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

WESLLEY ALVES DE SOUSA

CRIMES DIGITAIS: MOVIMENTAÇÃO INDEVIDA DE VALORES E O DISCIPLINAMENTO DO CÓDIGO PENAL

SOUSA - PB
2007

WESLLEY ALVES DE SOUSA

CRIMES DIGITAIS: MOVIMENTAÇÃO INDEVIDA DE VALORES E O DISCIPLINAMENTO DO CÓDIGO PENAL

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

Orientador: Profº Me. Jonábio Barbosa dos Santos.

SOUSA – PB
2007

Weslley Alves de Sousa

CRIMES DIGITAIS: MOVIMENTAÇÃO INDEVIDA DE VALORES E O DISCIPLINAMENTO DO CÓDIGO PENAL

Trabalho de Conclusão de Curso apresentado ao Centro de Ciências Jurídicas e Sociais, da Universidade Federal de Campina Grande, em cumprimento dos requisitos necessários para a obtenção do título de Bacharel em Ciências Jurídicas e Sociais.

Aprovada em: 13 de dezembro de 2007.

Jonábio Barbosa dos Santos - UFCG
Professor Orientador

Nome – Titulação – UFCG
Professor(a)

Nome – Titulação – UFCG
Professor(a)

Sousa-PB
Novembro/2007

Primeiramente a Deus, que através de sua onipresença e onipotência me fez chegar até aqui, transpondo os obstáculos que não foram poucos; à minha mãe, Ângela, meu porto-seguro, pelos ensinamentos preciosos que tanto me fortaleceram nos momentos mais difíceis; à minha namorada Patrícia, meu norte, que muitas vezes me compreendeu quando nem mesmo fui capaz disso, que com suas palavras singelas, me fortaleceram a alma e me deram mais esta vitória.

AGRADECIMENTOS

A minha mãe Ângela, a qual todos os meus agradecimentos são insuficientes para expressar a minha satisfação de ser seu filho.

De forma muito especial a meus irmãos, Ana Maria e José Nairton pelo apoio incondicional na conquista desse objetivo, a vocês minha eterna gratidão pelo amor, amizade, carinho, cuidado e companheirismo que sempre dedicaram ao longo da vida.

À minha namorada Patrícia, que sempre ao meu lado, soube me compreender nos momentos mais difíceis, alimentando minha alma com o animo necessário para que não sucumbisse diante das dificuldades.

Aos grandes e verdadeiros amigos, Rômulo, Vivianne, Marília, Armando e Ana Paula, pela confiança e estima que sempre nutriram por mim ao longo desses anos, me fazendo entender o verdadeiro sentido da palavra amizade, que, trilhando comigo essa jornada única e oferecendo dia após dia os melhores incentivos, me deram força para que conseguisse superar os obstáculos, fazendo com que jamais desistisse dos meus objetivos.

De uma maneira especial, a minha grande amiga Danielle Lucena, a quem não faltou o dom de escutar e aconselhar nos instantes mais difíceis pelos quais passei. A você, a irmã mais nova que não tive, a minha eterna gratidão e a satisfação por chamá-la de colega.

E, finalmente, ao Professor Jonábio Barbosa dos Santos, que com maestria e paciência conduziu esta pesquisa, transmitindo dia após dia seus conhecimentos tão valiosos para a busca constante do Direito.

RESUMO

Nos dias atuais, a problemática da punição adequada e efetiva aos chamados criminosos virtuais tem sido discutida de forma veemente. No entanto, a legislação penal pátria por datar de uma época em que sequer existiam computadores, vem sendo atacada por não possuir um dispositivo específico para esse tipo de crime e, dessa forma, em respeito a princípios constitucionais consagrados, não poderia o referido Código ser invocado para a punição desse tipo de delinqüente. Tal situação acabaria por gerar uma instabilidade de conseqüências danosas dentro do crescimento vertiginoso da internet no país. Todavia, posicionamentos já existem no sentido da viabilidade da aplicação da lei vigente para esse tipo de crime, em especial ao denominado estelionato eletrônico. Assim, o objetivo geral deste trabalho é analisar os aspectos jurídicos dos crimes cometidos através da rede mundial, visando enquadrá-los dentro do ordenamento jurídico vigente, apesar dos novos conceitos deles decorrentes, dando ênfase ao estelionato eletrônico. Os objetivos específicos constituem em demonstrar que não há desrespeito aos princípios constitucionais da Legalidade, Reserva Legal, Anterioridade, consagrados pela Carta Magna, ao se invocar o ordenamento vigente para a punição de determinadas condutas praticadas através da rede mundial. Pretende-se, pois, demonstrar que a grande parte das condutas penais cometidas pela Internet aplica-se perfeitamente ao ordenamento em vigor, precisando apenas de pequenas modificações estabelecidas por leis esparsas já vigentes. Apenas um pequeno número de condutas é que precisariam de um ordenamento próprio, o que não é o caso da conduta núcleo deste trabalho, que é o estelionato eletrônico. Para tanto, serão utilizados os métodos histórico-evolutivo e dedutivo, adequados ao desenvolvimento da presente pesquisa, que aborda uma temática atual, controversa e que gera intenso debate na seara jurídica.

Palavras-chave: internet; criminoso virtual; estelionato eletrônico.

ABSTRACT

In today the problem of adequate and effective punishment to criminals called virtual has been discussed so strongly. However, the criminal law for homeland dating from an era that existed even computers, has been attacked for not owning a device specific for this type of crime, and thus, in respect to constitutional principles enshrined, the Code could not be pleaded for the punishment of such Delinquent. This would generate a damaging consequences of instability in the rapid growth of the Internet in the country. However, placements already exist in the sense of the feasibility of applying the law for this type of crime, especially when called estelionato card. Thus, the overall purpose of this work is to examine the legal aspects of the crimes committed by the global network, to frame them within the existing legal system, despite the new concepts derived with an emphasis on estelionato card. The specific objectives are to demonstrate that there is disregard for the principles of constitutional legality, Legal Reserve, Anterioridade, enshrined by the Letter More when invoke the current planning for the punishment of certain behaviors practiced through the worldwide network. Demonstrating that a great part of the criminal conduct committed by the Internet applies to the planning perfectly into force, stating only in small changes sparse already established by existing laws. Only a small number of pipelines that need is a town itself, which is not the case of conduct core of this work, which is the estelionato card. For both, are used methods evolutionary history - and deductive, suitable to the development of this research, which deals with a current topic, controversial and that generates intense debate in the legal harvest.

Word-key: Internet; Criminal virtual; Estelionato Electronic.

SUMÁRIO

RESUMO 05

ABSTRACT 06

INTRODUÇÃO 08

CAPITULO 1 INTERNET: ASPECTOS GERAIS 10

1.1 Origem 11
1.2 Conceito 16
1.3 Aspectos técinicos 16
1.4 Características 18

CAPÍTULO 2 CRIMES DIGITAIS: MOVIMENTAÇÃO INDEVIDA DE VALORES E CÓDIGO PENAL 22

2.1 Generalidades 23
2.2 O Código Penal 26
2.3 Uma questão de interpretação ou de um novo Ordenamento Jurídico? 29

CAPÍTULO 3 ESTELIONATO ELETRÔNICO 35

35

3.1 O Estelionato Eletrônico e os Princípios Constitucionais .....
3.2 Fatores influenciadores do crime 41
3.3 A jurisprudência e o Estelionato Eletrônico 44

CONSIDERAÇÕES FINAIS 47

REFERÊNCIAS 50

GLOSSÁRIO 52

ANEXOS 54

INTRODUÇÃO

A internet é, sem dúvida alguma, o aspecto mais palpável da globalização. As sociedades estão cada vez mais interligadas, formando uma intrincada rede de troca de informações jamais vista ao longo da história humana. Constitui dessa maneira a rede mundial um fenômeno único e cada vez mais consolidado.

O Estado não conseguiu acompanhar essas transformações. Seu gigantismo, sua burocracia, sua morosidade, associada ao crescimento avassalador da rede mundial no país, resultaram num fosso jurídico, isto é, não existe um ordenamento específico para a regulamentação da internet, que logo tornou-se um dos líderes em ocorrências criminais relacionadas com o mundo virtual.

No entanto, esse novo meio de interação precisa ser analisado com atenção especial por parte das ciências jurídicas. Isso se dá em virtude das novas relações oriundas desse novo universo. Torna-se imprescindível um estudo apurado a fim de ajustar o ordenamento jurídico vigente aos novos fatos, fenômeno este que nem sempre é possível, uma vez que em determinadas situações não há um direito positivo que regule determinadas ocorrências.

Ao longo deste trabalho perceber-se-á que significativas partes das condutas penais cometidas através da rede mundial são perfeitamente enquadráveis dentro do nosso ordenamento jurídico, em especial o estelionato eletrônico, apesar de existirem entendimentos em sentido contrário. Apenas para um pequeno número de condutas é que se prescindiria de um novo ordenamento. Esta é a principal celeuma no que concerne a esse assunto e constitui o tema central deste trabalho.

Inicialmente, torna-se indispensável o conhecimento pormenorizado da rede mundial. Sua origem, seu funcionamento, suas características, são alguns pontos que tratará, de maneira nítida, o primeiro capítulo deste trabalho, dando dessa forma uma visão detalhada do

mundo digital. É esse conhecimento técnico que servirá de base para a compreensão dos novos conceitos surgidos da massificação do uso da Internet.

Vê-se, que para certos tipos de crimes altera-se apenas o *modus operandi*. É a mesma conduta cometida de outra forma. O antigo Código Penal aplica-se plenamente ao caso concreto. É o fato do estelionato eletrônico. A obtenção de vantagem ilícita através da rede mundial não descaracteriza o tipo do art. 171 do referido código.

Não estão sendo violados, então, preceitos constitucionais fundamentais, como o princípio da legalidade e o principio da anterioridade da lei penal. É necessário apenas o enquadramento do caso concreto à norma. Destaca-se entre os inúmeros delitos cometidos através da rede mundial o estelionato eletrônico. Uma analise comparativa detalhada é realizada à luz do Código Penal. Estes serão os pontos que o segundo capítulo abordará.

Diante da necessidade ou não de se criar um ordenamento jurídico especifico para esse tipo de delito, tratará o terceiro capítulo da posição dos tribunais sobre a temática. A análise da jurisprudência e das correntes doutrinárias sobre a referida problematização, bem como as formas de integração das normas dentro do universo penal, em respeito ao art. 5º, XXXV da Constituição Federal, atendendo assim aos anseios e garantindo a segurança dessas relações sociais, também constituem o cerne do capítulo.

O tema do presente trabalho é uma análise da legislação brasileira diante das novas modalidades criminais que se avizinham, cometidas pelos novos recursos tecnológicos colocados à disposição da sociedade, em especial no tocante ao estelionato eletrônico. A inexistência de uma legislação específica para tais condutas criminosas vem causando divergências doutrinárias e jurisprudenciais quanto à abrangência e aplicabilidade das leis em vigor, resultando em uma insegurança dentro da sociedade quanto à utilização da rede mundial no país.

CAPITULO 1 INTERNET: ASPECTOS GERAIS

A internet é sem dúvida nenhuma um marco no que se refere às novas tecnologias que despontam para o século XXI. Poucas criações humanas ao longo de sua história tiveram um crescimento tão amplo e célere, no que tange ao aspecto quantitativo e qualitativo como a rede mundial de computadores. É indiscutivelmente um fenômeno sem precedentes no universo das comunicações.

A internet revolucionou de tal forma o universo dos computadores e das comunicações como nenhuma outra invenção foi capaz de fazer antes. Ela é ao mesmo tempo mecanismo de disseminação da informação mundial e um meio para elaboração e interação entre indivíduos e seus computadores, independente de quaisquer obstáculos geográficos. Em decorrência do aprofundamento da integração entre os Estados, com o barateamento dos meios de transporte e comunicações, a internet acabou por proporcionar a sensação de um mundo sem fronteiras. É a globalização que se mostra mais visível e perceptível pela rede mundial de computadores.

Em decorrência desse crescimento os mais longínquos recantos do planeta possuem acesso à rede mundial, transpondo e ultrapassando os obstáculos antes existentes, fossem estes de natureza geográfica ou política. Os computadores tornaram-se uma ferramenta indispensável ao cotidiano das pessoas e do próprio Estado. A importância da informática na sociedade tecnológica é indiscutível. No entanto, seu crescimento deu-se de forma desordenada. O Estado e a sociedade somente agora perceberam as conseqüências da sua omissão.

Dentre as transformações causadas pela internet existe um lado nefasto, onde se pode destacar dentro desse universo, condutas criminosas comuns, como por exemplo, a pedofilia e o estelionato, no qual aqueles que praticam tais crimes têm recebido uma proteção da rede,

visto que crimes cometidos por meio desta são caracterizados pelo anonimato, facilitado pela falta de regulamentação da lei. Tímidas ações vêm sendo desenvolvidas nesse sentido. Entretanto, é imprescindível um esforço conjunto dos governos e da sociedade com o propósito de tornar a internet um ambiente seguro e confiável.

1.1 Origem

Entre as décadas de 1960 e 1970, durante o apogeu do conflito político-ideológico entre os Estados Unidos, defensores do capitalismo, e a União Soviética, defensora do socialismo, o qual foi denominado de Guerra Fria, em virtude de não terem existido combates físicos e sim uma luta econômica, política e ideológica, o governo norte-americano, temeroso em sofrer algum ataque soviético, começou a desenvolver um sistema de proteção no qual seus computadores estivessem interligados, trocando informações entre as bases militares, com a finalidade de garantir o funcionamento de todo o sistema no caso de um eventual ataque inimigo, inexistindo, dessa forma, um centro de comando único.

Dessa forma, o Ministério da Defesa americano estudava como melhor proteger os importantes dados militares, pois, mesmo com um ataque inimigo, não seria possível destruí-los. A única solução viável era uma rede eletrônica de dados no qual estes deveriam estar armazenados em diversos computadores distantes uns dos outros. Quando houvesse modificações, as informações deveriam ser atualizadas em todos os computadores no menor espaço de tempo possível e cada um deles deveria ter várias opções de vias de comunicação com todos os outros. Desta forma, a rede continuaria funcionando mesmo que um computador ou uma via de comunicação fossem destruídos.

De tal modo, criou o governo norte-americano ARPANET (Advanced Research Projects Agency Net), com o objetivo de garantir a segurança de suas informações militares.

Esse sistema assegurava a integridade das informações, uma vez que o tráfego, caso fosse interrompido, automaticamente seria encaminhado para outras conexões.

Com o término da Guerra Fria, a ARPANET tornou-se tão desnecessária que os militares já não a consideravam tão importante para mantê-la sob sua guarda. Deste modo, foi permitido o acesso aos cientistas que, mais tarde, cederam a rede para as universidades, as quais, sucessivamente, passaram-na para as universidades de outros países, permitindo o acesso aos pesquisadores domésticos. Posteriormente, houve a criação de um ramo civil da rede, direcionado para outras áreas de pesquisa e desenvolvimento educacional e tecnológico.

Contudo, a internet como hoje se conhece, como arcabouço de redes interligadas de computadores e conteúdos de multimídia, só se tornou possível pela contribuição do cientista Tim Berners Lee e do Centro Europeu de Pesquisas Nucleares, que criaram a Word Wibe Web, a WWW. Foi a partir desse momento que a rede mundial se universalizou, aumentando exponencialmente sua utilidade.

De acordo com os dados divulgados pela Associação Brasileira de Provedores de Acesso, Serviços e Informações de Internet (ABRANET-2000), quando implementada, a velocidade de acesso era de 4.800 bits por segundo (bps). Uma conexão discada hoje pode ser superior 11(onze) vezes a esse número. Atualmente, percebe-se que o internauta pode perder a paciência quando um *site* demora 30(trinta) segundos para abrir. Mas, há dez anos, era comum uma única página demorar de 15(quinze) a 20 (vinte) minutos para surgir na tela. É o retrato da evolução da Internet na última década.

A internet constitui a principal das novas tecnologias de informação de comunicação (NTICs). O salto tecnológico a que o mundo assiste é gigantesco. A evolução da técnica entre a época dos césares romanos e a do absolutismo europeu foi, em termos, pouco significativa, se comparada ao que se tem visto nos últimos cinqüenta anos. Ao iniciar o século XX, a humanidade não conhecia a televisão nem os foguetes. O automóvel, o rádio e o telefone eram

inventos presentes nas cogitações humanas, mas pouco conhecidos. Ao findar o vigésimo século, já tinha o computador, a internet e as viagens espaciais.

Segundo as informações divulgadas pelo Ministério de Ciências e Tecnologia (1996), no Brasil, o serviço foi inaugurado oficialmente em 1989. Entretanto, somente em 1995 a rede brasileira deixou de ser somente acadêmica, passando a atender também empresas e indivíduos, através de um projeto pioneiro da Embratel, sendo liberada pelo Ministério das Comunicações e da Ciência e Tecnologia no âmbito comercial. A disseminação dos computadores pessoais é, no plano da História, um fenômeno recentíssimo.

O Instituto Brasileiro de Geografia e Estatística (IBGE), registra da década de 1990 a disseminação dos computadores dentro da sociedade brasileira e, ainda assim, apenas os integrantes das classes A, B e C têm suas máquinas domésticas, em virtude de uma série de fatores, como por exemplo, o baixo poder aquisitivo da população.

Em 1988, Oscar Sala, professor da Universidade de São Paulo (USP) e conselheiro da Fundação de Amparo à Pesquisa no Estado de São Paulo (Fapesp), desenvolveu a idéia de estabelecer contato com instituições de outros países para compartilhar dados por meio de uma rede de computadores. Assim, chegou ao Brasil a *Bitnet* (*Because is Time to Network*).[1]

A rede conectava a Fapesp ao Fermilab, laboratório de Física de Altas Energias de Chicago (EUA), por meio de retirada de arquivos e correio eletrônico. O serviço foi inaugurado oficialmente em 1989. Em 1991, o acesso ao sistema, já chamado internet, foi liberado para instituições educacionais e de pesquisa e a órgãos do governo. Nessa época ocorriam fóruns de debates, acesso a bases de dados nacionais e internacionais e a supercomputadores de outros países, além da transferência de arquivos e softwares. No entanto, tudo estava reservado a um seleto grupo de pessoas.

[1] TRADUÇÃO LIVRE: "Porque é tempo de trabalhar em rede".

Em 1992, o Instituto Brasileiro de Análises Sociais e Econômicas (IBASE) assinou um convênio com a Associação para o Progresso das Comunicações (APC), liberando o uso da internet para ONGs. No mesmo ano, o Ministério da Ciência e Tecnologia inaugurou a Rede Nacional de Pesquisa (RNP) e organizou o acesso à rede por meio de um backbone (tronco principal da rede).

Entretanto, apenas em 1993 ocorreu a primeira conexão de 64 (sessenta e quatro) kbps à longa distância, estabelecida entre São Paulo e Porto Alegre. Em 1994, estudantes da USP criaram centenas de páginas na Internet. Os primeiros *sites* brasileiros surgidos eram de notícias. Depois, surgiram os de compras, entretenimento e pesquisa. Assim, a rede nacional começou a crescer. Para o público médio, *e-mail* e as salas de bate-papo (chats) foram dois dos principais carros-chefe para a popularização da Internet.

Em nosso país, a exploração da Web consiste em um mercado bastante promissor. O país apresenta um dos maiores contingentes de internautas de todo o mundo e um considerável número de usuários em potencial. Ao contrário do que ocorre em países europeus e asiáticos, nos quais existem resistências à aceitação da rede, em função da língua dominante ser o inglês, não existe entre os brasileiros qualquer rejeição desta natureza. O principal empecilho à massificação da rede, na nação, continua sendo o elevado custo dos computadores e a baixa renda da maioria da comunidade. Tais fatores, porém, não prejudicam as perspectivas amplamente favoráveis ao desenvolvimento da rede mundial.

A internet, graças aos fatores velocidade, economia e anonimato tem superado em preferência os demais meios de comunicação na esteira do fenômeno globalizante, expandindo-se vertiginosamente a cada dia, em todos os campos de utilização da vida moderna. A cada minuto, milhões de computadores interligam-se por meio das linhas telefônicas no mundo inteiro, fazendo circular bilhões de informações que se traduzem em movimentação financeira, intercâmbio cultural e inter-relacionamento entre pessoas e

instituições de todas as partes e das mais variadas culturas.

Ainda tendo com referência os dados fornecidos pelo IBGE no ano de 2000, em 1999 o número de internautas era superior a 2,5(dois milhões e quinhentos mil). O país contava com 7,68(sete milhões e seiscentos e oitenta mil) usuários de internet em 2002. Hoje, a Pesquisa Nacional por Amostra Domiciliar – (PNAD) mostra que o país se aproxima dos 30 milhões de indivíduos com acesso direto à rede e conta com 18,3(dezoito milhões e trezentos mil) de computadores pessoais. O número de internautas representa 17% (dezessete por cento) da população, ou uma em cada seis pessoas; o brasileiro navega uma média de 14 (quartoze) horas e meia por mês. Tais dados demonstram a dimensão do crescimento da rede no país.

É importante ressaltar, no entanto, que a grande rede não tem existência autônoma. As relações que se desenvolvem nela têm repercussões no mundo real. O virtual e o real são apenas figuras de linguagem, não definindo, de fato, dois mundos diferentes, não dependentes. Em verdade, tudo o que se passa no ciberespaço acontece na dimensão humana e depende dela.

Por conseguinte, a vida *on line* nada mais é do que, em alguns casos, uma reprodução da vida real somada a uma nova forma de interagir no qual representa um diferente modo de vida ou de atuação social que está sujeito às mesmas restrições e limitações ético-jurídicas e morais aplicáveis à vida comum, e que são imprescindíveis à convivência. Tudo tendo em mira que não existem direitos absolutos e que os sujeitos ou atores desse palco virtual e os objetos desejados, protegidos ou ofendidos, são elementos da cultura ou do interesse humano.

Mas a Internet não é só isso, visto que a revolução tecnológica propiciada pelos computadores e a interconexão dessas máquinas em grandes redes mundiais, extremamente capilarizadas, é algo sem precedentes na história humana, acarretando uma revolução jurídica de vastas proporções, que atinge institutos do Direito Tributário, Direito Comercial, Direito do Consumidor, temas de direitos autorais e traz implicações à administração da Justiça, à

cidadania e à privacidade.

Portanto, não é por outra razão que, do ponto de vista cartorial, a internet já conta com uma estrutura legal no País, representada pelo Comitê Gestor da Internet no Brasil, que delegou suas atribuições à FAPESP – Fundação de Amparo à Pesquisa do Estado de São Paulo, e tem regulamentado principalmente a adoção, o registro e a manutenção de nomes de domínio na rede brasileira.

1.2 Conceito

Por internet, compreende-se um conjunto de computadores interligados em escala mundial, utilizando um protocolo de comunicação capaz de permitir o acesso de qualquer máquina a outras, gerando dessa maneira uma infinita base de dados, possibilitando transferências de quaisquer tipos de informações.

Deste modo, esta se constitui em um conglomerado de redes em escala mundial que permite todo tipo de transferências de dados de qualquer natureza. É uma infindável teia de grandes e pequenas máquinas interligadas que se estendem pelo mundo inteiro.

Percebe-se facilmente uma abstração física que gera todo o conceito, ainda que de certa forma inestimável e passível de precisão, da virtualidade, uma vez que todo o conteúdo da Internet é marcado pela informação tecnológica ou digitalizada.

1.3 Aspectos Técnicos

Foi em 1983 que foi estabelecido o TCP/IP (Transmission Control Protocol/ Internet protocol), a linguagem comum usada pelos computadores que integram a rede. É através desse esquema técnico que ocorre o tráfego de informações. No entanto, a internet não funcionava como se conhece hoje. Foi com a criação da chamada WWW, através do mecanismo do hipertexto, que a rede mundial tornou-se sinônimo de praticidade e

entretenimento.

Corrêa (2000, p. 11) conceitua a WWW como:

> A WWW é um conjunto de padrões e tecnologias que possibilitam a utilização da Internet por meio dos programas navegadores, que por sua vez tiram todas as vantagens desse conjunto de padrões e tecnologias pela utilização de hipertexto e suas relações com a multimídia, como som e imagem, proporcionando ao usuário maior facilidade na sua utilização, e também a obtenção de melhores resultados.

A figura do hipertexto é bem simples. Desenvolvido na década de 70, constitui um sistema cujos documentos contêm referências internas para outros documentos (na computação, os *hiperlinks*, ou simplesmente *links*). Foi através desse sistema que a rede ganhou qualidade e quantidade de informações.

Para se tornar usuário da rede, é necessário dispor de um computador, uma linha telefônica e um modem ou um acesso por rádio freqüência. Os dados são transmitidos na forma de *bits* através de fibras ópticas. À medida que as redes de computadores crescem e que o volume armazenado de informações aumenta, emergem novas e engenhosas ferramentas para facilitar a localização e o acesso às informações disponíveis. A atividade mais comum na Internet é a interação com outros usuários, e o mais comum dos meios utilizados é o correio eletrônico (e-mail).

A internet tem uma característica *sui generis* de organização. Ela é um conjunto de redes de computadores operando por diversas organizações (tais como a Internet Society) em mais de setenta países, onde as decisões de natureza tecnológica são tomadas em pequenos comitês de voluntários (como professores universitários e pesquisadores), os quais estabelecem os padrões de interoperabilidade da rede.

Assim sendo, do ponto de vista da infra-estrutura física, a internet é usualmente entendida com apresentação de uma hierarquia em três níveis: no nível inferior estão as redes de dimensão local-LANs, como as redes existentes nos *campi* universitários. Estas redes são conectadas às redes regionais ou de porte médio, como as redes metropolitanas-WANs. Estas

últimas redes conectam-se a um ou mais *backbones* (redes principais ou alicerces), conformando o segundo nível hierárquico. Finalmente, estes *backbones* em um determinado país conectam-se a outras redes de *backbones* em outros países.

1.4 Características

A rede mundial constitui um universo com características peculiares. São inúmeros aspectos que merecem uma análise detalhada que transcendem esse trabalho. Divergências doutrinárias ocorrem no que tange, por exemplo, se o universo virtual merece ou não uma legislação específica, se conceitos antigos aplicam-se sobre os novos delitos oriundos do crescimento vertiginoso e descontrolado da rede, a questão do pseudo-anonimato, pseudo devido já existirem estudos recentes que admitem a possibilidade de identificação do usuário, mediante recursos que, segundo alguns, violam princípios constitucionais.

Uma das características mais marcantes do uso da internet e que merece ser analisado, é o fato da instataneidade, ou seja, a extrema rapidez e mesmo a fugacidade com que são mantidos os contatos mais usuais, tal qual ocorre com as comunicações telefônicas, volatilizando-se seus registros tão logo sejam implementados tais contatos, com ainda uma agravante: o usuário pode e em geral mantém-se mais facilmente no anonimato, não precisando de muitos recursos para preservar sua identidade em sigilo. Ora, naturalmente isso afigura-se como um fator complicador quando o uso socialmente sadio é distorcido e o acesso à internet se presta a servir de meio para a prática de condutas nocivas, algumas delas verdadeiramente criminosas.

As transformações pelas quais passou o Direito ao longo dos séculos foram úteis e relevantes, servindo ao menos para que esse produto cultural, bom ou mau, perdurasse. Mas tais transformações sempre se deram com um certo atraso. Nenhuma delas, contudo, equipara-se à verdadeira revolução jurídica que se avizinha, em conseqüência de uma segunda

revolução industrial, característica da era da informação.

Com o desenvolvimento das novas tecnologias da comunicação, e, principalmente, com o advento da internet, novas questões surgem, demandando respostas do operador do Direito. E, em face da velocidade das inovações da técnica que se vislumbra 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 o ordenamento jurídico nacional e invencível para os profissionais que não se adequarem.

Nesse contexto, os principais problemas que se apresentam são os relativos à necessidade de uma legislação penal para a proteção de bens jurídicos informáticos e de outros, igualmente relevantes, que possam ser ofendidos por meio de computadores. Busca-se também, analisar as questões de tipicidade, determinação de autoria e competência jurisdicional, mormente nos delitos cometidos pela internet, que assumem, em alguns casos, feição de crimes transnacionais, encaixando-se na classificação doutrinária de crimes à distância.

Destarte, será imperioso concluir que, se há lesão ou ameaça a liberdades individuais ou ao interesse público, deve o Estado atuar para coibir práticas violadoras desse regime de proteção, ainda que realizadas por meio de computadores. Isto porque, tanto a máquina quanto a rede, são criações humanas e, como tais, têm natureza ambivalente, dependente do uso que se faça delas ou da destinação que lhes dê. Do mesmo modo que aproxima as pessoas e auxilia a disseminação da informação, a internet permite a prática de delitos à distância no anonimato, com um poder de lesividade muito mais expressivo que a criminalidade dita convencional, em alguns casos.

Embora a internet no Brasil já tenha um certo grau de regulamentação (por meios autônomos e heterônomos), a legislação de informática ainda é esparsa, pouco abrangente e desconhecida. Pior que isso: ainda não há uma cultura de informática jurídica e de Direito da

Informática no País, no sentido da necessidade de proteção de bens socialmente relevantes e da percepção da importância da atuação limitada do Estado no ciberespaço. Isto bem se vê no tocante ao posicionamento da FAPESP, que se dispõe a bloquear um registro de domínio por falta de pagamento, mas costuma exigir dos órgãos investigativos um mandado judicial de bloqueio diante de um crime.

Um dos principais problemas que urge do crescimento descontrolado da internet e que a caracteriza essencialmente é a questão do anonimato. Entre os principais motivos relacionados a esse fator, pode-se relacionar o cadastro falso em provedores, através até mesmo de dados de outrem, dificultando significativamente dessa maneira a identificação de usuários que distorcem e contaminam o universo virtual.

No entanto, evoluções recentes já permitem identificar usuários mal intencionados. Isso se dá através do IP, que constitui uma identidade dentro da rede, apesar de que, em alguns casos, essa identidade pode variar, advindo uma certa dificuldade, mas nada que torne impossível tal identificação. Outro fato que merece ser destacado é a falta de colaboração dos provedores de acesso, que retardam o processo de identificação, vindo a ajudar mediante mandado judicial. Esse retardo favorece tão somente aos criminosos. Dessa maneira, a identificação do criminoso é difícil e demorada, sujeita a variáveis, entretanto não é impossível.

A internet, diante do exposto, acaba por consistir na interligação de milhares de redes de computadores que se encontram espalhados ao redor do mundo inteiro, com a utilização dos mesmos padrões de transmissão de dados, os chamados protocolos. Em razão dessa generalização, onde se estabelece um verdadeiro padrão na transmissão das informações, as diversas redes passam a funcionar como se fossem uma só, possibilitando o envio de dados e até mesmo de sons e imagens a todas as partes do mundo, com eficiência e agilidade ímpares.

Os efeitos da revolução que a internet vai provocar mal começaram a serem sentidos.

Ultimamente, o comércio eletrônico começou a expandir-se a velocidades inimagináveis. Não se poderia prever, até a algum tempo, que as pessoas acabariam se interessando cada vez mais pelo poder de comprar e vender infinita e ilimitadamente. Porém, é o que vem acontecendo a todo o momento; a exemplo disso, podem-se citar as milhares de transações *on line* que são efetivadas instantaneamente por pessoas e empresas em diversas áreas do globo.

Destarte, a Internet tem ainda muito para se expandir. Seja no âmbito comercial, seja no que se refere ao entretenimento. No entanto, faz-se imperioso o maior controle Estatal nessa expansão, uma vez que a rede mundial não pode continuar rotulada como uma terra sem lei, não devendo esta ser utilizada como meio para o cometimento de delitos e sob o argumento de estar sendo assegurada a liberdade de expressão.

CAPITULO 2 CRIMES DIGITAIS: MOVIMENTAÇÃO INDEVIDA DE VALORES E O CÓDIGO PENAL.

A comodidade advinda do crescimento da internet criou uma realidade que não se adequa plenamente ao ordenamento jurídico vigente. A sociedade, ávida por meios que facilitem e estimulem o seu desenvolvimento, tornou-se vítima de sua própria criação.

A informatização crescente das várias atividades desenvolvidas individual ou coletivamente na sociedade veio colocar novos instrumentos nas mãos dos criminosos, cujo alcance não foi corretamente avaliado, pois surgem a cada dia novas modalidades de lesões aos mais variados bens e interesses que incube ao Estado tutelar, propiciando a formação de uma criminalidade especifica da informática, cuja tendência é aprimorar seus meios de execução.

Acirradas discussões giram em torno da aplicabilidade ou não das normas vigentes dentro do universo virtual. Posicionamentos à parte, o certo é que a utilização da rede mundial é cada vez maior, crescendo na mesma proporção o número de delitos realizados por meio da internet; e a não aplicação das normas existentes ou a criação de um ordenamento novo faz que nosso país seja um dos líderes dentro da comunidade internacional no que se refere ao estelionato eletrônico.

2.1 Generalidades

Entre tantos fatos típicos penais oriundos da expansão da internet volta-se à atenção para um em especial: as movimentações indevidas de valores. É o denominado estelionato eletrônico.

Os primeiros registros desse tipo de crime em nosso país datam do final da década de 90, onde misteriosos desaparecimentos de valores de contas bancárias movimentadas pela internet eram noticiadas pela imprensa. O fato interessante é que os golpistas não roubaram os cartões magnéticos e tampouco as senhas.

Num primeiro momento, tais crimes eram cometidos apenas com o intuito de conseguir invadir *sites* ditos seguros. Agora, diante da possibilidade de obtenção de vantagem financeira ilícita sem a necessidade de uso de força ou violência, usando apenas um computador e um mouse, os criminosos mudaram de intuito. São inúmeras vantagens sem grandes riscos.

A internet transformou-se num ambiente de vasta riqueza. Tanto pelo comércio eletrônico, como através de movimentações financeiras, onde vultuosas quantias valores trafegam diariamente pela rede, através de um simples apertar de tecla. E de acordo com o brocardo, onde há riqueza há criminosos, e a rede mundial acabou por despertar o interesse dos delinqüentes. Também contribui para esse tipo de ilícito fatores como o anonimato, a instataneidade das operações, legislação deficiente, entre outros.

Segundo estatísticas da Polícia Federal, os assaltos virtuais já superam em muito os assaltos às agências. O departamento de serviços periciais e informática do referido órgão divulgou recentemente que um assalto a um a agência são levados em média R$ 30(trinta) mil e os assaltantes tem 75% (setenta e cinco por cento) de chance de serem presos; nos assaltos virtuais, os valores desviados são em média R$ 1.5(hum milhão e quinhentos mil) e o risco de prisão é de 5%(cinco por cento).

De acordo com a Associação Brasileira das Empresas de Cartões de Crédito e Serviços — ABECS (2000), as perdas com fraudes no ano passado atingiram R$200(duzentos) milhões. No ano anterior, o prejuízo foi de R$ 260(duzentos e sessenta) milhões e, em 1998, de R$300(trezentos) milhões. A ABECS tem se preocupado com os cibercrimes praticados

mediante o uso fraudulento de cartões de crédito e está introduzindo no mercado os cartões com chips eletrônicos, que têm alto nível de segurança.

De acordo com a Federação Brasileira de Bancos – FEBRABAN (2003) – as transações por meio da internet cresceram 117%(cento e setenta e sete) em 2002 se comparados a 2001. Diante de tal crescimento, viu-se também o surgimento dessas novas modalidades de roubos, como o envio de e-mails falsos para induzir os clientes a informar suas senhas, e outros dados pessoais. Nesses casos os fraudadores desenvolvem programas de captura desses dados que se instalam quando o e-mail é aberto e permanece na máquina imperceptível pelo usuário.

As dimensões da rede mundial e a quantidade de informações nela contidas consubstanciam-se em empecilhos a um controle mais rígido das relações travadas em seu ambiente. A superveniência de normas com a função teleológica de impor uma maior fiscalização, um maior controle sobre as operações na Internet, pode resultar na ineficácia da lei correspondente, tendo em vista as características dessa forma revolucionária de comunicação.

A atuação por meio do computador requer investigação especializada e ação efetiva. Há raríssimos policiais no Brasil preparados para combater esse tipo de crime, e geralmente estão lotados em seções cuja especialidade é diversa dos conhecimentos muitas vezes adquiridos por iniciativa própria e não por políticas internas (administrativas) de qualificação de pessoal.

Os raros investimentos que são feitos na área de qualificação em termos digitais restringem-se a: de um lado, preparar pessoal apto a manusear dados eletronicamente, tais como arquivos e sistemas internos, transmissão eletrônica de dados, coleta de informações em bancos de dados internos, ou seja, restringem-se à atuação na área digital as intranets que constituem as redes internas e nas necessidades de compilação e consulta instantânea; de

outro lado, qualificar servidores para atuar na elaboração de laudos periciais específicos, característicos da área de criminalística, tais como a decodificação de senhas e/ou arquivos de computadores usados para cometer ilícitos ou que contenham matéria probante relacionada a inquéritos ou processos em andamento, visando à obtenção de evidências fáticas a partir de apreensões autorizadas.

Percebe-se assim que as iniciativas na área pública relacionadas à informática restringem-se ao treinamento de servidores para serem digitadores, arquivistas, usuários de sistemas de dados de um lado, ou aptos a perfazerem autópsias eletrônicas.

No que se refere ao combate a crimes perpetrados via internet, malgrado as iniciativas de estudo e deliberação de cunho exclusivamente normativo, de intercâmbio cultural, ou de tímidas investidas oficiais na área de segurança e proteção, tão somente, não se percebe ousadas alterações estruturais ou de atribuição no campo específico dos crimes de internet. Está faltando visão, planejamento, preparo e treinamento nessa área específica, na polícia brasileira.

Paralelamente, empresas em diversos pontos do País, públicas e privadas, têm sido vítimas dos crimes cometidos através de computadores, e a gravidade da questão é mascarada pela síndrome da má reputação, que leva tais empresas a assumirem os prejuízos, encobrindo os delitos, temendo uma propaganda negativa ou um estímulo a outros delinqüentes do gênero. Consideram ainda que o grupo de criminosos digitais atuando no Brasil ainda é pequeno, restrito aos que dominam idiomas estrangeiros e detém tecnologia de ponta e habituados à área financeira.

Como se pode notar, parece haver uma encruzilhada jurídica, pela dificuldade de delimitar o verdadeiro sentido e alcance das normas jurídicas eventualmente aplicáveis a esse vasto campo que se abre com a utilização da internet. O que não tem impedido iniciativas individuais no sentido de coibir os comportamentos daninhos.

Com efeito, a par do incipiente equacionamento legal do tema, as medidas preventivas e repressivas das distorções do uso socialmente saudável da internet caminham independentes e já surtem efeitos. Por iniciativa de vários grupos, tais esforços servirão de base para que este direito difuso internacional, que hoje dissolve todas as barreiras tradicionais, possa firmar-se amoldando-se, se não em leis, pelo menos em princípios.

Vislumbra-se os direitos advindos do uso pacífico das infovias como mais um interesse difuso, na medida em que, a exemplo da defesa do consumidor e do meio ambiente, também atingem um grupo indeterminado e indeterminável de pessoas. Considerando que a solução individual e a coletiva são insuficientes para resolver juridicamente esta questão, considera-se necessário desenvolver mecanismos adequados para operacionalizar sua prevenção e seu ressarcimento.

2.2 O Código Penal

Com o desenvolvimento da internet, novas questões surgem, demandando respostas do operador do Direito. E, em face da velocidade das inovações da técnica que se comtempla 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.

No Brasil, a Lei n. 7.646 dispôs sobre a proteção da propriedade intelectual sobre os programas de computador e sua comercialização no país. Algumas dessas disposições, no entanto, foram modificadas e/ou revogadas pela lei n. 9.609/98 (ANEXO A), que veio por substituí-la. No entanto, tais normas não dispuseram sobre as principais questões que hoje envolvem o tema, notadamente sob o enfoque do direito penal em si. Segundo parte da

doutrina, o nosso Código Penal de 1940, acompanhado por um número muito grande de outras leis esparsas não se mostra suficiente nem adequado para o tratamento desses novos crimes. Esses crimes vêm sendo praticados de variadas formas e com uma gama notável de diversidades.

Assim, tê-se visto manipulações nos caixas de instituições financeiras, pirataria de programas (*softwares)*, nas próprias redes de telecomunicações, além de outras inúmeras façanhas realizadas por *hackers*. Tudo isso revela a vulnerabilidade do sistema informático como um todo.

Deveremos considerar, como pressupostos, alguns dispositivos constitucionais, a saber:

> a) O art. 5°, inciso II, segundo o qual ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei;
> b) O art.5°, inciso X, que considera invioláveis a intimidade, a vida privada, a honra e a imagem da pessoas, assegurado o direito à 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 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 de direito, na forma do art.5°, inciso XXV, da Constituição Federal; e
> e) A garantia segundo a qual Não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal!(inciso XXXIX, art.5°).

Optando o Estado brasileiro pela diretriz da legalidade e em prol do princípio da inafastabilidade da jurisdição, inclusive na internet, afastando já aqui dois dos mitos muito divulgados nos primeiros tempos do ciberespaço: o de que a internet não podia ser regulamentada pelo Estado e o de que haveria liberdade absoluta nesse ambiente.

Destarte, será imperioso concluir que, se há lesão ou ameaça a liberdades individuais ou ao interesse público, deve o Estado atuar para coibir práticas violadoras desse regime de proteção, ainda que realizadas por meio de computadores. Isto porque, tanto a máquina quanto a rede são criações humanas e, como tais, têm natureza ambivalente, dependente do

uso que se faça delas ou da destinação que se lhes dê. Do mesmo modo que aproximam as pessoas e auxilia na 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 dita convencional, em alguns casos.

Em face dessa perspectiva e diante da difusão da internet no Brasil, o Estado deve prever positivamente os mecanismos preventivos e repressivos de práticas ilícitas, na esfera civil e penal, e os órgãos de persecução criminal (a Polícia Judiciária e o Ministério Público) devem passar a organizar setores especializados no combate à criminalidade informática.

Assim já vêm fazendo, no Rio de Janeiro, o Ministério Público Estadual, que instituiu a Promotoria Especializada em Investigações Eletrônicas, e também a Polícia Federal, que criou o Departamento de Crimes por Computador, que funciona no Instituto Nacional de Criminalística, em Brasília e a nível nacional destaca-se a atuação do Conselho de Controle de Atividades Financeiras (COAF), criado em 1998 com a finalidade de monitorar inicialmente a lavagem de dinheiro, tendo posteriormente ampliada suas atribuições, passando a acompanhar a vida financeira dos cidadãos.

O que se percebe na área da informática é que a maioria dos ilícitos que têm previsão nas legislações penais e no próprio Código Penal podem ser praticados pelo instrumento computador. Destarte podemos, v.g., apontar o estelionato, cuja figura típica consiste na obtenção de vantagem ilícita com prejuízo alheio mediante a utilização de inúmeros expedientes que se alteram com a criatividade do autor-executor. Ora, obviamente, se é praticada a conduta com o uso do computador, o agente está incurso nas penas do dispositivo penal, sendo descipiendo criar-se uma nova figura penal a fim de se coibir à conduta ilícita.

É certo que há ocasiões e haverá hipóteses específicas na área da informática em que será necessária a criação do tipo legal, até mesmo para a fiel observância do princípio da legalidade. Mas, com certeza, a maioria das condutas já tem essa mesma previsão, alterando-

se tão-somente a forma, o instrumento da prática delituosa, infrações contra o patrimônio (artigos 155 a 183 do nosso Código Penal), infrações contra a inviolabilidade de correspondência (artigos 151 e 152 – e aí poderíamos incluir o e-mail).

Certas condutas criminosas na área da informática, com certeza, merecem ser positivadas, com previsão em leis penais e mesmo no Código Penal. É, aliás, o que se pode observar visto em alguns países, como é o caso da Itália (lei 547, de 23 de Dezembro de 1993), de Portugal (lei n. 109 de 17 de Agosto de 1991), além de outros.

As medidas do Legislativo, adotadas até o momento, contudo, revelam-se absolutamente insuficientes para atribuir solidez às relações travadas por meio da rede. Certo que diversos diplomas legais podem ser perfeitamente aplicáveis nas relações em tela. A título de ilustração, cite-se o Código de Defesa do Consumidor e as regras de direito autoral. A tendência mundial, entretanto, consiste na formulação de regras específicas para a regulamentação das operações realizadas pela rede mundial.

2.3 Uma Questão de Interpretação ou de um novo Ordenamento Jurídico?

Trata-se de característica fundamental do ordenamento jurídico o dinamismo de seus preceitos, que permite a adequação das normas jurídicas às constantes evoluções nos diversos campos da atividade humana. Seria temerário se o Poder Legislativo restasse inerte aos relevantes fenômenos sociais, por não editar os ditames legais a reger as novas situações de fato.

Ressalva-se que, evidentemente, seria impossível abranger no texto legal todos casos que se possam verificar em concreto. Por este motivo, nos casos de lacunas na legislação, o próprio ordenamento dita os meios a supri-lo, uma vez que o Judiciário não pode escusar-se de apreciar a questão sob a alegação de falta de disposição legal quanto à matéria. Não se

demonstra coerente, porém, que os operadores do direito vejam-se obrigados a utilizarem, por longo lapso temporal, as fontes subsidiárias para a resolução das celeumas. A necessidade de criação da norma pode ser indicada por diversos fatores, dentre estes, a conjectura econômica, política ou social do país.

Diante destas considerações iniciais, propõe-se breve análise da atuação do legislador pátrio, no que se refere a uma das maiores revoluções na comunicação em toda a história da humanidade: a internet. Recente lei (Lei n. 9.800/99) preceitua sobre a possibilidade do envio de petições para o Poder Judiciário através de mensagens eletrônicas. Encontra-se, também, em tramitação no Congresso Nacional, projeto de lei (n. 1589/99), o qual versa sobre o *spam*, ou seja, mensagens indesejadas ou não solicitadas, via e-mail. O conteúdo do referido projeto de lei revela-se satisfatório, já que determina que aqueles que optarem por esta modalidade de envio devem informar sobre o que a mensagem aborda.

A breve recepção do citado projeto no ordenamento jurídico demonstra-se salutar, na medida em que observa-se atualmente a proliferação do acesso gratuito à rede mundial. Revela-se notório que a percepção dos lucros por parte das empresas que disponibilizam este serviço dar-se-á por meio da vinculação de propaganda. Assim, nada mais conveniente do que regularizar a forma de envio das mensagens aos usuários da internet.

O Projeto de Lei n. 22 do Senado dispõe acerca dos documentos produzidos e armazenados em meio eletrônico. Outro Projeto de Lei, PL n. 148, trata da assinatura digital e fatura eletrônica. Os temas de ambos os Projetos de Leis correspondem a aspectos fundamentais para a validade jurídica dos documentos formulados e subscritos na internet.

As medidas do Legislativo, adotadas até o momento, contudo, revelam-se absolutamente insuficientes para atribuir solidez às relações travadas por meio da rede. Certo que diversos diplomas legais podem ser perfeitamente aplicáveis nas relações em tela. A título de ilustração, cita-se o Código de Defesa do Consumidor e as regras de direito autoral. A

tendência mundial, entretanto, consiste na formulação de regras específicas, uma vez que os países desenvolvidos, bem como os vizinhos argentinos, já possuem regras jurídicas próprias para os serviços *on-line*.

Deve-se analisar também que a questão da criminalidade virtual como um problema de todo o globo. Em decorrência da interconectividade oriunda do processo de globalização, quando as pessoas em diferentes países estão compartilham informações em tempo real, os crimes de informática tendem a assumir efeitos internacionais. Por isso, não há como negar que se tratam de crimes transnacionais por excelência, isto é, crimes cuja pratica e/ou cujos efeitos diretos ou indiretos envolvem mais de um país.

Dessa forma, o esforço isolado de um ou de alguns países não é o suficiente para coibir a pratica desse tipo de crime. Tornam-se imprescindíveis atitudes conjuntas por parte da comunidade internacional para a solução desse problema.

Não obstante todos os países não tenham criminalizado tais condutas, destaca-se a postura que a Organização das Nações Unidas vem tomando com o intuito de mobilizar os países para a elaboração de um tratado, no qual seriam indicados os mecanismos a serem estabelecidos para prevenir e investigar esse tipo de delito, bem como a celebração de acordos prevendo a adoção de medidas de cooperação, treinamento e combate de tais práticas entre as autoridades legais dos países signatários.

No Brasil, existe um descompasso Legislativo que envolve tanto a Constituição Federal de 1988, visto que a rede mundial somente em 1995 ganhou destaque, como também as normas infraconstitucionais, que ainda esparsas, regulam pontos específicos, como a Lei n. 9.609/98, que regula a propriedade intelectual de programas de computador, deixando dessa maneira os aplicadores do direito sem um norte quanto à punição para esse tipo de delito.

Alguns dos atos ilícitos e típicos efetivados na rede podem ser caracterizados como um dos crimes previstos no vigente Código Penal. Recentemente, contudo, um preocupante

ataque de *hackers* representou alerta para todos aqueles que investem seus rendimentos e a própria carreira na internet. Mister torna-se a previsão legal da transgressão descrita.

O ataque clandestino aos dados de uma empresa ou corporação pode ter implicações danosas a um extenso número de indivíduos. Não há como qualificar de forma idônea a ação dos *hackers* com algum dos tipos penais inseridos no Código Penal. O legislador deve considerar o grau de ofensa da conduta correlata e cominar os limites da penalidade à qual será submetido o agente. Assim, ao se estipular punição severa a estes criminosos, pode-se coibir a atuação dos piratas da internet.

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

Com a normatização das operações em tela, atribuir-se-ia maior segurança às mesmas, fator que propiciaria a captação de novos investimentos para o setor. Além disso, os profissionais do direito não teriam que utilizar de criatividade e princípios gerais do direito para defender os interesses de seus constituintes, nas causas que versam sobre a rede mundial de computadores.

Urge-se, assim, breve iniciativa das autoridades competentes, a fim de que sejam elaborados e discutidos novos projetos de lei voltados à regência das operações via internet, este inovador e fantástico veículo de informações.

Intenso é o debate entre os doutrinadores a cerca da necessidade ou não da criação de um ordenamento jurídico especifico para a regulamentação em nosso país da rede mundial. No entanto, o entendimento predominante dos juristas pátrios é o fato de que para certos tipos penais, como o elencado no *caput* do art. 171 do Código Penal, logo transcrito:

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

É plenamente aplicável ao estelionato cometido via computador, sendo este apenas o meio como delito foi cometido. O prejuízo em si é o mesmo, independentemente do meio utilizado, mudando apenas o meio técnico para o cometimento do delito.

No entanto, lacunas na lei existem e merecem uma atenção do nosso legislador o mais rápido possível. Carece nosso Direito de uma nova lei que regule o tema e venha a proteger os bens jurídicos ligados à informática, criando novos tipos penais, uma vez que existem inúmeros conceitos novos que precisam ser definidos a fim de que se possa punir de maneira adequada esse tipo de delinqüente, ficando a cargo do julgador a aplicação da pena ao caso que foi apresentado, sob pena, de se assim não o fizer, descumprir princípios constitucionais, como o que garante o cumprimento da função jurisdicional a todos que a ela recorrer.

Destarte, diante do artigo 5º, em seu inciso XXXV, já transcrito anteriormente, não pode o indivíduo ter seu direito violado em decorrência da omissão do poder estatal, devendo obter resposta jurisdicional para a sua demanda. Tem-se ainda como fundamento para a atuação do Estado-Juiz o art. 4º da Lei de Introdução ao Código Civil, que é bastante claro ao elencar: Quando a lei for omissa, o juiz decidirá o caso de acordo com a analogia, os costumes e os princípios gerais do direito.

Vale ressaltar, no entanto, que no campo penal o aplicador do direito não possui a mesma liberdade de integração das normas que possui em relação a outros campos jurídicos. A analogia, por exemplo, somente poderá ser utilizada no âmbito penal para beneficiar o réu. Essa é apenas uma das limitações dentro do âmbito penal no que diz respeito à integração das normas. Existem inúmeros outros exemplos que poderiam ser citados, merecedores de uma análise mais ampla que, no entanto refutariam aos objetivos desta obra.

Assim, é imprescindível a tomada de ações enérgicas por parte do Estado brasileiro para coibir esse tipo de delito. É preciso inicialmente atualizar nossa legislação, sendo criando novos tipos penais, seja adaptando os já existentes para os crimes em tela, a fim de que possa tornar a rede mundial um ambiente seguro e confiável.

CAPITULO 3 ESTELIONATO ELETRÔNICO

O crescimento veloz e desordenado da rede mundial em nosso país, ainda carente de um maior controle estatal, seja através de uma legislação, seja através de uma estrutura física adequada, vem resultando no crescimento de práticas delituosas realizadas pela Internet cada vez mais danosas à sociedade e ao governo, transformando dessa maneira a internet em um ambiente instável e de perspectivas sombrias.

Os crimes virtuais já não são casos esporádicos. Cresceram de tal maneira que precisam de uma atenção especial por parte do Estado. Não podem continuar sendo tratados como ocorrências de segunda classe dentro do universo da segurança pública, merecendo um tratamento singular para que possam ser efetivamente coibidos.

Os prejuízos decorrentes dessas condutas são cada vez maiores, atingindo toda a sociedade, não acompanhado as autoridades esse crescimento. Não apenas os detentores de grandes valores que estão ameaçados como outrora: o pequeno correntista também passou a ser alvo desses criminosos.

Dessa forma, devem os órgãos estatais atuar de maneira mais firme nesse campo, estabelecendo marcos regulatórios sólidos, determinando quais condutas devem ser proibidas e quais podem ser permitidas no universo da rede mundial, fazendo assim com que o julgador, no caso concreto, não se desvie da sua atribuição principal, que é aplicar a justiça, para regular ou integrar as normas penais, em virtude da omissão do legislador, funções estas que estas que extrapolam seu mister.

3.1 O Estelionato Eletrônico e os Princípios Constitucionais

Na hierarquia do ordenamento jurídico pátrio, tem de ser respeitada a supremacia da Carta Magna, uma vez que, ocupando o ápice do ordenamento jurídico, é ela que estabelece os parâmetros que devem ser seguidos por toda a legislação infraconstitucional.

Partindo dessa premissa, é necessária a análise de alguns princípios constitucionais que, no âmbito penal, constituem verdadeiras garantias, com o intuito de verificar se os meios de integração das normas na situação em tela violam os preceitos estabelecidos pela Constituição Federal de 1988. É o Estado Democrático de Direito que, através de suas diretrizes, protege o cidadão das eventuais arbitrariedades do Estado.

Destaca-se o Principio da Legalidade entre os vários trazidos no bojo da Constituição Federal de 1988. Nascido para proteger a sociedade de estadistas autoritários, pode ser facilmente compreendido pelo brocardo o que não for proibido é permitido. É o inciso II, do artigo 5º, ora transcrito: ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude da lei.

Deste importante principio, decorre dois outros não menos importantes, que são imprescindíveis para uma melhor análise da situação ora em foco: Reserva Legal e Anterioridade da Lei. É o artigo 5º da supracitada Constituição, em seu inciso XXXIX, a seguir: não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal.

Assim, é tão somente a lei em seu sentido estrito, decorrente de um processo legislativo adequado para a sua aprovação, assim como também deve esta vigorar anteriormente ao cometimento do delito, que tem o condão de proteger determinados bens jurídicos; caso contrário, estar-se-ão violando preceitos constitucionais. De maneira brilhante, Alexandre de Moraes expõe as razões históricas e filosóficas para que a função legiferante

deva ser atribuição exclusiva do Poder Legislativo, garantindo dessa maneira maior segurança ao cidadão (2003, p.69):

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

É diante de tais princípios que gira toda a celeuma dos crimes digitais, uma vez que, para determinadas condutas existe previsão legal, como é caso daquela descrita no art. 155 do CP. O fato de ter sido utilizada a rede mundial para a subtração de determinada quantia de uma conta corrente, por exemplo, não desnatura a conduta do referido artigo; para outras, no entanto, não há previsão legal, sendo, portanto condutas atípicas dentro do universo penal e, em respeito aos princípios constitucionais, não podem se penalizadas.

No entanto, já constitui entendimento predominante que o diferencial nesse tipo de crime não é o tipo penal em si, nem mesmo os conceitos incidentes sobre este; a inovação está no *modus operandi.* O resultado alcançado com a conduta independe da abrangência jurídica atribuída a *res.*

Em que pesem as considerações de que a lei material penal deve ser interpretada restritivamente, proibida a extensão analógica, o revés de tal interpretação, para o Direito de Informática, ausente qualquer traço análogo, o dinheiro retirado de uma conta corrente via internet é furto como outro qualquer, diferenciando-se apenas quanto à maneira e quanto ao agente que pratica o delito.

Constitui dessa maneira o estelionato eletrônico a mesma conduta prevista no art. 171 do Código Penal. Não fere os princípios constitucionais da legalidade e os dele decorrentes. O

fato de ter sido o computador usado como meio para o cometimento do ilícito em nada altera o preceito primário ou secundário da norma em tela.

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

De fato, inúmeras condutas criminosas praticadas por esse instrumento ainda podem perfeitamente ser incursas em dispositivos do nosso velho Código Penal. Evidentemente, há outras que dependerão, para que tenham força coercitiva, de novas previsões e definições legais.

Há ilícitos perfeitamente enquadráveis no Código Penal pátrio e legislação extravagante, quais sejam aqueles em que a internet, ou outro ambiente eletrônico, informático ou computacional, é tão-somente o seu meio de execução, estando a tipificação perfeita ao ato proferido; são estes os crimes eletrônicos.

Constituem exemplos de crimes eletrônicos a exposição em *sites* de Internet de fotos pornográficas com crianças ou adolescentes - enquadrando-se no art. 241 do Estatuto da Criança e do Adolescente - pedofilia; bem como o plágio de textos de terceiros e sua publicação em um *site*, caso em que há violação ao direito de autor - art. 184 do Código Penal.

Estes crimes, cometidos pelo meio eletrônico, não necessitam de legislação específica, pois já se encontram sob a égide da legislação vigente. Alguns necessitam apenas de ligeiras mudanças, para se adaptarem à sua consumação via internet.

Entretanto, há aquelas condutas em que o objeto da ação lesa direito relativo a bens ou dados de informática e estes em sua maioria não encontram tipificação em nosso

ordenamento jurídico; são os chamados crimes informáticos, nada obstando que um crime informático seja perpetrado pelo meio eletrônico - o que, aliás, corriqueiramente acontece. É o caso do acesso indevido de *hackers* a computador de terceiro, que atualmente não encontra amparo criminal, mas às vezes se tenta qualificar, para esfera cível, como invasão de privacidade; em que se pese, existem opiniões contrárias.

Com propriedade, ao se falar de ilícito eletrônico ou informático, a conduta, mesmo que não prevista em lei penal, pode ensejar reparação cível, com multas variáveis de acordo com o resultado obtido, a ser estipulada pelo juiz. Assim, aqueles que se sentirem lesados por atos de terceiros, advindos da Internet, podem intentar ações judiciais cíveis, em que se requer a devida reparação, geralmente sob a forma de multa.

Dessa forma, são crimes que podem admitir sua consecução no meio cibernético: calúnia, difamação, injúria, ameaça, divulgação de segredo, furto, dano, apropriação indébita, estelionato, violação ao direito autoral, escárnio por motivo de religião, favorecimento da prostituição, e ato obsceno escrito ou objeto obsceno.

Como também a incitação ao crime, apologia de crime ou criminoso, falsa identidade, inserção de dados falsos em sistema de informações, adulteração de dados em sistema de informações, falso testemunho, exercício arbitrário das próprias razões, jogo de azar, crime contra a segurança nacional, preconceito ou discriminação de raça, cor, etnia, etc, pedofilia, crime contra a propriedade industrial, interceptação de comunicações de informática, lavagem de dinheiro e pirataria de software.

Na área da Informática, especificamente, várias mudanças ainda estão por ocorrer. Há inclusive uma preocupação em escala mundial da conceituação básica e da adoção de uma terminologia básica para esse campo. Mesmo a noção de documento vem sendo veementemente objeto de digressões doutrinárias e mesmo jurisprudenciais. De fato, veja que, no âmbito mundial, na área do comércio internacional, a comunidade internacional tem-se

engajado na elaboração de um modelo de lei universal sobre comércio eletrônico e acaba apontando a importância para uma lei paradigma, que defina o que seja esse comércio eletrônico. No Brasil, já há um projeto de lei que define certos conceitos desse novo Direito da Informática.

Diz o artigo primeiro do projeto de lei n. 2.644 de 1996 (ANEXO B): Art. 1° Considera-se documento eletrônico, para os efeitos desta Lei, todo documento, público ou particular, originado por processamento eletrônico de dados e armazenado em meio magnético, optomagnético, eletrônico ou similar. Vê-se que o tradicional conceito de documento e stá mudando para dar lugar a uma nova forma de visualizar uma relação jurídica. Não se deve esquecer, não obstante, que o princípio básico do direito penal é justamente o da legalidade lapidado na expressão latina *nullum crimen nulla poena sine praevia legem.*

Pela *web* e no ciberespaço circulam valores, informações sensíveis, dados confidenciais, elementos que são objeto de delitos ou que propiciam a prática de crimes de variadas espécies.

Nas vias telemáticas, transitam nomes próprios, endereços e números de telefone, números de cartões de crédito, números de cédulas de identidade, informações bancárias, placas de veículos, fotografias, arquivos de voz, preferências sexuais e gostos pessoais, opiniões e idéias sensíveis, dados escolares, registros médicos e informes policiais, dados sobre o local de trabalho, os nomes dos amigos e familiares, o número do *IP — Internet Protocol)*, o nome do provedor de acesso, a versão do navegador de Internet (*browser*), o tipo e versão do sistema operacional instalado no computador.

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, respeitando dessa forma os princípios estabelecidos pela Constituição.

3.2 Fatores Influenciadores do Crime

A internet nada mais é do que a interligação simultânea de computadores de todo o planeta, constituindo verdadeira forma e fonte de poder, sendo seu domínio e disponibilidade de uso um verdadeiro patrimônio econômico, político e cultural, dado o valor estratégico proporcionado pela Informação.

Entretanto, nem tudo são rosas nesse mundo digitalizado, e ao lado dos benefícios surgiram os crimes e os criminosos digitais, proliferando-se na mesma razão por todo o mundo, sendo que mesmo as mais otimistas previsões apontam para um epidêmico e exponencial crescimento. Tais crimes, também chamados de crimes digitais ou transnacionais, podem afetar dezenas de países, sem que o agressor sequer saia de sua casa, mesmo estando em outro extremo do planeta.

Esta peculiaridade tem preocupado e chamado à atenção das polícias de todo o mundo, em especial no que diz respeito à materialidade e à coleta de evidências, localização do agente, como adequar a conduta típica a nossa legislação positiva, como agir diante dos princípios da territorialidade e da soberania. Estas são algumas características que torna o estelionato eletrônico e os demais crimes digitais delitos *sui generis*, mesmo no caso de ser plenamente aplicável o ordenamento em vigor ao caso concreto.

A experiência tem mostrado o quão delicada é uma investigação de crimes por computador, seja pela falta de experiência policial, seja pela adoção de procedimentos desatualizados para a alta tecnologia empregada.

O perfil do criminoso, baseado em pesquisa empírica, indica pessoas jovens, inteligentes acima da média, educados, com idade entre 15 e 32 anos, do sexo masculino, magros, caucasianos, audaciosos e aventureiros, 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 que agiram, simplesmente, por brincadeira.

Ademais, têm preferência por ficção científica, música, xadrez, jogos de guerra e não gostam de esportes de impacto. As condutas do delinqüente típico de informática geralmente passam por três estágios: o desafio, o dinheiro extra e, por fim, os altos gastos e o comércio ilegal.

Tal perfil dificulta sobremaneira, especialmente em se tratando de menores inimputáveis, que o cyber-criminoso seja surpreendido em flagrante ou mesmo que se suspeite dele. Imagine-se um estudante universitário, por exemplo, que trabalhe num Departamento de Processamento de Dados de uma universidade ou ainda um jovem digitador em uma instituição financeira, cometendo crimes contra seus empregadores e se terá uma dimensão alarmante da questão.

Cabe ressaltar que a internet é hoje 80% (oitenta por cento) comercial (IBGE 2006), e as campanhas preventivas ou educativas são extremamente incipientes, além de não serem lucrativas. Os resultados assim, de tais iniciativas, mostram-se na maioria das vezes inócuos e restritos, considerando-se ainda o fato de não ser o tema ainda prioritário na maioria dos países, a exemplo da questão do meio ambiente, que enfrenta desafios semelhantes.

As iniciativas de combate aos crimes registrados têm-se limitado a contra-ataques e ações de caráter repressivo ou de assistência a vítimas, sejam pessoas ou instituições. Diante do impacto da alta tecnologia, a perspectiva de alívio é dada pela constatação de que, em recente passado, tecnologias novas provocaram aflição -tais como quando da invenção do telefone, do fax e outros aparelhos que vieram a aumentar a qualidade de vida do cidadão -, mas que logo foram assimiladas.

Cabe aqui fazer uma observação quanto ao importante papel representado em nosso país pelos provedores de internet, no que se refere à sua responsabilidade social, muito

semelhante a dos meios de comunicação, uma vez que são estes quem viabilizam originariamente a conexão do usuário com a internet, possibilitando o tráfego de dados bidirecional.

Tal papel, ao contrário do que muitos advogam, não deve ser exercido de maneira leviana, a título de livre hospedagem e fluxo de conteúdo, devendo ser disciplinada por um mínimo ético e em colaboração com compromissos de ordem legal, social, empresarial ou educativa a que estão submetidas por imperativo legal ou de consciência as mais diversas associações de classe ou categorias profissionais, visando reprimir condutas nefastas.

Diversos projetos de Lei que tramitam pelo Congresso Nacional, como por exemplo, o de autoria do senador Eduardo Azeredo (PSDB – MG), que se encontra atualmente na Comissão de Constituição e Justiça, aguardando deliberação, atribui responsabilidades aos provedores de acesso à rede mundial que constituem uma verdadeira afronta aos princípios constitucionais do sigilo e inviolabilidade das informações. Por tal projeto de lei, os provedores passam a ser vigilantes da rede, monitorando e controlando todos os acessos de seus clientes.

Dessa forma, mostra-se um equívoco a atribuição de responsabilidades aos provedores, pelo menos da forma como consta no referido projeto, como se fossem os únicos responsáveis pela segurança da rede mundial, como forma de coibir os delitos pela rede, em especial o estelionato eletrônico. Não se trata de isentar tais empresas de suas responsabilidades, mas o peso de tal atribuição, que seja, garantir a segurança da rede, deve ser atribuição também do Estado e da sociedade como um todo.

Notória é a colocação de Liliana Minardi Paesani em sua obra Direito e Internet (2000; p. 90), ora transcrita, sobre a excessiva responsabilidade atribuída aos provedores para a segurança da rede:

> Não é com uma histérica caça as bruxas que se protegem os menores ou se garante a segurança na rede. O instrumento viável é um só: a vigilância dos pais e educadores. Essa orientação deveria se destinar também a outras áreas das novas

> técnicas e alegam quer se não é correto deixar uma criança sozinha diante de um televisor, também não se deve ser deixada só diante de um computador.

Dessa forma, o estelionato eletrônico, assim como os demais crimes da rede mundial, só poderão ser efetivamente combatidos e as sanções devidamente aplicadas quando houver um esforço conjunto do governo, da sociedade e das empresas no sentido de cada um dentro das suas atribuições desenvolverem ações que possam, ao mesmo tempo, desenvolver a rede mundial transformando-a num ambiente seguro e proteger o usuário através de mecanismos que garantam sua privacidade, de tal forma que seu direito de inviolabilidade de suas comunicações não se transforme num manto protetor para os delinqüentes virtuais.

3.3 A Jurisprudência e o Estelionato Eletrônico.

Os Tribunais Superiores, através de suas decisões, posicionam-se no sentido de ser adaptável o ordenamento vigente aos delitos cometidos por meio do computador. É o caso de ter sido negado o pedido de Liberdade Provisória pelo Superior Tribunal de Justiça em face do cometimento desse tipo de crime (STJ – HC 200501585699 – (48225 GO) – 5° T. – Rel. Min. Gilson Dipp – DJU- 19.12.2005 – p.00462)

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

Os Tribunais Superiores estão seguindo os entendimentos doutrinários preponderantes, que trata o estelionato eletrônico e outros crimes praticados por meio do computador e da rede mundial, como delitos sujeitos às mesmas sanções em relação àquelas cuja forma tradicional

de realização vem trazida pelo ordenamento positivo vigente. É dessa maneira um entendimento já pacifico por parte dos nossos julgadores.

Não se trata dessa forma de analogia ou qualquer outra forma de integração normativa. Existe uma conduta já prevista pelo ordenamento, com a respectiva sanção a ser cominada, isto é, seus preceitos primários e secundários, alterando-se tão somente a forma como é cometida.

Oportuna se faz à menção do que seja analogia, pelas palavras do eloqüente Damásio de Jesus (2003, p.50), logo transcrita:

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

Vale ressaltar que a analogia dentro do âmbito penal possui pontos que devem ser observados, sob pena de se desrespeitar mandamentos constitucionais. Não pode criar tipos penais, por exemplo. Se assim o fosse, estaria-se-ia usurpando atribuições que são próprias do Poder Legislativo, fato este inadmissível dentro da tripartição das funções estatais e do Estado Democrático de Direito. Rogério Grecco (2004, p.48) traz de forma clara e concisa que:

> É terminantemente proibido, em virtude do princípio da legalidade, o recurso à analogia quando esta for utilizada de modo a prejudicar o agente, seja ampliando o rol de circunstâncias agravantes, seja ampliando o conteúdo dos tipos penais incriminadores, a fim de abranger hipóteses não previstas expressamente pelo legislador, etc.

Pode-se ilustrar o fato ora analisado com as palavras de José Carlos Gobbis Pagliuca (2006, p.39): A analogia no Direito Penal exerce um papel singular. Sendo o Direito Penal nada mais que a lei escrita, definida e delimitada pela interpretação, não é possível, portanto, preencher lacunas existentes com a analogia.

Dessa maneira, sendo a jurisprudência a interpretação reiterada que os tribunais dão à lei, nos casos concretos submetidos ao seu julgamento, e diante de seu papel dentro do universo jurídico pátrio, constata-se a orientação dominante no sentido de que significativa parcela dos crimes digitais, em destaque o estelionato eletrônico, nada tem de um novo tipo penal, e sim de um tipo já determinado pelas leis já vigentes, que apenas teve seu modo de ação diferenciado, ponto este que nada obsta a aplicação da sanção prevista, devendo os aplicadores do direito fazer apenas as adaptações que forem necessárias para a correta e adequada punição aos criminosos.

CONSIDERAÇÕES FINAIS

A internet foi responsável por transformações na maneira como o homem se relaciona jamais vistas ao longo da história. As facilidades advindas do avanço tecnológico são indiscutivelmente indispensáveis para o contínuo desenvolvimento da sociedade. No entanto, o novo ambiente oriundo desse avanço tecnológico tornou –se também propício para o cometimento de crimes sendo resultado da fragilidade que existe em todo o tráfego de informações.

O ambiente virtual fez surgir novos conceitos, especialmente no que diz respeito às condutas criminosas, merecendo dessa maneira um estudo pormenorizado por parte do direito positivo, que deve estar em sintonia com tais transformações, evitando assim lacunas jurídicas e, conseqüentemente, instabilidades nas relações firmadas.

O crescimento acelerado da rede mundial no país, associado a um Estado burocrático e moroso, que não acompanha as evoluções tecnológicas e as mudanças no comportamento social daí decorrentes, resultou em um ambiente virtual sem regulamentação, sem um ordenamento especifico, tornando-o terreno fértil para a propagação de condutas perniciosas.

No entanto, tais circunstâncias não podem servir de pretexto para a não punição desse tipo de criminoso. Se, de um lado, é imperioso que o ordenamento jurídico pátrio acompanhe também as sofisticadas formas de invadir o bem jurídico de outrem, em desrespeito a bens muitas vezes já consagrados na Constituição Federal, por outro lado, mostram-se perfeitamente aplicáveis em muitas situações as leis ora vigentes, apesar de entendimentos contrários, devendo apenas ocorrer o enquadramento do caso concreto à lei em abstrato.

Assim sendo, a legislação aplicável aos delitos virtuais na sua grande maioria será a vigente, com algumas adequações na esfera infraconstitucional. Como norma-base, ter-se-á a Constituição Federal, servindo as demais leis para a proteção dos bens jurídicos atingidos por

meio do computador, sendo plenamente aplicável o Código Civil, o Código de Defesa do Consumidor, a Lei dos Direitos Autorais, a Lei do Software e o próprio Código Penal.

De fato, inúmeras condutas criminosas praticadas por esse instrumento ainda podem perfeitamente ser incursa em dispositivos do nosso velho Código Penal. Evidentemente, há outras que dependerão, para que tenham força coercitiva, de novas previsões e definições legais. Estes crimes, cometidos pelo meio eletrônico, não necessitam de legislação específica, pois já se encontram sob a égide da legislação vigente. Alguns necessitam apenas de ligeiras mudanças, para se adaptarem à sua consumação via internet.

Entretanto, há aquelas condutas em que o objeto da ação lesa direito relativo a bens ou dados de informática e estes em sua maioria não encontram tipificação em nosso ordenamento jurídico.

Evidentemente, existirão casos em que o ordenamento em vigor não poderá ser aplicado, uma vez que se encontra desatualizado, pois remonta a uma época que jamais se imaginaria que o desenvolvimento tecnológico alcançaria tal patamar, e se assim for feito, estar-se-á desrespeitados princípios consagrados pela Carta Magna. Muitos conceitos vigentes em nosso Código Penal merecem serem reavaliados.

É imprescindível redimensionar o alcance normativo da lei em vigor. Os bens protegidos pela lei penal, em especial, devem ser submetidos a uma nova classificação, com critérios voltados a uma nova conjuntura social, a fim de que se possa ser efetivamente aplicada à justiça.

No tipo penal em foco, o estelionato eletrônico, poder-se-á afirmar, de acordo com as analises realizadas, ser plenamente aplicável os preceitos primários e secundários vigentes, com relação à conduta realizada através do ambiente virtual. A nova forma de cometer o delito, de maneira alguma descaracteriza a conduta descrita no art. 171 do Código Penal. Não

se pode dessa forma invocar princípios constitucionais, a saber, da legalidade, da anterioridade, reserva legal, entre outros, com o intuito de não punir esse tipo de criminoso.

Destarte, conquanto se faz necessário a provação de leis que regulem o universo virtual, como por exemplo, o Projeto de Lei que se encontra parado no Congresso Nacional, de autoria do Deputado Luis Piauhyino (PSDB – PE), em virtude de novos conceitos surgidos em decorrência da expansão do universo virtual e do desenvolvimento tecnológico; determinadas condutas, contudo, são perfeitamente enquadráveis dentro do ordenamento vigente, sendo merecedoras apenas de uma interpretação no que tange a seu enquadramento diante do caso concreto, uma vez que a forma de cometimento em nada alterou o tipo penal, e dessa forma, é plenamente possível efetuar a devida responsabilização e punição desse tipo de infrator, garantido assim segurança social.

REFERÊNCIAS

BOGO, Kellen Cristina. *A história da Internet – como tudo começou.* Disponível em: <http://www.komedi.com.br/juridico/informatica. Acesso em: 25 de setembro de 2007.

CORREA, Gustavo Testa. *Aspectos jurídicos da Internet.* 26. ed. São Paulo: Saraiva, 2000.

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

Disponível:http://www.ibge.gov.br/home/estatistica/populacao/trabalhoerendimento/pnad2006/default.shtm Acesso em: 10 set.2007.

GRECO, Rogério. *Curso de Direito Penal.* 4. ed. Rio de Janeiro: Impetus, 2004.

MATA, Breno Gonçalves Alves da. *Análise e Tendência do Cenário Jurídico atual na internet.* Jus Navegandi, Teresina, ano 4, nº 46, out.2000. Disponível em: http://jus2.uol.com.br/doutrina/texto/asp?id=1771 . Acesso em: 25 de outubro de 2007.

MEDONÇA, Arnaldo. Em tempos de Internet. Disponível em: http://www.nic.br/imprensa/htm. Acesso em: 10 de setembro de 2007.

Disponível em: <http://www.agenciact/mct.htm> Acesso em: 24 out de 2007.

MIRANDA, Marcelo Baeta Neves. *Abordagem dinâmica aos crimes via internet.* Jus Navegandi, Teresina, ano 4, nº 37, dez. 1999. Disponível em: http://jus2.uol.com.br/doutrina/texto.asp?id=1828. Acesso em 23 de setembro de 2007.

MORAES, Alexandre de. *Direito Constitucional.* 13. ed. São Paulo: Atlas, 2003.

PAESANI, Liliana Minard. *Direito e Internet.* São Paulo: Atlas, 2000.

PABLIUCA, José Carlos Gobbis. *Direito Penal: Parte Geral.* São Paulo: Rideel, 2006. (Resumos de Direito Penal Rideel).

RODRIGUES, Francisco de Assis. *A tutela penal dos sistemas de computadores* . Jus Navigandi, Teresina, ano 6, n. 55, mar. 2002. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=2813>. Acesso em: 10 nov. 2007.

SCHOUERI, Luis Eduardo. *Internet: O Direito na era virtual*. 2. ed. Rio de Janeiro: Forense, 2001.

SOUSA, Marco Antônio Cardoso. *Legislação e Internet*. Jus Navegandi, Teresina, ano 4, n. 41, maio 2000. Disponível em: http://jus2.uol.com.br/doutrina/texto.asp?id=1767. Acesso em: 15 out. 2007.

GLOSSÁRIO

BACKBONES: linha de fibra óptica com grande capacidade de transmissão de dados. Constituem o nível mais alto da estrutura da internet;

BITES: menores unidades da linguagem dos computadores;

CIBERESPAÇO: é o espaço das comunicações por rede de computador. Sua comunicação acontece de forma virtual;

E MAIL: correio eletrônico;

HACKERS: pessoa com conhecimento técnico na área de comunicações em rede e programação avançada que busca meios de invadir/ acessar sistemas de informática de forma não autorizada;

INFOVIAS: consiste no backbone para acesso a redes de informação estruturada pela necessidade de atender grandes e pequenas cidades dos Estados;

INTRANET: termo usado pra descrever redes privadas de computadores que utilizam os mesmos padrões de comunicação de dados e aplicações da Internet;

LINK: ponto no site que remete a navegação para outro site;

MODEM: aparelho conversor de sinais telefônicos em sinais digitais;

ON LINE: consiste em estar disponível para acesso em tempo real, de acordo com o contexto da internet;

SITE: é um conjunto de páginas Web, isto é, de hipertextos acessíveis geralmente pelo protocolo HTTP na Internet;

SOFTWARS: conjunto de componentes que não fazem parte do equipamento físico propriamente dito e que incluem as instruções e programas em empregados durante a utilização do sistema;

TCP/IP: conjunto de conversões e regras para iniciar, manter e fechar uma comunicação. É o modelo adotado pela internet.

ANEXOS

ANEXO A

LEI DE SOFTWARE

LEI Nº 9.609, DE 19 DE FEVEREIRO DE 1998.

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

O PRESIDENTE DA REPÚBLICA

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

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

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

CAPÍTULO II

DA PROTEÇÃO AOS DIREITOS DE AUTOR E DO REGISTRO

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

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

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

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

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

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

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

Art. 3° Os programas de computador poderão, a critério do titular, ser registrados em ór entidade a ser designado por ato do Poder Executivo, por iniciativa do Ministério resp pela política de ciência e tecnologia. (Regulamento)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

CAPÍTULO III

DAS GARANTIAS AOS USUÁRIOS DE PROGRAMA DE COMPUTADOR

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

Art. 8º Aquele que comercializar programa de computador, quer seja titular dos direitos do programa, quer seja titular dos direitos de comercialização, fica obrigado, no território nacional, durante o prazo de validade técnica da respectiva versão, a assegurar aos respectivos usuários a prestação de serviços técnicos complementares relativos ao adequado funcionamento do programa, consideradas as suas especificações.

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

CAPÍTULO IV

DOS CONTRATOS DE LICENÇA DE USO, DE COMERCIALIZAÇÃO

E DE TRANSFERÊNCIA DE TECNOLOGIA

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

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

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

§ 1º Serão nulas as cláusulas que:

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

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

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

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

Parágrafo único. Para o registro de que trata este artigo, é obrigatória a entrega, por parte do fornecedor ao receptor de tecnologia, da documentação completa, em especial do código-fonte comentado, memorial descritivo, especificações funcionais internas, diagramas, fluxogramas e outros dados técnicos necessários à absorção da tecnologia.

CAPÍTULO V

DAS INFRAÇÕES E DAS PENALIDADES

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

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

§ 1º Se a violação consistir na reprodução, por qualquer meio, de programa de com[illegible] no todo ou em parte, para fins de comércio, sem autorização expressa do autor ou de quem o represente:

Pena - Reclusão de um a quatro anos e multa.

§ 2º Na mesma pena do parágrafo anterior incorre quem vende, expõe à venda, introduz no País, adquire, oculta ou tem em depósito, para fins de comércio, original ou cópia de programa de computador, produzido com violação de direito autoral.

§ 3º Nos crimes previstos neste artigo, somente se procede mediante queixa, salvo:

I - quando praticados em prejuízo de entidade de direito público, autarquia, empresa pública, sociedade de economia mista ou fundação instituída pelo poder público;

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

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

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

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

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

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

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

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

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

CAPÍTULO VI

DISPOSIÇÕES FINAIS

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

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

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

FERNANDO HENRIQUE CARDOSO
José Israel Vargas

ANEXO B

PROJETO DE LEI Nº 84, DE 1999.
(do Sr. Luiz Piauhylino)

Dispõe sobre os crimes cometidos na área de informática, suas penalidades e dá outras providências.

O Congresso Nacional decreta:

CAPÍTULO I
DOS PRINCÍPIOS QUE REGULAM A PRESTAÇAO DE SERVIÇO POR REDES DE COMPUTADORES

Art. 1º - O acesso, o processamento e a disseminação de informações através das redes de computadores devem estar a serviço do cidadão e da sociedade, respeitados os critérios de garantia dos direitos individuais e coletivos e de privacidade e segurança de pessoas físicas e jurídicas e da garantia de acesso às informações disseminadas pelos serviços da rede.
Art. 2º - É livre a estruturação e o funcionamento das redes de computadores e seus serviços, ressalvadas as disposições específicas reguladas em lei.

CAPÍTULO II
DO USO DE INFORMAÇÕES DISPONÍVEIS EM COMPUTADORES OU REDES DE COMPUTADORES.

Art. 3º - Para fins desta lei, entende-se por informações privadas aquelas relativas a pessoa física ou jurídica identificada ou identificável.
Parágrafo único. É identificável a pessoa cuja individuação não envolva custos ou prazos desproporcionados.
Art. 4º - Ninguém será obrigado a fornecer informações sobre sua pessoa ou de terceiros, salvo nos casos previstos em lei.
Art. 5º - A coleta, o processamento e a distribuição, com finalidades comerciais, de informações privadas ficam sujeitas à prévia aquiescência da pessoa a que se referem, que poderá ser tomada sem efeito a qualquer momento, ressalvando-se o pagamento de indenizações a terceiros, quando couberem.
§ 1º. A toda pessoa cadastrada dar-se-á conhecimento das informações privadas armazenadas e das respectivas fontes.
§ 2º. Fica assegurado o direito à retificação de qualquer informação privada incorreta.
§ 3º. Salvo por disposição legal ou determinação judicial em contrário, nenhuma informação privada será mantida à revelia da pessoa a que se refere ou além do tempo previsto para a sua validade.
§ 4º. Qualquer pessoa, física ou jurídica, tem o direito de interpelar o proprietário de rede de computadores ou provedor de serviço para saber se mantém informações a seu respeito, e o respectivo teor.

Art. 6º - Os serviços de informações ou de acesso a bancos de dados não distri. informações privadas referentes, direta ou indiretamente, a origem racial, opinião política, filosófica, religiosa ou de orientação sexual, e de filiação a qualquer entidade, pública ou privada, salvo autorização expressa do interessado.

Art. 7º - O acesso de terceiros, não autorizados pelos respectivos interessados, a Informações privadas mantidas em redes de computadores dependerá de prévia autorização judicial.

CAPÍTULO III
DOS CRIMES DE INFORMÁTICA
Seção I
Dano a dado ou programa de computador

Art. 8º - Apagar, destruir, modificar ou de qualquer forma inutilizar, total ou parcialmente, dado ou programa de computador, de forma indevida ou não autorizada.
Pena: detenção, de um a três anos e multa.
Parágrafo único. *Se* o crime é cometido:
I - contra o interesse da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;
II-com considerável prejuízo para a vítima;
III - com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;
IV - com abuso de confiança;
V - por motivo fútil;
VI - com o uso indevido de senha ou processo de identificação de terceiro, ou
VII - com a utilização de qualquer outro meio fraudulento.
Pena: detenção, de dois a quatro anos e multa.
Seção II
Acesso indevido ou não autorizado
Art. 9º Obter acesso, indevido ou não autorizado, a computador ou rede de computadores.
Pena: detenção, de seis meses a um ano e multa.
Parágrafo primeiro. Na mesma pena incorre quem. sem autorização ou indevidamente, obtém, mantém ou fornece a terceiro qualquer meio de identificação ou acesso a computador ou rede de computadores.
Parágrafo segundo. Se o crime é cometido:
I - com acesso a computador ou rede de computadores da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;
II - com considerável prejuízo para a vítima;
III - com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;
IV - com abuso de confiança;
V - por motivo fútil;
VI - com o uso indevido de senha ou processo de identificação de terceiro; ou
VII - com a utilização de qualquer outro meio fraudulento.
Pena: detenção, de um a dois anos e multa.
Seção III
Alteração de senha ou mecanismo de acesso a programa de computador ou dados
Art. 10. Apagar, destruir, alterar, ou de qualquer fama inutilizar, senha ou qualquer outro mecanismo de acesso a computador, programa de computador ou dados, de forma indevida ou não autorizada.

Pena: detenção, de um a dois anos e multa.

Seção IV

Obtenção indevida ou não autorizada de dado ou instrução de computador

Art. 11 - Obter, manter ou fornecer, sem autorização ou indevidamente, dado ou instrução de computador.

Pena: detenção, de três meses a um ano e multa.

Parágrafo Único. Se o crime é cometido:

I - com acesso a computador ou rede de computadores da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;

II - com considerável prejuízo para a vítima;

III - com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;

IV - com abuso de confiança;

V - por motivo fútil;

VI - com o uso indevido de senha ou processo de identificação de terceiro; ou

VII - com a utilização de qualquer outro meio fraudulento.

Pena: detenção, de um a dois anos e multa.

Seção V

Violação de segredo armazenado em computador, meio magnético, de natureza magnética, óptica ou similar

Art. 12. Obter segredos, de indústria ou comércio, ou informações pessoais armazenadas em computador, rede de computadores, meio eletrônico de natureza magnética, óptica ou similar, de forma indevida ou não autorizada.

Parágrafo Único. Se o crime é cometido:

I - com acesso a computador ou rede de computadores da União,

Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;

II - com considerável prejuízo para a vítima;

Pena: detenção, de um a três anos e multa.

Seção VI

Criação, desenvolvimento ou inserção em computador de dados ou programa de computador c nocivos

Art. 13. Criar, desenvolver ou inserir, dado ou programa em computador ou rede de computadores, de forma indevida ou não autorizada com a finalidade de apagar, destruir, inutilizar ou modificar dado ou programa de computador ou de qualquer forma dificultar ou impossibilitar, total ou parcialmente, a utilização de computador ou rede de computadores.

Pena: reclusão, de um a quatro anos e multa.

Parágrafo único. Se o crime é cometido:

I - contra o interesse da União, Estado, Distrito Federal. Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;

II - com considerável prejuízo para a vítima;

III - com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;

IV - com abuso de confiança;

V - por motivo fútil;

VI - com o uso indevido de senha ou processo de Identificação de terceiro; ou

VII - com a utilização de qualquer outro meto fraudulento.

Pena: reclusão, de dois a seis anos e multa.

Seção VII

Veiculação de pornografia através de rede de computadores
Art. 14 - Oferecer serviço ou informação de caráter pornográfico, em rede de computadores, sem exibir, previamente, de forma facilmente visível e destacada, aviso sobre sua natureza, indicando o seu conteúdo e a inadequação para criança ou adolescentes.
Pena: detenção, de um a três anos e multa.

CAPITULO IV
DAS DISPOSIÇÕES FINAIS

Art. 15 - Se qualquer dos crimes previstos nesta lei é praticado no exercício de atividade profissional ou funcional, a pena é aumentada de um sexto até a metade.
Art. 16 - Nos crimes definidos nesta lei somente se procede mediante representação do ofendido, salvo se cometidos contra o interesse da União, Estado, Distrito Federal Município, órgão ou entidade da administração direta ou indireta, empresa concessionária de serviços públicos, fundações instituídas ou mantidas pelo poder público, serviços sociais autônomos, instituições financeiras ou empresas que explorem ramo de atividade controlada pelo poder público, casos em que a ação é pública incondicionada.
Art. 17 - Esta lei regula os crimes relativos à informática sem prejuízo das demais comunicações previstas em outros diplomas legais.
Art 18. Esta lei entra em vigor 30 (trinta) dias a contar da data de sua publicação.