, na grande maioria das vezes, sanções muito mais severas que aquelas adotadas pelo Direito Civil. Na doutrina, abundam as conceituações de crime, que variam de acordo com o sistema adotado. A doutrina tradicional considera o crime em si como toda conduta proibida por lei sob ameaça de pena. Seria o fato típico e antijurídico. Já os doutrinadores modernos, ou seja, a doutrina classificada como "finalista", considera o crime sob o aspecto analítico como sendo a conduta típica, antijurídica e culpável. Pormenorizadamente, o fato típico é o comportamento humano (ação ou omissão) que provoque um resultado, sendo previsto como infração penal. A antijuridicidade é a relação de contrariedade entre o fato típico e o ordenamento jurídico, por isso, deixará de existir a ilicitude se o agente estiver amparado por uma causa excludente da mesma, e por fim, a culpabilidade, considerada como a reprovação da ordem jurídica em face de o homem está ligado a um fato típico e antijurídico. Seria, em suma, a contrariedade entre a vontade do agente e a vontade da norma penal.

Sob o aspecto formal, crime é toda conduta descrita na lei penal que implica na imposição de uma pena. Já sob o ponto de vista material, o crime é analisado ontologicamente, sendo toda conduta que a juízo do legislador atinge bens e interesses considerados relevantes pela sociedade, o que acarreta a imposição de uma pena. Assim, considera-se que uma conduta não é

denominada como delituosa por mero arbítrio do legislador. Pelo contrário, para ser ilícita deve estar prevista em lei por razões formais e materiais. No Direito Pátrio deve ser contemplada, necessariamente, no Código Penal ou na legislação extravagante, onde a tipicidade é conseqüência direta do Princípio da Legalidade. A ausência das condutas nessas duas espécies de instrumentos normativos descaracteriza-a como criminosa, ainda que cause resultados prejudiciais e danosos a terceiros e seja um crime do ponto de vista material. Evidentemente, que tais condutas danosas, ainda não citadas na lei, serão também as mais propensas a serem regulamentadas como delito pelo legislador, que basicamente a analisa levando em consideração o poder ofensivo dela, como acontece com os delitos que causam danos ao sistema de dados ou se utilizam dele para a prática do evento danoso, tendo em vista bens que, de maneira genérica, estão resguardados no ordenamento, mas que ainda não encontraram a tipificação necessária para considerá-los crimes puníveis, em seu aspecto formal.

A par da respectiva apreciação dogmática, é importante compreender que para se admitir um novo tipo penal no ordenamento brasileiro torna-se imprescindível que o legislador atenda outras regras constitucionais, no sentido de elaboração legislativa. No que se refere aos delitos praticados no seio do sistema informático, a competência é duplamente federal, conforme o Art. 22, inciso I da Constituição Federal, que assegura que compete privativamente à União legislar sobre Direito Penal e, segundo o inciso IV, do mesmo artigo a União também detém a competência para legislar sobre Informática. A percepção desse problema, a partir dos dispositivos constitucionais, tem relevância porque, em se tratado de Internet, encontram-se velhos delitos executados por diferentes

modos, ou seja, muda o *modus operandi*, ao mesmo tempo em que se está diante de uma nova criminalidade, atingindo novos valores sociais.

Sabe-se que para uma nova realidade deve existir uma nova disciplina. Embora se constate que a escassa regulamentação gera facilidades no espaço cibernético, deve-se ter em mente que, como base na averiguação objetiva dos delitos, a Internet pode se constituir um ambiente provido de regulamentação. Nesse espaço, circulam infinitos valores seja de ordem privada,seja de ordem pública, e assim, o legislador pátrio deve estar atento ao desrespeito destes, inserindo tais fatos no ordenamento de maneira legítima, sob pena de causar um indesejável hiato entre a realidade social e o seu sistema normativo. Nesse novíssimo contexto e sem perder de vista a função precípua da lei penal em proteger bens juridicamente relevantes, quais sejam, os bens da vida, certamente serão necessárias redefinições de institutos, no tocante a bens imateriais colocados como novos valores pelos avanços tecnológicos, tendo em conta que a sociedade tecnológica reconhece como bens de relevante valor os dados e informações, já que são vitais para uma empresa ou uma organização pública ou privada e por isso, devem ser enquadradas em figuras penais precisas e delimitadas. Sem esquecer que, no plano constitucional dos direitos fundamentais e no plano civil dos direitos da personalidade, as ameaças por meio de computadores, a bens indispensáveis à realização da personalidade humana também devem ser evitadas e combatidas, e isso se dá, em respeito ao Princípio da Reserva Legal, por um processo que se destaca desde a cognição do legislador atento às novas condutas sociais até efetiva regulamentação, por uma lei específica, que qualifique a conduta como nociva ao meio e que impute uma sanção.

Por isso, há a necessidade da legislação brasileira acompanhar a evolução da criminalidade, já que seu Código Penal data de 1940, época impossível de imaginar que existiriam delitos informáticos. Na tentativa de compensar o atraso está em tramitação no Congresso Nacional o Projeto de Lei nº. 84/99, de autoria do Deputado Luiz Piauhylino, herdado de seu antecessor o Deputado Cássio Cunha Lima, e que trata justamente da proteção desses novos bens colocados em vulnerabilidade pelo avanço tecnológico, como por exemplo, o processamento e a distribuição comercial de dados informatizados, exigindo autorização prévia do titular para manipulação ou comercialização pelo detentor. Mister se faz também a iniciativa legiferante no que tange à sanção a ser aplicada a estes crimes que, como em qualquer outro momento do Direito Penal, a sanção deve ser proporcional a conseqüência do ato. Entre as penas alternativas poderiam ser inclusas no ordenamento penal, as participações do condenado nas investigações de outros delitos que envolvessem recursos tecnológicos, pois para a repressão de crimes que utilizam intensamente o conhecimento, somente uma repressão à mesma altura é capaz de inibir outro conhecimento, tornando-o superado e, portanto, desvendável.

A classificação em crimes digitais puros e impuros ganha importância justamente no momento em que o legislador necessita visualizar aqueles bens ditos relevantes para a sociedade e, em seguida, se estes já estão ou não enquadrados no ordenamento jurídico em vigor, quando utilizam o meio virtual apenas para executar o crime e não quando fere o processamento de dados em si mesmo, isso em decorrência do Princípio do *no bis idem,* ou seja, que o indivíduo não seja inserido no texto criminal duplamente, tendo em vista que a maioria dos bens violados já se encontra tipificado no ordenamento pátrio,

estando à margem da regulamentação apenas aqueles que tem o seu conceito e desenvolvimento ligado à própria história da rede. Fazendo a distinção e visualizando a conduta indesejável que se encontra sem o manto da proteção estatal, cabe ao legislativo operar de maneira atualizada ou, pelo menos, aproximar a letra da lei dos fatos que devem, por ela, ser enquadrados.

As peculiaridades que a nova realidade virtual proporciona no que tange ao necessário acompanhamento jurídico, ainda colocam em questão uma das maiores dificuldades, que é a repressão do mau uso do meio, diante da difícil responsabilização do agente, daquele que executa sua conduta danosa através da Internet, pela ilimitada proporção territorial que esse recurso alcança. Com isso, urge a criação de uma justiça ou Organização Internacional da Informática intergovernamental, que legisle e aplique seu preceito secundário, ou seja, a sua sanção penal com ajuda de Estados componentes dela. A adesão ou não dos Estados a tal justiça ficaria a cargo dos chefes de Governo de cada um deles, porém uma vez aceita tal justiça ou organização, estaria o Estado obrigado a cumprir todas as determinações da organização internacional, logicamente, não ferindo sua Constituição nem muito menos sua soberania o que se mostra bastante complexo, mas que foge ao tema em análise. Enquanto não é uma realidade tal justiça em nível internacional, o Estado deverá, urgentemente, em nível nacional a atualizar legislação brasileira e aprovar o Projeto de Lei nº84/99 do Deputado Luiz Piauhylino que dispõe sobre alguns crimes ligados à informática e que está em tramitação no Congresso Nacional.

Atualizar a legislação pátria significa a criação e implementação de uma legislação aplicável, que vise à segurança, às penalidades cabíveis e à prevenção do crime digital. Não resta, pois atualizar e aprovar o Projeto de Lei que defendam

uma intersecção entre a modernidade e sua respectiva regulamentação, sem a criação e o constante investimento em órgãos repressivos, ou seja, uma Polícia Judiciária informatizada e competente para reprimir crimes "inteligentes", ensejando assim, uma possível e eficaz praticidade da lei incriminadora. Enfim, a atualização da legislação associada à criação e legitimação de órgãos repressivos seriam medidas sem as quais não se poderia adentrar o novo século sem medo de perder o rumo do crescimento tecnológico.

CAPITULO 3 A NECESSIDADE DE TIPIFICAÇAO DOS CRIMES DIGITAIS

O homem é um ser eminentemente inquieto por novos horizontes. Avança diuturnamente em busca de uma comodidade vital que lhe proporcione facilidades cada vez mais prazerosas, e é com esse fulcro que dar passos em maiores proporções em termos de tecnologia.

Diante do inegável envolvimento das relações humanas, como um todo, com o aspecto eletrônico e tecnológico, grandes questões surgem para que esse mesmo homem que desenvolveu a máquina e seus recursos possa respondê-las através de novos conceitos bem como a necessária normatização coerente com a nova realidade digital. Uma dessas questões a serem respondidas é justamente a falta de um sistema teórico, pela imprecisão que os bens prejudicados por esse sistema ainda possui, que direcione a aplicabilidade normativa perante os perigos que a informática expõe. Estatuir quais os bens que podem ser resguardados por leis já existentes, ou seja, as leis que podem ser aplicadas aos crimes cometidos através do sistema de dados, a identificação daqueles fatos que não encontram amparo legal no ordenamento atual, quando se apresentam ao órgão julgador com bens inéditos, nas quais afastam a possibilidade do uso dos meios integrativos do ordenamento e o posicionamento dos Tribunais a respeito dessa celeuma no que tange aos fatos delituosos ainda imprecisos diante da Ciência Jurídica tradicional, além da descrição dos crimes de maior habitualidade no espaço digital, são discussões tratadas amiúde nesse capitulo.

3.1 Principais Crimes Digitais

3.1.1 Pornografia na Internet

Pornografia consiste na prática de fazer, adquirir ou ter sob sua guarda, para fim de comércio, distribuição ou qualquer exposição pública, escrito, pintura, desenho, estampa, de qualquer objeto obsceno. Mais precisamente, na representação, por quaisquer meios, de cenas ou objetos obscenos destinados a serem apresentados a um público e também expor práticas sexuais diversas, com o intuito de instigar a libido do observador.

A Internet constitui-se um novo meio de comunicação, e, historicamente, todos estes meios foram utilizados para a difusão da pornografia. Exemplo disso está no fato de fotos de jovens prostitutas aparecerem um pouco depois da invenção da câmera fotográfica, como também a crescente indústria de filmes e vídeos baseados naquela atividade. Com a Internet não seria diferente, ainda mais quando esse meio de comunicação dispõe de elementos que proporcionam uma crescente atratividade através de recursos de multimídia, oferecido pelo desenvolvimento da "WWW". Antes mesmo dessa "popularização", em meados dos anos 80, era possível encontrar imagens obscenas e acessar listas de discussões sobre sexo explícito, mesmo sabendo que nessa época a Rede era utilizada principalmente por universidades e pesquisadores. Isso mostra que mesmo quando não havia uma popularidade aguçada, a Internet já se mostrava atrativa para o desenvolvimento de práticas pornográficas, devido,

especialmente, a sua aptidão para distribuir imagens sem obstáculos, facilitando o seu intercâmbio de maneira impessoal.

Atualmente, podemos dividir a pornografia difundida na Internet em três categorias. A primeira categoria é relacionada ao começo da Rede, ou seja, usuários interessados em fotografias eróticas de pouca intensidade, e que as tornavam públicas por meio de mensagens nas listas de discussões. Naquele tempo, a Rede era utilizada por uma população essencialmente adulta, fazendo com que a publicação dessas fotos não tivesse como finalidade precípua o constrangimento de qualquer pessoa. Passado esse primeiro momento, com o desenvolvimento tecnológico aliado ao interesse econômico, uma segunda categoria começava a se destacar. Nela, a tecnologia desenvolvida foi utilizada por empresas baseada no acesso à pornografia mediante publicações *online*, ou seja, através de publicações feitas por meio de confecção de pagina eletrônica disponibilizada na rede. Essas empresas foram responsáveis por inovações no campo de segurança e transações financeiras por meio da Internet, pois seus serviços só podiam ser acessados depois do pagamento de uma taxa que "destrancava" a porta virtual da página eletrônica, tornando as imagens acessíveis, caracterizando, então, o comércio pornográfico, maneira mais utilizada nos dias de hoje.

A terceira categoria, a mais preocupante, é aquela relacionada à pedofilia e outros materiais obscenos, que variam de rituais macabros a fotos de mutilações. Justamente pelo anonimato e pelas técnicas de criptografias (arte e a ciência de manter seguras mensagens que serão compartilhadas). O material pedófilo é disseminado por intermédio de uma comunidade virtual fechada, geralmente sem relação com empresas que cobram pelo serviço. Os

integrantes dessa comunidade podem ser chamados de "oportunistas", por aproveitarem da alta tecnologia para manter oculta a ilicitude de suas transmissões, deixando claro o motivo do grande sucesso da Rede nesse contexto, seja devido à facilidade de ocultar, ou ao menos manter anônimo o ato de capturar o material pornográfico, seja pela habilidade de importação de imagens sem ser rastreado ou deixar "pistas".

O ato pedófilo é classificado como um crime digital impuro, por existir por si mesmo, independente da existência da Internet, embora seja esse um importantíssimo meio para o alcance de seu objetivo ultimo, que é justamente a publicação de imagens eróticas, de maneira que o desenvolvimento da Rede se confunde com a própria expansão dessa prática delituosa. O problema se torna de maior gravidade quando se trata da divulgação de imagens que envolvam crianças e adolescentes, constituindo, assim um crime nefasto e repudiado pela maior parte da população. A pornografia infantil, quanto ao aspecto etário, pode se apresentar de três formas; pornografia ou cenas explícitas apenas entre crianças, ou apenas entre crianças e adolescentes; ou entre adultos e adolescentes e pornografia e cenas resultantes da prática de pedofilia, ou seja, cenas de sexo explicito entre adultos e crianças pré-púberes.

No Brasil, o legislador ordinário teve uma atitude progressiva além de extremamente necessária, atualizando o Estatuto da Criança e do Adolescente, através da Lei nº. 10.764 / 2003, de autoria da Senadora e atual Ministra do Meio Ambiente, Marina Silva (PT/AC), modificando a conceituação legal e passando a prever pena mais severa. De maneira muito especial o artigo 214 desse diploma legal.

> Art. 241. Apresentar, produzir, vender, fornecer, divulgar ou publicar, por qualquer meio de comunicação, inclusive rede mundial de computadores ou internet, fotografias ou imagens com pornografia ou cenas de sexo explicito envolvendo crianças e adolescentes.
> Pena – Reclusão de 2 (dois) a 4 (quatro) anos.

Muito apropriada à adaptação do Estatuto da Criança e do Adolescente no que tange a descrição legal em consonância com a realidade e facilidade que os recursos oferecidos pela Internet, proporcionam aos criminosos dessa espécie, uma vez que a rede mundial tem sido um ambiente extremamente favorável à proliferação da pornografia e, de um modo ainda mais sensível, tem servido como campo fértil para a disseminação da pedofilia. Por isso, não poderia o Estado assistir essa fertilidade de maneira inerte e permitir que crianças e adolescentes figurassem com protagonistas de atos nefastos e repugnantes, violando sua imagem e dignidade humana, em nome de prazeres que ferem, antes de tudo, a moral e os bons costumes.

3.2 Pirataria de "software" através da Rede

A chamada pirataria de *software* consiste na apropriação e venda de cópias de programas de computador sem a licença do autor, estando regulada no Brasil pela Lei nº. 9.609, de 19 de fevereiro de 1998, que dispõe sobre a proteção de propriedade intelectual de programa de computador e sua comercialização no País. *Software*, segundo o dicionário Aurélio (643,1997) seria;

> Em um sistema computacional, o conjunto dos componentes que não fazem parte do equipamento físico propriamente dito e que

> incluem as instruções e programas, como também dados a eles associados, empregados durante a utilização do sistema.

É possível, atualmente, fazer uma cópia perfeita de um programa de computador em meios de mídia, como por exemplo, um CD. Feita tal cópia, também há necessidade da replicação de toda a embalagem e manuais do programa, objetivando maior autenticidade, tal cópia da embalagem e do manual é, na maioria das vezes, muito mais cara que a cópia do programa em si.A Rede entre nesse contexto como grande alternativa para o barateamento do processo de duplicação, pois por meio dela é possível distribuir sem a necessidade de quaisquer "meios físicos" e embalagens. No Brasil e demais países latino-americanos, para se ter um parâmetro dessa realidade, a pirataria é responsável por um rombo de mais de 1,1 bilhões de dólares. De acordo com o autor Gustavo Testa Corrêa (47; 2000), "a taxa de pirataria é superior a 80% dos programas vendidos, perdendo apenas para os países asiáticos".

Importante frisar que a Internet possibilita a aquisição de uma vasta gama de programas, sendo muito destes chamados de *freeware* e *shareware.* No primeiro, como a própria denominação sugere, o autor ou detentor dos direitos autorais licencia a utilização destes para o uso público sem que haja necessidade de pagamento, e no segundo a gratuidade está restrita a um período de experiência. Também existem variedades de programas que devem ser pagos para serem adquiridos, por intermédio, por exemplo, do fornecimento do número do cartão de crédito ou similar , a fim de que se tenha acesso ao *site* de

dowload[1]. Isso dá margem ao cometimento de outros crimes, tais como a utilização indevida de cartões de crédito.

Poder-se-ia dizer que a Internet é um mecanismo perfeito para a obtenção de programas, sejam estes sofisticados ou simples. O questionamento assente é a maneira como o "pirata", assim denominado por navegar de maneira ilícita pela grande Rede explorando riquezas de outrem, atuaria para obter êxito nessa prática delituosa, que se traduz, justamente, na vantagem oferecida pela Internet de copiar ilicitamente, permitindo que compradores tenham acesso ao programa duplicado, mediante provedores diversos. Alguns desses "piratas" seriam até mesmo idealistas, com intuito de distribuir cópias através da Internet, de forma gratuita, sem ônus algum e sob o pretexto de que a indústria de programação teria lucros exorbitantes. Torna-se inegável, então, que os maiores problemas relacionados à pirataria na Internet residem justamente na facilidade de distribuição proporcionada por ela. Existem e existirão cada vez mais países-refugios para piratas que desejam distribuir ilegalmente programas, vídeos, filmes, músicas e textos a qualquer individua conectado à Internet.

O que mais preocupa a legislação e o próprio Direito enquanto ciência, é identificar que os mesmos artifícios utilizados por *hackers*, para ocultar material pedófilo ou pornográfico em sistemas externos sem deixar vestígios podem ser usados para "furtar" espaços em discos, por meio de arquivos ocultos e mascarados por nomes falsos, e que contenham em seu bojo milhões de dólares em programas de computador apropriados indevidamente. Muitos computadores de universidades foram utilizados, por exemplo, temporariamente para alojar

[1] Transferência de dados ou arquivos de software de um computador principal para outro de caráter pessoal, usando um modem ou uma outra ligação de rede.

arquivos "ilícitos" e tornar a distribuição viável para o pirata. Nesse ponto surge o ponto sensível e passível de muitas preocupações no campo legal, pois se questiona a extensão da responsabilidade do proprietário do computador "hospedeiro" dessas atividades ilegais, exigindo assim, um estudo pormenorizado e especifico da Informática, sugerindo até mesmo, a criação de uma disciplina especifica que proporcione o direcionamento doutrinário do alcance da responsabilização quando se tratar de crimes dessa natureza.

Entre os pontos importantes da legislação pátria de *software,* qual seja, a Lei nº 9.609 de 19 de fevereiro de 1998, que atualiza a antiga Lei n. 7.646/87, devem ser destacados: a aplicação da pena de 6 (seis) a 2 (dois) anos de reclusão e multa quando o ato versar sobre violação de direitos do autor do programa, agravando-se a situação daquele que viole a proteção autoral com intuito de comercialização de programas "piratas" para terceiros, quando a pena é de 1(um) a 4 (quatro) anos de prisão e multa de até 3 (três) mil vezes o valor de cada cópia ilegal. Aquele que estiver utilizando ou reproduzindo ilegalmente *software* poderá ainda ser processado por crime de sonegação fiscal, em razão da perda de arrecadação tributaria pelo Estado, pela prática ilegal. Assim, a Receita Federal tem o poder de fiscalizar empresas para confirmar a procedência legal do *software* utilizado nos computadores. Prevê, ainda, a expansão da proteção ao produtor do *software,* que agora passa a ser de 50 anos.

3.3 Fraudes na Internet

O Direito não tolera fraudes. Esta máxima, tão repetida e utilizada por diversos juristas nos mais variados contextos e nas mais diferentes épocas, pode

ser considerada um princípio que emana do nosso ordenamento jurídico; como uma regra de resolução de controvérsias; como norma de natureza programática e como uma interferência da Moral no campo estritamente jurídica.

O caput do artigo 171, do Código Penal diz:

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

A seqüência de atos que estimulam a erro, no intuito de que esta se comporte como se estivesse em plena lucidez da realidade é denominada fraude. O agente da fraude delineia e executa uma série de acontecimentos, produzindo uma ação na vítima, que sem todo esse percurso ele não o faria. Pelo fato de a Internet estar-se tornando um meio global para troca de mercadorias, o aparecimento de companhias ou indivíduos oferecendo produtos e serviço faz dela um ambiente propicio para que esse percurso se torne cada vez mais atrativo. A peculiaridade apresentada é o fato destas companhias ou indivíduos, aproveitarem recursos que somente a Internet proporciona como o anonimato e a inexistência de regras e legislação especifica apropriada, para atuarem de maneira "enganosa" nesse meio com maior liberdade.

O tipo fundamental de fraude dentro da Rede é o que envolve um falso comerciante e um consumidor com boas intenções, visando adquirir uma mercadoria oferecida à venda. Diante desse exemplo clássico, poder-se-ia classificar a fraude na Internet, tendo em vista a natureza da mercadoria, em três espécies; a fraude que envolve mercadorias físicas através da Rede.Seria equivalente à compra de produtos via correio, sendo, por isso, suscetível das mesmas práticas ilegais que surgem de tal transação. Nesse caso, os bens

oferecidos pela Rede podem ser furtados, descritos de maneira errônea ou o fornecedor representar determinada empresa sem que possua vinculo algum com ela. Na segunda hipótese, estar-se-á diante de fraudes envolvendo bens "digitais", ou seja, bens considerados intangíveis, como programas de computador, por exemplo. Aqui, o comprador paga a empresa com o intuito de adquirir uma cópia do programa diretamente da Internet. O que, na prática, acontece é que o consumidor paga pelo programa, mas a empresa não permite, posteriormente, a agravação deste, utilizando de artifícios maliciosos, tais como apresentar sinais de erro no seu *site*, modificar os dados no momento da transmissão do programa ou não transmitir dado algum.

A terceira espécie de fraude na Internet se refere aos serviços e publicações próprios da Internet. Enquanto o acesso a alguns jornais e revistar eletrônicas não exige o pagamento de taxas, no caso de sites pagos, como na maioria dos pornográficos, criam-se brechas para a ocorrência de fraudes, o que significa que essa espécie de fraude mais se aproxima das proezas que o sistema informático proporciona em termos de facilidades para enganar o sujeito passivo desse delito. Nesse ultimo caso se pode dizer que as fotos por cujo acesso o consumidor pagou não condizem com a qualidade e quantidade mencionadas pelo *site*. Pode ainda, o proprietário do endereço eletrônico abusar do mecanismo de pagamento, cobrando taxas bem maiores do que aquelas anunciadas. As queixas mais freqüentes, no entanto, são os casos de pirâmides e marketing de multilevel, ofertas de cartões de crédito, oportunidade de negócios mirabolantes, entre outros. Assim, vale o bom senso e a cautela antes de realizar qualquer negócio via Internet.

3.4 Abusos quanto a cartões de crédito

Da mesma forma que no cotidiano, os pagamentos feitos pela Internet podem ser realizados através de vários mecanismos, como a troca de dinheiro, o débito em conta, a utilização de cartões de crédito, etc. Dentro dela, a maneira mais popular para efetivação de pagamentos é o cartão de crédito. Atualmente estão sendo desenvolvidos muitos mecanismos visando a constituição e consolidação do "dinheiro eletrônico" e bancos via Internet (internet *banking*), ampliando a capacidade da utilização de moeda pela Rede.

Faz-se importante frisar que, pelo fato de os cartões de crédito oferecerem uma significativa proteção para seus usuários, fazem com que sua popularidade seja bem maior que os outros mecanismos, assim como a facilidade de funcionamento; um comprador escolhe determinado bem e preenche uma ordem de cobrança para seu cartão. Dentro dessa ordem de cobrança, geralmente representada por um formulário constante nas paginas de uma loja virtual, informações como o número do cartão, a data de vencimentos e o nome do titular são preenchidos como pressupostos para a consumação da venda. Devido à simplicidade desse mecanismo de funcionamento, os cartões de crédito são suscetíveis de um grande número de abusos e fraudes. No caso de fraudes a cartões de crédito, temos como núcleo da ação a intenção, o desejo de enganar o titular daquele cartão para obter informações necessárias para seu débito, atividade esta não exclusiva do mundo "virtual", mas sim constante nas relações materiais, ou seja, aquele que não for no ciberespaço. Para se ter idéia desse problema, na Inglaterra, a "Associação para Pagamento e Compensação de

Serviços", em 1999, apurou que fraudes relacionadas a cartões de crédito ultrapassaram a marca dos 200 milhões de dólares.

As companhias de cartões, reiteradamente, alertam seus clientes sobre o custo dessas fraudes, um prejuízo dividido por meio do pagamento de taxas de anuidade, de juros e outras despesas. Mas o que difere a Internet do mundo real, no que tange à prática desse crime em especifico, é o "esconderijo", proporcionada por aquela aos fraudadores. A maioria das transações relacionadas aos cartões de crédito ocorre sem a percepção de seu titular. Uma vez preenchida a autorização de débito pela Rede, o titular do cartão não tem nenhum meio de determinar com quem está fazendo negócio. A partir daí começaram os abusos, pois recebidas as informações necessárias, os maus comerciantes debitam do cartão sem remeter o bem comprado, e até mesmo debitam do cartão sem remeter o bem comprado, e até mesmo debitam dele várias vezes, simplesmente desaparecendo apostais práticas. Podem, eventualmente, processar o pedido de maneira exata, mantendo, porém, detalhes sobre o cartão de crédito para eventual fraude futura, talvez até vendendo o número do cartão de crédito para quadrilhas organizadas para esse tipo específico de fraude.

O interessante, e o mais comum, é que a fraude quanto ao cartão não se limita ao comerciante. Pelo fato da Internet, até agora, em termos, não ser particularmente segura, é possível que a transmissão sejam interceptadas, e o número do cartão, conseqüentemente, também. A explicação é simples: o provedor ao qual o usuário está conectado é o local responsável pelo processamento de todo o correio eletrônico e das paginas eletrônicas. Toda

página carregada ou transmitida é também *cached* [2] ,ou seja, armazenada temporariamente dentro do sistema. A partir disto, o administrador do provedor, ou quem tenha acesso a ele, pode facilmente ler o conteúdo dessas páginas, podendo ate mesmo, mudá-lo.

Pelo fato de não existir regulamentação especifica, em termos, desses serviços no Brasil, a não ser nos vários projetos de lei, qualquer pessoa responsável por um provedor de acesso tem condições de usar tais informações para fins ilícitos.E correto afirmar que tanto os provedores que transmitem quanto os que recebem informações têm o acesso aos dados de cartões de crédito e podem utiliza-los ilegalmente. Porém, os provedores não são os únicos capazes de interceptar tais informações; qualquer pessoa que tenha ferramentas e o conhecimento apropriado para tanto também consegue lograr êxito nessa prática delitiva. Outras fraudes relacionadas aos cartões de crédito são os programas capazes de gerar novos números de cartão e modificar informações detalhadas nas faixas magnéticas de outros.Também, tais cartões podem debitar de contas diversas, e não apenas daquelas com as quais realmente possuem vinculo.

As empresas de cartão de crédito, devido à fragilidade dos mecanismos de segurança da Internet, vêm aconselhando, em alguns casos, seus clientes a não informar detalhes sobre seu cartão por meio da Rede. Para evitar tais problemas, elas vêm desenvolvendo mecanismos que programem a segurança, como a tecnologias da criptografia. Podemos, também, citar a utilização de um mecanismo chamado SET (*secure eletronic transaction),* que significa "transação econômica segura", funcionando como uma máscara para os dados enviados

---

[2] Memória cached – aquela intermediaria entre o processador e a memória RAM, responsavel pela melhoria na performance, alocando as ultimas informacoes processadas.

pela Internet, onde somente o transmissor e o receptor podem "entender" o significado dos dados intercambiados pela Rede. A segurança dessas transações é fundamental para o crescimento do comércio eletrônico, pois ainda há uma insegurança por parte dos usuários da Rede quanto às compras eletrônicas, e o principal fator dessa timidez é o receio de ter sua privacidade invadida e seus dados usados de maneira ilícita.

3.5 Lavagem eletrônica de dinheiro

Sabemos que peças eletrônicas de computadores podem ser furtadas por criminosos, assim como a pornografia relacionada a crianças pode ser distribuída entre o "circulo" organizado de pedófilos. Isso não significa, porém, que se caracterizam essas espécies delituosas como "crimes organizados". Crime organizado constitui a consolidação de quadrilhas por um longo espaço de tempo, desenvolvendo e coordenando inúmeras atividades ilícitas, tendo como maior exemplo o tráfico de drogas. A produção, a distribuição e a venda podem ser complexas, mas não são comparáveis ao processamento de dinheiro ganho com essa atividade para ser utilizado por esses criminosos, de novo, dentro do processo. Gustavo Testa Corrêa (53; 2000) utilizando consideração feita por Neil Barret argumenta por palavras deste;

> Se pudéssemos rastrear os verdadeiros chefões, através da prisão dos traficantes responsáveis pela venda nas ruas, poderíamos acabar com o problema das drogas em um curto espaço de tempo, já que descobriríamos para onde vai o dinheiro das drogas vendidas. Mas infelizmente, os traficantes não deixam o dinheiro diretamente com os seus chefes. Ao contrário, o dinheiro passa por uma complexa série de intermediários, e por igualmente complexa série de contas e investimentos bancários.

Tais divisas ilegais entram pela Internet ou por outra rede de contas de companhias e empresas, e em seguida, são transferidas rapidamente para outras contas e assim sucessivamente. Enquanto o dinheiro obtido pelo traficante da esquina é considerado "sujo", ele é posteriormente legitimado por uma complexa série de transações bancárias, dentro de uma rede eletrônica, até que chegue, aparentemente "limpo", às mãos do chefe. A lavagem de dinheiro é feita por meio de um complicado mecanismo de transações em cadeia, que dificultam em muito seu rastreamento. O dinheiro "sujo" acaba misturado com fundo de investimentos legítimos, que à primeira vista são completamente legais. Torna-se, no mínimo, espantosa a estimativa relativa ao volume desse dinheiro classificado como "sujo", presume-se que supere a cifra de 780 bilhões de dólares anuais. Além do tráfego de drogas, outros tipos de atividades necessitam lavar dinheiro "sujo", como o furto de bancos digitais, dinheiro para atividades terroristas, furto de lojas virtuais, etc. Em todos esses casos existe um ponto em comum; o processo de lavagem de dinheiro visa confundir o detetive, com a utilização de uma complexa rede de companhias, contas, transações e investimentos.

A lavagem está baseada em uma cadeia de rápidas transações, envolvendo mais do que a mera movimentação de dinheiro dentro do país; envolve também a movimentação para fora do país, para fora do controle jurisdicional , tornando o seu rastreamento e controle quase impossível. Inegavelmente a responsabilidade pela investigação e punição é do Estado, pois esse dinheiro "sujo" é aquele na qual deveria ter sido tributado e confiscado, por ser resultado de atividades imorais e ilegais, constituindo, assim, uma tarefa muito difícil, tendo em vista a necessidade de uma espécie de explicação sobre todas as transações que representam a rápida transferência de fundo ilegais em juízo,

para enfim processar e julgar os responsáveis por essa ação. Isso significa que toda uma rede, muito complexa, deve ser descrita e apreciada por magistrados e advogados, na maioria leiga quanto a técnica do assunto. O envolvimento de computadores e redes nessa lavagem de dinheiro acarreta o aparecimento de características únicas dentro desse processo. Primeiro porque um criminoso pode usar computadores para gravar, carregar e até estabelecer um controle de complexa rede de transações que envolvem tais atividades. Quanto mais complexa fica essa rede mais difícil identificá-la, entendê-la e explicá-la, mas por outro lado, fica também difícil para o criminoso seu controle.

Importante ressaltar que, na Era da Informação, a tecnologia digital está intimamente relacionada com tal situação. Os bancos, por exemplo, transferem dinheiro de suas contas por meio de arquivos digitais. A transmissão é feita pela utilização de um formato criptográfico internacionalmente, irreconhecível por terceiros, e é justamente aí onde reside o perigo. Primeiramente devido ao fato de os próprios criminosos utilizarem esse sistema de segurança para ocultar suas transações ilegais, assim como também, pelo fato de todo sistema de segurança ser passível de falhas. Organizações de criminosos podem obter acesso a sistema bancário contratando *hackers* profissionais no assunto, ou, até mesmo, torturando, seqüestrando ou forçando funcionários e administradores do sistema do banco a lhes dar acesso. Ver-se, então, que no caso de segurança oferecida por computadores, devem se dar ênfase tanto ao aspecto tecnológico, quando o uso do sistema é inseparável da ação em si, quanto o aspecto pessoal, para que assim, estabeleçam a seguridade do sistema, sem ignorar o elemento humano. Sem perder de vista que o rápido crescimento da Internet, aliado ao fato da mesma oferecer cada vez mais oportunidades para a aquisição de bens de

consumo, evidencia a potencialidade de materialização de tais crimes, culminando na necessidade da implementação da sua segurança.

A Lei nº. 9.613 tipificou, no ordenamento pátrio, os crimes de lavagem de bens, direitos e valores, criando para a fiscalização do sistema financeiro e de molde a prevenir as operações de "branqueamento". Administrativamente, o Conselho de Atividades Financeiras (COAF), foi formado por servidores públicos de reputação ilibada, provenientes dos quadros discriminados no artigo 16 da supracitada lei, mais especificadamente criada, no âmbito do Ministério da Fazenda, com a finalidade de disciplinar, aplicar penas administrativas, receber, examinar e identificar as ocorrências suspeitas de atividades ilícitas previstas nesta lei, sem prejuízo da competência de outros órgãos e entidades.

3.6 Crime Digital de "hancking"

O crime de "hancking" envolve o acesso a um determinado sistema por particular que tenha permissão insuficiente, ou um determinado usuário externo ao sistema, acessando-o sem nenhuma permissão. Seria, portanto, aquela ação que tem como agente ativo, o *hacker,* por ser este aquele que penetra em sistemas sem a devida autorização. O crime de *hancking* seria seu peculiar ato, sendo o mesmo que ultrapassar, quebrar ou entrar em algum lugar para o qual é necessária a previa autorização. Poder-se-ia dizer que o *hacker* é um individuo dotado de conhecimentos técnicos em informática capaz de quebrar barreiras, dando margem a total acessibilidade de sistemas alheios.

Tal atitude pode ser direcionada por um grande número de razões, pode ele adentrar o sistema apenas para obter uma informação particular mais caracterizando um auto-desafio do que propriamente um crime, como também

pode invadir esse mesmo sistema com fins ilícitos, como extorquir alguém, ter acesso a mensagens particulares, furtar informações de relevante valor pecuniário, destruir dados, disseminar vírus, enfim realizar atividades nocivas àquele meio, sendo caracterizado pela doutrina com outra denominação; são os *crackes*, que diferenciam dos *hackers* pelo dolo, ou pela motivação do ato, distinção essa de caráter didático o que não significa que não seja o ato deste ultimo um crime de "hancking".

Necessária se faz a distinção da natureza da informação obtida pelo *harcker* pela prática desse delito. Podendo ser relativa a dados pessoais de determinada pessoa, cometendo ele então um crime por ter violado a seara intima do individuo, como, por exemplo, violar dados através do correio eletrônico. Ou pode ela representar bens digitais, como programas de computador, informação legalmente protegida, a qual o *harcker* não possuía licença alguma para modificar, apropriar e destruir. No Brasil, não existe um tipo especifico para tal crime, o que significa que perpetrar sistema alheio é penalmente desprotegido. O problema é que dentro da legislação brasileira inexistem tipos penais que conceituem dados do computador, como coisa propriamente dita daí a impropriedade de se qualificar o crime de *hancking* no crime de dano tradicional. Estar-se, então diante de um caso atípico, não sendo possível punir aquele que penetra em sistema alheio, pois tudo que não for proibido será permitido.

3.7 A Aplicação da Legislação existente e seus reflexos quanto aos crimes digitais

O art. 5º da Constituição Federal de 1988, em seu inciso XXXV reza: "a lei não excluirá da apreciação do Poder Judiciário lesão ou ameaça a direito". Essa norma princípio está consagrada na Magna Carta para dar a necessária

segurança àqueles que se sentirem prejudicados por quaisquer atos que lhe tragam prejuízo moral ou material, assegurando às pessoas naturais ou jurídicas, o acesso ao Poder Judiciário. Por isso, é também conhecido como o princípio de acesso à justiça. Em que pese o destinatário principal dessa norma, qual seja o legislador, o comando constitucional atinge a todos indistintamente, vale dizer, não pode o legislador e ninguém mais impedir que o jurisdicionado vá a Juízo deduzir sua pretensão, e isso materialmente se dá através do direito de ação. Em outras palavras, o individuo que tiver alguma lesão ou ameaça de direito seu poderá acionar o Estado, mais precisamente sua função jurisdicional, com o objetivo de solucionar a lide apresentada, de maneira que o Direito apresente a possível "resposta" àquela demanda.

Diante deste princípio, que se apresenta como uma garantia constitucional, a Lei de Introdução ao Código Civil (LICC) em seu art. 4º determina que; "Quando a lei for omissa, o juiz decidirá o caso de acordo com a analogia, os costumes e os princípios gerais do direito". A Lei de Introdução é considerada a normas das normas, e esse comando legal em particular, é o artifício usado pelo próprio ordenamento para não permitir que situações advindas das progressivas relações humanas fiquem à margem de uma solução jurídica. Como não se pode permitir que indivíduos apresentem situações perante o Poder Judiciário e este não lhes proporcione a respectiva resposta, diante do caso concreto, esta lei estabelece "caminhos" a serem seguidos pelos operadores do Direito, de maneira que a lacuna seja apenas aparente e que, o ordenamento encontre em seu próprio corpo a solução pleiteada. A analogia é o primeiro passo para essa integração, pois proporciona uma interpretação que mais aproxima o texto legal do caso em

exame. Damásio de Jesus (2003, p. 50) expõe brilhantemente o conceito de analogia em sua obra, da seguinte maneira:

> A analogia consiste em aplicar a uma hipótese não prevista em le a disposição relativa a um caso semelhante. Ao solucionar uma questão por analogia, o juiz está somente aplicando determinada disposição legal que irá resolver, por semelhança, casos não expressamente contemplados.

O fundamento desse recurso integrativo é o critério valorativo, pois para a aplicação de uma norma que não regula, o caso posto a mesma razão deve ser aplicada àquela na qual ela protegeu, pois onde há a mesma razão, aplica-se o mesmo dispositivo de lei. No aspecto Penal a questão da analogia toma feições diferentes do Direito Civil, se torna mais restrita e respeita muito mais o Princípio da Legalidade do que propriamente o Princípio da Inafastabilidade da Jurisdição. A aplicação do procedimento analógico no Direito Penal se encontra proibida em relação às normas penais em sentido estrito, quais sejam, aquelas que definem infrações e cominam penas, as denominadas normas penais incriminadoras. Não pode a analogia criar figura delitiva não prevista expressamente, ou pena que o legislador não haja determinado. Como mostra José Carlos Gobbis Pagliuca (2006, p. 39):

> A analogia no Direito Penal exerce um papel singular. Sendo o Direito Penal nada mais que a lei escrita, definida e delimitada pela interpretação, não é possível, portanto, preencher lacunas existentes com a analogia.

Deveras que será imperioso concluir que se há lesões ou ameaças a direitos, deve o Estado atuar para coibir tais práticas violadoras da paz social, ainda que estas sejam realizadas por intermédio de um sistema criado e

desenvolvido posteriormente à visão de bem tutelado pelo legislador daquela norma incriminadora, como é o caso da Internet. Isso por que tanto a máquina quanto a própria Rede são criações humanas e, como tais, tem natureza ambivalente, dependente do uso que se faça dela ou da destinação que lhes dê. Do mesmo modo que aproxima as pessoas e auxilia a disseminação da informação, a Internet permite a prática de delitos que, assim como os ditos "convencionais", precisam ser solucionados, mesmo porque os delitos praticados nesse meio apresentam um poder de lesividade bem maior que aqueles. As várias teorias que o Direito se deparou ao longo de sua existência claramente demonstram a necessidade do aprimoramento social e estatal, principalmente do trato da questão criminal, e mais precisamente quando este estar em "atraso" quanto às novas modalidades de condutas delitivas.

Como não há, ainda, uma legislação própria que delimite os bens juridicamente protegidos diante da ofensividade do sistema digital, surgem diversas soluções para essa questão pelos aplicadores do Direito, gerando uma instabilidade por residir a solução na interpretação pessoal de cada aplicador. Os Tribunais,de todos os modos, tentam conter os chamados "crimes virtuais", cada qual observando o caso em concreto, aplica uma solução que se acha justa. Ora, na medida em que a lei é omissa, deixa margens a ação do aplicador legal, que muitas vezes se ver numa tarefa árdua, que foge sua competência originária, pois é forçado a legislar, em decorrência de um caso concreto que lhe foi apresentado. Nascem desse dever de aplicar a lei ao caso concreto, pela Inafastabilidade da Jurisdição, dois grandes problemas: primeiramente, no Direito Penal, ao contrário do que ocorre no Direito Civil, só pode o Magistrado aplicar a analogia se a mesma for considerada benéfica ao acusado, pois a aplicação da analogia em

norma penal fere o Princípio da Reserva Legal, uma vez que um fato não definido em lei como crime não seria considerado com tal; o segundo reside nas diferentes conceituações que os bens juridicamente protegidos pelas normas em vigor possuem em decorrência dos novos valores apresentados pelos crimes virtuais, o que dificulta a aproximação do caso concreto, apresentando bens ainda não enquadrados no ordenamento penal, da lei em vigor.

Embora a impunidade existente atinja um pequeno número de condutas, não se pode afirmar que tudo na Internet é permitido e que não há uma necessidade urgente de enquadrar esses delitos em tipos definidos. Os crimes já mencionados, assim como também o de racismo e discriminação são alguns exemplos de delitos perfeitamente enquadrados no ordenamento penal em vigor. Não se sugere a confecção de um novo Código Penal, mas que esta lei possa e deva ser adaptada,como também apresentar soluções adequadas perante as celeumas que existem nas leis esparsas do ordenamento atual , por carecerem de uma regulamentação na área digital. O Direito precisa de uma norma segura e específica, que regule o tema e que seja destinado a proteger os bens jurídicos ligados à informática, suprindo as já existentes, mas que deixam a desejar e criando aquelas que necessitam de um direcionamento voltado aos novos conceitos advindos do uso desse novo sistema digital na sociedade, como imprescindível.

Algumas iniciativas legiferantes merecem destaque, por está em vigor algumas leis esparsas tratando da proteção de alguns bens ligados aos crimes de informática, tais como a Lei nº. 9.609 de fevereiro de 1988, conhecida por "Lei dos Softwares", que dispõe sobre a proteção da propriedade intelectual de programa de computador e sua comercialização no País, mas que tutela tão somente o

direito do autor de programas de computador. Assim como a Lei nº 9.983 de 14 de julho de 2000, que tem a função precípua de alterar alguns artigos do Código Penal vigente, mas somente no que se refere a identificação e inserção do equipamento eletrônico, e dos respectivos sistemas,nos crimes descritos pela legislação em vigor, como por exemplo o δ 1º, inciso I , do art. 325 que prevê : " divulgação sem justa causa de informações sigilosas ou reservadas , assim definidas em lei, contidas ou não nos sistemas de informação ou banco de dados da Administração Pública", carecendo , porém, da precisão que a peculiaridade dos crimes de informática exige.

3.6 Posicionamento da Jurisprudência diante do enquadramento penal dos crimes digitais

A Jurisprudência dominante, enquanto conjunto harmônico de decisões, vêm se posicionando de maneira sensível perante o surgimento das "novas" modalidades de crimes, perpetrados através da Internet. Apresentam-se os Tribunais, concatenados aos novos valores postos em expressividade diante da conjuntura atual, tanto que passa a analisar as normas já existentes e aplicá-las sob uma nova perspectiva. Reavalia bens constitucionalmente assegurados e amplia a idéia que protege os bens tutelados pelo ordenamento infra-constitucioal em vigor de maneira que se assegure a jurisdição e que não existam fatos alheios ao manto da lei.

A estreita e cada vez mais intensa vinculação que passou a existir entre a Internet e o crime exige muita parcimônia dos órgãos jurisdicionais na qualificação da conduta delituosa, na medida em que se percebe o desvio de finalidade na utilização dessa tecnologia, tomando em conta, inclusive, o Princípio da Reserva

Legal, assim como também os diversos valores jurídicos tutelados pela lei e pela Constituição Federal. A experiência subministrada ao magistrado pela observação do que ordinariamente acontece, tendo em vista o enquadramento do meio fraudulento da norma penal em vigor, exige um conhecimento ampliativo, do *modus operandi* e da admissibilidade diante do caso abstratamente tipificado.

Resta evidenciado que em face dos crimes já consolidados pelo Código Penal em vigor e que utilizam do instrumento tecnológico para sua execução, ou seja, dos crimes digitais impuros, os órgão superiores vem realizando interpretações cada vez mais "progressivas", na medida em que consideram esse "meio" como perfeitamente adaptável ao fato típico em vigor, como demonstra o Superior Tribunal de Justiça ao denegar o pedido de Liberdade Provisória em face do cometimento do crime de fraude na Internet (STJ – HC 200501585699 – (48255 GO)- 5º T. – Rel. Min. Gilson Dipp – DJU – 19.12.2005 – p. 00462)

> A situação em que foram perpetrados os delitos imputados ao réu enseja a possibilidade concreta de reiteração criminosa, tendo em vista que o crime praticado via computador, podendo ser cometido no interior do próprio lar, bem como em diversos locais, sem alarde e de forma sigilosa, indicando necessidade de manutenção da custódia cautelar.

Diante disso, percebe-se que esses órgãos superiores exercem uma função precípua no ajuste do que está em vigor e dos fatos e valores evidenciados pelo surgimento da Internet. Na medida em suas interpretações possibilitam novas decisões, mais seguras no que tange às duvidas inerentes ao Poder Judiciário, não preparado de todo, para julgar crimes dessa natureza, mais precipuamente quando existem termos passiveis de duvidas ou mesmo situações onde a decisão exige um juízo de valor restrito e técnico, para enfim, alcançar a

razão ou objeto da lei. Exemplo disso está no crime pedofilia ou pedosexualidade, prevista no art. 241 do ECA, cometida também por meio da Internet, onde se constitui uma conduta delituosa de ação múltipla, sendo a objetividade do crime fotografar e publicar crianças e adolescentes em poses eróticas. Surge daí a hesitação sobre o termo publicar diante do relativo conceito do que seja publicar diante desse recurso tecnológico. O Tribunal Regional Federal, assim interpretou com muita lucidez que;

A consumação da modalidade de fotografar ocorre com o simples fato de fotografar". Basta fotografar. Não ação de publicar é necessário que a fotografia seja vista, ainda que por uma só pessoa. A publicação pode dar-se por qualquer meio de comunicação, inclusive rede mundial de computadores ou Internet. Aquele que publica as fotos pode não ser o mesmo que fotografou.

Ver-se, pois, que a Jurisprudência exerce um papel preponderante no ajustamento dos novos delitos, denominados crimes digitais, ao ordenamento penal em vigor, pois diante de seus julgados e suas decisivas interpretações amenizam as possíveis duvidas que necessariamente surjam quando da prática de subsumir uma norma promulgada num contexto longe dos valores atuais, aos fatos "novos", proporcionando uma maior segurança, arma maior da Jurisdição. O que não significa que o legislador fique desobrigado de proporcionar ao aplicador do Direito uma ferramenta penal especifica, adequada para enfrentar esta nova realidade jurídica que é a Informática e seus efeitos nocivos para o próprio Estado e para o cidadão.

CONSIDERAÇOES FINAIS

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

A preocupação e o debate residem no aprimoramento do fator normativo em relação à nova espécie delituosa, perante a evolução da Internet no Brasil e a dificuldade de sua regulamentação. Isso se dá pela maneira lenta que o processo legislativo acontece, impedindo uma análise pormenorizada e atualizada dos crimes digitais, tendo em vista a avançada maneira que se aprimoram.

É preciso que o ordenamento jurídico brasileiro acompanhe também as sofisticadas formas de invadir bem jurídico de outrem, em desrespeito a bens, muitas vezes, já abstratamente consagrados na Constituição Federal, mas que ainda não encontram uma fiel tipificação que se coadune com suas atuais transgressões, perpetradas pela Internet e suas ferramentas. Verifica que as leis atualmente em vigor ainda se encontram desatualizadas, pois além de terem sido elaboradas fora do contexto atual, estão se adaptando de maneira muito tímida, não proporcionando aos aplicadores do Direito e à comunidade como um todo, uma norma específica e segura que solucione os crimes envolvendo conceitos ligados à Internet.

Diante disso, poder-se-á afirmar que o Direito Brasileiro não oferece soluções seguras para condutas lesivas ou potencialmente lesivas que possam ser praticadas pela Internet, quando se trata de crime digital puro ou propriamente dito, e que não encontram adequação típica no rol dos delitos

existentes no Código Penal, nas leis especiais ou nos Tratados Internacionais, em matéria penal, na qual o Estado Brasileiro faça parte. Necessitando, pois, de uma atividade legiferante atualizada e especializada que possa reprimir, através de leis precisas e de um órgão repressor eficaz, crimes que possuam como característica principal a informação.

E pelo valor atual que a informação possui, que tantos conceitos, institutos e bens merecem ser reavaliados. É preciso redimensionar o alcance normativo da lei em vigor. Os bens protegidos pelo ordenamento penal, em especial, devem ser submetidos a uma nova classificação, com critérios voltados à nova conjuntura social, pois, para o aplicador de Direito há de existir conceitos consagrados na sociedade para então se apresentar legitimamente, na letra da lei, ocasionando uma decisão calcada em necessidades sociais eminentes.

Enquanto houver este "silêncio" normativo perante os crimes de Informática, o próprio recurso integrativo utilizado e defendido pela maior parte da doutrina, também possui um caráter ineficaz, quando não perigoso, pois o uso da analogia em matéria penal, quando imputa ou agrava a situação do acusado, se reveste de uma proibição inconstitucional pelo Princípio da Reserva Legal.

Malgrado se reconheça atualmente o legitimo desejo de reduzir a atuação do Direito Penal em face das relações humanas, de acordo com a diretriz da intervenção mínima, é imperioso notar que certas condutas que atentam contra bens informáticos ou informatizados, ou em que o agente se vale do sistema em si para alcançar fins ilícitos devem ser penalmente sancionadas ou criminalizadas.

De maneira que se espera a necessária e urgente aprovação por parte do Congresso Nacional do Projeto de Lei nº 84/99 do Deputado Luiz Piauhylino,

onde se busca classificar as condutas que podem redundar em crimes na Internet e na área de Informática, proporcionando maior segurança para o usuário e para a sociedade em geral, indubitavelmente dependente dos recursos tecnológicos oferecidos pelo processamento de dados. Enquanto essa integração entre a norma e a realidade factual não se realiza, não é concebível que os usuários da Internet fiquem vulneráveis a delitos praticados por *harckers* ou criminosos do mundo real, que usam o computador como arma do crime. Restando a esses, então, o uso da Informação, dessa vez como prevenção contra abusos cometidos através da rede.

REFERÊNCIA

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

DE JESUS, Damásio Evangelista. *Direito Penal*. 26. ed. São Paulo: Saraiva, 2003. 1 v

DEL-CAMPO, Eduardo Roberto Alcântara; OLIVEIRA, Thales Cezar de. *Estatuto da Criança e do Adolescente*. São Paulo: Atlas, 2005. – (Série leituras jurídicas; provas e concursos).

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

JULIANA CARPANEZ. 07/01/2006 - 16h05 .Legislação tradicional "julga" crimes de informática. http://www1.folha.uol.com.br/folha/informatica/ult124u19453.shtml. Acessado em 23/11/2006.

MATA, Brenno Guimarães Alves da. Análise e tendências do cenário jurídico atual na Internet . Jus Navigandi, Teresina, ano 4, n. 46, out. 2000. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=1771>. Acesso em: 01 de novembro de 2006.

MIRANDA, Marcelo Baeta Neves. Abordagem dinâmica aos crimes via Internet . Jus Navigandi, Teresina, ano 4, n. 37, dez. 1999. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=1828>. Acesso em: 23/ 09/ 2006.

MORON, Fernanda de Almeida P. "A Internet e o Direito". [online] Disponível na Internet via www.url:http://www.travelnet.com.br/juridico/art1_96htm. (26.02.96). Arquivo capturado em 17 de novembro de 2006.

PABLIUCA, José Carlos Gobbis. *Direito Penal: parte geral*. São Paulo: Editora Ridel, 2006. (Resumos de Direito Penal Ridel).

PAIVA, Mário Antônio Lobato de. Primeiras linhas em Direito Eletrônico. Jus Navigandi, Teresina, ano 7, n. 61, jan. 2003. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=3575>. Acesso em: 08/11/2006.

ROSA, Fabrízio. *Crime de Informática.* Campinas-SP: Editora Bookseller, 2002.

SCHOUERI, Luiz Eduardo Org. *Internet*: o direito na era digital. Rio de Janeiro: Editora Forense, 2001.

SOUZA, Carlos Antônio Farias de. "O Direito na Era Digital". [online] Disponível na Internet via www.url:http://www.braznet.com.br/~arrabal/artigos/desousal.htm. Arquivo capturado em 19 de novembro de 2006.

ANEXOS

ANEXO - I

LEI DE SOFTWARE

LEI Nº 9.609, DE 19 DE FEVEREIRO DE 1998.

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

O PRESIDENTE DA REPÚBLICA

Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

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

CAPÍTULO II

DA PROTEÇÃO AOS DIREITOS DE AUTOR E DO REGISTRO

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

CAPÍTULO III

DAS GARANTIAS AOS USUÁRIOS DE PROGRAMA DE COMPUTADOR

Art. 7º O contrato de licença de uso de programa de computador, o documento fiscal correspondente, os suportes físicos do programa ou as respectivas embalagens deverão consignar, de forma facilmente legível pelo usuário, o prazo de validade técnica da versão comercializada.

Art. 8º Aquele que comercializar programa de computador, quer seja titular dos direitos do programa, quer seja titular dos direitos de comercialização, fica

obrigado, no território nacional, durante o prazo de validade técnica da respectiva versão, a assegurar aos respectivos usuários a prestação de serviços técnicos complementares relativos ao adequado funcionamento do programa, consideradas as suas especificações.

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

CAPÍTULO IV

DOS CONTRATOS DE LICENÇA DE USO, DE COMERCIALIZAÇÃO E DE TRANSFERÊNCIA DE TECNOLOGIA

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

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

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

§ 1º Serão nulas as cláusulas que:

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

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

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

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

Parágrafo único. Para o registro de que trata este artigo, é obrigatória a entrega, por parte do fornecedor ao receptor de tecnologia, da documentação

completa, em especial do código-fonte comentado, memorial descritivo, especificações funcionais internas, diagramas, fluxogramas e outros dados técnicos necessários à absorção da tecnologia.

CAPÍTULO V

DAS INFRAÇÕES E DAS PENALIDADES

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

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

§ 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:

Pena - Reclusão de um a quatro anos e multa.

§ 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;

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

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

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

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

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

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

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

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

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

CAPÍTULO VI

DISPOSIÇÕES FINAIS

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

Art. 16. Fica revogada a Lei nº 7.646, de 18 de dezembro de 1987.

Brasília, 19 de fevereiro de 1998; 177º da Independência e 110º da República.

FERNANDO HENRIQUE CARDOSO

José Israel Vargas