FACULDADE DE CIÊNCIAS E EDUCAÇÃO DE RUBIATABA - FACER

CURSO: DIREITO

GERLEI SILVA MATOS

CRIMES VIRTUAIS – UM ESTUDO SOBRE A TIPIFICAÇÃO PENAL

RUBIATABA/GOIÁS

GERLEI SILVA MATOS

CRIMES VIRTUAIS – UM ESTUDO SOBRE A TIPIFICAÇÃO PENAL

Trabalho de Curso submetido à Faculdade de Ciências e Educação de Rubiataba – FACER, como parte dos requisitos necessários para a obtenção do Grau de Bacharel em Direito. Sob a orientação do Professor Cláudio Kobayashi.

RUBIATABA/GOIÁS, 2008

GERLEI SILVA MATOS

CRIMES VIRTUAIS – UM ESTUDO SOBRE A TIPIFICAÇÃO

Trabalho de Curso submetido à Faculdade de Ciências e Educação de Rubiataba – FACER, como parte dos requisitos necessários para a obtenção do Grau de Bacharel em Direito.

Cláudio Kobayashi
Especialista

Roseane Cavalcante de Souza
Mestre

Samuel Balduino Pires da Silva
Especialista

Rubiataba, 2008

Dedico este trabalho e tudo que ele significou para mim, às pessoas que amo. Aos meus pais, Gercino José de Matos e Noranei Francisca da Silva Matos que são meus incentivadores, que sempre acreditaram e confiaram na minha pessoa. Ao meu Irmão Ewerton Silva Matos pelo apoio. Muito obrigado e sintam-se presenteados com esta monografia.

AGRADECIMENTOS

Agradeço a todos os que me ajudaram na elaboração deste trabalho: Em especial ao meu orientador Cláudio Kobayashi, visto que sem ele nada disto teria sido possível.

"A adaptação é a grande lei da vida e do mundo não-vivo. São condições exteriores e interiores que tornam necessárias as adaptações, sem as quais não se estabeleceria um modus vivendi e desapareceriam os seres".

Pontes de Miranda

RESUMO

O propósito deste trabalho monográfico consistiu em analisar no âmbito penal à tipificação dos crimes virtuais e se tal resolveria os problemas decorrentes destas condutas ilícitas. Tendo em vista, as discussões no âmbito jurídico sobre o tema que vem ganhando força nos últimos anos, impulsionado pela evolução da Internet que é um dos principais meio de comunicação na atualidade. Esta analise deu-se de forma exploratória com caráter qualitativo, através do método de compilação bibliográfico. A Revisão bibliográfica deu-se através da análise do conceito de crime, a classificação de crimes virtuais em puros, impuros e mistos, aplicabilidade do princípio da legalidade ou reserva legal, requisitos do tipo, e projetos de leis que estão em andamento no congresso. Notando-se assim, que é necessária uma política forte para inibir os crimes virtuais que culmine em uma legislação que determine sanções eficazes para os praticantes destas condutas, tanto no âmbito civil, como também no âmbito penal objetivando a punição mais severa dos agentes que cometerem os crimes virtuais.

Palavras-chave: Crimes Virtuais, Tipificação, Bem Jurídico, Agente, Culpabilidade.

ABSTRACT

The purpose of this monographic study was to examine under the criminal ambit, classification of virtual crimes and if it such, solve the problems arising from illegal conduct. In view, the discussions in the legal framework about the subject that has been gaining strength in recent years, driving by the evolution of the Internet that is a major means of communication in today. This review took place in exploratory character with quality, through the method of compiling bibliography. The literature review took place through the analysis of the concept of crime, the classification of crimes in virtual pure, impure and mixed, applicability of the principle of legality or legal reserve requirements of the type, and projects of laws that are under way in Congress. Noting, so it is necessary a strong policy to stifle the virtual crimes that will culminate in a virtual law establishing effective for the practitioners of these pipelines, both within society, bur also under criminal targeting the most severe punishment of officials who commit the virtual crimes.

Keywords: Virtual Crimes, Grading, Legal Well, Agent, Fault.

LISTA DE ABREVIATURAS E SIGLAS

ARPA	Advanced Research Projects Agency
ARPANET	Advanced Research Projects Agency Network
CD	Compact Disc
CP	Código Penal;
CPP	Código Processo Penal;
DARPA	Defense Advanced Research Projects Agency
ECA	Estatuto da Criança e Adolescente;
IP	Internet Protocol
LAN	Local Area Network
MILNET	Military Network
NSF	National *Science* Foundation
OECD	Organização de Cooperação e Desenvolvimento Econômico;
SPAM	Spiced Ham
TCP	Transmission Control Protocol

SUMÁRIO

INTRODUÇÃO

A discussão sobre a importância de uma possível tipificação de novas condutas consideradas crimes virtuais vem ganhando força nos últimos anos, impulsionada pela evolução da Internet que é um dos principais meio de comunicação.

A elevação do número de crimes cometidos no âmbito virtual reflete e alimenta este debate na sociedade. Verificando assim que existem algumas condutas que já estão tipificadas no ordenamento jurídico de forma esparsa.

Assim, o problema de estudo proposto versa sobre a correta tipificação dos crimes virtuais, visto que a evolução tecnológica avança sobremaneira e o direito demora a estabelecer normas de tratamento para os crimes.

Desta forma, surgem conceitos e análises que observam a necessidade de uma adequada tipificação para coibir tais condutas além de explicar e especificar quais são os objetos a serem tutelados por essa tipificação na norma penal.

Portanto, nesta pesquisa será trabalhada a classificação dos crimes virtuais em puros, impuros e mistos; objetivando determinar quais condutas devem ser tipificadas, levando-se em consideração o princípio da legalidade e o da anterioridade.

Todavia, observa-se a necessidade de uma análise detalhada, objetivando-se especificamente analisar no âmbito penal à tipificação dos crimes virtuais e estudar os princípios da anterioridade e legalidade.

Esta pesquisa foi feita de forma exploratória com caráter qualitativo, através do método de compilação bibliográfica.

No Capítulo 1, tratou-se da metodologia utilizada para a realização deste estudo monográfico.

No Capítulo 2, observaram-se algumas considerações gerais sobre a evolução histórica da Internet e a termologia de crime, de forma a se verificar a relação íntima do

Direito Penal com a Internet, visto que aquele regula as formas de condutas definidas como crime que se potencializa no âmbito virtual da Internet.

Neste Capítulo também, estudou-se as definições de crimes virtuais: puro, impuro ou misto, verificando-se quais condutas deveriam ser tipificadas. Como também a aplicabilidade dos princípios da legalidade ou reserva legal, para garantir a legitimidade legal dessas possíveis tipificações.

Ainda neste, analisou-se como ocorrem os crimes virtuais e quais seriam os seus efeitos no mundo jurídico. Observo quais as providências que já foram tomadas para uma possível tipificação dessas condutas no código penal. Tendo por fim observado a viabilidade da tipificação dos crimes virtuais no Código Penal.

No Capítulo 3, apresentaram-se as Discussões e Resultados da pesquisa, analisando pontos convergentes e divergentes como resultado da compilação estabelecida.

Nas Considerações Finais, buscou-se demonstrar o que se procurou estudar no trajeto percorrido deste trabalho, ressaltando a íntima relação da Internet com o Direito Penal e o que tal relação ocasionou no âmbito doutrinário em relação às pesquisas e conceituações dos crimes virtuais, como também a necessidade de uma adequada análise da tipificação para não ocasionar injustiça no âmbito penal nem no civil.

1 - METODOLOGIA

1. 1 Tipo de Pesquisa

A metodologia serve como meio para realização, em termos de construção e definição, da pesquisa anunciada nos objetivos do projeto.

Desta forma, neste tópico serão apresentados os procedimentos metodológicos utilizados nesta pesquisa monográfica.

Em primeiro lugar observar-se-á que o tipo da pesquisa é exploratório, pois segundo Gil (2002, p. 41) "tem como objetivo, proporcionar maior familiaridade com o problema, com vistas a torná-lo mais explícito ou a constituir hipóteses", visando assim, proporcionar uma visão geral de um determinado fato, promovendo um maior conhecimento sobre o tema ou e o problema da pesquisa.

Sendo assim, serão pesquisados artigos, livros, ou seja, documentos e matérias, que segundo Gil (2002, 44) se define como pesquisa bibliográfica, que é "desenvolvida com base em material já elaborado, constituído principalmente de livros e artigos científicos".

A partir desta pesquisa bibliográfica, efetuou-se uma análise qualitativa que segundo Minayo (2003, p. 16-18):

> Trata-se de uma atividade da ciência, que visa à construção da realidade, mas que se preocupa com as ciências sociais em um nível de realidade que não pode ser quantificado, trabalhando com o universo de crenças, valores, significados e outros construtos profundos das relações que não podem ser reduzidos à operacionalização de variáveis.

Observa-se ainda que a análise qualitativa "depende de muitos fatores, tais como a natureza dos dados coletados, a extensão da amostra, os instrumentos de pesquisa e os pressupostos teóricos que nortearam a investigação. Pode-se, no entanto, definir esse processo como uma seqüência de atividades, que envolve a redução dos dados, a categorização desses dados, sua interpretação e a redação do relatório" (GIL, 2002, p. 133).

Ainda utilizou-se também, o método de pesquisa de compilação, visto que, este tipo de monografia é um trabalho que "consiste na exposição do pensamento dos vários autores que escreveram sobre o tema escolhido" (NUNES, 2001, p. 19). Desta forma, procurou-se demonstrar o maior número possível de obras publicadas sobre o assunto versado, sendo assim possível "organizar as várias opiniões, antepô-las logicamente, quando se apresentam antagônicas, harmonizar os pontos de vista existentes na mesma direção" (NUNES, 2001, p. 19). Observando ainda que neste tipo de pesquisa o estudante pode "dar sua opinião sobre os pontos relevantes, bem como suas conclusões" (NUNES, 2001, p. 19).

1. 2 Coleta de Dados

Nas orientações de ROESCH (1999) observa-se que a coleta de dados trata-se do um meio utilizado para que se possa conseguir absorver as informações através de dados que interessa aos objetivos da pesquisa proposta.

Desta forma, observado essa visão, esta coleta de dados se deu através da pesquisa em fontes primárias, que segundo Nunes (2001, p. 48) podem ser considerados os levantamentos em "publicações em livros" sem ser virtual, as quais foram transcritas em fichas bibliográficas e de apontamentos que segundo Nunes (2001, p. 81) podem ser definidas como sendo a "primeira para anotar as referências bibliográficas e a última para o registro de idéias, hipóteses etc.".

Como o método de pesquisa escolhido foi o da compilação, optou o pesquisador, por delimitar o estudo às obras e autores constantes da biblioteca da faculdade.

Também foram coletadas informações através de fontes secundárias, que segundo Nunes (2001, p. 48) é "toda aquela que indiretamente estiver sendo utilizada como complemento do texto principal, quer para servir de contraposição, quer para servir de fundamentação mais ampla"; esta foi feita através da organização de arquivos e de artigos encontrados na Internet.

Há que se ressaltar neste ponto, que as informações coletadas através da internet se deram através de motores de pesquisa, por palavras chaves ligadas ao tema.

E que segundo Gil (2002, p. 74) constitui "um dos mais importantes veículos de informações".

1.3 Análise dos Dados

Para Lakatos (2005, p. 169) a etapa de análise dos dados representa "a aplicação da lógica dedutiva e indutiva do processo de investigação", isto é, nesse momento os dados devem proporcionar respostas às investigações.

Desta forma, a análise de dados ocorreu em duas etapas. A primeira foi à organização das informações obtidas através da coleta em fichas.

A segunda se deu após o fichamento, onde o autor começou a comparar os autores a fim de verificar as convergências e os antagonismos de pensamento, podendo elaborar inclusive algumas considerações próprias, a respeito.

2 - REFERENCIAL TEÓRICO

Este tópico pretende traçar algumas considerações gerais sobre a evolução histórica da Internet e a termologia de crime. Sem a pretensão de esgotar o assunto e objetivando dar embasamento para se entender o que é a conceituação de crime virtual no próximo tópico.

2.1 Internet

2.1.1 Conceito

O vocábulo Internet é uma expressão tornada cada vez mais popular, visto a grande incidência causada na atividade diária pelo desenvolvimento tecnológico. Entretanto, tal termo não é tão conhecido em seu significado. Desta forma, O vocábulo Internet sob o ponto de vista técnico pode ser conceituado na ciência da informática, como sendo:

> uma sociedade cooperativa que forma uma comunidade virtual, estendendo-se de um extremo a outro do globo. Como tal, a Internet é um portal para o espaço cibernético, que abrange um universo virtual de idéias e informações em que nós entramos, sempre que lemos um livro ou usamos um computador (ROSA, 2002, p. 23).

Na mesma corrente, Paesani (2000, p. 27) demonstra que a Internet é "uma imensa rede que liga elevado número de computadores em todo o planeta. As ligações surgem de várias maneiras: redes telefônicas, cabos e satélites"; e Castro (2003, p. 2) diz que:

> a Internet é uma grande rede de comunicação mundial, onde estão interligados milhões de computadores, sejam eles universitários, militares, comerciais, científicos ou pessoais; todos interconectados. É uma rede de redes, que pode ser conectada por linhas telefônicas, satélites, ligações por microondas ou por fibra ótica.

Assim, a Internet consiste em conjunto de tecnologias para acesso, distribuição e disseminação de informação em redes de computadores, visando em especial, disponibilizar informações ou serviços que as pessoas desejam compartilhar.

A Internet cresce e se modifica em uma velocidade que não se pode prever que rumo tomará. Tudo indica que se ainda não for, se tornará o principal meio de transações comerciais e distribuição de informação.

Contudo, é necessário entender esta conceituação no prisma jurídico, visto que a Internet potencializa determinadas condutas criminosas e apresenta novas condutas lesivas. Desta forma, como ensina Rosa (2002, p. 33) a Internet é conceituada no âmbito jurídico como sendo: "uma rede transnacional de computadores interligados, com a finalidade de trocar informações diversas e na qual o usuário ingressa, por vários meios, mas sempre acaba por realizar fato jurídico, gerando conseqüências inúmeras nas mais variadas localidades".

Com isso, surge a necessidade de regulamentar esses fatos jurídicos que são gerados por meio da Internet, "seja nas relações de Direito Privado[1], seja no campo do Direito Público[2]" (CASTRO, 2003, p. 8). E em especial o tema proposto ao Direito Penal, por causa das novas condutas que surgem por meio da Internet e as que ela potencializa.

2.1.2 Um pouco de Historicidade da internet

A internet se espalhou por todo mundo, contudo poucos dos usuários conhecem de forma mais aprofundada como se deu a origem desse novo mundo virtual. Como ensina Rosa (2002, p. 29), "a maior parte, apenas ouviu falar que a grande rede foi idealizada para resistir á ataques nucleares – algo bastante tangível durante a guerra fria[3], época em que foi concebida".

O fato marcante, embrionário, do surgimento da internet foi o anúncio do presidente americano Dwingt Eisenhower em meados de 1957, sobre a criação de uma agência federal

---

1 Direito Privado segundo Diniz (2004, p. 17) "é o que disciplina as relações entre particulares, nas quais predomina, de modo imediato, o interesse de ordem privada, como, p. ex., a compra e venda, a doação, o usufruto, o casamento, o testamento, o empréstimo, etc.".

2 O Direito Público segundo Dinis (2004, p. 17) "seria aquele que regula as relações em que o Estado é parte, ou seja, rege a organização e atividade do Estado considerado em si mesmo (direito constitucional), em relação com o outro Estado (direito internacional), e em suas relações com os particulares, quando procede em razão de seu poder soberano e atua na tutela do bem coletivo (direitos administrativos e tributários)".

3 A Guerra Fria foi à designação atribuída ao conflito político-ideológico entre os Estados Unidos (EUA), defensores do capitalismo, e a União Soviética (URSS), defensora do socialismo, compreendendo o período entre o final da Segunda Guerra Mundial (1945) e a extinção da União Soviética (1991). É chamada "fria" porque não houve qualquer combate direto entre as superpotências, uma vez que ambas acabaram apenas financiando guerras em outros países para mostrar o seu poder de fogo - embora o mundo todo temesse a ocorrência de um novo conflito mundial e por se tratar de dois países com grande arsenal de armas nucleares. Wikipédia, enciclopédia livre. Rand. Disponível em: http://pt.wikipedia.org/wiki/Guerra_fria. Acessado em: 8 de setembro de 2008.

norte-americana, ARPA[4], com a "missão de pesquisar e desenvolver alta tecnologia para as forças armadas" (ROSA, 2002, p. 29).

A ARPA em 1969, "confiou a *Rand Corporation*[5] a elaboração de um sistema de telecomunicações, que garantisse que um ataque nuclear russo não interrompesse a corrente de comando dos Estados Unidos" (ROSA, 2002, p. 29).

A solução, a priori tomada por *Rand Corporation* para garantir que os comandos dos Estados Unidos não fossem interrompidos, "foi à criação de pequenas redes locais (LAN)[6] " (PAESANI, 2000, p. 25), de forma que poderiam ser criadas em qualquer local estratégico e que posteriormente poderiam ser interligadas por meio de redes de telecomunicação. Desta forma, se uma cidade viesse a ser destruída por um ataque, essas redes conexas não seriam destruídas.

No entanto, como ensina Rosa (2002) à decolagem deste novo sistema de comunicação, de pequenas redes locais (LAN), aconteceu em meados dos anos 70, quando ARPA verificou a viabilidade de se aplicar esta forma de comunicação ao mundo acadêmico e científico, visto que disponibilizaria uma gama maior de informações a estes, e foi a partir dessa finalidade que houve a sua grande propagação de liberdade de expressão. Sua primeira demonstração pública aconteceu em 1972, durante uma "Conferência Internacional sobre Comunicações Computacionais, em Washington" (ROSA, 2002, p. 29).

Devido ao rápido crescimento dessas pequenas redes de comunicação (LAN) surge a ARPANET[7], que cresceu aceleradamente e por causa disto:

---

[4] Advanced Research Projects Agency - Agência de Projetos de Pesquisa Avançada. Ferramentas de idiomas. Disponível: http://www.google.com.br/language_tools. Acessado 02/11/08.

[5] A RAND Corporation (investigação e desenvolvimento) é uma entidade sem fins lucrativos política global, formado primeiro a oferecer investigação e de análise para os Estados Unidos às forças armadas. A organização, desde então, expandiu-se para trabalhar com outros governos, fundações privadas, organismos internacionais e organizações comerciais. Ela é conhecida por seu rigor, muitas vezes-quantitativa, e não partidário. Wikipédia, enciclopédia livre. Rand. Disponível em: http://en.wikipedia.org/wiki/RAND_Corporation. Acessado em: 8 de setembro de 2008.

[6] Podemos conceituar LAN como sendo qualquer rede de micros que englobe um pequeno espaço, uma sala ou mesmo um prédio. Carlos E. Morimoto. Significado das Siglas. Disponível em: http://www.guiadohardware.net/artigos/significado-siglas/. Acessado em 29-09-2008.

[7] ARPANET (Advanced Research Projects Agency Network - Agência de Projetos de Pesquisa Avançada de rede). Uma das primeiras redes de computadores, montada pelo governo dos EUA. Fabrício, Rafael. Como a Internet começou? Você sabe?. Disponível em: http://sml-adoff.blogger.com.br/2004_02_01_archive.html. Acessado em 29-09-2008.

Vinton Cerf, do Departamento de Pesquisa avançada da Universidade da Califórnia, registrou o protocolo TCP/IP[8]; trata-se de um código que consente ás diversas redes incompatíveis por programas e sistemas, comunicarem-se entre si (PAESANI, 2000, p. 25).

No entanto, em meados da:

> década de 1980, a ARPANET foi dividida em duas redes: ARPANET e MILNET (rede militar). Esta interconexão de redes foi denominada DARPA internet. Em 1986 foram interligados os supercomputadores do centro de pesquisa da entidade NSF – *National Science Foundation* (Fundação Nacional de Ciências) com os da ARPANET. Os conjuntos de todos os computadores e redes ligados a esses dois supercomputadores formaram um backbone (espinha dorsal de rede), e, a partir daí, esta estrutura foi denominada Internet (CASTRO, 2003, p. 2-3).

O governo "estadunidense abriu a rede às empresas e continuou financiando a ARPANETE até o ano de 1989" (ROSA, 2002, p. 30).

Com a liberação do acesso ao público, a Internet passou a crescer a taxas vertiginosas. Ainda em 1990, entra no ar o primeiro provedor de acesso[9] comercial do mundo o World (Mundo), permitindo que usuários comuns, desde que dispusessem de um microcomputador e de um modem, alcançassem a grande rede mundial, internet. Em 1990, como ensina Rosa (2002, 30), "a Argentina, Áustria, Bélgica, Brasil, Chile, Grécia, Índia, Irlanda, Coréia do Sul, Espanha e Suíça", se conectam nesta rede. Dando assim, a concretização á internet que conhecemos hoje.

2.2 Crime

Ao se analisar crime é importante entender sua etimologia e a partir deste, observar as formas de conceituação em crime formal, material e analítico.

A priori, a termologia crime, deriva da palavra do latim *Crimen* (crime); e o Delito é derivado de *delinquere*, "que significa abandonar, resvalar, desviar-(se)" (JESUS, 2003, p. 150).

---

[8] Transmission Control Protocol: Controle de Transmissão de Protocolos; Internet Protocol: Protocolo de Internet. Ferramentas de idiomas. Disponível: http://www.google.com.br/language_tools. Acessado 02/11/08.

[9] Os provedores de acesso ou de informações são os efetivos prestadores de serviços aos usuários finais da Internet, que os utilizam normalmente por meio da rede telefônica. Esses provedores, por sua vez, estão conectados aos backbones. Cabe ao usuário a escolha do melhor provedor, de acordo com a sua conveniência. ABUSAR.ORG: Associação Brasileira dos Usuários de Acesso Rápido. Disponível em: http://www.abusar.org/provedores.html. Acessado em 18 de novembro de 2008.

Jesus (2003) demonstra que tais termologias tiveram o início de sua aplicabilidade com maior ênfase na Idade Média. Tais termos (*crimen* e *delictum*) foram empregados para diferenciar o que seria infração leve e grave: *crimen* sendo infração grave; *delictum* sendo infração leve.

Diferentemente da Idade Média, no Brasil a termologia crime e delitos não determinam o que é infração leve e grave, visto que:

> O termo infração é genérico, abrangendo os crimes ou delitos e as contravenções. Pode ser empregado o termo delito ou crime. O Código Penal usa as expressões infração, crime e contravenção, áquela abrangendo estes. O Código de Processo Penal emprega o termo infração, em sentido genérico, abrangendo os crimes (ou delitos) e as contravenções (ex.: arts. 4º, 70, 72, 74, 76, 77, 92 etc.). Outras vezes, usa a expressão delitos como sinônimo de infração (exs.: arts. 301 e 302) (JESUS, 2003, p. 150).

Todavia, para entender o que é crime, é necessário observar os sistemas de conceituação adotados na doutrina.

2.2.1 Conceituação Formal

O primeiro sistema de conceituação é o formal, este diz que crime é "uma conduta contrária ao Direito, a que a lei atribui uma pena" (PIMENTEL, 1983, p. 2), ou seja, é "toda ação ou omissão proibida pela lei sob a ameaça de pena" (FRAGOSO, 1991, p. 144).

Shintati (1999, p. 42), na mesma linha de pensamento, afirma que o crime na visão formal "é toda ação ou omissão proibida ou ordenada pela lei, sob a ameaça de pena". Desta forma, "é o comportamento humano, proibido pela norma penal, ou, simplesmente, a violação desta norma" (TELES, 2004, p. 152).

Na mesma corrente, Nucci (2006, p. 158) ensina que o crime:

> É a concepção do direito acerca do delito, constituindo a conduta proibida por lei, sob ameaça de aplicação de pena, numa visão legislativa do fenômeno. Cuida-se, na realidade, de fruto do conceito material, devidamente formalizado.

A Lei de Introdução ao Código Penal define crime em seu art. 1º, *in verbis*:

> Considera-se crime a infração penal que a lei comina pena de reclusão ou de detenção, quer isoladamente, quer alternativa ou cumulativamente com a pena de multa; contravenção, a infração penal a que a lei comina, isoladamente, pena de prisão simples ou de multa, ou ambas. Alternativa ou cumulativamente.

Estas conceituações formais determinam o crime "sob o aspecto da técnica jurídica, do ponto de vista da lei" (JESUS, 2003, p. 150).

Todavia, Teles (2004, p. 152) afirma que estes conceitos formais não: "São insuficientes para os estudiosos do Direito Penal que pretendem e devem debruçar-se sobre esse fenômeno, de modo a conhecê-lo em sua inteireza, em sua profundidade, porque não desnudam os aspectos essenciais do crime".

É necessário observar, além dos conceitos formais que determina como crime, exatamente a conduta que está tipificada em lei. Os conceitos materiais, visto que estes são antecedentes ao Código Penal, porque analisa a razão pela qual foi tipificada determinada conduta.

2.2.2 Conceituação Material

Este fornece ao legislador um critério político-criminal de forma a embasar o que o Direito Penal deverá punir e o que deixará de punir, ou seja, é nos conceitos materiais de crime, que se verifica "a lesão do bem jurídico" (TELES, 2004, p. 153).

Portanto, o segundo sistema é a conceituação material; este procura conceituar crime "sob o ângulo ontológico, visando a razão que levou o legislador a determinar como criminosa, uma conduta humana, a sua natureza danosa e conseqüências" (JESUS, 2003, p. 150). Desta forma, este conceito observa "a ação ou omissão que, a juízo do legislador, contrasta violentamente com valores ou interesses do corpo social, de modo a exigir que seja proibida sob ameaça de pena" (FRAGOSO, 1991, p. 145).

Desta forma, o crime é conceituado materialmente como sendo: "a concepção da sociedade sobre o que pode e deve ser proibido, mediante a aplicação de sanção penal. É, pois a conduta que ofende um bem juridicamente tutelado, ameaçado de pena" (NUCCI, 2006, p. 157).

Na mesma corrente, Shintati (1999, p. 42) ensina que sob o aspecto material, "o crime é um desvalor da vida social, ou seja, uma conduta que se proíbe, com ameaça de pena, porque constitui ofensa a um valor da vida social, ou seja, a um bem jurídico".

Teles (2004, p. 153) ensina que quando o legislador observa esses aspectos materiais do crime ele:

> Verifica se o mesmo é daqueles que lesionam bens jurídicos, ou pelo menos expõem-nos a grave perigo de lesão, e se tais lesões são de gravidade acentuada, de modo a serem proibidas sob a ameaça da pena criminal. Do contrário, não poderá o legislador considerá-las crime.

Na conceituação formal determina qual é o elemento dogmático da conduta qualificada como crime por uma norma penal. Na conceituação material determina quais os elementos que deram conteúdo e razão de ser ao esquema legal.

2.2.3 Conceituação Analítica

Todavia, ainda tem a corrente da conceituação analítica que determina que o crime é um fato típico, ilícito e culpável, como ensina Jesus (2003, p. 150): "crime é um fato típico e antijurídico". Nucci (2006, p. 158) afirma que esta corrente de conceituação "é majoritária no Brasil e no exterior". É a que determina de forma mais clara, o que é crime.

Conceituar "analiticamente o crime, é extrair de todo e qualquer crime aquilo que for comum a todos eles, é descobrir suas características, suas notas essenciais seus elementos estruturais" (TELES, 2004, p. 155). Portanto, para que este seja feito é necessário entender os três critérios para se determinar o que é crime, sendo eles: fato típico, ilicitude e culpabilidade.

2.2.3.1 Fato Típico

A conceituação do tipo:

> Remonta historicamente ao de corpus *delicti*, sendo empregado na antiga doutrina para significar o conjunto das características de determinado delito. Adquiriu função autônoma na estrutura do fato punível [...] o conceito de tipo limitava às características objetivas do crime, por contraposição â antijuridicidade e à culpabilidade (FRAGOSO, 1991, p. 153).

O fato típico é "um fato da vida, um acontecimento que se amolda, se ajusta, a um tipo legal de crime" (TELES, 2004, p. 156).

É um "comportamento humano (positivo ou negativo) que provoca um resultado (em regra) e é previsto na lei penal como infração" (JESUS, 2003, p. 154).

Para que surja a possibilidade jurídica de imposição da sanção penal é necessário que o sujeito culpado tenha praticado um fato típico e antijurídico.

2.2.3.2 Fato Antijurídico ou Ilícito

A ilicitude é a relação "de contrariedade entre o fato típico e o ordenamento jurídico" (JESUS, 2003, p. 155). É o fato "proibido pelo Direito, injustificado, não permitido, proibido pela ordem jurídica" (TELES, 2004, p. 157). É a conduta descrita em norma penal incriminadora que é expressamente declarada ilícita por ser contrária aos valores sociais, ou seja, a um interesse que é protegido por lei, como por exemplo: a inviolabilidade dos direitos autorais.

Para ser ilícito, não pode haver ou ocorrer qualquer "causa de exclusão da ilicitude (estado de necessidade, legítima defesa, estrito cumprimento de dever legal ou exercício regular de direito)" (JESUS, 2003, p. 356), visto que esses requisitos podem afastar a ilicitude por causa da necessidade da pessoa se proteger, como por exemplo: de uma agressão atual ou perigo atual que não possa tomar outra postura que não seja de defesa ou salvamento.

Todavia, se ultrapassar os limites da defesa em um dos casos de excludentes de ilicitude, este será penalizado no dano que ocasionar a outrem.

2.2.3.3 Culpabilidade

Culpabilidade é a "reprovação do fato praticado pelo agente, a censurabilidade do comportamento humano" (TELES, 2004, p 158). É a "reprovação da ordem jurídica em face de estar ligando o homem a um fato típico e antijurídico" (JESUS, 2003, p. 155).

É a reprovação que vem recair sobre o agente, visto que sua conduta não se enquadrou nas previsões do ordenamento jurídico. Porque tinha a possibilidade de não fazer

uma conduta tipificada, como não permitida perante determinada sociedade e escolheu fazê-la.

Jesus (2003, p. 156) ensina que culpabilidade "não é um requisito do crime, funcionando como condição de imposição da pena".

Depois de observados os conceitos de crime, há a necessidade de se analisar a relação da internet com o Direito Penal.

2.3 Relação da Internet com o Direito Penal

O avanço da tecnologia na área da informática provocou uma grande revolução nas relações sociais. As facilidades alcançadas pelo uso do computador, em especial a Internet, transformaram a vida moderna.

Estas inovações atingem o Direito em todas as suas áreas, todavia, no âmbito penal se observam várias condutas que são potencializadas com o advento da Internet, como por exemplo:

> A violação do direito do autor que é violentamente atacado na rede, a pirataria reina impune, seja na área artística, como no campo do software. Este último foi protegido pela Lei nº 9.609/98. Os usuários bem equipados trocam músicas na Internet, e gravam CDs com suas canções preferidas, sem sair de casa; assim não vão mais às lojas e, por conseqüência, não é repassado ao artista o valor referente ao direito autoral (CASTRO, 2003. 7).

Tantas inovações na área tecnológica propiciaram o aparecimento de novos tipos de crimes (como a proliferação de vírus[10], spam[11], entre outros) ou novas formas de praticar os já conhecidos e tipificados no código penal, visto a vulnerabilidade do ambiente computacional

---

[10] Em informática, um vírus de computador é um programa malicioso desenvolvido por programadores que, tal como um vírus biológico, infecta o sistema, faz cópias de si mesmo e tenta se espalhar para outros computadores, utilizando-se de diversos meios. Wikipédia, a enciclopédia livre. Vírus de computador. Disponível em: http://pt.wikipedia.org/wiki/V%C3%ADrus_de_computador. Acessado em: 4 de setembro de 2008.

[11] O termo Spam, abreviação em inglês de spiced ham (presunto condimentado), é uma mensagem eletrônica não-solicitada enviada em massa. Na sua forma mais popular, um spam consiste numa mensagem de correio eletrônico com fins publicitários. O termo spam, no entanto, pode ser aplicado a mensagens enviadas por outros meios e noutras situações até modestas. Geralmente os spams têm caráter apelativo e na grande maioria das vezes são incômodos e inconvenientes. Wikipédia, enciclopédia livre. Spam. Acessado em: http://pt.wikipedia.org/wiki/Spam. em 28 de setembro de 2008.

e as circunstâncias adicionais que surgem no ambiente de trabalho, criando assim oportunidades que implicam num baixo risco para a prática do ato ilícito.

Essas questões, até então não constavam no cotidiano, mas, de forma surpreendente e acelerada, passam a preocupar a muitos.

Desta forma, o Direito Penal se vê em uma relação íntima com a Internet, visto que este que regula as formas de condutas definidas como crimes que se potencializam no âmbito virtual ou com novas condutas ilícitas que surgem na Internet. "O uso da Internet e dos demais meios eletrônicos para a prática de crimes tem sido uma constante. Algumas das capitais brasileiras já dispõem de delegacias especializadas no combate a esse tipo de crime." (ROHRMANN, 2005. 40).

De acordo com Rohrman (2005, 41):

> Um ponto muito importante é o tratamento jurídico a ser dispensado aos *hackers*[12] e *crakers*[13], bem como àqueles que utilizam o meio virtual para disseminar pequenos programas de computador nocivos ao funcionamento dos sistemas computacionais e outros programas ou dados que podem dificultar o acesso à rede e o uso do computador.

O Brasil ainda não "dispõe de legislação específica para o combate eficaz da criminalidade eletrônica" (ROHRMANN, 2005. 41) de forma a inibir essas condutas.

Por fim, observada a evolução histórica da internet e a termologia da palavra crime, observar-se-á, no próximo tópico, a conceituação de crimes virtuais, objetivando vislumbrar suas características, para posteriormente, no próximo tópico, estudar sua aplicabilidade no Direito, tendo em vista o princípio da Legalidade ou Reserva Legal e a Teoria do Tipo.

---

[12] Hackers (singular: hacker) indivíduos que elaboram e modificam software e hardware de computadores, seja desenvolvendo funcionalidades novas, seja adaptando as antigas. Os Hackers utilizam toda a sua inteligência para melhorar softwares de forma legal. Os hackers geralmente são pessoas com alta capacidade mental e com pouca atividade social. Eles geralmente são de classe média e alta, com idade de 12 a 28 anos. Wikipédia, enciclopédia livre. Rand. Disponível em: http://pt.wikipedia.org/wiki/Hacker. Acessado em: oito de setembro de 2008.

[13] Cracker é o termo usado para designar quem pratica a quebra (ou cracking) de um sistema de segurança, de forma ilegal ou sem ética. Este termo foi criado em 1985, por hackers em defesa contra o uso jornalístico do termo hacker. O uso deste termo reflete a forte revolta destes contra o roubo e vandalismo praticado pelo cracking. Wikipédia, enciclopédia livre. Rand. Disponível em: http://pt.wikipedia.org/wiki/Cracker. Acessado em: 8 de setembro de 2008.

2.3.1 Crimes virtuais

Este tópico pretende traçar algumas considerações gerais sobre crimes virtuais: analisando sua conceituação, características, derivações em puro, impuro e/ou misto. Sem a pretensão de esgotar o assunto.

2.3.2 Breve histórico do surgimento dos crimes virtuais

O surgimento dos crimes virtuais:

> Remonta à década de 1960, época que apareceram na imprensa e na literatura científica os primeiros casos de uso do computador para a prática de delitos, formados, sobretudo, por manipulações, sabotagens, espionagem e uso abusivo de computadores e sistemas, denunciados em matérias jornalísticas. Somente na década seguinte é que se iniciariam os estudos sistemáticos e científicos sobre essa matéria, com emprego de métodos criminológicos, analisando-se um limitado número de delitos informáticos que haviam sido denunciados, entre os quais, alguns casos de grande repercussão na Europa por envolverem empresas de renome mundial (FURLANETO NETO, 2003, p. 68).

A partir de 1980, que houve:

> O aumento de ações criminosas que passaram a incidir em manipulações de caixas bancários, pirataria de programas de computador, abusos nas telecomunicações etc., revelando vulnerabilidade que os criadores do processo não haviam previsto. Acrescente-se ainda, o delito de pornografia infantil na rede, igualmente difundido na época. (FURLANETO NETO, 2003, p. 68).

Esse aumento da criminalidade de 1980 em diante, possui a característica de ter um espaço transnacional, pois todos os países, de uma forma ou de outra, gozam da informatização; logo "a delinqüência correspondente, ainda que em graus distintos, também está presente em todos os continentes" (FURLANETO NETO, 2003, p. 68), visto a universalidade que proporciona a todos os integrantes de vários níveis sociais e econômicos, o acesso aos produtos informatizados, atingindo assim, todos os setores e em todos os lugares.

2.3.3 Conceito

Foi em 1983, com a Organização de Cooperação e Desenvolvimento Econômico – OECD, que se "iniciou um estudo sobre a possibilidade de se aplicar e harmonizar um plano internacional ás leis penais, a fim de lutar contra o uso indevido dos programas de computadores" (ROSA, 2002, p. 53). Assim, em 1986, a OECD conceitua esse tipo de crime

como sendo "qualquer conduta ilegal não ética, ou não autorizada que envolva processamento automático de dados e/ou transmissão de dados" (ROSA, 2002, p. 53).

Posteriormente a esta conceituação, vários pensadores do direito começaram a estudar e analisar o que seriam os crimes virtuais, e a partir destas análises surgiram vários conceitos, que algumas vezes até divergiam do conceito proposto pela OECD, sendo alguns desses conceitos:

Para Rocha (1994, p. 38) os crimes virtuais são "aqueles que têm por instrumento ou por objeto, sistema de processamento eletrônico de dados, apresentando-se em múltiplas modalidades de execução e de lesão de bens jurídicos".

Já Colares (2002, p. 01) diz, que são "aquelas condutas em que o objeto da ação lesa direito, relativo á bens ou dados de informática".

Rosa (2002, p. 54) ensina como "sendo aquela conduta típica, ilícita e culpável, praticada sempre com a utilização de dispositivos, de sistemas de processamento ou comunicação de dados, da qual poderá ou não suceder á obtenção de uma vantagem indevida e ilícita".

Pinheiro (2006, p. 16) ainda diz que é "ação típica, antijurídica e culpável, cometida contra ou pela utilização de processamento automático de dados ou sua transmissão, em que um computador conectado à rede mundial de computadores – Internet – seja o instrumento ou o objeto do delito."

Observados estes conceitos, nota-se que esses pensadores do direito procuram na gênese de seus conceitos, determinar que o procedimento "que atenta contra os dados, que faz na forma em que estejam armazenados, compilados, transmissíveis ou transmissão" (ROSA, 2002, p. 53) serão crimes virtuais. E que a ação típica desses crimes se realiza contra ou pela utilização de processamentos automáticos de dados ou a sua transmissão, ou seja, "a utilização de um sistema de informática para atentar contra um bem ou interesse juridicamente protegido, pertença ele à ordem econômica, à integridade corporal, à liberdade individual, à privacidade, à honra, ao patrimônio público ou privado, à Administração Pública etc." (ROSA, 2002, p. 54).

Contudo, os doutrinadores criminalistas classificam os crimes virtuais em três grandes grupos, sendo eles: a) crimes próprios ou puros; b) crimes impróprios ou impuros; c) crimes mistos.

O crime virtual tem atraído a atenção de vários juristas. Desta forma, várias nomenclaturas são utilizadas, como demonstra Castro (2003, p. 9): "crime de computador, crimes via Internet, crime praticado por meio da Informática, crimes tecnológicos, crimes na Internet, crimes digitais, entre outros".

O presente trabalho sugere a denominação Crimes Virtuais, visto que esta expressão procura designar "as possibilidades de certas condutas delituosas cometidas com o uso do computador, visando atingir sistemas informáticos e/ou bancos de dados contidos na máquina" (ROSA, 2002, p. 51). Contudo as conceituações de crime virtual serão vislumbradas melhor no decorrer deste tópico.

2.3.4 Crimes Virtuais Próprios ou Puros

Os crimes virtuais puros surgiram com a evolução desta Ciência que é a Informática e com a implantação da Internet. Esses são tipos novos, que agridem "a informática como bem juridicamente protegido" (CASTRO, 2003. 10).

O crime virtual puro seria: "toda e qualquer conduta ilícita que tenha por objetivo exclusivo o sistema de computador, pelo atentado físico ou técnico ao equipamento e seus componentes, inclusive dados e sistemas" (FURLANETO Neto, 2003. 69). Ou seja, são aquelas condutas que:

> O sujeito ativo visa especificamente o sistema de informática, em todas as suas formas. Entendemos serem os elementos que compõem a informática o "software", o "hardware" (computador e periféricos), os dados e sistemas contidos no computador, os meios de armazenamento externo, tais como fitas, disquetes, etc. Portanto são aquelas condutas que visam exclusivamente a violar o sistema de informática do agente passivo. As ações físicas se materializam, por exemplo, por atos de vandalismos contra a integridade física do sistema, pelo acesso desautorizado ao computador, pelo acesso indevido aos dados e sistemas contidos no computador. Portanto, é crime de informática puro, toda e qualquer conduta ilícita, que tenha por objetivo exclusivo o sistema de computador, seja pelo atentado físico ou técnico do equipamento e seus componentes, inclusive dados e sistemas (COSTA, 1995. 2).

Todavia, Rohrmann (2002, p. 121) discorda da afirmativa que diz que "o sujeito ativo visa especificamente ao sistema de informática, em todas as suas formas" (COSTA, 1995. 2), ele diz que os crimes virtuais puros:

> Somente são possíveis de serem praticados com a utilização dos sistemas de computadores (ainda que seja apenas um computador simples e não conectado em redes de computadores). Exemplos, em tese, desses tipos de crime seriam os casos de acesso não-autorizado á sistemas de computadores; á obtenção de senhas de computador; á criação e á conseqüente disseminação dos chamados vírus (outros tipos assemelhados como os cavalos de tróia) de computadores; entre outros casos próprios da técnica computacional que evolui constantemente.

Mas Castro (2003, p. 11) reafirma a linha de pensamento de Costa dizendo que os crimes virtuais puros "são aqueles em que o sujeito visa especificamente ao sistema de informática, ás ações se materializam, por exemplo, por atos de vandalismo contra a integridade do sistema ou pelo acesso desautorizado ao computador".

Contudo, mesmo havendo essa pequena variação nas doutrinas observa-se que quando a ação do criminoso se dirigir contra os dados contidos no sistema, este será definido como crime de informática puro, porque nesse último, o computador é essencial para a existência do delito, ou seja, os crimes só podem ser praticados através da informática "sem ela é impossível a execução e consumação da infração, como por exemplo: danos provocados em arquivos por causa de vírus, este não se enquadra:

> Como crime de dano previsto no Código Penal, pois seria necessário que se provocasse prejuízo econômico. Assim, se o agente envia um vírus e destrói apenas os e-mails de outro usuário e estes tratam de assunto sentimental ou mensagens de amizade, não haverá crime [...] e não se confunde este crime com o ato pelo qual o agente entra em uma *homepage* e lá deixa mensagens, 'pichando' a página (CASTRO, 2003, p. 28-29)

Desta forma, a proliferação de vírus, é um crime virtual puro, visto que o ato lesivo só pode ser praticado pela informática.

2.3.5 Crimes Virtuais Impuros ou Impróprios

Os crimes virtuais impróprios são aqueles que "podem ser praticados de qualquer forma, inclusive através da informática ou Internet" (CASTRO, 2003, p. 10).

Os agentes que praticam este tipo de crime utilizam "a internet apenas como instrumento para a realização de um delito já tipificado pela lei penal" (FURLANETO NETO, 2003, p. 69).

Nesse sentido, Costa (1995, 2) ensina que os crimes virtuais impróprios:

> São todas aquelas condutas em que o agente se utiliza do sistema de informática como [...] ferramenta a perpetração de crime comum, tipificada na lei penal, ou seja, a via eleita do sistema de informática não é essencial à consumação do delito, que poderia ser praticado por meio de outra ferramenta. Como exemplo, os casos de estelionato (art. 171, CP), e as suas mais amplas formas de fraude. Quando o computador é ferramenta escolhida pelo agente ativo, que poderia escolher outros meios diversos da informática. [...] Despiciendo aclarar a aplicabilidade aos crimes comuns das normas penais vigentes, porém, poder-se-ia, atendendo a essa classificação, incorporar ao Código Penal, agravantes pelo uso de sistema de informática, vez que é meio que necessita de capacitação profissional e a ação delituosa por esta via reduz a capacidade da vítima em evitar o delito. Posto isto, entendemos ser a presente classificação apta à elaboração de legislação que possa alcançar os delitos de informática, sem, contudo, correr-se o risco de sobreposição de normas, e assim, também, entendemos que é meio hábil à formação de um eficaz Direito Penal de Informática.

Assim o agente para cometer o delito utiliza eventualmente o sistema de informática (computador, internet, entre outros) como meio e instrumento de perpetração de crime comum, não comete assim um crime virtual puro. Como por exemplo: a divulgação de segredo previsto no artigo 153 do Código Penal, que tem como bem tutelado a inviolabilidade dos segredos do indivíduo e da Administração Pública. Este pode ou não, ser cometido por meio da informática, uma vez que "o dispositivo legal menciona que as informações podem estar contidas ou não, no banco de dados da Administração. Estando no sistema de informática da Administração, o uso do computador será instrumento essencial para a prática delituosa" (CASTRO, 2003, p. 24), ou seja, o agente tem que utilizar o computador para adquirir as informações, mas este é uma mera ferramenta para adquirir esta informação, e a partir do momento que o agente tem a informação ele pode usar de qualquer meio para descobrir e divulgar o segredo.

Portanto, quando o computador for utilizado apenas como instrumento de escolha pelo agente ativo para o cometimento do crime comum, não essencial à consumação do delito, este será crime virtual impuro, como nos exemplos já citados.

2.3.6 Crimes Virtuais Mistos

O crime virtual misto se consubstancia nas ações em que o agente visa, bem juridicamente protegido, diverso da informática; porém a informática é ferramenta imprescindível, como ensina Furlaneto Neto (2003, p. 69):

> Crime virtual misto seria aquele em que o uso da internet é condição *sine qua non* para a efetivação da conduta, embora o bem jurídico visado seja diverso do informático, como, por exemplo, as transferências ilícitas de valores em uma *homebanking* ou no chamado *salamislacing*, onde o *cracker* retira de milhares de contas correntes, diariamente, pequenas quantias que correspondem a centavos e as transfere para uma única conta. Embora esses valores sejam ínfimos para o correntista, que, na maioria das vezes nem se dá conta do furto, representam para o cibercriminoso uma expressiva quantia em seu montante.

Quando o agente tem como objetivo, por exemplo:

> Realizar operações de transferência ilícita de valores de outrem, em uma determinada instituição financeira utilizando-se do computador para alcançar o resultado da vantagem ilegal, e, o computador é ferramenta essencial, defrontamo-nos com um crime de informática misto. Porque incidiriam normas da lei penal comum e normas da lei penal de informática. Da lei penal comum, por exemplo, poder-se-ia aplicar o artigo 171 do Código Penal combinado com uma norma de mau uso de equipamento e meio de informática (COSTA, 1995, p. 2).

A partir deste conceito, percebe que o sistema de informática é ferramenta imprescindível a sua consumação. Desta forma verifica-se existência de duas categorias de crimes de informática: aqueles praticados por meio do computador e os praticados contra os dados ou sistemas informáticos. Nos primeiros, o computador será o instrumento; no segundo, o objeto material.

2.3.7 Condutas Consideradas Crimes Virtuais

É interessante observar que os crimes virtuais podem envolver atividades criminais tradicionais, como furto, fraude, falsificação, dano, etc. e específicas, ou seja, o acesso não autorizado, a transmissão de vírus, material ofensivo divulgado na rede, etc. Com o aumento das redes de telecomunicações e o surgimento da Internet, globalizaram-se as atividades criminais.

Nesse aspecto:

> Há os que sustentam que uma subtração de um dado via Internet é um Furto como outro qualquer, diferenciando-se apenas quanto à maneira. Outros, por sua vez, sustentam que, conforme o caso pode ser que o bem, juridicamente protegido, seja justamente os sistemas de processamento ou a comunicação de dados, bens esses, imateriais e intangíveis. Por isso, é que não se deveria confundir como Furto, por exemplo, aquele que subtrai um dado, uma informação; naquele onde o bem é material; neste, o bem juridicamente protegido é imaterial (ROSA, 2002, p. 57).

Ainda podemos citar além dessa visão do furto, outra dúvida; agora no âmbito da sabotagem ou inutilização de dados ou programas que mesmo que:

> Alguns especialistas definam essa atitude como crime de dano, há quem entenda que a informação não pode se tornar objeto de dano, supressão ou falsidade documental porque não é nem documento nem coisa; para esses, o que vale, não são as representações digitais, mas o equipamento de informática. Utilizando-se do mesmo raciocínio, o Desembargador Dínio de Santis Garcia, do Tribunal de Justiça de São Paulo, lembrou [..] 'que programas de computador ou dados armazenados em computador são considerados, na maioria dos países, como bens imateriais, concluindo, portanto, que 'não se pode falar em furto quando alguém se apodera de tais bens' (ROSA, 2002, p. 57).

Observando essas visões, pode-se dizer que os crimes virtuais se dividem em dois tipos de situações típicas e distintas:

> Primeiramente, temos aqueles crimes que são praticados com a utilização dos sistemas de computadores (aí incluídas as redes de computadores, entre elas a Internet) com vista a um bem jurídico protegido, estranho ao próprio funcionamento do sistema de computação (uma fraude eletrônica que vise à transferência de fundos de uma conta para outra, por exemplo). O Segundo caso refere-se à prática de atos delituosos, por meio do uso dos sistemas de computadores contra os mesmos sistemas computacionais (caso, por exemplo, da utilização do computador com a finalidade de causar alguma conseqüência exclusivamente limitada aos sistemas e aos programas de computador em funcionamento) (ROHRMANN, 2005, p. 120).

Desta forma, "não se deve confundir um crime comum praticado pelo uso, ou contra o computador, de um crime de informática propriamente dito" (ROSA, 2002, p. 55). Há, pois que se distinguir entre os casos de crimes eletrônicos: "aqueles que utilizam o computador, mais como um meio para a prática do ato criminoso, daqueles que vislumbram o computador com a finalidade do ato criminoso" (ROHRMANN, 2005, p. 121).

2.3.8 Bem Jurídico a ser Protegido

O bem "é aquilo que pode satisfazer ás necessidades humanas" (JESUS, 2003, p. 4). Todo valor reconhecido pelo Direito torna-se um bem jurídico, ou seja, um bem protegido pelas normas que regulamentam e materializam o Direito.

Desta forma, a função do Direito Penal é a tutela jurídica, visando assim proteger os bens jurídicos, impondo sanções aos sujeitos que praticam condutas que afrontam estes bens. Com a aplicação destas sanções o Direito Penal reforça, na consciência da sociedade, o valor dos bens jurídicos, dando força às normas que os protegem.

Portanto, como ressalta Costa (1995, p. 2), os bens que deverão ser protegidos pelo Direito Penal em uma possível tipificação dos crimes virtuais são "os sistemas de computadores e de comunicação", ou seja, "a proteção dos seus componentes imateriais ou intangíveis, o software e dados, e os dados que ainda não contam com a mesma proteção do outro componente, o hardware".

2.3.9 Sujeito Ativo

Sujeito "ativo é quem pratica o fato descrito na norma penal incriminadora. Só o homem possui capacidade para delinqüir" (JESUS, 2003, p. 165).

O sujeito ativo nos crimes de informática são aqueles que "utilizam meios eletrônicos para consecução da atividade ilícita, desde que esta seja plenamente tipificada" (SOUTO, 2005, p. 1).

Os crimes virtuais podem ser cometidos por qualquer pessoa, ou seja, não são cometidos apenas por especialistas, visto a evolução dos meios de comunicação, o aumento de equipamentos, o crescimento da tecnologia e a acessibilidade aos sistemas disponíveis, qualquer pessoa pode ser um criminoso de informática. Para se cometer um crime virtual basta "apenas ter conhecimentos rudimentares para tanto; uma pessoa com o mínimo de conhecimento é potencialmente capaz de cometer crimes virtuais" (ROSA, 2002, p. 59). Contudo, "em regra, o delinqüente de informática é um operador de computadores e de sistemas, mas, como dito, não se pode generalizar" (ROSA, 2002, p. 59).

Rosa (2002, p. 59) ainda nos esclarece quais são a definições para alguns sujeitos ativos, sendo elas:

> Hacker: é aquele que tem conhecimentos profundos de sistemas operacionais e linguagens de programação. Conhece as falhas de segurança dos sistemas e está sempre à procura de novas falhas. Invade sistemas pelo prazer de provar a si mesmo que é capaz, sem alterar nada. Cracker: o mesmo que hacker", com a diferença de utilizar seu conhecimento para o "mal". Destruir e roubar são suas palavras de ordem. Assim, o cracker usa os seus conhecimentos para ganhar algo; rouba informações sigilosas para fins próprios e destrói sistemas para se exibir. Preaker: especializado em telefonia, atua na obtenção de ligações telefônicas gratuitas e instalação de escuta, facilitando o ataque á sistemas a partir de acesso exterior, tornando-se invisível ao rastreamento ou colocando a responsabilidade em terceiros. Lammer: é quem está tentando ser hacker, sai perguntando para todo mundo o que fazer para tornar-se um, com isso possui um pouco de conhecimento sobre invasão de sistemas e fica se exibindo na Internet por causa disso. Wannabe: é o principiante que já aprendeu a usar os programas prontos dos hackers. Aracker: são os chamados hackers de araque. Pensam que sabem tudo e acabam acessando revistas virtuais pornográficas nas madrugadas. Guru: o "supra-sumo" (mestre) dos hackers. É aquele que tem conhecimentos superiores e grande domínio sobre todos os tipos de sistemas.

Todavia, existem, porém, alguns delitos que normalmente são praticados:

> Pelos representantes legais das pessoas jurídicas relacionadas com a rede. Por exemplo: um provedor de acesso à Internet que, diante de uma ordem judicial, se recusa a informar o endereço de um usuário. Os representantes legais desta empresa podem responder por crime de desobediência (CASTRO, 2003, p. 12).

Em regra, como visto, qualquer pessoa pode cometer um crime virtual, por causa da ampla disponibilidade de equipamentos, tecnologias e informações. Desta forma, o sujeito ativo ou agente do crime virtual, não se enquadra somente no perfil de um especialista envolvido no mundo da informática.

2.3.10 Sujeito Passivo

O Sujeito passivo "é o titular do interesse cuja ofensa constitui a essência do crime" (JESUS, 2003, p. 171).

O sujeito também pode ser conceituado como sendo o:

> Ente sobre o qual recai a ação ou omissão realizada pelo Sujeito Ativo. É a pessoa ou entidade titular do bem jurídico, tutelado pelo legislador e sobre a qual recai a

> conduta. De qualquer modo, o Sujeito Passivo pode ser qualquer pessoa, Física ou Jurídica, de natureza Pública ou Privada (ROSA, 2002, p. 61).

O sujeito passivo no crime virtual é "o detentor de direitos violados, através de meios digitais, eletrônicos" (SOUTO, 2005, p. 1). Todavia, sendo o bem tutelado pelo direito penal, sempre haverá um sujeito passivo formal no crime praticado, "pelo simples fato de ter sido praticado, independentemente de seus efeitos. Esse sujeito passivo formal é o Estado, Titular do mandamento proibitivo" (JESUS, 2003, p. 171). Quaisquer uns desses sujeitos passivos podem propor a ação penal.

Desta forma, existem duas espécies de sujeito passivo: "a) Sujeito passivo constante, geral, genérico ou formal, que é o estado; b) Sujeito passivo eventual, particular, acidental ou material, que é o titular do interesse penal protegido" (JESUS, 2003, p. 172).

2.4 Teoria do Tipo

A primeira característica do crime "é ser um fato típico, descrito, como tal, numa lei penal. Um acontecimento da vida, que corresponde exatamente a um modelo de fato contido numa norma penal incriminadora, a um tipo" (TELES, 2004, p. 165).

Para que o operador do Direito possa chegar á conclusão de que determinada conduta da vida em sociedade seja um fato típico, "deve debruçar-se sobre ele e, analisando-o, decompô-lo em suas faces mais simples, para verificar, com certeza absoluta, se entre o fato e o tipo, existe relação de adequação exata, fiel, perfeita, completa, total e absoluta" (TELES, 2004, p. 165).

O primeiro passo para esta análise é entender o conceito de tipo, que é "o conjunto dos elementos descritivos do crime, contidos na lei penal" (JESUS, 2003, p. 269), ou seja, é a descrição abstrata dos elementos do fato ou suposto de fato, da vida prevista na norma penal incriminadora.

Na mesma corrente, Teles (2004, p. 204) demonstra que o tipo "é o modelo de conduta que a lei considera crime, proibida pela norma penal".

Desta forma, nota-se que o tipo é a descrição do fato (conduta) que deve ser evitada, visto que é proibida por lei sob ameaça de pena, visto que tem a função de indiciária da

ilicitude, visto que indica qual é a conduta por ele definida como proibida, ilícita, contrária ao ordenamento jurídico.

O tipo varia de acordo com o ato ilícito determinado como crime. Assim, tomando como exemplo o crime previsto no artigo 10 da Lei nº 9.296/96, in verbis: "Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei". Nota-se, de acordo com as considerações de Castro (2003), que o tipo é a interceptação de comunicação. Todavia, para que este seja punível é necessário que esteja complementada com o conjunto dos elementos da conduta punível definido pela lei, ou seja, a interceptação feita por via "[...] telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei".

O tipo, desta forma, é o ponto de partida da construção jurídico-penal, visto que:

> Cria o mandamento proibitivo (norma implícita da lei penal incriminadora); concretiza a antijuridicidade; assinala o injusto; limita o injusto; [...] marcando o início e o término da conduta e assinalando os seus momentos penalmente relevantes; ajusta a culpabilidade ao crime considerado; constitui uma garantia liberal, pois não há crime sem tipicidade (JESUS, 2003, p. 269).

Além deste, proteger o cidadão contra o arbítrio estatal, que não poderá exercer sua autoridade sobre a liberdade do indivíduo na ausência de uma prévia definição legal do crime, que se dá por meio dos tipos.

2.4.1 Elementos do Tipo

Os delitos estão impressos no tipo penal, que se refere às condutas humanas, sendo assim modelos abstratos de comportamento para os quais o legislador seleciona os comportamentos lesivos aos bens jurídicos e impondo uma sanção penal que proporciona um dano àquele que infringir a norma.

Cada tipo penal tem a função de proteger determinado bem jurídico. O legislador ao elaborar o tipo penal observa os comportamentos que a sociedade determina como danosos e atribui um valor. Esses valores são observados pelos elementos dos tipos que se subdividem em: objetivos, subjetivos e normativos.

2.4.2 Elemento Objetivo

Os elementos objetivos "são os que se referem à materialidade da infração penal, no que concerne à forma de execução, tempo, lugar etc. são também chamados descritivos" (JESUS, 2003, p. 272).

Na mesma corrente, Teles (2004, p. 26) diz que os elementos objetivos do tipo são os "que se referem à materialidade do fato, do acontecimento. São aqueles que se referem à forma em que o fato é executado, ao tempo, à ocasião, ao lugar, aos meios empregados, aos sujeitos, ao objeto".

Os elementos objetivos apresentam a materialidade do delito, ou seja, demonstram a fórmula pela qual é composta o tipo, sendo ela, de acordo com Jesus (2003, p. 272):

> De um verbo que expressa a conduta (como por exemplo: matar alguém), [...]o qual nem sempre indica uma conduta injusta (como ocorre com a difamação que é composta pelo verbo "imputar" (atribuir), que por si só, não corresponde a uma conduta antijurídica, porém, com o acréscimo de outros elementos, tais quais "fato ofensivo à reputação", passa a conduta a ser antijurídica.

Desta forma, observa-se que os elementos objetivos têm a natureza descritiva, visto que além do verbo que expressa a conduta, tem os elementos que são acrescidos para a conduta ser considerada ilícita. Portanto os elementos objetivos "são facilmente identificáveis, porquanto, não pertencem ao âmbito do psiquismo do homem, o agente do fato, mas são perceptíveis pelos sentidos, independentemente de qualquer valoração de natureza normativa".

2.4.3 Elemento Normativo

Os elementos normativos, nos esclarecimentos de Jesus (2003, p.272), "são certos componentes que o legislador insere na figura típica, que exige sua ocorrência, dentro de um campo de valoração do próprio campo da tipicidade".

De acordo com as orientações de Faustino (2008), observa-se que tais componentes não são vistos nos elementos objetivos, visto que estes são demonstrados através da valoração que deve ser alcançada pelo agente quando este estiver subordinado à norma, possuindo referências ao injusto, ou á termos extrajurídicos, cuja identificação é colhida no meio social.

Para a compreensão destes elementos normativos, nas orientações de Jesus (2003), é necessário observar a valoração sobre o injusto, que esses verbos (como por exemplo, "matar alguém") recebem, visto que implicam valores sociais acerca de determinada circunstância. Com isto, os elementos normativos se referem, em regra, à antijuridicidade.

Outro exemplo está no artigo 10 da lei 9.296/96, esta protege a inviolabilidade da correspondência, assim in verbis: "Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei".

O elemento normativo está na expressão "sem autorização", que significa que para esta ser interceptada deve haver uma autorização da lei ou do detentor do direito. Portanto, este só será fato típico se o sujeito devassar o conteúdo da correspondência injustamente, ou seja, contrariando a norma, fazendo sem autorização.

2.4.4 Elemento Subjetivo

Há alguns elementos do fato proibido, que "vivem no interior do psiquismo do sujeito, na esfera de seu pensamento, em sua motivação, em sua intenção, em seu intuito, em seu ânimo, em sua consciência, na cabeça do homem" (TELES, 2004, p. 207).

Esses elementos são os subjetivos, que tratam dos "estados e processos externos, suscetíveis de serem determinados, espacial e temporalmente, perceptíveis pelos sentidos, fixados na lei pelo legislador em forma descritiva, e que devem ser apreciados pelo juiz mediante simples atividade de conhecimento" (JESUS, 2003, p. 274).

Nas orientações de Jesus (2003), estes elementos estão relacionados com o fim das condutas, ou seja, observa o dolo do agente para o fim desejado, a sua intenção, o intuito que o encoraja na execução do fato.

Desta forma, nota-se que esses elementos subjetivos versam sobre o estado psicológico do agente, onde a conduta típica só se completa, se mediante á intenção descrita no tipo, por parte do agente.

2.4.5 Imputação

A Imputação significa "atribuir á alguém, a realização de uma conduta criadora de um risco relevante e juridicamente proibido e á produção de um resultado jurídico" (JESUS, 2003, p. 280).

Esta teoria liga a finalidade do agente ao resultado, analisando a conduta descrita na norma penal, como por exemplo, nos crimes virtuais que têm a característica de:

> Utilização do computador e seus acessórios para a prática do crime. Assim, a acusação deve expor o mecanismo empregado pelo agente em sua conduta delituosa. Se o crime foi praticado através da Internet, é importante salientar como foi feito, se por e-mail, ou site etc. Se tratar de um vírus, a acusação deve descrever como o vírus atingiu o computador, se por um disquete, CD ou e-mail (CASTRO, 2003, P. 81)

A partir da exposição do mecanismo deve-se analisar se esta "conduta criou ao bem jurídico, um risco juridicamente desaprovado e relevante; o perigo realizou-se no resultado jurídico; o alcance (âmbito) do tipo incriminador abrange o gênero de resultado jurídico produzido" (JESUS, 2003, p. 285).

2.4.6 Ilicitude

Portanto, para que seja feita uma possível tipificação deve-se analisar a ilicitude, ou seja, o porquê desta conduta não poder ser praticada na sociedade.

Observado assim a relevância de proteção aos bens imateriais, de forma a caracterizar a antijuricidade dessas condutas virtuais, que é o outro requisito para se determinar o crime. Nas palavras de Jesus (203, 155) "antijuridicidade é a relação de contrariedade entre o fato típico e o ordenamento jurídico. A conduta descrita em norma penal incriminadora será ilícita ou antijurídica quando não for expressamente declarada lícita".

A teoria da tipicidade determina através de classificação em normas penais proibitivas, ou negativas, incriminando os fatos de condutas que não estão sendo aceitos pela sociedade.

Para os transgressores destas relações, entre o fato típico e antijurídico (ilícito) que determina o crime, é imposta uma sanção penal, que é geralmente a pena privativa de liberdade.

Contudo, observa que em relação ao processo para se determinar ou verificar uma transgressão á norma penal, faz-se necessário a tipificação desta conduta. Portanto, a ausência desta norma, determina que, os atos praticados pelos *hackers* não podem ser determinados como crime, e estes não podem ser punidos, visto que, como nos ensina Jesus (2003, 55), "é proibido a analogia in malam partem", desta forma os Tribunais não podem se socorrer na analogia para o ajustamento da conduta atípica à norma penal, como é garantido no princípio da legalidade.

2.4.7 Uso da Analogia

A analogia é o primeiro recurso fornecido pela ciência jurídica para solucionar os problemas da integração da norma penal aos fatos que acontecem perante a sociedade. Desta forma, a analogia:

> Consiste em aplicar a hipótese não prevista em lei, à disposição relativa a um caso semelhante. [...] É, pois, forma de auto-integração da lei para suprir lacunas porventura existentes. Em seu emprego, o intérprete parte da própria lei para elaborar a regra concernente ao caso não previsto pela legislação (JESUS. 2003, 50).

Todavia, como observa Teles (2004, 145):

> O uso da analogia, no que diz respeito às normas penais incriminadoras é terminantemente proibido, pelo princípio da legalidade. [...] só a lei pode definir crimes e cominar penas. Se não há lei, considerando o fato, um crime, o juiz está impedido de, usando a analogia, aplicar uma pena à pessoa que praticou.

Hungria (2000, 21) ainda leciona que:

> A lei penal é, assim, um sistema fechado: ainda que se apresente omissa ou lacunosa, não pode ser suprida pelo arbítrio judicial, ou pela analogia, ou pelos 'princípios gerais de direito', ou pelo costume.

Devidamente observados, os crimes virtuais: analisando sua conceituação, características, derivações em puro, impuro e misto e a não aplicabilidade da analogia para resolver o problema de tais infrações, sobe pena de se cometer um constrangimento ilegal. Observar-se-á no próximo tópico, aplicabilidade dos princípios da legalidade ou reserva legal. Sem contudo, esgotar o assunto visto, que fugiria ao propósito do tema.

2.5 Crimes virtuais e os Princípios da Legalidade ou Reserva Legal no Direito Penal

Este tópico pretende traçar algumas considerações gerais sobre aplicabilidade dos princípios da legalidade ou reserva legal, entre outros. Contudo, sem objetivar o esgotamento do assunto, visto que fugiria o propósito deste tópico.

2.5.1 Conceito e Previsão Legal

A lei penal é fundamento dos delitos e das sanções penais. É a garantia dos que praticam condutas delituosas e pressuposto para aplicação da sanção penal.

Desta forma, ao se falar do princípio da legalidade, é necessário observar a Constituição Federal do Brasil de 1988, visto que é neste diploma legal que está previsto o conceito do Princípio da Legalidade ou Reserva Legal, mais precisamente no art. 5º, inciso XXXIX, *in verbis*: "não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal".

Delmanto (2002, p. 4) observando esta previsão do conceito da legalidade, afirma que "somente a lei, elaborada na forma que a Constituição permite, pode determinar o que é crime e indicar a pena cabível. Deve, portanto, ser lei federal, oriunda do Congresso Nacional".

O princípio da Legalidade é ratificado, de forma infraconstitucional, pelo legislador no art. 1º do Código Penal, *in verbis*: "não há crime sem lei que o defina; não há pena sem cominação legal".

Através destas previsões se determina que só a lei seja fonte imediata de Direito Penal, como demonstra Jesus (2003, 61):

> A lei penal é pressuposto das infrações das sanções. Mas não é só a garantia dos que não realizam condutas sancionadas; pois dela advêm pretensões para o Estado e para os próprios criminosos. Da lei, nasce a pretensão punitiva do Estado a reprimir os atos catalogados em seu texto, como delitos, com a pena cominada, e por isso, a lei é fonte e medida do direito de punir.

Nota-se que qualquer indivíduo só praticará uma conduta tida como crime, se a mesma, assim estiver expressamente tipificada como tal no ordenamento jurídico vigente.

2.5.2 O Princípio da Legalidade e Previsão do Princípio da Anterioridade da Lei

O princípio da legalidade, como deixa bem claro Jesus (2003, 61), "tem significado político", ou seja, visa ser uma forma de garantia, constitucionalmente, de proteção aos Direitos Humanos, pois protege o cidadão, ou garante a este, de forma fundamental, a proteção ao Direito da liberdade Civil, visto que ele diz que o cidadão só não pode fazer o que estiver previsto em uma lei. Portanto, fica clara a intenção do legislador, visto que, através deste princípio, ele compreende que somente a lei determina e fixa as condutas que serão consideradas criminosas. Portanto, é essa a garantia de liberdade de cada indivíduo como demonstra Bitencourt (2003, 2): "O princípio da legalidade ou da reserva legal constitui efetiva limitação ao poder punitivo estatal". Desta forma, "só a lei pode definir crimes e cominar penas" (TELES, 2004, 73), por isso que se dá o nome de Princípio da Legalidade ou da Reserva Legal.

Diante disto, observa-se que para se punir um cidadão, por prática de uma conduta é necessário que o fato esteja tipificado como sendo ilícito, todavia, por outro lado, não se pode aplicar uma lei posterior, para punir uma conduta que até então não era considerada ilícita, como ensina Jesus (2003,61), "é necessário que o tipo (conjunto de elementos descritivos do crime contido na lei penal) tenha sido definido, antes da prática delituosa". Desta forma, compreende que o legislador, ao retificar o princípio, no art. 1° do Código Penal, visa determinar, além da aplicabilidade do princípio da legalidade como forma obrigatória, por ser um princípio geral do direito, também a aplicabilidade do Princípio da anterioridade da lei, como nos ensina Jesus (2003, 65):

> Assim, o art. 1° do CP (código penal) contém dois princípios: 1°) Princípio da legalidade (ou reserva legal): não há crime sem lei que o defina; não há pena sem cominação legal; 2°) Princípio da anterioridade: não há crime sem lei "anterior" que o defina; não há pena sem "prévia" imposição legal. Para que haja crime é preciso que o fato que o constitui, seja cometido após a entrada em vigor da lei incriminadora que o define.

Tal previsão procura impedir que o legislador vote normas penais sancionadoras de coação direta, objetivando punir determinadas práticas que foram cometidas antes de se entender que tais, eram prejudiciais aos preceitos para garantir uma existência pacífica na sociedade.

2.5.3 Princípio da Legalidade e os Crimes Virtuais

De acordo com o princípio da legalidade, não pode ser considerado crime, conduta que não esteja prevista em lei e que a analogia que incrimine uma situação não prevista na lei é vedada.

Assim, a conduta que não esteja prevista na lei penal é lícita, como destaca Ramalho Terceiro (2002) dizendo que pela "exegese do princípio penal da legalidade, os crimes praticados atualmente pelos *hackers*, são isentos de punição, [...] visto a ausência de norma que tipifique tais crimes", pois são novas formas de condutas que ainda não têm previsão legal, como no exemplo de Pinheiro (2007. p. 250-251): "contaminação por vírus, sabotagem do sistema, destruição ou invasão de bancos de dados, cópia indevida de informações, etc."

Não havendo essas previsões, verifica-se nas palavras de Azeredo (2006), a necessidade de "medidas eficazes no combate ao crime cibernético. Não é mais possível que divergências hermenêuticas acerca da possível aplicabilidade das nossas normas jurídicas a esse tipo de conduta continuem a impedir a punição de condutas extremamente nocivas ao País". Visto que é imperioso notar que certas condutas que atentam contra bens informáticos ou informatizados, devem ser penalmente sancionadas ou criminalizadas, devido ao seu elevado potencial lesivo, numa sociedade global cada vez mais conectada e cada vez mais dependente de sistemas de comunicação via Internet.

È certo então, em face do princípio da legalidade, que todas as condutas praticadas em ambientes virtuais e que se pretende criminalizar estejam descritas em lei, pois, do contrário, há de se deparar com uma série de condutas atípicas, visto que os crimes virtuais têm modalidades distintas, dependendo do bem jurídico tutelado que se pretende proteger. Neste sentido, Pinheiro (2008) dá o exemplo do:

> Crime de Correspondência Eletrônica, que tem como bem jurídico tutelado o e-mail, ou seja, o que se quer proteger é a transmissão de dados e coibir o uso do e-mail para fins delituosos como o 'e-mail bombing' (envio de e-mails imensos ou vários e-mails), o "e-mail com vírus", o "spam". Este tipo penal protege também a questão da inviolabilidade das correspondências eletrônicas.

Desta forma, nota-se que o Direito Penal:

> Será imprescindível em alguns casos, por conta da natureza dos bens jurídicos em jogo. Pois, pela web e no ciberespaço circulam valores, informações sensíveis, dados confidenciais, elementos que são objeto de delitos ou que propiciam a prática de crimes de variadas espécies. Nas vias telemáticas, transitam nomes próprios, endereços e números de telefone, números de cartões de crédito, números de cédulas de identidade, informações bancárias, placas de veículos, fotografias, arquivos de voz, preferências sexuais e gostos pessoais, opiniões e idéias sensíveis, dados escolares, registros médicos e informes policiais, dados sobre o local de trabalho, os nomes dos amigos e familiares, o número do IP, o nome do provedor de acesso, a versão do navegador de Internet (browser), o tipo e versão do sistema operacional instalado no computador (ARAS, 2008, p.01).

A interceptação de tais informações e dados não autorizada devem ser, tipificadas, a fim de proteger esses bens que são relevantes à segurança das relações cibernéticas e à realização da personalidade humana no espaço eletrônico.

Todavia, notam-se no sistema normativo penal, normas arcaicas para regulamentação desses novos bens jurídicos, o que acarreta na falta de tipificação de vários atos que não poderiam ser previstos há várias décadas.

Há então, a necessidade da evolução das normas penais, visto que o Código Penal data de 1940 e esta deve ser feita, de acordo com o princípio da legalidade, através da tipificação dessas novas condutas, visando á proteção desses novos bens jurídicos, visto que, como já foi ressaltado, as pessoas que praticaram ilícitos no âmbito virtual, e esses não estando tipificados, apesar de toda sua reprovação, não poderão ser condenadas.

Desta forma, observar-se-á no próximo tópico quais as providências que já foram tomadas para uma possível tipificação, de algumas condutas no Código Penal.

2.6 Aplicabilidade da Lei Penal Brasileira nos crimes virtuais

Este tópico pretende observar quais as providências que já foram tomadas para a possível tipificação de algumas condutas no Código Penal. Contudo, sem objetivar ao esgotamento do assunto, mas sim, demonstrar alguns pontos relevantes.

2.6.1 Algumas Providências Que Já Foram Tomadas

Como demonstra Aras (2001, 2), alguns tipos penais, que descrevem crimes virtuais já existem, como por exemplo:

> a) o art. 153, §1°-A, do Código Penal, com a redação dada pela Lei Federal n. 9.983/2000, que tipifica o crime de divulgação de segredo: 'Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública', punindo-o com detenção de um a quatro anos, e multa;

> b) o art. 313-A, do Código Penal, introduzido pela Lei n. 9.983/2000, que tipificou o crime de inserção de dados falsos em sistema de informações, com a seguinte redação: 'Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano', punindo-o com pena de reclusão, de 2 (dois) a 12 (doze) anos, e multa.

Além desses tipos penais, existem também alguns projetos de leis que tratam da tipificação de condutas lesivas, como por exemplo:

a) O Projeto de Lei nº 76/2000 do Senador Renan Calheiros que define "crimes de informática" (CASTRO, 2003, 66).

b) O Projeto de Lei nº 4.833/98, do Deputado Paulo Paim que está:

> Definindo o crime de veiculação de informação que induzam ou incitem a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacionais, na rede Internet, ou em outras redes destinadas ao acesso público (CASTRO, 2003, 66).

Todavia, essas:

> Tipificações esparsas 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 aos dados de interesse da Administração Pública e do Estado democrático, bem como à privacidade "telemática" do indivíduo (ARAS, 2001, 2).

Na visão de Aras (2001, apud Ferreira, 2000, p. 208) essas tipificações:

> Longe de esgotarem o assunto, deixaram mais patente a necessidade do aperfeiçoamento de uma legislação relativa à informática para a prevenção e repressão de atos ilícitos específicos, não previstos ou não cabíveis nos limites da tipificação penal de uma legislação que já conta com mais de meio século de existência.

2.6.2 Projetos de Leis que Prevêem Novos Tipos Penais para os Crimes Virtuais

Alguns projetos de Lei já formam formulados com objetivo de tipificar algumas condutas no Código Penal, sendo o mais relevante deles o Projeto de Lei nº 84/99, que surge com a previsão de sete tipos penais para serem inclusos no Código Penal, que são o:

> Dano a dado ou programa de computador, acesso indevido ou não autorizado, alteração de senha ou mecanismo de acesso a programa de computador ou dados, obtenção indevida ou não autorizada de dados ou instrução de computador, violação de segredo armazenado em computador, criação, desenvolvimento ou inserção de dados ou programa de computador com fins nocivos e veiculação de pornografia através da rede de computadores. Excetuando-se o último tipo, todos os outros protegem os dados, informações e programas do computador, tratando-se de crimes de informática próprios, posto que só podem ser praticados com o auxílio da informática (CASTRO, 2003, 67).

Esse projeto do Senador Eduardo Azeredo passa a ser designado como Projeto de Lei nº 89/2003, após seu encaminhamento ao senado federal em 12 de novembro de 2003. Este passa a ter previsões de 13 novos crimes virtuais para serem enquadrados no Código Penal.

Este Projeto de Lei tem como principal visão com estas previsões, de resguardar os bens jurídicos que ainda não possuem uma proteção efetiva no Código Penal, tal como:

Acesso não autorizado á rede de computadores, dispositivo de comunicação ou sistema informatizado, *in ver*bis, Art. 285-A. Acessar, mediante violação de segurança, rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso: Pena - reclusão, de 1 (um) a 3 (três) anos, e multa. Parágrafo único. Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte (ARAS, 2001, 2).

Dentre essa inovação que foi trazida por este projeto ao Código Penal, pode-se destacar também, a qualificação do que vem a ser meio eletrônico e sistema informatizado, assim como os objetos que fazem parte de cada um desses contextos.

O projeto também visa:

> Combater, não apenas, as malas diretas eletrônicas que são abastecidas com a cópia não autorizada dos dados de pessoas e que são armazenadas em empresas ou órgãos públicos e privados, como também, a venda de CDs de computador com dados de terceiros para empresas de mala direta. Assim também estará se alcançando os indivíduos que coletam dados de terceiros e os fornecem indiscriminadamente às

> empresas que criam as malas diretas eletrônicas, conhecidas como spams. Com isso, os endereços eletrônicos e os e-mails, estarão protegidos e só poderão ser divulgados mediante autorização expressa de seu possuidor (MATTOS, 2007, p. 14).

Mattos (2007, apud ABRUSIO, 2004, p. 1) ainda ratifica e complementa dizendo que este projeto:

> Trará a previsão de condutas hoje, não presentes em lei, tais como a disseminação de vírus, a invasão de sistemas e outros delitos relacionados aos meios eletrônicos. Não há dúvidas de que essa alteração na legislação brasileira fará com que a sociedade em geral, por intermédio de profissionais especializados, amplie o número de processos relacionados aos crimes pela internet.

Martinelli (2004, p. 01), ao comentar este Projeto explica que "até o momento presente, só constituem crime, as invasões seguidas de danos. Pelo projeto de lei, a simples invasão já poderá incriminar o autor e passam a ser crimes a criação, o desenvolvimento e o armazenamento de vírus".

Colares (2004) enfatiza que "o Projeto de Lei nº 84/99, é o que melhor procura suprir a necessidade preeminente que urge em nossa sociedade, da tipificação penal de condutas que lesam dados ou bens de informática".

Com essas observações verifica-se a importância e a abrangência do referido projeto de lei para o Direito Penal, mostra-se um avanço no direito penal pátrio.

Perante o exposto, observa que já houve preocupação dos congressistas em tipificar as condutas lesivas que surgem no âmbito virtual. Desta forma é de se louvar essa posição tomada pelos legisladores. Contudo, ainda se nota uma morosidade em relação ao enquadramento dessas condutas no âmbito penal, visto a complexidade do assunto. Todavia, já se nota os projetos visando solucionar algumas dessas questões de enquadramento de condutas no Código Penal.

3 - DISCUSSÕES E RESULTADOS

O Direito está indissociavelmente ligado à vida em comunidade. Não se consegue conceber uma sociedade harmônica, sem admitir concomitantemente a incidência de normas, ainda que na forma de costumes ou de simples regras de convivência.

Desta forma, com o desenvolvimento das novas tecnologias da comunicação, e, principalmente, com o advento da Internet , novas questões surgem, demandando respostas do operador do Direito sobre a aplicação dessas normas, para proteção da harmonia social. Estas tecnologias, a cada dia que passa, apresentam novidades e melhorias nos processos e máquinas existentes, tendo crescimento incrivelmente rápido, e mal dando tempo para que a sociedade se acostume com a mesma, uma vez que um novo, já está sendo trabalhado e em pouco tempo disponível para a população.

Após a compilação, efetuada no capítulo anterior, apresenta-se algumas questões e análises, as quais só puderam ser feitas, após a referida compilação.

A primeira indagação está relacionada com a possibilidade do juiz, diante de um fato a ele relatado, como a proliferação de vírus pelos *crackers*, na ausência de norma penal incriminadora para este fato, aplicar a analogia?

Nota-se que para esta indagação há proibição do emprego da analogia no direito penal para punir um cidadão, visto que, em se tratando de direito penal não se aplica analogia para o mal da parte, porque não se pode criar conduta delitiva em face do princípio da legalidade, ou seja, uma conduta no âmbito penal só poderá ser considerada crime se assim a lei definir de forma como previsto no artigo 5º, inciso XXXIX da CF/88, *in verbis*: "não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal" (Conhecido comumente com o princípio da legalidade).

Desta forma, como Jesus, Teles, Rosa, Castro, Azevedo, Aras, Colares, entre outros, deixam claro, o Juiz não poderia aplicar norma penal semelhante para punir a conduta de proliferação de vírus pelos *crackers*, visto que esta não vem definida no âmbito penal como

crime e se o Juiz usar a analogia ele estaria criando uma conduta delitiva, se baseando em outra para punir tais indivíduos.

Observada essa proibição do uso da analogia para punir o responsável por um litígio no âmbito penal, surge então outra questão, a da tipificação dessas novas condutas, ou seja, desse litígio, ocasionado por essas novas condutas que se enquadram no âmbito puramente virtual. Visto que se observa uma necessidade de medidas que visem inibir tais atos que afrontam a sociedade, como por exemplo, no aspecto da integridade dos dados armazenados nos computadores e nos sistemas de comunicação. Todavia, como fazer essa tipificação?

Nota-se que para haver uma tipificação, a priori (na visão de Teles, Jesus, entre outros) deve-se determinar a conduta que deve ser punida e a partir dessa determinação transcrevê-la de forma abstrata, possibilitando assim, definir qual será a conduta lesiva e qual será o bem protegido. A partir dessa tipificação será possível determinar qual será a pena aplicada para inibir tal fato.

Um exemplo que poderia ser dado a respeito de como fazer essa tipificação e qual bem deve ser protegido está no Projeto de Lei nº 89/2003, ou seja, na previsão que este faz em respeito à Inserção ou difusão de código malicioso. Nessa previsão, o legislador transcreve de forma abstrata, a conduta de proliferação de vírus, com a frase de inserção ou difusão de código malicioso e a partir dessa transcrição ele determina os elementos que devem acontecer para se caracterizar essa infração, sendo eles *in verbis*: "Art. 163-A. Inserir ou difundir código malicioso em dispositivo de comunicação, rede de computadores, ou sistema informatizado". Determinando assim, o bem que deve ser protegido; sendo ele, a integridade dos dados que estiverem armazenados nos computadores ou dispositivos de comunicação. Nota-se ainda, que a previsão do artigo 163-A do Projeto de Lei nº 89/2003, traz implícitas as conseqüências educativas e disciplinares, ou seja: é educativo, pois visa demonstrar que tais condutas de inserção de dados não podem ser feitas, visto que prejudica interesses alheios, como por exemplo, a integridade dos dados que estão armazenados ou em constante processamento nas redes de computadores e dispositivos de comunicação; é disciplinador visto que, se o agente se enquadrar na conduta tipificada ele sofrerá uma sanção punitiva do Estado, de perda da liberdade, visando assim inibir novas condutas que possam acontecer no futuro.

Destaca-se ainda, a obrigatoriedade desses elementos transcritos na norma, acontecerem para a determinação do crime de inserção ou difusão de códigos maliciosos. Se

tais requisitos não forem constatados, a imputação de uma determinada conduta a um agente fica excluída em face de ausência de risco, juridicamente reprovável e relevante, ou seja, fica excluído se não tiver o elemento de conduta que determina o tipo penal reprovável pela sociedade.

Os doutrinadores deixam claro, que para acontecer um crime (mesmo sendo crime virtual) é necessário que a conduta que será praticada pelo agente esteja devidamente positivada, ou seja, descrita como crime na legislação penal. Visto que, se assim não o estiver, não se pode falar em crime.

Estes seriam alguns dos pontos que deveriam ser observados na questão em como fazer essa tipificação.

Apresentados os aspectos necessários à tipificação, cumpre ainda abordar qual bem deve ser protegido?

A doutrina (sendo alguns de seus representantes Costa, Pinheiro, Aras), diz que os bens que deverão ser protegidos pelo Direito Penal em uma possível tipificação dos crimes virtuais são os sistemas de computadores e de comunicação, ou seja, a proteção dos seus componentes imateriais ou intangíveis, o software e dados, e os dados que ainda não contam com a mesma proteção do outro componente, o hardware. Visto a relevância que estes têm na sociedade atual.

Em relação à questão de como ocorrem os crimes virtuais e quais seriam seus efeitos no mundo jurídico, há de se ressaltar que:

Em relação à primeira questão nota-se que na visão de Rohrmann, só ocorrem crimes virtuais se estes forem praticados com a utilização dos sistemas de computadores (ainda que seja apenas um computador simples e não conectado em redes de computadores). Exemplos, em tese, desses tipos de crime seriam os casos de acesso não-autorizado á sistemas de computadores; a obtenção de senhas de computador; a criação e a conseqüente disseminação dos chamados vírus (outros tipos assemelhados como os cavalos de tróia) de computadores. Todavia, na corrente majoritária, sendo alguns de seus representantes Rosa, Castro, Furlaneto Neto, os crimes virtuais ocorrem quando o sujeito visa especificamente ao sistema de

informática e ás ações se materializam, por exemplo, por atos de vandalismo contra a integridade do sistema ou pelo acesso desautorizado ao computador.

Mesmo havendo essa pequena variação nas doutrinas, observa-se que quando as ações do criminoso se dirigir contra os dados contidos no sistema, estas serão definidas como crime de informática puro, porque nesse último, o computador é essencial para a existência do delito, ou seja, os crimes só podem ser praticados através da informática; sem ela é impossível a execução e consumação da infração, como demonstram: Furlaneto Neto, Castro, Rosa, Pinheiro e Colare.

Em relação à segunda questão, nota-se que para haver um efeito no mundo jurídico é necessário que haja uma previsão legal sobre tais condutas, visto que, se esta não existir, as condutas dos *crackers* (como por exemplo, a proliferação de vírus) não serão ilícitas, desta forma, não poderão sofrer sanções inibidoras (em conformidade com o princípio da legalidade).

Ainda há que se vislumbrar algumas providências sobre a tipificação dessas novas condutas no âmbito penal.

Observa-se como exemplo, a previsão do art. 10 da Lei Federal n. 9.296/96, que considera crime, punível com reclusão de 2 a 4 anos e multa, os casos de interceptação de dados via informática ou telemática, *in verbis* "realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo de Justiça, sem autorização judicial ou com objetivos não autorizados em lei".

Outro exemplo seria o art. 153, §1°-A, do Código Penal, com a redação dada pela Lei Federal n. 9.983/2000, que tipifica o crime de divulgação de segredo, *in verbis*: "Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública", punindo-o com detenção de 1 a 4 anos, e multa.

Como também o art. 313-A, do Código Penal, introduzido pela Lei n. 9.983/2000, que tipificou o crime de inserção de dados falsos em sistema de informações, com a seguinte redação, in verbis: "Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de

dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano", punindo-o com pena de reclusão, de 2 (dois) a 12 (doze) anos, e multa".

Além desses, ainda há o projeto de Lei nº 89/2003 que prevê 13 novos crimes virtuais para serem enquadrados no Código Penal. Mesmo estando em tramitação ainda no congresso observa-se o interesse do legislador pelo mesmo.

Todavia, como demonstra Aras e Ferreira entre outros, essas tipificações não resolvem o problema da criminalidade na Internet, mas revela a preocupação do legislador infraconstitucional de proteger os bens informáticos e de assegurar, na esfera penal, a proteção aos dados de interesse da Administração Pública e do Estado democrático, bem como à privacidade na internet do indivíduo.

Ressalta-se ainda que tais previsões, longe de esgotarem o assunto, deixaram mais patente a necessidade do aperfeiçoamento de uma legislação relativa à informática para a prevenção e repressão de atos ilícitos específicos, não previstos ou não cabíveis nos limites da tipificação penal de uma legislação que já conta com mais de meio século de existência.

Entretanto, essa possível tipificação inibiria os crimes praticados a partir da entrada em vigência da lei que faria essas modificações no código penal, visto que, como a analogia, *in malam partem*, a lei não retroage para punir uma pessoa, de um fato que até então não era considerado como crime pela sociedade. Tal previsão se encontra no artigo 1º do Código Penal.

Contudo, nota-se que pode acontecer dos infratores seres menores de 18 anos, desta forma, inimputáveis, visto que o artigo 27 do Código Penal diz que, *in verbis*: "Os menores de 18 (dezoito) anos são penalmente inimputáveis, ficando sujeitos às normas estabelecidas na legislação especial".

Por isso, torna-se latente mais uma questão; se a tipificação no âmbito penal atingirá os propósitos do Estado.

Mattos e Abrusio acreditam que não, visto que, não atingiria os agentes que mais infringem ou prejudicam os direitos de terceiros que são os menores de idade. Desta forma, de acordo com esses doutrinadores, seria mais viável previsões no âmbito civil, visto que, sancionando os tutores desses menores a pagar uma indenização e reparar o dano, obrigá-los-

ia a terem maior preocupação na boa educação social de seus tutelados. Todavia, Rosa, Castro, Colares, Marinelli, observam a viabilidade, visto que, mesmo não atingindo diretamente estes infratores, a partir do momento que se comprovasse a autoria destes, nos crimes que viriam a serem tipificados, estes seriam remetidos às medidas sócio-educativas previstas no Estatuto da Criança e Adolescente, visto que o Código Penal e o ECA atuam, portanto, em sintonia, no sentido de excluir a pena, por razões de política criminal, o menor de dezoito anos autor de um delito. Todavia, cuida, de que a prática do ilícito penal, não reste livre de sanção, sendo a pena substituída por uma medida de cunho educativo.

Por isso, é necessária uma política forte para inibir os crimes virtuais que culmine em uma legislação, que determine sanções eficazes para os praticantes destas condutas, tanto no âmbito civil, objetivando a punição dos pais, que não educam seus filhos de forma adequada para integração social, quando esses forem agentes nos crimes virtuais, como também no âmbito penal, objetivando a punição mais severa dos agentes que cometerem os crimes virtuais. Desta forma, inibindo a ocorrência destes delitos. Visto que, essas condutas vêm sendo um dos maiores males deste novo século, atingindo os meios tecnológicos, que têm uma grande relevância atual para o desenvolvimento, não só social, como econômico, desta nova situação que convivemos.

Os trajetos percorridos neste estudo demonstram que as legislações que tratam sobre determinadas condutas que afetam o mundo virtual proporcionado pela Internet, no âmbito penal, ainda são singelas devido à ausência de tipificação legal de algumas condutas que se enquadram no âmbito de crimes virtuais puros.

Desta forma, agentes que utilizam a Internet como instrumentos, na prática de delitos, se encorajam cada vez mais, a continuar prejudicando interesses alheios, visto que, não sofrem nenhum tipo de sanção (nem no âmbito civil nem no penal).

Enquanto a legislação penal for omissa, não serão considerados crimes, tais como a proliferação de vírus. Por isso, estes agentes sempre serão agraciados com o benefício da impunidade, pois no direito penal não se pode atribuir uma pena, ou impor uma sanção, a uma conduta que o ordenamento penal não considere expressamente como criminosa.

De forma morosa verificam-se algumas providências por parte dos legisladores, com o surgimento de novos tipos legais, que, mesmo sendo singulares, surpreendem os operadores do direito em relação à iniciativa, visto a complexidade do assunto.

Ainda falta muito a analisar em relação à tipificação dos crimes virtuais, visto que é imprescindível uma adequada materialização de tais atos, na formulação de leis que qualifiquem, discriminem e tipifiquem as ações destes agentes, como criminosas, para que não aconteça nenhuma imposição legislativa injusta, ou seja, uma legislação que ao invés de inibir determinadas condutas, delimite determinados direitos ou liberdades que a Internet proporciona e que possam se perpetuar no tempo, não estando à mercê das novidades tecnológicas lançadas a cada momento.

CONSIDERAÇÕES FINAIS

O trajeto percorrido deste estudo objetivou analisar no âmbito penal a tipificação dos crimes virtuais e se tal resolveria os problemas decorrentes destas condutas ilícitas.

Neste sentido, demonstrou que a Internet está intimamente ligada ao direito penal, visto que, as condutas que até então estão tipificadas, se materializam de forma mais intensa no âmbito virtual, porque são impulsionadas pela evolução da Internet que é um dos principais meios de comunicação.

Juntamente com o aumento de ocorrências de fatos que já estavam tipificados, observou-se o surgimento de novas condutas, que até então não eram possíveis de serem realizadas sem o meio tecnológico, como por exemplo, a proliferação de vírus.

Desta forma, observa-se que estas novas condutas (crimes virtuais) afetam de forma direta, uma grande parcela da população, que na maioria dos casos, não sabe sequer, que a situação em que se encontra (como a contaminação por um vírus em seu computador) pode lhe prejudicar seriamente.

Por esse motivo, essas novas condutas ocasionaram o surgimento de novos estudos por parte dos juristas, objetivando determinar e conceituar sua classificação, com o intuito de ajudar os legisladores na tipificação dessas condutas, ocasionando assim, a concretização do combate a esses atos que prejudicam os interesses alheios.

Através destas classificações (como por exemplo, em crimes virtuais puros) fica possível se analisar, quais atos ainda não foram regulamentados e que merecem ser positivados, visto a relevância do bem que é prejudicado.

Por conseguinte o trabalho chama a atenção para o entendimento desta questão, com o objetivo de esclarecer as dúvidas e propiciar os elementos para que se tenha um panorama preciso da situação atual, observando as providências legislativas que já foram tomadas.

Entende-se, portanto, que tal tipificação seria viável para resolver os problemas decorrentes desses atos lesivos, se devidamente tipificados, para não proporcionar nenhuma

imposição injusta, tanto no âmbito penal com a retirada da liberdade, como no âmbito civil, quando se tratar de menor de idade, punindo assim seus tutores por não terem dado uma educação adequada aos seus tutelados.

REFERÊNCIAS

BITENCOURT, Cezar Roberto. **Código Penal Comentado**. Ed. Saraiva, 2002.

CARRARA, Francesco. **Programa do curso de direito criminal: parte geral**. São Paulo: Saraiva, 1956.

CASTRO, Carla Rodrigues Araújo de. **Crimes de informática e seus aspectos processuais**. 2ª ed. amp. atual. Rio de Janeiro: Lumen Juris, 2003.

DINIZ, Maria Helena. **Curso de direito civil brasileiro, v.** 1: teoria geral do direito civil. 21 ed. ver., aum. e atual. de acordo com o novo Código Civil (Lei n. 10.406, de 10-1-2002) e o Projeto de Lei n. 6.960/2002. São Paulo: Saraiva, 2004.

DELMANTO, Celso. **Código penal comentado**. Rio de Janeiro: Renovar, 2002.

FRAGOSO, Heleno Cláudio. **Lições de direito penal: parte geral**. 13. ed. Rio de Janeiro: Forense, 1991.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2002.

HUNGRIA, Nélson. **Comentários ao Código Penal**, v. I, t. I, 5ª ed., Forense.

JESUS, Damásio E. de. **Direito penal: parte geral**, v. 1, 27 ed. Ver. E atual. São Paulo: Saraiva, 2003.

LAKATOS, Eva Maria e MARCONI, Marina de Andrade. **Fundamentos de metodologia cientifica** – 6. ed. – São Paulo: Atlas 2005.

MINAYO, Maria Cecília de Souza. **Pesquisa social: teoria, método e criatividade**. 22 ed. Rio de Janeiro: Vozes, 2003.

NUCCI, Guilherme de Souza. **Manual de direito penal: parte geral: parte especial**. 2ª ed. Ver. atual. E ampl. São Paulo: Editora Revista dos Tribunais, 2006.

NUNES, Luiz Antonio Rizzatto. **Manual da monografia jurídica**. 3 ed., ver. E ampl. São Paulo: Saraiva, 2001.

PAESANI, Liliana Minardi. **Direito e Internet: Liberdade de informação, privacidade e responsabilidade civil**. São Paulo: Atlas, 2000.

PIMENTEL, Manoel Pedro. **O crime e a pena na atualidade**. São Paulo: Revista dos tribunais, 1983.

PINHEIRO, Patrícia Peck. **Direito Digital**. 2 ed. São Paulo: Saraiva, 2007.

ROCHA, Manuel Lopes. **Direito da Informática Legislação e De Ontologia** – Lisboa: ed. Cosmos, 1994.

ROESCH, Sylvia Maria Azevedo; BECKER, Grace Vieira; MELLO, Maria Ivone de. **Projeto de Estágio e de pesquisa em administração: Guia para Estágios, trabalhos de conclusão, dissertação e estudos de caso**. 2. ed. São Paulo: Atlas, 1999.

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

ROSA, Fabrízio. **Crimes de informática**. Campinas: Bookseller, 2002.

SHINTATI, Tomas M. **Curso de direito penal, parte geral**. Rio de Janeiro: Forense, 1999.

SARAIVA. **Vade Mecum**. Obra coletiva de autoria da Editora Saraiva com a colaboração de Antonio Luiz de Toledo Pinto, Márcia Cristina Vaz dos Santos Windt e Lívia Céspedes. São Paulo: Saraiva, 2006.

TELES, Ney Moura. **Direito penal: parte geral**. Arts. 1° a 120, volume 1. São Paulo: Atlas, 2004.

Sites:

ARAS, Vladimir. **Crimes de informática**. Disponível em: http://www.informatica-juridica.com/trabajos/artigo_crimesinformticos.asp. Acessado em 15 de outubro de 2008.

_____. **Crimes de informática**. Uma nova criminalidade. Jus Navigandi, Teresina, ano 5, n. 51, out. 2001. Disponível em:

<http://jus2.uol.com.br/doutrina/texto.asp?id=2250>. Acesso em: 23 set. 2008 in FERREIRA, Ivette Senie. A criminalidade informática, p. 208.

_____. **Crimes de informática**. Uma nova criminalidade. Jus Navigandi, Teresina, ano 5, n. 51, out. 2001. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=2250>. Acesso em: 23 de setembro de 2008.

AZEVEDO, Eduardo. **Projeto de Leis referente a crimes de informáticos**. Disponível em: http://www.forum-invasao.com.br/novo/viewtopic.php?f=30&t=8522409. Acessado em 15 de outubro de 2008.

BRASIL. **Lei nº 9.296, de 24 de julho de 1996. Direito à Privacidade. Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal**. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L9296.htm. Acessado em 5 de outubro de 2008.

BRASIL. **Lei nº 9.983 de 14 de julho de 2000. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal e dá outras providências**. Disponível em: http://www010.dataprev.gov.br/sislex/paginas/42/2000/9983.htm. Acessado em 15 de outubro de 2008.

BRASIL. **Projeto de Lei nº 4.833 de 1998. Crime de veiculação de informações que induzam ou incitem a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional, na rede Internet, ou em outras redes destinadas ao acesso público**. Disponível em: http://www.camara.gov.br/Internet/sileg/Prop_Detalhe.asp?id=21164. Acessado em: 11 de outubro de 2008.

BRASIL. **Projeto de Lei nº 76 de2000. Tipificação e punição dos crimes de informática**. Disponível em: http://www.decodificando.com.br/wp-content/uploads/2007/05/projeto_de_lei_76_2000.pdf. Acessado em: 10 de outubro de 2008.

BRASIL. **Projeto de lei nº 84 de 1999. Crimes cometidos na área de informática, suas penalidades e dá outras providências**. Disponível em: http://www.brdatanet.com.br/infocenter/biblioteca/pl8499.htm. Acessado em 11 de outubro de 2008.

BRASIL. Projeto **de lei nº 89 de 2003. Tipifica condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra dispositivos de comunicação ou sistemas informatizados e similares, e dá outras providências**. Disponível em: http://www.senado.gov.br/sf/atividade/Materia/getHTML.asp?t=13674. Acessado em: 11 de outubro de 2008.

COLARES, Rodrigo Guimarães. **Cybercrimes: os crimes na era da informática.** Disponível no site Jus Navigandi, in http://www1.jus.com.br/doutrina/texto.asp?id=3271. Acesso em 13 de setembro de 2008.

COSTA, Marco Aurélio Rodrigues da. **Crimes de Informática**. Disponível em: http://jus2.uol.com.br/doutrina/texto.asp?id=1826&p=3. Acessado em 5 de outubro de 2008.

FABRÍCIO, Rafael. Como a Internet começou? Você sabe?. Disponível em: http://sml-adoff.blogger.com.br/2004_02_01_archive.html. Acessado em 29 de setembro de 2008.

FAUSTINO, Allan de Freitas. **A existência de um elemento subjetivo especial no tipo subjetivo segundo a doutrina finalista**. Disponível em: http://www.tj.ro.gov.br/emeron/sapem/2003/AGOSTO/0108/ARTIGO/A04.htm. Acessado em 13 de outubro de 2008.

FURLANETO NETO, Mário e José Augusto Chaves Guimarães. **Crimes na internet: elementos para uma reflexão sobre a ética informacional.** R. CEJ, Brasília, n. 20, p. 67-73, jan./mar. 2003. Disponível em: http://www.cjf.jus.br/revista/numero20/artigo9.pdf. Acessado em 13 de setembro de 2008.

MATTOS, Alexandre Magalhães de. **A Lei 84-d e as alterações no Código Penal**. Disponível em: http://www.portalbaw.com.br/direito/lei_84d.pdf. Acessado em 15 de outubro de 2008.

MARTINELLI, João Paulo Orsini. **Aspectos relevantes da criminalidade na Internet**. Jus Navigandi, Teresina, ano 4, n. 46, out. 2000. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=1829>. Acesso em: 15 out. 2008.

MORIMOTO. Carlos E. **Significado das Siglas**. Disponível em: http://www.guiadohardware.net/artigos/significado-siglas/. Acessado em 29 de setembro de 2008.

PINHEIRO, Emeline Piva. **Crimes virtuais: uma análise da Criminalidade Informática e da Resposta Estatal**, 2006. Disponível em: http://www.buscalegis.ufsc.br/arquivos/Vi-%203.03.pdf. Acessado em 14 de junho de 2008.

PINHEIRO, Patrícia Peck. **Crimes Eletrônicos**. Disponível em: http://www.pppadvogados.com.br/paginas_unicas.asp?PaginaUnicaTipoID=17&intePaginaUnicaID=35. Acessado em 15 de outubro de 2008.

RAMALHO TERCEIRO, Cecílio da Fonseca Vieira. **O problema na tipificação penal dos crimes virtuais**. Jus Navigandi, Teresina, ano 6, n. 58, ago. 2002. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=3186>. Acesso em: 17 de setembro de 2008.

SOUTO, Erick Nilson Souto. **Impactos da Tecnologia Digital no Direito Penal**. Disponível em: http://www.souto.adv.br/np/tecnologiadigitaledireitopenal.pdf. Acessado em 30 de setembro de 2008.

WIKIPÉDIA, enciclopédia livre. **Spam**. Acessado em: http://pt.wikipedia.org/wiki/Spam. em 28 de setembro de 2008.

WIKIPÉDIA, enciclopédia livre. **Rand**. Disponível em: http://en.wikipedia.org/wiki/RAND_Corporation. Acessado em: 8 de setembro de 2008.