UNIVERSIDADE CATÓLICA DE GOIÁS
DEPARTAMENTO DE CIÊNCIAS JURÍDICAS
CURSO DE DIREITO

APLICAÇÃO DA LEI PENAL NA INTERNET

Goiânia
2002

APLICAÇÃO DA LEI PENAL NA INTERNET

MARCIO SOARES DA CUNHA

APLICAÇÃO DA LEI PENAL NA INTERNET

Monografia Jurídica apresentada para a conclusão do curso de Graduação em Direito, no Departamento de Ciências Jurídicas, da Universidade Católica de Goiás, sob orientação da Prof. **Isabel Valverde**.

Goiânia
2002

Banca Examinadora:

Nota para a monografia jurídica:

_____

Isabel Valverde Duarte
Professora Orientadora

_____

_____

Marilene S. B Viggiano

Para meus pais, minha eterna gratidão e carinho, por conduzirem minha vida nos caminhos da sabedoria e do conhecimento.

Aos professores Nivaldo dos Santos e Isabel Valverde Duarte pela indispensável ajuda sem a qual não seria possível a realização desse estudo.

SUMÁRIO

INTRODUÇÃO.....1
CAPÍTULO I – HISTÓRIA DA INTERNET
1.1 – História da “Internet”.....4
1.2 – Importância da “Internet”.....6
1.3 – As relações da “Internet”.....8
1.4 – O conceito de “Internet” pelo prisma jurídico.....10
CAPÍTULO II – SEGURANÇA NA INTERNET.....12
CAPÍTULO III – INTERNET E DIREITO
3.1 – Influência da “Internet” no direito.....17
3.2 – Direito penal de informática.....21
3.3 – O ciberespaço e o direito penal.....24
CAPÍTULO IV – SUJEITO ATIVO – O CRIMINOSO DA “WEB”
4.1 – Tipos de sujeito ativo.....27
4.2 – O perfil do sujeito ativo.....31
CAPÍTULO V – PERSECUÇÃO PENAL
5.1 – Obtenção de provas.....34
5.2 – Delegacia especializada em São Paulo..... 36
CAPÍTULO VI – CLASSIFICAÇÃO DOS CRIMES DE INFORMATICA
6.1 – Da classificação.....38
6.2 – Delitos de informática puro.....39
6.3 – Delitos de informática misto.....40
6.4 – Delitos de informática comum.....40
CAPÍTULO VII – O PROBLEMA DA AUTORIA.....42
CAPÍTULO VIII – O PROBLEMA DA COMPETÊNCIA..... 45
CAPÍTULO IX – APLICAÇÃO DA LEI PENAL NA INTERNET
9.1 – A lei penal brasileira e a “Internet”..... 49
9.2 – Bens tuteláveis.....55

9.3 – Legislação sobre crimes de informática.....62
CONSIDERAÇÕES FINAIS..... 65
REFERÊNCIAS BIBLIOGRÁFICAS..... 67

INTRODUÇÃO

O advento da “Internet” possibilitou a sociedade, adquirir, obter um vasto número de informações que vão desde assuntos escolares, pesquisas, culinária até tratados científicos. Como não poderia deixar de ser, questões jurídicas acabam por surgir em meio a essa revolução tecnológica.

Dados informam que a “Internet” possui hoje 159 milhões de pessoas em todo o mundo conectados à rede, até 2003 serão 510 milhões. Essas novas relações surgidas com o advento da “Internet” trouxe questões que já deveriam ter começado a ser pensadas e refletidas pelos operadores do direito.

A livre circulação de idéias e manifestação do pensamento surge como o principal valor a ser protegido pelas regras do Direito. Em seguida, ganham corpo as questões tradicionalmente ligadas à propriedade.

Propriedade e uso da informação, propriedade e direito autoral no uso de imagem e de criações intelectuais; marcas comerciais e outros signos distintivos.

Por fim, vem a tona as atividades com finalidade lucrativa para a forma digital, ou a circulação do bem intangíveis, transacionados na “Internet”. É o comércio eletrônico.

Além disso, a “Internet”, como se sabe, não possui proprietário e tem como característica principal a liberdade “ilimitada” de seus usuários.

A inexistência, assim, de linhas delimitadoras recai para a circulação da informação digital e o acesso à rede acarretam neo-problemas para a disciplina jurídica.

Entretanto uma coisa é certa: esse território existe e não pode ficar imune ao Direito.

Há duas posições diversas quanto a regulamentação da Rede Internacional:

a) A visão clássica: dizem que a anarquia prepondera na Internet, inviabilizando a aplicação de qualquer norma ou princípio do direito;

b) Visão Yankee: pretendem a aplicação da lei na Internet em qualquer das situações. Detalhe: da sua própria lei e jurisprudência.

Um exemplo dessa segunda corrente é o aviso contido no site da Promotoria do Estado de Minessota-EUA, onde se lê que qualquer pessoa que transmite informações ilegais (naquele Estado) via "Internet" - sabendo que tal informação será disseminada em Minessota - ficará sujeito a jurisdição nas cortes daquele Estado por violações das leis criminais e civis.

O alerta que se faz é que os abusos cometidos na "Internet" e que hoje são destacados na imprensa como novidade, em pouco tempo podem vir a se tornar rotina, e sendo assim, é de suma importância o preparo dos juristas para esse novo desafio.

Nosso propósito é desenvolver um estudo que possa informar as dimensões desse problema expondo as lacunas existentes em nossa legislação e demonstrar a necessidade da reunião de esforços no sentido de criar uma legislação que impeça a utilização indevida da "Internet".

Despertada a necessidade de criação de uma legislação para coordenar as relações humanas, impedindo a utilização indevida da “Internet” achamos por bem, diante da vasta problemática acerca desse assunto nos atermos a questão dos crimes cometidos via “Internet” e que não são punidos pela legislação penal. Inclui-se no nosso objetivo específico sucitar breves polêmicas sobre um dos neo-problemas que a informática trouxe para a humanidade e, conseqüentemente, para o Direito em sentido ampo: o aparecimento dos “hackers”, micreiros ou ciberladrões (invasões de coontas bancárias), o que faremos com o enfoque voltado para o Direito Positivo Brasileiro.

Para tanto, usaremos como método de trabalho o dedutivo, em que se parte de um conhecimento geral para um particular, onde o nosso tema, referindo-se ao enquadramento do direito na era digital, ficará circunscrita à sua relação com o Direito Penal.

A pesquisa será baseada em dados bibliográficos que enfoquem o tema de forma geral e de forma específica, principalmente, artigos em revistas especializadas, livros e jornais.

CAPÍTULO I

INTERNET

1.1. História da “Internet”

A “Internet” nasceu em 1969 nos Estados Unidos, durante a guerra fria através de projetos desenvolvidos pelo Departamento de Defesa dos Estados Unidos. A intenção era constituir uma rede de computadores para a comunicação dos principais centros militares de comando que pudessem sobreviver a um possível ataque nuclear e que atendesse a seguintes exigências: a) não fosse vulnerável a ataque militar, pois sendo Washington atacada, outros pontos deveriam estar funcionando; b) não existisse um centro de comando, pois no caso de um ataque o centro seria o primeiro lugar a ser atacado; e c) possuísse flexibilidade para adaptar-se as mais diversas situações possíveis.

Inicialmente, a rede era composta por 4 (quatro) supercomputadores de laboratórios de pesquisas, a qual foi denominada ARPAnet (ARPA: *Advanced Reserarch Projects Agency*).

A rede mundial de computadores, a “Internet”, passou a ser utilizada nos moldes conhecidos hoje a partir do ano de 1970, quando os pesquisadores começaram a utilizar o “correio eletrônico” para troca de informações.

No ano de 1980, a rede foi dividida em ARPAnet, de caráter civil, e a MILnet, com finalidades militares.

Posteriormente, já em 1985, criou-se a NSFnet que objetivava interligar todos os maiores centros americanos de pesquisa. Em 1986, a NSFnet e a ARPAnet fundiram-se, dando origem à “Internet”, que foi liberada para uso comercial em 1987, surgindo, então, os primeiros provedores de acesso comercial a partir de 1993.

As primeiras conexões do Brasil foram feitas em 1988, pela Fundação de Amparo a Pesquisa do Estado de São Paulo e pelo Laboratório Nacional de Computação Científica do Rio de Janeiro, criando-se uma Rede Nacional de Pesquisa em 1989 pelo Ministério da Ciência e Tecnologia.

A utilização comercial da “Internet” no Brasil ocorreu no ano de 1995, facultando-se as empresas denominadas “provedores de acesso” comercializar o acesso à rede mundial de computadores.

A “Internet” é uma gigantesca rede mundial de computadores em que não há um único lugar que a controla, sua organização se dá através dos administradores das redes que a compõe e dos próprios usuários.

Os computadores conectados a “Internet” estão ligados através de linhas comuns de telefone, linhas de comunicação privada, cabos submarinos, canais de satélite e diversos outros meios de telecomunicação.

Não há dúvidas que a sociedade mundial tem sofrido e vai sofrer grandes mudanças sociais e culturais radicais nos próximos anos em razão desse fenômeno denominado “Internet”, já podendo ser considerada como um dos mais revolucionários eventos da história da humanidade.

1.2. Importância da “internet”

Há quem diga que o século XX, foi o que mais propiciou as mais relevantes transformações na história da humanidade.

As formas de comunicações inventadas foram as mais diversas, note-se que há 500 anos surgiu a imprensa; há 160 anos, o telégrafo; há 120 anos, o telefone; há 95 anos, o rádio e há 50 anos, a televisão.

As mudanças no mundo se fazem de forma exageradamente rápida, a partir das quais surgem inovações das mais variadas, as quais permitem ao homem melhor conviver e melhor conhecer a si e a seus semelhantes.

Essa revolução da humanidade é relatada por Fábio Malina Losso[1] da seguinte forma:

> "de fato, da então revolucionária máquina de escrever evoluiu-se aos poderosos computadores; do rangedor carro de bois aos céleres aviões supersônicos; do engenhoso gramofone aos fidelíssimos sons dos CDs; do rádio de fugitivas ondas à eficiente televisão digital; do temível bisturi às cirugias a laser; dos documentos copiados em bem desempenhadas letras góticas ao fantástico fax; ao então inovador telégrafo sem fio à impressionante Internet; do mecanismo cartesiano ao pensamento sistêmico."

O fenômeno da informatização, o qual encontra-se consolidado em nossa sociedade, passou a ter ainda maior importância nos últimos anos, pois aumentou a quantidade de usuários da "Internet", corroborando a assertiva de que a rede mundial tornou-se um evento cada vez mais presente no nosso cotidiano.

Afirma-se que no Brasil existam cerca de 8 (oito) milhões de usuários, movimentando um mercado de US$ 1.5 bilhão em transações comerciais com perspectivas ainda maiores de negócios futuros.

---

[1] Fábio Malina Losso, *Internet, um desafio jurídico*. p. 2.

O crescimento da informação disponível só foi possível em razão de fatos ocorridos no campo do processamento eletrônico de dados e no de computadores. A expansão dessa informação tem se dado em razão da criação dessa enorme Rede Internacional que permite aos computadores compartilhar serviços e comunicar-se diretamente como se fosse parte de uma grande engrenagem. Esse instrumento de comunicação tem atingido proporções sem precedentes.

A utilização da "Internet" surgiu diante do mundo de informações, curiosidades e lazer a que o usuário tem acesso dos mais variados e inusitados pontos do planeta. Com isso têm-se verificado uma miscigenação de culturas, dados e descobertas numa velocidade espantosa.

A importância da rede é tamanha que a mídia sempre a tem em pauta, dando origem a revistas especializadas e encartes próprios nos jornais e revistas, demonstrando que é impossível ficar alheio a essa tecnologia, mormente diante da globalização.

O uso do computador é necessário em todos os segmentos econômicos e sociais e, por isso, o direito não poderia ficar ausente a essa nova realidade.

A Rede Mundial de Computadores tem servido de instrumento à educação, tornado o computador, na mão de excelentes professores capacitados, um excelente meio de ensino.

No Brasil, advogados e clientes com interesses em decisões do Supremo Tribunal Federal, poderão acessar "site" com fins a obter a íntegra do acórdão desejado; em São Paulo, a Policia Civil aceita ocorrências pelo

computador. Enfim, essa rede pode desburocratizar o serviço público e permitir ao cidadão exercer a plenitude de seus direitos.

As compras realizadas na "Internet" vão de CDs a carros, sendo a parte mais visível e colorida da era do comércio eletrônico.

Diante das várias possibilidades de utilização da “Internet”, pode-se dizer que ou você é *alguem@algum_lugar.com* ou você não é ninguém.

1.3. As relações da “Internet” com o direito.

As discussões a respeito dos efeitos da informática no direito são cada vez mais intensas. Dispõe Paulo de Sá Elias[2] que

> *“em 1997, no Rio de Janeiro, no I Congresso Nacional sobre a Internet, juristas de renome já discutiam a revisão de aspectos legais clássicos frente às novas situações jurídicas decorrentes da informática nos diversos campos do direito brasileiro. Discutiam na ocasião a respeito da necessidade de que fossem repensados antigos dogmas jurídicos no intuito de adaptá-los a uma nova realidade”*.

Os avanços tecnológicos atingem todas as áreas do direito, impulsionando a legislação frente a tecnologia que traz inevitáveis conseqüências ao mundo jurídico. É importante, também, adequar os casos concretos ao sistema legal existente e capaz de solucionar maioria dos conflitos decorrentes.

---

[2]Paulo de Sá Elias, *Alguns aspectos da informática e suas conseqüências no direito*. p.1.

Hodiernamente, é impossível ao operador do direito trabalhar sem "Internet", fax e CD-ROM.

Com o advento da informática, o dia-a-dia do profissional do Direito ficou mais fácil, permitindo-o redigir petições com recursos que torna desnecessário novamente redigi-las em razão de erros ou melhoramentos, além do vasto número de modelos de petições, pareceres ou sentenças e da grande facilidade de se realizar pesquisas jurisprudenciais tanto em CD-ROM ou por meio da "Internet".

Diz Paulo Gustavo Sampaio Andrade[3] que

> *"...a internet representa o coroamento de todo um processo de informatização que facilitou o acesso do jurista à informação."*

Assim, para saber o estado de um processo nos tribunais superiores basta acessar a "Internet", ressaltando-se que os "sites" do Supremo Tribunal Federal e do Superior Tribunal de Justiça dispõem de sistemas de pesquisas de jurisprudência com os respectivos acórdãos na íntegra, estando dentre os principais "sites" jurídicos.

O direito ganhou grande dinamismo com os artigos veiculados pela Rede Mundial, pois, em outras épocas, se fazia necessário esperar as edições mais recentes das doutrinas para o jurista atualizar-se, hoje em dia isso pode ser feito diariamente pela "Internet".

1.4. Conceito de Internet pelo prisma jurídico.

[3]Ibidem, mesma página.

A “Internet”, segundo Fábio Malina Losso[4], pode ser entendida como

> “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 diversas localidades”.

Vejamos a definição de “Internet” dada por David S. Willing[5]:

> “A internet é uma rede mundial, não regulamentada, de sistemas de computadores, conectados por comunicações de fia de alta velocidade e compartilhando um protocolo comum que lhes permite comunicar-se”.

A primeira definição permite extrair os seguintes elementos:

a. a formação de uma rede que não está restrita a apenas um país. As informações dentro da rede cruzam as fronteiras virtuais de vários países sem qualquer barreiras ou limitações, acionando-se os mais variados ordenamentos jurídicos;

b. vários são os objetivos da “Internet”, que vai do entretenimento até o uso comercial da informação;

c. o acesso do usuário pode ser feito por meio de um "notebook", computador pessoal ou terminais públicos situados em bibliotecas, todos conectados através de modem;

---

[4]Ibidem, p. 4.
[5]David S. Willing, *A internet e a Constituição dos Estados Unidos.* p. 30.

d. o “inernauta” pode praticar ato jurídico até pelo simples recebimento de um “e-mail” ou a visualização de uma página, uma vez que pode gerar conseqüências variadas.

Da última definição, o elemento mais importante é a não regulamentação. Esse elemento é que traz problemas sob o aspecto jurídico, pois a falta de regulamentação legal dificulta inibir os abusos que eventualmente ocorram na utilização da “Internet”.

CAPÍTULO II

SEGURANÇA NA INTERNET

A “Internet” conecta milhões de pessoas diretamente, nos mais diversos lugares e por variados motivos, bastando que elas possuam um microcomputador, um "modem" e uma linha telefônica.

Essa característica é um atrativo à sua utilização intensa, porém deve-se observar as ressalvas feitas por Arthur José Concerino[6], que dispõe:

> *“Em princípio, ao leigo, isto é ótimo, pois pode obter informações sobre um sem número de assuntos, de qualquer lugar do planeta, independente do horário. Associada a esta facilidade vem uma palavra de cinco letras que faz repensar tudo: RISCO!!!”*

A difusão do comércio eletrônico, foi um dos fatores de expansão da “Internet”, como já ressaltado, sendo a parte mais conhecida da rede, cujo desenvolvimento está submetido a barreiras significativas sob o aspecto da segurança.

Verifica-se que não são todos os *sites* que proporcionam recursos de segurança, de notório conhecimento, como se tem divulgado na mídia, que o sistema de compras na “Internet” não são totalmente seguros, trazendo desconfiança do usuário nos dispositivos de segurança que são passíveis de serem burlados.

Deve-se observar, em relação a essa insegurança, dois obstáculos ao comércio eletrônico: a falta de confiança do público no processo das transações “on line”, além do lapso temporal existente entre a disponibilização de uma nova tecnologia e a capacidade da base instalada para suportar essas mudanças.

---

[6]José Arthur Concerino. *Internet e segurança são compatíveis ?*. p. 130

Com a grande expansão da Rede Mundial, a "Internet", e consequentemente com a transmissão de documentos e troca de mensagens por meio do computador, se faz necessário criar sistemas que tornem seguras as informações transmitidas, bem como sua autenticidade.

A falta de segurança na "Internet" demonstra sua vulnerabilidade, facilitando o acesso de "invasores" e dificultando sua identificação.

Tais "invasões" podem se dar contra um usuário comum ou uma empresa, podendo ter conseqüências mais danosas a essa última, como coloca Elias Barenboin[7], a respeito do assunto:

> *"..a menor é a perda de tempo recuperando a situação anterior, uma queda na produtividade, uma perda significante de dinheiro, horas de trabalho, devastação da credibilidade ou oportunidade de marketing um negócio não habilitado para competir..."*

Na área jurídica o maior problema esta relacionado com a aceitação de um documento, petição ou certidão, enviado por computador ou fax, além da verificação da assinatura.

A introdução da criptografia permitiu uma segurança relativa na utilização da *assinatura digital.* É através dela que se tem permitido assinar o documento, isto é transmiti-lo com uma assinatura codificada e garantir sua autenticidade, sem possibilidade de adulteração ou falsificação, contudo, ainda não é possível se conseguir 100% (cem por cento) de segurança nos dados

[7]Elias Barenboin, *Segurança na internet*. p. 3

transmitidos pela rede, mesmo porque, como já foi dito, as formas de tecnologia se diversificam e evoluem a todo tempo.

Os dados que demonstram o crescimento, no Brasil, das ameaças e prejuízos decorrentes da falta de segurança na infra-estrutura de Tecnologia da Informação.

Uma pesquisa nacional sobre segurança da informação realizada pela Módulo[8], empresa de segurança para redes, "Internet" e intranet, demonstra os níveis de insegurança na rede:

> *"...30% das empresas brasileiras sofreram algum tipo de invasão nos últimos dois anos, sendo que 50% dos ataques registrados aconteceram há menos de 6 meses. E o que é mais preocupante: 39% dos entrevistados não sabem sequer se foram invadidos...81% das empresas invadidas, não foram possível quantificar o prejuízo com os problemas de insegurança ocorridos"*

A insegurança não se limita aos chamados "hackers", indivíduos que invadem computadores por meio da "Internet", utilizando-se indevidamente de senhas, furtando dados relevantes, fazendo transferências bancárias, causando prejuízos de toda a ordem ao cidadão.

Dados da referida pesquisa nacional sobre segurança da informação revelam que os principais inimigos são os próprios funcionários das empresas, segundo os dados da referida pesquisa, que demonstram que 35% (trinta e cinco por cento) dos problemas ocorridos com segurança foram causados

[8]PESQUISA NACIONAL SOBRE SEGURANÇA. Fev. 2000. Realizada pela MÓDULO, empresa de segurança para redes, internet e intranet. p. 3

propositalmente pelos seus funcionários e apenas 17% (dezessete por cento) por "hackers".

Os riscos de invasões são maiores quando o acesso à "Internet" e feito por meio de um "modem" e sem medidas de proteção e controle.

Os especialistas chamam a atenção para a importância da elaboração de uma política de segurança corporativa, formalizando procedimentos para o manuseio adequado das informações estratégicas.

É de se ponderar que as empresas não destinam, ainda, investimentos necessários à questão da segurança de seus sistemas, como se verifica da pesquisa realizada pela Módulo[9], que dispõe da seguinte forma sobre esse item:

> *"...o orçamento de segurança para 44% das empresas ainda não é calculado isolado da verba de informática. Mesmo assim, 74% responderam que esse orçamento aumentou para 1999. Pode-se verificar que o maior investimento realizado por 12% das empresas - que estão aplicando um milhão de reais por ano."*

Tal insegurança traz como conseqüência uma grande ocorrência de ilícitos penais, que passam a ser perpetrados por meio da "Internet".

Vejamos o que diz a advogada Debora Fisch Nigri[10], sobre o assunto:

> *"O campo de proliferação de crimes informáticos é extremamente fértil. É possível transferir-se grandes quantidades de dados pessoais para qualquer sistema que esteja conectado na rede. A transferência*

[9] Ibidem, p. 5.
[10] Debora Fisch Nigri, *Crimes e a segurança na internet*. p. 34.

pode ser interceptada a qualquer momento e os dados podem ser alterados ou suprimidos, gerando muita insegurança."

Os crimes na "Internet" não se circunscrevem aos delitos de ordem econômica, mas englobam a criação e inserção de vírus, criação de sites de pedofilia, pornografia infantil, "sites" incitando racismo, violações de direitos autorais, usurpação de nomes de domínio.

Portanto, esbarramos no maior problema da "Internet" que é a segurança, a qual não poderá ser resolvido apenas com o desenvolvimento de tecnologia, com sistemas seguros, mas com a ajuda do Direito.

CAPÍTULO III

INTERNET E DIREITO

3.1. Influência da Internet no Direito

As variadas possibilidades que a tecnologia nos propicia vem acompanhada de problemas bastante novos e desafiadores da propensão humana de conviver harmoniosamente em sociedade para garantir a sobrevivência. Nesse ponto, surge o Direito com sua vocação eminente para sempre regular a vida humana, torna-la melhor e mais segura através da imposição de regras generalizadas, o melhor remédio para as lides, para as tensões sociais de qualquer natureza.

O desenvolvimento da sociedade industrial em direção a uma sociedade pós-industrial informatizada, o crescente valor das novas técnicas de informatização e de comunicações para a economia, a cultura e a política, juntamente com a importância dos computadores no âmbito dos assuntos sociais, nos traz a necessidade de analisar a informática sob a ótica jurídica.

Com os computadores veio um ponderável elenco de problemas, muitas vezes questões complexas e absurdamente capazes de sucederem de modo lépido, rápido, deixando sempre para trás os ordenamentos jurídicos internos dos países integrantes da Comunidade Internacional e, até mesmo, seus tratados e convenções.

O Direito é o meio de controle social de maior eficácia face a coercibilidade por ele imposta, sendo necessário à organização da sociedade seja manifestado por meio de costumes ou normas.

Esse meio é que dá segurança às relações interpessoais e interinstitucionais quando harmonizado com outros meios de estabilização da vida em sociedade.

O desenvolvimento das novas tecnologias da comunicação, e, principalmente, com o advento da Internet, novas questões surgem, demandando respostas principalmente do operador do Direito, como adverte Vladimir Aras[11]:

> *"E, em face da velocidade das inovações da técnica que vislumbramos no mundo contemporâneo, tais respostas devem ser imediatas, sob pena de o 'tradicional' hiato existente entre o Direito e a realidade social vir a se tornar um enorme fosso, intransponível para os ordenamentos jurídicos nacionais e invencível para os profissionais que não se adequarem".*

Nesse contexto, se faz necessário, além da aplicação da lei penal vigente, a criação de uma legislação penal para a proteção de bens jurídicos informáticos e de outros que possam ser ofendidos por meio de computadores e, mais especificamente, da "Internet".

Para tanto, é necessário considerar como pressupostos alguns dispositivos constitucionais:

a) o artigo 5°, inciso II, segundo o qual "ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei";

b) o artigo 5°, inciso X, que considera "invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito a indenização pelo dano material ou moral decorrente de sua violação";

c) o inciso XII do mesmo cânone, que tem por "inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações

[11] Vladmir Aras. *Crimes de Informática; uma nova criminalidade*. p. 3

telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal";

d) o dogma de que "A lei não excluirá da apreciação do Poder Judiciário lesão ou ameaça a direito", na forma do artigo 5°, inciso XXV da Constituição Federal;

e) a garantia segundo a qual "não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal"(inciso XXXIX, do artigo 5°).

Tendo o Estado feito a opção pela legalidade, logo decai a premissa de que a "Internet", devido às suas características, não pudesse ser regulamentada pelo Estado, perdurando a liberdade absoluta nesse ambiente.

Havendo lesão ou ameaça a liberdades individuais ou ao interesse público, deve o Estado autuar para coibir práticas violadoras desse regime de proteção, inclusive as realizadas por meio do computador ou da "Internet", como ressalva o citado autor[12]:

> *"Do mesmo modo que aproxima as pessoas e auxilia a disseminação da informação, a Internet permite a prática de delitos à distância no anonimato, com um poder de lesividade muito mais expressivo que a criminalidade convencional nalguns casos."*

Obvio é que a "Internet" não foi criada para facilitar o cometimento de crimes, porém é possível se cometer crimes através dela. Esses crimes, devido a proporção que tem tomado, estão sendo divulgados por toda empresa, seja ela

[12] Ibidem, p. 6

escrita ou falada. As manchetes noticiam a entrada indevida e não permitida aos "sites" dos mais diversos, dentre eles o do Supremo Tribunal Federal, do DETRAN, da NASA, além da invasão de sistemas bancários.

Dessa forma, impõe-se ao Estado estruturar-se materialmente, com mecanismos preventivos e repressivos às práticas ilícitas, civil ou criminal, mormente os órgãos da persecução criminal (a Polícia Judiciária e o Ministério Público).

Deve se destacar que no Brasil não há uma cultura de informática jurídica e de Direito da informática no País.

O combate a criminalidade ainda não é efetivo face as dificuldades prosaicas do Estado, ainda inapto para acompanhar essas transformações cibernéticas e as novas formas de criminalidade.

Com efeito, impõe-se ao operador do direito o melhor conhecimento desses dissídios trazidos pelo uso da "Internet".

3.2. Direito Penal de Informática

O amoldamento do Direito à Informática, muito antes de individualizar-se no Direito Penal passa, necessariamente, por uma ótica mais ampla, mais geral. Essa ótica deve-se ao surgimento de limites essenciais que impulsionam a um novo ramo do direito, que, a princípio, denomina-se Direito da Informática.

Diante desses fatos, chama-se a atenção para intervenção do Direito Penal, conforme coloca o referido autor[13]:

> *"Malgrado se reconheça o legítimo desejo de reduzir a atuação do Direito Penal em face das relações humanas, de acordo com a diretriz da intervenção mínima, é imperioso notar que certas condutas que atentam contra bens informáticos ou informatizados, ou em que o agente se vale do computador para alcançar outros fins ilícitos, devem ser penalmente sancionadas ou criminalizadas, devido ao seu elevado potencial de lesividade e ao seu patente desvalor numa sociedade global cada vez mais conectada e cada vez mais dependente de sistemas on-line".*

A principal "interface" da "Internet", a *WWW - Word Wide Web*, surgiu na década de 1990, em contraposição ao Código Penal que é de 7 de dezembro de 1940, porém tal fato não impede a aplicação do Código Penal.

Em verdade, será necessário adequar institutos, rever conceitos, especificar novos tipos, interpretar adequadamente os elementos dos tipos existentes e definir, eficazmente, regras de competência e de cooperação jurisdicional em matéria penal, a fim de permitir o combate à criminalidade de informática.

Esse novo ramo do Direito, o Direito Penal de Informática, é definido pelo por Vladimir Aras[14], da seguinte forma:

> *"...ramo do direito público, voltado para a proteção de bens jurídicos computacionais inseridos em bancos de dados, em redes de computadores, ou em máquinas isoladas, incluindo a tutela penal do*

[13] Ibidem, p. 8
[14] Ibidem, p. 11.

> *software, da liberdade individual, da ordem econômica, do patrimônio, do direito de autor, da propriedade industrial, etc. Vale dizer: tanto merecem proteção do Direito Penal da Informática o computador em si, com seus periféricos, dados, registros, programas e informações, quanto outros bens jurídicos, já protegidos noutros termos, mas que possam também, ser atingidos, ameaçados ou lesados por meio do computador."*

Em relação ao desenvolvimento desse ramo, Marco Aurélio Rodrigues da Costa[15] faz a seguinte recomendação:

> *"...deve ser desenvolvido com extrema rapidez e segurança de modo a serem sistematizadas normas que atingem os crimes empiricamente tipificados, que são cometidos com o emprego de computadores e sistemas relacionados com o conceito de provas, principalmente provas técnicas".*

O legislador deverá, diante dos elementos indicadores de crimes de informática, redigir o Direito Criminal Brasileiro de Informática.

Trata-se de uma nova fase do Direito Penal, como preleciona Marco Aurélio Rodrigues da Costa[16]:

> *"...é seguro afirmar que estamos vivendo a primeira fase de um novo direito, o Direito Criminal de Informática. Devendo, pois, o legislador pátrio extirpar este, ainda que efervescentes na cabeça e nos rabiscos de nossos doutrinadores, e transformá-lo em um direito - com direito à maioridade - portanto, codificando-o em lei"*

---

[15] Marco Aurélio Rodrigues Costa. *Direito e Internet*. p. 9.
[16] Ibidem, p. 9.

Com está visão genérica, o Direito Criminal da Informática deve ser desenvolvido com extrema rapidez e segurança, de modo a serem sistematizadas normas que atinjam os crimes empiricamente tipificados, que são cometidos com o emprego de computadores e sistemas, desenvolvendo proteção e privacidade, a instrumentalização da produção de provas, inclusive reciclando os conceitos de provas, principalmente aquelas provas técnicas. Tais iniciais parâmetros, ao nosso entender, são importantes para que se amplie a própria incipiente ciência do Direito Criminal da Informática, com a abertura da exata compreensão do que representa o computador na vida de cada um, e, como tal, os riscos do avanço dos crimes de informática.

Os delitos computacionais têm sido designado pelos doutrinadores por várias formas, não havendo, ainda, consenso sobre seu "nomem juris" genérico.

Dentre essas designações, as mais comumente utilizadas têm sido as de crimes informáticos ou crimes de informática, sendo que essas expressões “crimes telemáticos” ou “cibercrimes” são mais apropriadas para identificar infrações que atinjam redes de computadores ou a própria Internet ou que sejam praticados por essas vias.

Como quer que seja, a criminalidade informática, fenômeno surgido no final do século XX, designa todas as formas de condutas ilegais realizadas mediante a utilização de um computador, conectado ou não a uma rede, que vão desde a manipulação de caixas bancários à pirataria de programas de computador, passando por abusos nos sistemas de comunicação.

Com relação a essas condutas, diz Ivette Sensine Ferreira[17]:

[17] Ivete Senise Ferreira, *Criminalidade de Informática*, p.214.

> *"...revelam uma vulnerabilidade que os criadores desses processos não haviam previsto e que careciam de uma proteção imediata, não somente através de novas estratégias de segurança no seu emprego, mas também de novas formas de controle e incriminação das condutas lesivas".*

3.3 - O ciberespaço e o Direito Penal

As proposições de que a Internet é um espaço sem leis ou terra de ninguém, em que haveria liberdade absoluta e onde não seria possível fazer atuar o Direito Penal ou qualquer outra norma jurídica.

Estabelecido que a incidência do Direito é uma necessidade inafastável para a harmonização das relações jurídicas espaciais, é preciso rebater outra falsa idéia a respeito da "Internet": a de que seriam necessárias muitas e novas leis para a proteção dos bens jurídicos a serem tutelados pelo Direito Penal da Internet.

Destarte, a legislação aplicável aos conflitos cibernéticos será a já vigente, com algumas adequações na esfera infraconstitucional. Como norma-base, teremos a Constituição Federal, servindo as demais leis para a proteção dos bens jurídicos atingidos por meio do computador, sendo plenamente aplicáveis o Código Civil, o Código de Defesa do Consumidor, a Lei dos Direitos Autorais, a Lei do Software e o próprio Código Penal.

A atuação do 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, número 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 informações policiais, dados sobre o local de trabalho, os nomes dos amigos e familiares.

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

É impossível se conceber um espaço como a "Internet" de forma a lhe deferir liberdade absoluta com afastamento total do estado, como defendem alguns.

O Promotor de Justiça do Ministério Público do Estado da Bahia, Wladirmir Aras[18], dá seguinte solução ao problema:

> *"O ideal seria haver uma constituição para a Internet, não no sentido de documento jurídico escrito - como entenderam alguns publicistas - mas com o significado de arquitetura ou moldura , que estruture, comporte, coordene e harmonize os poderes jurídicos e sociais, a fim de proteger os valores fundamentais da sociedade e da cibercultura"*

Por fim, esse estudo quer chamar a atenção para o conflito de interesses emergente pelo uso dos computadores, clamando-se por uma tomada de posição do Direito, solicitando-se, assim, a intervenção do Direito Penal.

---

[18] Vladmir Aras. *Crimes de Informática; uma nova criminalidade*. p. 18.

CAPÍTULO IV

SUJEITO ATIVO – O CRIMINOSO DA “WEB”

4.1 – Tipos de sujeitos ativos

Como já foi dito anteriormente, ao mesmo tempo em que surge toda esta explosão de serviços e oportunidade, além da figura do indivíduo que usa o computador para atos ilegais.

Trata-se da figura do criminoso digital, cujo perfil é diverso daqueles que se utilizam arma para intimidar ou assaltar pessoas, por ser alguém jovem, muito inteligente, que senta confortavelmente atrás de uma máquina, e com alguma paciência e uns toques chaves no teclado de um computador pode dar desfalques milionários em bancos, surrupiar cartões de crédito de cidadãos inocentes ou até deixar um estado inteiro sem energia elétrica.

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

No jargão dos “iniciados”, um jovem que recém ganhou um computador e já quer invadir o Pentágono com programinhas simples, obtidos na "Internet" (chamados receitas de bolo), é chamado de “Lamer” e além de ser inofensivo (se tiver sorte é capaz de não destruir seu computador na primeira tentativa), é desprezado por quem entende de informática.

Há, também, os famosos “Hackers” que na verdade são jovens que tem conhecimentos reais de programação e de sistemas operacionais de computadores, conhece as falhas do sistema de segurança e, por diversão (como uma espécie de desafio), procura conhecer novas falhas e usa técnicas próprias de invasão, desprezando as “receitas de bolo”, além de não gostarem de ser

confundidos com criminosos, pois limitam-se a invadir sistemas pelo prazer de ultrapassar as barreiras lhe impostas, sem todavia, destruírem os mesmos ou se utilizarem das informações pessoais para fins pessoais ou de terceiros.

Vejamos o seguinte texto denominado Manifesto Hacker, parte do artigo científico de Marcelo Marzochi[19], em que um "Hacker" se autodescreve:

> *"Eu sou um Hacker, entre para o meu mundo:*
> *Meu mundo é aquele que começa na escola...Eu sou mais esperto que os outros...esta besteira que nos ensinam me aborrece...Cacete trapaceiro. Eles todos são iguais. Eu estou no ginásio. Eu ouvi os professores explicarem pela qüinquagésima vez como reduzir uma fração. Eu entendo como. 'Não. Sra. Smith, eu não mostrei meu trabalho. Eu fiz na cabeça...'Cacete criança. Tudo o que ele faz é jogar jogos. Eles são todos iguais. E então aquilo acontece...uma porta aberta para o mundo... surfando pela linha telefônica como adrenalina nas veias, um comando enviado, um refugo da incompetência de procurar no dia-a-dia...*
> *Uma BBS é achatada. É isto...é aquilo que eu pertenço. Eu conheço o mundo aqui...Mesmo que eu nunca conheci eles, nunca conversei e até numa os vi...Eu conheço todos vocês. Cacete criança...*
> *Nós fomos alimentados com comida de bebê na escola queríamos bifes...Os pedaços de carne que você deixou escapar pré-cozidos e sem gosto. Não formos dominados por sádicos, ou ignorados por patéticos. Os poucos que tiveram algo a nos ensinar quando éramos crianças, acharam-nos dispostos a tudo, mas estes ão como lagos d'água no deserto. Este é o nosso mundo agora..*
> *O mundo do elétron e da mudança, a beleza do modem. Nós fazemos uso de um serviço já existente sem pagar por aquilo que seria bem barato se não fosse usado por gulosos atrás de lucros e vocês chama criminosos. Nós explorávamos..e vocês nos chamam de criminosos.*

[19] Marcelo Marzochi, *Manifesto Hacker*, p. 1

> *Nós procuramos por conhecimento...e vocês nos chamam de criminosos. Vocês constróem bombas atômicas, vocês começam as guerras, assassinam, trapaceiam, mentem para nós e tentam fazem que acreditamos que é para nosso próprio bem, sim, nós somos os criminosos.*
> *Sim, eu sou um criminoso. Meu crime é o da curiosidade. Meu crime é o de julgar pessoas pelo o que elas pensam, não como elas se parecem. Meu crime é desafiar você, algo que vocês nunca me farão esquecer.*
> *Eu sou um Hacker e este é o meu manifesto. Vocês também podem me parar, mas não podem para todos nós...apesar de tudo, nós somos iguais..."*

Os verdadeiros criminosos são os chamados "Crackers", conhecidos também como "hackers do mal", aquele que invade sistemas, roubam arquivos, destrói discos rígidos, espalham vírus, fazem espionagem industrial na lavagem de dinheiro sujo internacional. Este é o indivíduo nocivo a sociedade digital do novo milênio, pois as policias e a sociedade ainda não estão preparados para conte-los.

Aliás, o termo "Cracker" foi cunhado em 1985 pelos próprios "Hackers", como inequívoco objetivo de não serem confundidos com aqueles

Vejamos a definição dada por Amaro Moraes e Silva Neto[20]:

> *"Os crakers são aqueles que rompem a segurança de um sistema em busca de informações confidenciais com o objetivo de causar dano ou obter vantagens pessoais"*

Há grandes diferenças entre os "Hackers" e os "Crackers", sendo aquele atiçado exclusivamente pelo desfio intelectual de romper as defesas de

[20] Amaro Moraes e Silva Neto, *Resgatemos os Hackers*. p. 25.

um sistema operacional e aí encerrar sua batalha mental, já o segundo inicia sua batalha quando do rompimento das defesas do sistema operacional sob ataque, tendo em vista a obtenção de benefícios para si ou para outrem, sempre em dentrimento de terceiros.

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

4.2 - O perfil do sujeito ativo

O perfil do criminoso, baseado em pesquisa empírica, indica jovens inteligentes, educados, com idade entre 16 e 32 anos, do sexo masculino, caucasianos, audaciosos e aventureiros, com inteligência bem acima da média e movidos pelo desafio da superação do conhecimento, além do sentimento de anonimato, que bloqueia seus parâmetros de entendimento para avaliar sua conduta como ilegal, sempre alegando ignorância do crime e, simplesmente, uma brincadeira.

Segundo Celso H. Leite[21], é possível descrever as principais características daqueles que praticam crimes por computador, na atualidade, porém os dados tomados per ele referem apenas a agentes internos de empresas e não a “crackers” ou “hackers”, mas merecem ser analisados:

a) Idade: 18 a 35 anos;

b) Sexo: masculina, na maioria;

c) Função: administrador de alto nível;

d) Perfil: estável no emprego, brilhante, ativo, motivado, diligente, de confiança (acima de qualquer suspeita), laborioso, primeiro a chegar e o último a sair, não tirar férias, zeloso com relações pessoais, preocupado com a manutenção do prestígio, individualista, gosta de resolver problemas de forma independente;

e) Antecedentes Criminais: nenhum;

f) Método: executando uma ação ordinária no curso de uma operação de sistema normal e legal, como por exemplo: cálculo de salário, contas a receber, pagamentos de fornecedores, transferência de fundos, etc.

g) Reações ao ser apanhado:

“Isso não é crime”

“Eu não prejudiquei ninguém”

“Todo mundo faz isso”

[21] Celso H. Leite, *Crimes por computador.* p. 2.

"Eu apenas tentei demonstrar ao meu superior que isto é possível ser feito"

O advogado Marco Aurélio Rodrigues Costa[22], estudando o perfil do delinqüente de informática, inclusive as condutas dos "crackers" e dos "hackers" diz que é inequívoca a idéia de que esses criminosos digitais são "*experts*", pois os sistemas disponíveis, qualquer pessoa pode ser autor do delito de informática, bastando ter conhecimentos de computação, para ser capaz de comete-los.

Dispõe, ainda, o estudo do referido advogado[23] que:

> *"através das inumeráveis compilações que circulam pelo mundo da informática, são os crimes dessa espécie cometidos à égide da 'special opportunity crimes', qual sejam, os crimes afeitos à oportunidade, perpetrados por agentes que tem a sua ocupação profissional ao manuseio de computadores e sistemas, em várias atividades humanas, e em razão dessa ocupação cometem delitos, invariavelmente, contra seus empregadores".*

A conclusão que se chega quando comparamos os diversos estudos sobre esse tipo de delinqüente é que em qualquer parte do mundo eles mantém esse perfil, que dificulta ao máximo que seja surpreendido em ação delituosa ou que se suspeite dele.

---

[22] Marco Aurélio Rodrigues Costa. *Direito e Internet*. p. 14.
[23] Ibidem, p. 15.

CAPÍTULO V

PERSECUÇÃO PENAL

5.1 – Obtenção de Provas

A idéia de que a *World Wild Web* é um novo espaço em que os delitos costumam ficar impunes, como já dissemos, carece de fundamentos. As mesmas vantagens que a Rede trás ao delinqüente moderno podem também ser de

serventia para técnicos que participam das investigações em busca de provas e evidências da identidade e origem do suposto infrator. As novas técnicas e modalidades geram um outro tipo de investigação que podem ter resultados inequívocos na determinação da autoria e mecânica de um delito, porém exige do investigador um conhecimento bem mais específico da matéria.

Por outro lado, a grande inovação que a Internet proporciona as técnicas de investigação, é a possibilidade de obter uma cópia exata dos elementos que fizeram parte da transação ilícita. Desde mensagens transmitidas pelos participantes até os próprios efeitos e mecânica do delito.

A obtenção dos elementos de provas deve sempre observar os limites constitucionais e suas regras estão devidamente expressas na Lei de Interceptação Telefônica, porém nosso aparato técnico ainda deixa a desejar.

Inúmeras são as ferramentas para auxiliar a persecução penal, a primeira delas é a base de dados WHOIS e no Brasil a FAPESP ambas de acesso público e gratuito que permitem conhecer a titularidade de um domínio e seus responsáveis administrativos e financeiros. Das informações ali contidas consta o nome, o domicílio, e o telefone, assim como o IP do servidor primário e secundário.

Também existem outras ferramentas que permitem através da análise do correio eletrônico chegar a sua origem e traçar a rota desde a mesma.

Como visto existem numerosas fontes de informação de acesso público, que permitem associar a direção de correio eletrônico a uma pessoa determinada sem alterar o titular.

Especificamente no caso de e-mail gratuito, se pode conhecer a identidade do usuário, estando os servidores desse tipo obrigados a facilitar os dados de seus usuários a autoridade judicial que o requerer.

Apesar de tantas ferramentas existem alguns obstáculos que devem superados não somente no que tange ao Brasil, tendo em vista a característica de transnacionalidade desse tipo de delito. Dentre eles temos: a escassez de meios técnicos, burocracia do judiciário no momento da emissão dos competentes mandados e principalmente os problemas de jurisdição.

5.2 - Delegacia especializada em São Paulo

Ocorre que face ao surgimento desses delitos, concomitantemente, surgem os policiais do século XXI, cujas armas não são revólveres.

No Estado de São Paulo já existe uma delegacia especializada da Polícia Civil destinada a investigar os delitos informáticos, onde a *noticia criminis* pode ser apresentada no local da delegacia, por telefone ou "e-mail".

A referida delegacia tem ao seu comando o Delegado Mauro Marcelo de Lima e Silva que possui vários casos já resolvidos e, dentre eles, o que diz respeito ao empresário Ricardo Mansur que, utilizando-se de nome falso (Marco C. – obtido através do serviço gratuito de mensagens eletrônicas, denominado "Hotmail", que não exige confirmação de dados pessoais), enviou "e-mail" para

empresários, espalhando o boato de que o Banco Bradesco estaria com capital negativo de treze bilhões de reais. O delegado, em sua incessante busca, descobriu que a mensagem havia sido enviada de um "*cybercafé*" em Londres.

Como muito provavelmente os dados pessoais teriam sido preenchidos também de maneira falsa, a localização do autor ficaria muito difícil. Porém, Mansur foi rasteado e localizado no momento em que tento checar se havia resposta para suas mensagens, por meio de computadores de sua empresa na Inglaterra.

Portanto, há possibilidades, apesar das dificuldades, de se rastear os agentes dos delitos de informática com a finalidade de puni-los, porém a máquina estatal terá que se modernizar para esses repreender esses delitos trazido pela modernidade, cuja investigação não pode ser realizada com a utilização de máquinas de escrever.

CAPÍTULO VI

CLASSIFICAÇÃO DOS CRIMES DE INFORMÁTICA

6.1 - Da classificação

Antes de iniciarmos qualquer forma de classificação, faz-se necessário determinar a diferenciação de dado e informação.

Dado é o conjunto de caracteres (letras/números) que por si só não transmitem nenhum significado. Na informática, refere-se a dados, tudo aquilo que é fornecido ao computador de forma “bruta”. Quando os dados são vistos dentro de um contexto e transmitem algum significado as pessoas, tornam-se

informações. No caso da informática refere-se aos resultados processados que o computador nos dá de volta.

Assim, dado é o que fornecemos ao computador e informação é o resultado obtido do computador. Podemos dizer que a informação é o dado aplicado na situação prática.

O National Center For Computer Crime Data, dos E.E.U.U. defende posição de que o "Direito Criminal da Informática" é concebido para proteger os sistemas de computadores e das comunicações, além da informação.

Existindo inúmeras classificações que são propostas para o estudo da matéria. Contudo, creio que a classificação quanto ao objeto material é o mais recomendado, visto que acaba englobando as outras existentes. Essa é, exemplificando, a classificação de Ivete Senisse Ferreira[24].

Dessa forma, segundo o objetivo material dos delitos de informática são: a) delitos de informática puro; b) delitos de informática misto e c) delitos de informática comum.

6.2 - Delitos de informática puro

Se constituem naqueles em que o sujeito ativo visa especificamente ao sistema de informática, em todas as suas formas, ou seja, o "software", o "hardware", os dados e sistemas contidos no computador, os meios de armazenamento externo, tais como fitas, disquetes, etc.

---

[24] Ivete Senise Ferreira, *Criminalidade de Informática*, p.213-215.

As ações físicas se materializam, por exemplo, por atos de vandalismos contra a integridade física do sistema, pelo acesso desautorizado ao computador, indevido a dados e sistemas contidos em 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.

6.3 - Delitos de informática misto

Qualquer ação em que o agente tem por objetivo um bem juridicamente protegido da informática, porém, o sistema de informática se constitui em ferramenta, em meio imprescindível a sua consumação.

Quando o agente tem por objetivo, por exemplo, realizar operações de transferência ilícita de valores de outrem, em uma determinada instituição financeira utilizando-se do documento para alcançar o resultado da vantagem ilegal, sendo o computador, ferramenta essencial, defrontamo-nos com um crime de informática misto.

É “crime de informática misto” porque incidiram norma da “lei penal de informática” da lei penal comum, combinando-se, por exemplo, o artigo 171 do Código Penal e uma norma de mau uso de equipamento de informática.

Em vista do exposto, não seria, então, um delito comum apenas, pois incidiria a “norma penal de informática”, teríamos certamente o concurso formal de crimes (artigo 70 do Código Penal).

6.4 - Delitos de informática comum

Correspondem aquelas condutas em que o agente se utiliza do sistema de informática como mero auxiliar a perpetração de crime comum, tipificável na lei penal, ou seja, a utilização do sistema de informática não é essencial à consumação do delito, que poderia ter sido praticado por meio de outra ferramenta.

Como exemplo, os casos de estelionato e suas variadas formas de fraude. Nesses casos, o agente ativo poderia ter escolhido ferramenta diversa da informática.

A partir da presente classificação entendemos que a elaboração de legislação se torna algo mais concreto e certo, ou seja, poderá haver a criação de legislação que englobem os delitos de informática, sem contudo, haver riscos de sobreposição de normas, evitando futuros conflitos de normas. Pois, se tem a exata noção do que é específico, e do que se tem que criar com as normas penais já existentes.

CAPÍTULO VII

O PROBLEMA DA AUTORIA

Os delitos de informática, face ao anonimato assegurado aos "internautas" na Rede Internacional, impõe dificuldades na apuração de sua autoria.

Enquanto no mundo real é possível a identificação por meio de documento de identidade, aparência física e outros dados, no mundo “virtual” essa identificação é muito dificultosa, pois quando um cidadão está conectado à "Internet", utilizando o seu computador e uma linha telefônica, só poderemos identificar o endereço da sua máquina pelos chamados IP – “*Internet Protocol*”, sendo, porém não revelam nada sobre o usuário da Internet, nem tampouco sobre os dados que estão sendo transmitidos.

Ademais, a preocupação com a autenticidade dos documentos telemáticos é uma das maiores preocupações na transmissão e recebimento de informações.

A utilização da referida técnica se baseia num sistema de chaves públicas e chaves privadas, diferentes entre si, que possibilitam um elevado grau de segurança as informações trocadas quando utilizada, porém não garante a total inviolabilidade de informações.

No entanto, em relação a atribuição da autoria do documento, mensagem ou conduta ilícita, os problemas processuais persistem, porque, salvo quando o usuário do computador faça uso de uma assinatura digital, dificilmente se poderá examinar quem praticou a conduta.

A assinatura digital apenas permite presumir quem foi o autor do ilícito, sendo pois incompatível com o Direito Penal, onde se exige a prova da verdade real para efetuar uma condenação.

O único método realmente seguro de atribuição de autoria em crimes informáticos é o que se funda no exame da autuação do responsável penal, quando este tenha valido de elementos corporais para obter acesso a redes de computadores. Há mecanismos que somente validam acesso mediante a verificação de dados biométricos do indivíduo. Sem isso a entrada no sistema é vedada. As formas mais comuns são análise do fundo de olho do usuário ou a leitura eletrônica de impressão digital, ou ainda, a análise da voz do usuário.

Mas a criptografia avançada assimétrica, tanto quanto a "Internet" e a informática, em si mesma, ambivalente. Se de um lado se presta a proteger a

privacidade dos cidadãos honestos e os segredos industriais e comerciais de empresas, presta-se também a assegurar tranqüilidade para os "ciberdelinqüentes", espaço sereno para transações bancárias ilícitas e campo fértil para o terrorismo e outras práticas criminosas, colocando os órgão investigativos do Estado em difícil posição e, consequentemente, minando a defesa social.

Assim, estamos diante dos velhos conflitos entre direitos fundamentais e interesse público, entre segurança pública e privacidade, entre ação do Estado e a intimidade do indivíduo, questões que somente se resolvem por critérios de proporcionalidade e mediante a análise do valor dos bens jurídicos postos em confronto.

CAPÍTULO VIII

O PROBLEMA DA COMPETÊNCIA

O número de procedimentos judiciais relativos a delitos que utilizam a Internet tende a aumentar em progressão geométrica. Os efeitos transnacionais de algumas atividades denunciadas obrigam a determinar qual deve ser a jurisdição competente para julgar os delitos que tem origem em um país e produzem seus resultados em outro.

No Estados Unidos, no caso de materialização de delitos que extrapolem os limites territoriais são investigados pelo FBI, de jurisdição federal. Já na União Européia as investigação são feitas com colaboração mútua, utilizando tratados assinados entre vários países permitindo assim colaboração

mútua. A proposição diz com a questão da aplicação da lei penal no espaço e não é tema de interesse exclusivo do ordenamento brasileiro.

Coloca Marco Aurélio[25] que:

> *"Além das repercussões na idéia de soberania e na eficácia das legislações, não se pode deixar de mencionar os reflexos que serão gerados em relação ao exercício da função jurisdicional".*

O problema de soberania, jurisdição e competência estarão cada vez mais presente no cotidiano dos juristas e dos operadores do Direito que se defrontarem com questões relativas à Internet.

Alguns autores questionam a possibilidade da "Internet" ser controlada pelo Estado, inferindo-se que a "Internet" prestará à ruína das idéias de soberania e território, conduzindo a uma remodelagem da noção de Estado-nacional, conduzindo ao chamado neoliberalismo ou novo feudalismo.

Em verdade, o grande problema de se trabalhar o conceito de jurisdição e territorialidade na "Internet", reside no caráter internacional da Rede.

Em tese um crime que seja perpetrado na Internet ou por meio dela, cosam-se em todos os locais onde a rede seja acessível. No crime de calúnia, por exemplo, o agente atribui a outrem um fato tido como criminoso e lança essa declaração na "Internet", tal ofensa poderá ser lida em qualquer local do mundo.

---

[25] Marco Aurélio Greco, *Direito e Interet: relações jurídicas na sociedade informatizada*, p. 203.

Há autores que sugerem aplicar a solução dada pela Lei de Imprensa (art. 42 da Lei n.° 5.250/67), que considera competente para o processo e julgamento o foro do local onde for impresso o jornal.

Coloca Ives Gandra Martins e Rogério Vidal Gandra da Silva Martins[26] que:

> *"(...) toda comunicação eletrônica pública deve ter o mesmo tratamento para efeitos ressarcitórios da comunicação clássica pela imprensa(...) a desfiguração da imagem por informações colocadas fora da soberania das leis do país ensejaria os meios ressarcitórios, se alavancada no Brasil"*

Estabelece o artigo 72 do Código de Processo Penal que a competência do foro do domicílio do réu, quando não conhecido o lugar da infração.

Entendemos que, no tocante aos crimes à distância, deve-se aplicar a teoria da ubiqüidade, que foi acolhida pelo artigo 6° do Código Penal.

Entretanto, no caso de crimes plurilocais deve-se determinar a competência com fulcro no artigo 70 do Código de Processo Penal.

Com relação a aplicação extraterritorial da lei brasileira, nos termos do artigo 7° do Código Penal, não seria possível sua aplicação.

Dispõe, ainda, o artigo 88 do CPP que no processo por crime praticado fora do território brasileiro, será competente o juízo da Capital do Estado onde houver por último residido o acusado, caso nunca tenha residido no Brasil, será competente o juízo da capital da República.

---

[26] Ives Gandra Martins e Rogério Vidal Gandra da Silva, *Privacidade na comunicação eletrônica*. p. 44.

O art. 109, inciso V da Constituição dispõe, *in verbis*:

> *"os crimes previstos em tratado ou convenção internacional, quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente."*

Ademais, com a internacionalização da criminalidade de informática, é indispensável que todos os países harmonizem suas normas penais, para prevenção e repressão eficientes, tal recomendação é feita pela ONU e pelo Comitê de Ministros do Conselho da União Européia que estão tomando providências para efetivá-la.

Tais considerações são relevantes face ao disposto no artigo 5° do Código Penal que assim dispõe, *in verbis*:

> *"a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido no território nacional.*

Certo é que a lei penal brasileira poderá ser aplicada extraterritorialmente para punir delitos informáticos praticados fora do País ou cujo resultado se tenha dado, ressalvando as contravenções, nos termos do artigo 2° do Decreto-Lei n° 3688/41, em que só se permite a aplicação da lei brasileira no caso de contravenção praticada em território nacional.

O Projeto de lei, para crimes de informática n.° 76/2000 no Senado Federal silencia e remete, em sua justificação, aos dispositivos já existentes para solucionar o problema da competência.

CAPÍTULO IX

APLICAÇÃO DA LEI PENAL NA INTERNET

9.1 – A lei penal brasileira e a Internet

Dentre os crimes praticados por meio da "Internet", os mais comuns são o furto, fraude, estelionato, falsificação, sabotagem, inclusive terrorismo. O computador, nesses casos, torna-se um meio facilitador do delito.

Os crimes informáticos ainda incluem o uso não autorizado de computador, furto de tempo de rede de sistema de computador, o abuso de

correio eletrônico, o acesso indevido ou a violação de sistemas de processamento de dados, a implantação do vírus eletrônicos em sistemas de computadores com o intuito de corromper dados, destruir, modificar e alterar programas e informações, elaboração de *sites* de pedofilia, pornografia infantil, incitação ao racismo, pornografia infantil, violação de marcas através de registros de domínio, violação de direitos autorais.

A preocupação vigente não se restringe somente ao campo da fraude e do estelionato. Existem casos de terrorismo e sabotagem, colocando em risco vidas humanas.

Vejamos os exemplos dados pela advogada Debora Fisch Nigri[27]:

> *"A manipulação maldosa de uma base de dados de um hospital pode colocar em risco a vida de pacientes. A alteração de dados de um computador que auxilia um piloto de avião coloca em risco a vida dos passageiros. Teríamos, nos dois últimos casos, crimes contra a vida e não contra bens materiais, portanto, os crimes informáticos não são crimes puramente sócio-econômicos."*

A principal característica desses tipos de delitos é o ato lesivo cometido através de computador ou de um periférico com a intenção de se obter vantagem indevida. Se um vírus eletrônico é inserido na base de dados de um hospital e, devido a este ato, arquivos são corrompidos resultando em morte de pacientes, não temos um crime informático, mas um caso de homicídio. Neste caso o Código Penal estaria equiparado para lidar com o crime de homicídio. Ocorre que o que se pretende é punir o ato inicial da criação do vírus eletrônico. Se tal ato fosse tipificado como crime, o resultado morte poderia ser evitado.

---

[27] Debora Fisch Nigri, *Crimes e a segurança na internet*. p. 35.

Com relação aos esses crimes surge a questão da possibilidade de se aplicar ou não a legislação existente, em que há dois entendimentos. O primeiro entendimento diz que o crime informático deve ser visto como qualquer outro, não havendo necessidade de se distinguir entre a informação contida num documento qualquer e aquela computadorizada. Sob essa ótica, o instrumento do crime é que mudaria, porém a conduta já estaria tipificada no Código Penal, devendo-se apenas adaptar a lei ao caso concreto. Já a segunda corrente, a qual nos filiamos, entende que as leis existentes não são suficientes para tratar dessas condutas e que seria necessário a criação urgente de leis para adaptação da legislação existente.

A tentativa de adaptação de leis antigas e ultrapassadas provou ser ineficaz em diversos países gerando impunidade para os réus.

Sendo o Brasil um Estado Democrático de Direito (art. 1° da CF), necessariamente aplicam-se em seu território os princípios da legalidade e da anterioridade da lei penal.

Com efeito o artigo 5° , inciso XXXIX da Carta Magna, estabelece, dentre as liberdades públicas, a garantida de que “não há crime se lei anterior que o defina, nem pena sem prévia cominação legal”. O artigo 1° do Código Penal, por sua vez, estatui que “Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal”.

A tipicidade é uma conseqüência direta do princípio da legalidade. Um fato somente será típico se a lei descrever, previamente e pormenorizadamente, todos os elementos da conduta humana tida como ilícita.

Em verdade, é preciso ver que para que se admita um novo tipo penal no ordenamento brasileiro, é imprescindível que se atendam outras regras constitucionais, no sentido de elaboração legislativa, como a competência prevista no artigo 22, incisos I e IV, atribuindo privativamente a União legislar sobre direito penal e informática.

Quanto aos delitos já capitulados no Código Penal e na legislação extravagante, não há dificuldades para operar o sistema penal. As fórmulas e diretrizes do processo penal como já colocamos, anteriormente, tem serventia.

Portanto, quando o Poder Judiciário pune infratores eletrônicos com base nos tipos já definidos em lei não estará violando o princípio da legalidade nem o da anterioridade da lei penal.

Não poderíamos deixar de citar nesse momento as palavras de Ivan Lira de Carvalho[28] que diz:

> *"(...) sendo perguntado, por exemplo, se a internet é um novo meio de execução de crimes "velhos" ou é, por si mesma, geradora de novos delitos, terei o atrevimento de dizer que as duas partes da perguntam se complementam para a resposta: há crimes novos, contemporâneos da formação da rede mundial de computadores, mas estão acontecendo, pela "net", delitos que já de muito tempo conhecidos da sociedade, só que agora perpetrados com requintes de bits."*

Todavia, o Direito Penal brasileiro não oferece solução para condutas lesivas ou potencialmente lesivas que possam ser praticadas pela Internet e que não encontrem adequação típica no rol dos delitos existentes no Código Penal e

[28] Ivan Lira Carvalho, a internet e o direito, p. 2.

nas leis especiais brasileiras ou nos tratados internacionais em matéria penal, do qual o Estado brasileiro seja parte.

Wladimir Aras[29] elenca alguns tipos penais, que descrevem crimes de informática, já existentes. São eles:

a) o artigo 10 da Lei Federal n.° 9.296/96, que considera crime, punível com reclusão de 2 a 4 anos e multa, "realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo de Justiça, sem autorização judicial ou com objetivos não autorizados em lei".

b) o artigo 153, § 1°-A do Código Penal, com a redação dada pela Lei Federal n° 9983/2000, 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 1 a 4 anos.

c) o artigo 313-A, do Código Penal, introduzido pela Lei n° 9983/2000, que tipificou o crime de inserção de dados falsos em sistemas 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 a 12 anos e multa;

d) o artigo 313-B, do Código Penal, introduzido pela Lei n.° 9983/2000, que tipificou o crime de modificação ou alteração não autorizada de sistema de informações, com a seguinte redação: "Modificar ou alterar, o

[29] Vladmir Aras. *Crimes de Informática; uma nova criminalidade*. p. 28

funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente", cominando-lhe pena de detenção, de 3 meses a 2 anos, e multa;

e) o artigo 325, §1°, incisos I e II, introduzidos pela Lei n.° 9983/2000, tipificando novas formas de violação de sigilo funcional, nas condutas de quem "I - permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou bancos da Administração Pública" e de quem "II - se utiliza, indevidamente, do acesso restrito", ambos sancionados com penas de detenção de 6 meses a 2 anos, ou multa;

f) o artigo 12, *caput*, §§ 1° e 2°, da Lei Federal n° 9609/98, que tipifica o crime de violação de direitos de autor de programa de computador, punindo-o com detenção de 6 meses a 2 anos, ou multa; ou com pena de reclusão de 1 a 4 anos e multa, se agente visa lucro;

g) o artigo 12, inciso V, da Lei n° 8137/90, que considera crime "utilizar ou divulgar programa de processamento de dados que permita ao sujeito passivo da obrigação tributária possuir informação contábil daquela que é, por lei, fornecida à Fazenda Pública"; e

h) o artigo 72 da Lei n° 9504/97, que cuida de três tipos penais eletrônicos de natureza eleitoral. Vejamos *in verbis*:

> *"Art. 72. Constituem crimes, puníveis com reclusão, de cinco a dez anos:*
> *I - obter acesso a sistema de tratamento automático de dados usado pelo serviço eleitoral, a fim de evitar a apuração ou a contagem de votos;*

> *II - desenvolver ou introduzir comando, instrução, ou programa de computador capaz de destruir, apagar, eliminar, alterar, gravar ou transmitir dado, instrução ou programa ou provocar qualquer outro resultado diverso do esperado em sistema de tratamento automático de dados usados pelo serviço eleitoral;*
> *III - causar, propositadamente, dano físico ao equipamento usado na votação ou na totatalização de votos ou suas pastas."*

Verifica-se, portanto, a preocupação do legislador infraconstitucional de proteger bens informáticos e de assegurar, na esfera penal, a proteção a dados de interesse da Administração Pública e da privacidade "telemática" do indivíduo.

Como se pode verificar a legislação existente não é suficiente para garantir a punição do criminoso fazendo-se necessária uma tipificação induvidosa e eficaz, com condutas ainda não tipificadas em lei.

9.2 - Bens tuteláveis

A advogada do Rio de Janeiro Deborah Fisch Nigri[30] em seu artigo intitulado "Crimes e Segurança na Internet" elenca algumas condutas que poderiam ser passíveis de tipificação. Esta lista, segundo a autora, é exemplificativa, podendo ser ampliada. Tais condutas são baseadas em modelos internacionais, levando-se em conta a legislação já existente nessa área em diversos países, como Estados Unidos e Inglaterra.

a) Acesso indevido aos sistemas de computador

[30] Debora Fisch Nigri, *Crimes e a segurança na internet*. p. 38

Ganhar acesso ou tentar ganhar acesso, indevidamente, a um sistema de computador ou a uma rede de computadores, fazendo o sistema produzir alguma função.

O simples acesso indevido a um computador, ou a uma rede de computadores, é punido. Pune-se o acesso não autorizado ou o indivíduo que excede os limites de sua autorização. O agente deve estar ciente, no momento do crime, que ele não estava autorizado a ter acesso ao sistema. O agente pode cometer tal crime fisicamente ou remotamente (através de um modem). Basta que o computador responda ao comando do agente indevidamente autorizado para tipificar-se o crime.

O bem jurídico tutelado neste caso é a integridade do sistema e conseqüentemente preservação das informações armazenadas no sistema.

b) Acesso indevido com o intuito de cometer crime mais grave

Ganhar acesso ou tentar ganhar acesso, indevidamente, a um sistema de computador ou a uma rede de computadores com o intuito de comer crime mais grave.

Várias formas qualificadas são previstas, tais como: causar dano, obter vantagem, alterar programas, devassar o sigilo de informações contidas em sistemas. Crime mais grave pode incluir fraude eleitoral, crime de calúnia, injúria e difamação, entre outros.

c) Violação de sistemas de processamento de dados através de senha de outrem

Utilizar senha de outrem sem a devida autorização com o intuito de ganhar acesso ao computador ou a rede de computadores.

A utilização de senha de outrem também é prevista como forma qualificada do acesso não autorizado.

d) Fraude através do uso do computador

Apropriar-se indevidamente de valores através da manipulação de qualquer sistema de processamento de dados, obtendo assim vantagem econômica para si ou para outrem.

O bem jurídico neste caso é de caráter financeiro: dinheiro, ações valores. A expressão qualquer sistema inclui computadores e redes de computadores diversas, tais como redes bancárias, do mercado de ações, caixa automáticas de serviços bancários.

e) Furto de informações contidas no computador

Apropriar-se indevidamente de informações contidas em qualquer sistema de processamento de dados, seja temporária ou permanentemente.

Protege-se aqui o direito à informação e ao acesso e uso legítimo da mesma parte do usuário. Protege-se igualmente a privacidade e integralidade do sistema.

f) Falsificação de documentos com o uso da tecnologia do computador

Alterar, apagar ou falsificar documento através de sistema de computador e seus periféricos e usar este documento falso com o intuito de induzir alguém em erro.

Incorre no mesmo crime a pessoa que usa documento sabendo ser ele falso.

Para efeitos penais, equipara-se documento o dado constante no sistema de computador e qualquer suporte físico tais como: disquete, fita, disco compacto, cd-rom, ou qualquer aparelho usado para armazenar informação seja por meio mecânico, ótico ou eletrônico.

g) Sabotagem

Impedir ou prevenir o funcionamento de um computador ou de um programa de computador, temporária ou permanentemente, interferindo no sistema de forma a causar distúrbios no mesmo.

O bem jurídico tutelado é a integridade do sistema, permitindo assim seu funcionamento normal.

h) Danos ao computador e às informações armazenadas no computador.

Causar danos ao computador, destruir, inutilizar, alterar, apagar, suprimir ou modificar os dados e informações contidas no computador, temporaria ou permanentemente, total ou parcialmente.

O bem jurídico tutelado é a integridade do sistema, permitindo assim seu funcionamento normal.

Pode haver superposição entre o crime de sabotagem e o de dano. No crime de sabotagem o criminoso tem a intenção de causar distúrbio no funcionamento normal do sistema. Por exemplo, fazer com que o sistema fique lento. Já no crime de dano a intenção é danificar o sistema.

i) Aquisição ilícita de segredos industriais ou comerciais

Adquirir segredos industriais ou comerciais ou informações de caráter confidencial com intenção de causar danos financeiros ou obter vantagem pecuniária para si ou para outrem.

O bem jurídico a ser protegido é o segredo industrial ou comercial.

j) Uso não autorizado de computador: furto de tempo do sistema

Utilizar sem autorização de quem de direito, ou abusar da autorização que lhe foi conferida, sistema de processamento de dados, de modo a causar perda significativa de recursos.

O furto de tempo de sistema de processamento de dados visa evitar abusos, normalmente realizados por empregados que utilizam o sistema de computador do empregador para desempenhar tarefas particulares sem a devida autorização do mesmo. O objetivo é, por exemplo, penalizar a pessoa que resolve estabelecer seu próprio negócio às custas do empregador. Uma grande dificuldade neste crime é estabelecer-se a pena a ser atribuída. Uma pena de multa seria aconselhável; ocorre que é difícil calcular-se a quantidade de

eletricidade despendida pelo agente. Um bom parâmetro seria estabelecer o valor de mercado da atividade realizada pelo perpetrador do delito.

l) Cópia/uso ilícito de programa de computador

Reproduzir, modificar, distribuir, importar, exportar, usar programa de computador protegido por lei com o intuito de obter vantagem pecuniária para si ou para outrem sem a devida autorização do autor do programa.

O bem jurídico a ser protegido é o circuito integrado e o direito de propriedade de seu autor original ou do detentor da licença para comercialização.

m) Violação de direito autoral

Usar ou ganhar acesso a rede de computadores com o intuito de reproduzir, distribuir obras literárias, artísticas e/ou científicas protegidas.

n) Criação, inserção e distribuição de vírus

Criar, inserir e distribuir programa de computador contendo informações capazes de destruir, modificar, alterar, inferir o impedir o funcionamento próprio de um sistema de computador ou provocar resultado diverso do esperado ao sistema, com o fim de causar dano físico ou material a outrem ou obter qualquer vantagem para si ou para outrem.

Para fins penais é irrelevante se o programa maléfico não causa dano ou modificação do sistema.

Pretende-se aqui punir logo de início a criação do vírus eletrônico, independente do fato de eles serem maléficos ou benéficos ao sistema. Mesmo o vírus mais inocente pode causar a lentidão do sistema, fazendo com que o funcionamento do computador seja afetado. O bem jurídico tutelado é a integralidade do sistema, permitindo assim seu funcionamento normal, e, em caso de dano físico, o bem juridicamente tutelado é a vida.

o) Espionagem

Obter acesso ilícito a um sistema de computadores com o intuito de apropriar-se de informações confidenciais ligadas a segurança nacional para furtar, copiar, vender ou transferir para outrem.

Pretende-se aqui proteger sistemas de computadores relativas a segurança nacional assim como a integridade de tais sistemas e informações.

p) Interceptação indevida de telecomunicações

Interceptar indevidamente a comunicação entre computadores através de grampos durante a transmissão de dados com o intuito de invadir a privacidade do usuário.

q) Violação de base de dados pessoais

Violar base de dados de caráter pessoal obtendo informações confidenciais do indivíduo.

O objeto aqui é proteger o indivíduo e suas informações pessoais que podem estar contidas em base de dados bancária, médica, policial, por exemplo. O bem jurídico tutelado é a privacidade.

r) Abuso de Rede ou correio eletrônico

Usar ou ganhar acesso a rede de computadores com o intuito de disseminar informações fraudulentas ou que gerem crime mais grave.

Pune-se aqui a utilização de rede de computador para disseminar informações fraudulentas tais como distribuição de programas de computador, de forma a violar direito de autor, ou a distribuição de senhas para quebra de sistema de segurança por *hacker*. Pode-se incluir aqui também a disseminação de pornografia, incitação ao nazismo e racismo através da rede.

9.3 - Legislação sobre crimes de informática

Como foi exposto, a legislação vigente não é suficiente se fazendo necessário a criação de novos tipos penais, nesse intuito encontram-se em tramitação alguns projetos de lei no Congresso Nacional, dentre eles o Projeto de Lei da Câmara dos Deputados n. 84/99, de autoria do deputado federal Luiz Piauhylino (PSDB-PE).

Em suas disposições gerais, o projeto de lei sobre crimes informáticos busca inicialmente conferir proteção à coleta, ao processamento e à distribuição

comercial de dados informatizados, exigindo autorização prévia do titular para a sua manipulação ou comercialização pelo detentor.

No projeto, são estabelecidos claramente os direitos de conhecimento da informação e de retificação dessa informação, o direito de explicação ao seu conteúdo ou natureza, bem como o de busca de informação privada, instituindo-se a proibição de distribuição ou difusão de informação sensível e impondo-se a necessidade de autorização judicial para acesso de terceiros a tais dados.

No tocante ao rol de novos tipos penais, o PLC 84/99 procura inserir no ordenamento brasileiro os crimes de dano a dado ou programa de computador, acesso indevido ou não autorizado; alteração de senha ou acesso a computador, programa ou dados; violação de segredo industrial, comercial ou pessoal em computador; criação ou inserção de vírus de computador; oferta de pornografia em rede sem aviso de conteúdo; e publicação de pedofilia, cominado-se bens privativas de liberdade que variam entre um e quatro anos.

Há todavia tipos com sanções menos graves, como o crime de que se cuida o artigo 11 do PLC 84/99, de obtenção indevida ou não autorizada de dado ou instrução de computador, com pena de três meses a um ano de detenção e, portanto, sujeito, em tese, à competência do Juizado Especial Criminal.

Se tais delitos forem praticados prevalecendo-se o agente de atividade profissional ou funcional ficará sujeito a causa de aumento de pena de um sexto até a metade.

Tramita também na Câmara, o PLC 1806/99, do deputado Freire Júnior (PMDB-TO) que altera o artigo 155 do Código Penal para considerar

crime de furto o acesso indevido aos serviços de comunicação e o acesso aos sistemas de armazenamento, manipulação ou transferência de dados eletrônicos.

Por sua vez, o PLC 2557/2000, do deputado Alberto Fraga (PMDB-DF), acrescenta o artigo 325-A ao Decreto-Lei n° 1001/69, Código Penal Militar, prevendo crime de violação de dados eletrônico, para incriminar a invasão de redes de comunicações eletrônica, de interesse militar, em especial a "Inernet", por parte de "hacker".

Já o PLC n° 2558/2000, também de autoria do deputado Aberto Fraga (PMDB-DF), pretende acrescentar o artigo 151-A ao Código Penal, tipificando crime de violação de banco de dados eletrônicos.

O PLC n° 4833/98 é de autoria do deputado Paulo Paim (PT-RS) e sua ementa "define o 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".

Resta-nos esperar a aprovação desses projetos para aplicação de um direito penal que iniba e puna a perpetração de crimes na Rede Mundial.

CONSIDERAÇÕES FINAIS

Os novos crimes tornam-se um desafio não só para os técnicos em computação, como também para os profissionais da área jurídica.

A precariedade da legislação, aliada à falta de conhecimento específicos sobre a rede mundial e acerca de métodos e forma utilizados pelos invasores, de um lado, e a incessante expansão da “Internet” e também o permanente avanço da criatividade dos criminosos da “web”, de outro, dificultam sobremaneira a questão da segurança digital. Isto porque, não só através de antivírus, criptografia, ou outros meios, se combate a ação desses “experts”. A falta de regulamentação no que pertine a aplicada, por exemplo, a legislação comum a alguns crimes praticados através da rede, o fato é que a sociedade clama por penalidades mais severas, veiculadas através de normas

específicas. Ademais, em matéria penal, faz-se mister a descrição de uma conduta específica (tipo penal), pois este ramo do direito repele o uso da analogia, quando aplicada em prejuízo do réu.

Em vista da total dependência do ser humano dos sistemas de computador, a adoção de legislação nessa área se justifica tanto pelo caráter patrimonial quanto pela preservação da integridade do sistema de computador como proporcionar de bens e serviços para a população. As mudanças tecnológicas refletem-se nesse novo fenômeno jurídico, afetando as relações humanas. Torna-se, assim, necessária uma proteção jurídica viável e aplicável, não podendo a lei representar um papel passivo nesta revolução sem retorno.

A tipificação legal induvidosa dos crimes informáticos deveria ocorrer através de uma lei específica, pois, de outro modo, seria de difícil acomodação na sistemática penal existente. Um texto específico, independente e sem compromisso com a disciplina já desgastada pelo tempo proporcionará o necessário suporte doutrinário e jurisprudencial para a regulamentação dos delitos.

Em face das lacunas oriundas da modernidade, a reprimenda aos novos crimes virtuais que afloram em nosso meio deverá acatar o princípio da reserva legal, conquanto verificada no artigo 1° do Código Penal Brasileiro e consagrado pelo artigo 5°, inciso XXXIX, da Constituição Federal de 1988.

Através dos mecanismos legais existentes e dos que estão por vir, deve brotar a resistência às condutas criminosas, anulando, assim, o desdém com que parte da sociedade prefere tratar das inovações eletrônicas presentes cada vez mais em nosso meio.

Outra questão importante a ser abordada pelo legislativo é o flagrante. Isto porque, em matéria de crimes virtuais, a verificação deste é praticamente impossível.

Todavia, uma legislação adequada também não é o bastante. O aperfeiçoamento dos meios de investigação, o progresso técnico dos profissionais ligados à área da persecução penal, a melhor formação e treinamento dos auxiliares da Justiça e a conscientização dos internautas e usuários constituem elementos essenciais a coibir práticas desonestas no mundo virtual.

REFERÊNCIAS BIBLIOGRÁFICAS

ALCÂNTARA, Eurípedes. **O homem que ficou rico vendendo idéias**. In: *Veja*. São Paulo, 12/07/1995. Computadores.

AMARAL, Sylvio do. **"Falsidade documental"**. 3.ed. São Paulo: RT, 1989.

ANDRADE, Paulo Gustavo Sampaio. **A importância para o profissional do direito**. Jan. 1998. Disponível em: http://www.jus.com.br/doutrina/impoinfo.html [capturado em 06 out 2000]

ARAS, Wladimir. **Crimes de Informática: uma nova criminalidade**. Jun. 2001. Disponível em: "www.direitocriminal.com.br" [capturado em 11 jun 2001].

ASCENSÃO, J. Oliveira. **"Direito do utilizador de bens informáticos"**. In: *Seqüência*, Florianópolis, v.28, junho/1994

BAREBOIN, Elias. **Segurança na Internet**. Jan. 2001. Disponível em: "http://www.onilux.com.br/segrurança/1" [capturado em 20 fev 2001]

BERTRAND, André. **A proteção dos programas de computadores**. Ed. Livraria do Advogado, Porto Alegre, 1996.

BLOOMBECKER, Buck. **"Crimes espetaculares de computação"**. Rio de Janeiro: LTC, jan.1992.

BLUM, Renato M. S. Opice. **"O bug do milênio"**. out. 1999. Disponível em: http://www.jus.com.br/doutrina/bug20003.html [capturado em 20 nov 2000]

CABRAL, Mauro. **"Pirata: fantasia ou rótulo ?"**. Disponível:http://www./trlex.com.br/resenha/cabral/pirata.htm [capturado em 20 nov 2000]

CAMPOS, Eduardo Cestari. **"Bandidos e Mocinhos no Espaço Digital"**. set. 1999. Disponível: http://www.cestari@br.homeshopping.com.br [capturado em 20 nov 2000]

CARMO, João Clodomiro do. **"O que é informática".** 4.ed., São Paulo, ed. Brasiliense, 1989.

CARVALHO, Ivan Lira. **A internet e o direito**. Jan. 2001. Disponível em: "http//www.jus.com.br" [capturado em 20 fev 2001]

CASTRO, Clarice Marinho Martins de Castro. **"Nome de domínio na Internet e a legislação de marcas"**. marc. 1999. Disponível: http://www/jus.com.br/dourina/dominet.html [caputrado em 20 fev 2001]

CEMBRANEL, João Carlos. **"Crimes Digitais".** jul. 1999. Disponível em: http://www.gpsnet.com.br/sembra.htlm [caputrado em 20 fev 2001]

CHAVES, Antônio. **Direito de autor**. Ed. LTR. São Paulo.

Concorrência Digital. Época. São Paulo, n. 87, jan. 2000

CONCERINO, Arthur José**. Internet e segurança são compatíveis ?**, in Direito & Internet, 1ª Ed., São Paulo, 2001.

COSTA, Cesar da. **"Crimes computadorizados: as conseqüências nao previstas no uso do computador"**. In: *INTERFACE*, São Paulo, v.2, 1984.

COSTA, Marco Aurélio Oliveira. **"O Direito e a Internet".** São Paulo, nov. 1998. Disponível em: http://www.trlex.com.br/resenha/marco/marco.htm [capturado em 20 dez 1999]

COSTABILE, Henrique. **"Combatendo crimes por computação"**. In: *BANAS*. São Paulo, v. 25, n. 1182, jul. 1978.

Crime Perfeito. *Época*. São Paulo, n. 87, jan. 2000.

Defenda-se. *INFOEXAME*. São Paulo, n. 164, nov. 1999.

DOTTI, René Ariel. **"Controle de informática"**. In: *Revist dos Tribunais*. São Paulo, n. 518, dez. 1978.

Epidemia de micro. *Época*. São Paulo, n. 90, fev. 2000.

ELIAS, Paulo de Sá. **Alguns aspectos da informática e suas conseqüências no direito**. Abr. 199. Disponível em http://www.jus.com.br/doutrina/aspeinfo.html [capturado em 05 out 2000]

FERREIRA, Ivete Senise. **"Os crimes de informática"**. In: *BARRA*, Rubens Prestes, ANDREUCCI, Ricardo Antunes.

Fim da inocência. *Veja*. São Paulo, n. 1636, fev. 2000.

FRANCO, Alberto da Costa; STOCO, Rui; COLTRO, Matias *et al.* **Leis especiais e sua interpretação jurisprudencial.** São Paulo: RT, 1995.

GALDEMAN, Henrique. **Como lidar com a pirataria na internet**. nov. 1999. Disponível: http://www.matemart.com.br/arrastao/balanca

GALDEMAN, Silvia Regina Dain. **"Propriedade Intelectual Aspectos Sociais e Legais dentro da Internet"**. In: *Boletim Legislativo Adcoas,* vol.29, n. 32, nov. 1995.

GARCIA, Basileu. **“Instituições de direito Penal”**. 2.ed. São Paulo: Limonad, vol. I, 1954.

GATES, Bill. **“A Estrada do Futuro”**. In: *Veja*, São Paulo, n. 47, nov. 1995.

Hackers invadem site do STF. *O Estado de São Paulo* [on line], São Paulo, 15 fev. 2000. Disponível em: http://www.estado.com.br [capturado em 20 ago 2000]

Hacker invadem site do MEC. *O Estado de São Paulo* [on line], São Paulo, 15 fev. 2000. Disponível em: http://www.estado.com.br [capturado em 20 ago 2000]

HEY, Raul. **“Aspectos Jurídicos da Internet”**. In: *Revista* da ABPI, n. 19, nov/dez. 1995.

Invasão Tropical. *Época*. São Paulo, n. 79, p. 110, jan. 2000.

JEHORAM, Hermann Cohen. **“Proteção do “chip””.** In: *Cadernos de direito econômico e empresarial.* Rio de Janeiro: RDP, jul./set. 1991

JESUS, Damásio E. de. **“Código Penal Anotado”**. 2.ed. São Paulo: Saraiva, 932p., 1991.

JESUS, Damásio E. de. **“Novas questões criminais”.** São Paulo: Saraiva, 1993.

LEITE, Celso H. **“Crimes por computador”.** jul. 1999. Disponível em: http://www.mingus.modulo.com.br/clip_22.htm. [capturado em 20 ago 2000]

LICKS, Otto Banho: ARAÚJO JÚNIOR, João Marcelo. **"Aspectos penais dos crimes de informática no Brasil"**. In: *Revista do Ministério Público*, São Paulo: Nova Fase, 1994.

LIMA NETO, José Henrique Barbosa Moreira. **"Aspectos jurídicos do documento eletrônico"**. out. 1999. Disponível em: http://www.jus.com.br/doutrina/dominet.html [capturado em 20 ago 2000]

LOPES NETO, Silvino Joaquim. **"Informática e simplificação processual".** XVI Conferência Nacional dos Advogados.

LOSSO, Fábio Malina. **"Internet um desafio jurídico".** Disponível em : http/www.infojur.ccj.ufsc.br/arquivos/informatica_juridica/Internet/Losso

LUCA, José Carlos Moreira de. **"A pirataria não compensa".** In: *Exame Informática*. São Paulo, n. 90, mai. 1992.

MARZOCHI, Marcelo. **Manifesto Hacker.** Mar. 2000. Disponível em: "http://www.jus.com.br" [capturado em jun. 2000]

MOROM, Fernanda de Almeida Pernambuco. **"A internet e o Direito",** consulex, Brasília, vol. 3, mar. 1997.

Nas redes da polícia. *Época*. São Paulo, n. 76, nov. 1999.

NEGROPONTE, Nicholas. **"O computador liberta".**In: *Veja*, São Paulo, v.28, n.30, jul. 1993.

NEVES, Iêdo Batista. **Vocabulário de tecnologia jurídica e de brocados latinos**. 4.ed. Rio de Janeiro, Fase, 1991.

NIGRI, Déborah Fisch. **"Crime e informática: um novo fenômeno jurídico".** In: *Revista Trimestral de Jurisprudência dos Estados.* V. 16, n.100, mai.1992.

NOBREGA, Evandro. **"Hacker invadiu provedor e agora pega cadeia"**. *O Norte*. Caderno de Informática. 11 fev. 1998.

NUNOMURA, Eduardo. **"O Sucesso da Rede".** In: *Veja*, São Paulo, Abril, n. 41, out. 1998.

NUNES, Luiz Antônio Rizatto. **Manual da Monografia Jurídica**.2ª ed., São Paulo: Saraiva, 1999.

PAESANI, Liliana Minardi. **Direito de Informática**. São Paulo, Atlas, 1997.

PALADINO, Enzo. **Novo dicionário técnico de informática**. São Paulo: Ciência Moderna. 1986.

PERTENSEN FILHO, Antônio Oscar de Carvalho. **"A nova lei de software".** Disponível em: http/www.trlex.com.br/resenha/blum/soft.htm [capturado em 20 ago 2000]

Pesquisa Nacional sobre Segurança da Informação. Fev. 2000. Disponível em: "http://www.modulo.com.br/noticias/pesquisa.htm".[capturado em 22 out 2001]

PRADO, Maurício Auvelo de Almeida**. Contrato Internacional de Transferência de Tecnologia**. Ed. Livraria do advogado, Porto Alegre. 2000.

Receita Bloqueia ataques de Hackers. O Estado de São Paulo [on line], São Paulo, 15 fev. 2000. Disponível em: http://www.estado.com.br [capturado em 20 ago 2000]

SANTOS, Manuel J. Pereira dos**. Proteção Jurídica do Software**. In: *O Estado de São Paulo*. 28 fev. 1986.

SAKAMOTO, Marcos. **"Direito das gentes e a informática"**. jan. 2000. Disponível em: http://www.sakamoto@embratel.net.br [capturado em 20 dez 2001]

SILVA NETO, Amaro Moraes. **"O direito e o espaço cibernético"**, consulex, Brasília, vol. 1, jan. 1997.

SILVA NETO, Amaro Moraes. **"Cookes, esses indigestos biscoitos"**. jan. 2000. Disponível em: "http://www.amaromorae@advogado.com" [capturado em 5 out 2000]

SILVA NETO, Amaro Moraes. **"O e-mail como prova no direito brasileiro"**. jan. 2000. Disponível em: "http://www.amaromorae@advogado.com" [capturado em 5 out 2000]

SILVA NETO, Amaro Moraes. **"O e-mail como prova no direito alienígena"**. jan. 2000. Disponível em: "http://www.amaromorae@advogado.com" [capturado em 5 out 2000]

GRECO, Marco Aurélio e MARTINS, Ives Gandra da Silva (coordenadores). **Direito e Internet: relações jurídicas na sociedade informatizada.** São Paulo: RT, 2001.

MARTINS, Ives Gandra Silva e SILVA, Rogério Vidal Gandra da. **Privacidade na comunicação eletrônica.** São Paulo: RT, 2001.

SILVA NETO, Amaro Moraes. **Resgatemos os hackers**. Jan. 2000. Disponível em: "www.jus.com.br/doutina/hackers.html" [capturado em 5 out 2000]

TEODORO JÚNIOR, Euclides. **Computador a serviço do crime**. In: *BANAS*. São Paulo. v. 25, n. 1192, dez. 1978.

TRUJILLO, Elcio. **"Mercosul e a documentação eletrônica"**. nov. 1998. Disponível em: http://www.advogado.com/zip/mercosul.htm" [capturado em 20 ago 2000]

WILLING, David S., **A internet e a Constituição dos Estados Unidos.** Consulex, Brasília, Vol I, jan. 1997.