

## **A LEGISLAÇÃO BRASILEIRA NOS CRIMES DA INTERNET**

**DANIEL GOUVEIA SOBRAL 1**

**ANA ROSA GOUVEIA SOBRAL DA CAMARA2**

### **RESUMO**

O presente artigo trata-se sobre a legislação brasileira nos crimes da internet. O objetivo deste trabalho é mostrar a importância de dar à rede uma atenção especial no âmbito legislativo. Até mesmo por questões metodológicas de aplicação do Direito nesta nova fase da História, pois a evolução da informática proporcionou uma dimensão da criminalidade. É um tema de grande importância, portanto, pouco discutido na doutrina e na jurisprudência, ele visa mostrar que a tecnologia trouxe diversos delitos praticados através da rede, até então inimaginável para a sociedade. O contato entre autor e vítima destes delitos tornou-se apenas virtual e os meios de execução que tornaram-se simplificados a um simples aparato eletrônico, bem como as penalidades aplicadas aos delinquentes e a falta de legislação existente para a grande dimensão dos delitos praticados na rede. É um dos temas mais palpitantes e problemáticos da atualidade, ante sua surpreendente expansão na sociedade e seus reflexos nas atividades humanas, contratuais e extracontratuais prodigiosas do avanço tecnológico. Utilizou-se de uma pesquisa eclética ou comparativa, a dogmática jurídica, baseando-se em legislação, doutrina e jurisprudência. Verifica-se que os internautas tem grande papel na contribuição para o combate deste crime, denunciando, pois assim ficará mais fácil de se chegar a estes delinquentes.

**Palavras-chave:** Crimes. Internet. Legislação.

---

**1 Daniel Gouveia Sobral – Pós- Graduação – MBA Gestão Estratégica de Negócios (UNI-RN), e-mail: Daniel.gouveia.sobral@yahoo.com.br**

**2 Ana Rosa Gouveia Sobral da Câmara – Mestre em Engenharia da Produção – Universidade Federal do Rio Grande do Norte – Natal / RN, email: anarosagsc@gmail.com**

## **ABSTRACT**

**This article comes up on the Brazilian legislation on the internet crimes. The objective of this work is to show the importance of giving special attention to the network in the legislative framework. Even for methodological issues of application of law in this new phase of history, because the evolution of information technology has provided a dimension of crime. It is a matter of great importance, so little discussed in doctrine and jurisprudence, he aims to show that technology has brought various offenses committed through the network, hitherto unimaginable to society. The contact between perpetrator and victim of these crimes became only virtual and the means of execution that became simplified to a simple electronic device, as well as fines imposed on offenders and the lack of existing legislation to the large size of the offenses charged in network. It is one of the most stimulating and problematic issues of today, compared to its amazing growth in society and its effects on human prodigious, contractual and non-contractual activities of technological advancement. We used an eclectic or comparative research, legal doctrine, relying on legislation, doctrine and jurisprudence. It appears that the internautas has great role in contributing to combat this crime, denouncing, for thus will be easier to reach these offenders.**

**Keywords: Crimes. Internet. Legislation.**

## 1 INTRODUÇÃO

Esse trabalho comportará como. analise a evolução da informática e suas principais consequências, tais como, o surgimento dos crimes de informática, que servem para identificar essa nova revolução criminosa advinda do uso do computador conectado à rede.

O tema a ser apresentado, é um tema recente, ele está começando a ganhar lugar de destaque em razão de ser uma questão latente da sociedade, e pelo fato de causar um grande furor social, bem como pela impunidade dos delinquentes diante da falta de legislação específica, deixando vários delitos praticados através da rede impunes.

Far-se-á uma análise geral deste instituto, demonstrando que para a adequação típica dos crimes ocorridos via internet, será necessário, certamente, um esforço interpretativo e podendo deparar com o argumento de que não se admite analogia *in malam partem* em direito penal, levando à conclusão de que tais delitos seriam atípicos e os infratores acabam ficando totalmente impunes.

Este trabalho tem como escopo mostrar a importância de dar à rede uma atenção especial no âmbito legislativo. Até mesmo por questões metodológicas de aplicação do Direito nesta nova fase da História, pois a evolução da informática proporcionou uma dimensão da criminalidade.

Os objetivos específicos deste trabalho apresentam um caráter mais concreto. Apontará o "modus operandi" que a tecnologia trouxe até então inimaginável para a sociedade. Quem são os autores do delito, os meios de execução que tornaram-se simplificados a um simples aparato eletrônico e a falta de legislação existente para a grande dimensão dos delitos praticados na rede.

Para se chegar a uma conclusão final, será necessário responder a algumas questões sobre o assunto estudado, conforme apresentado a seguir: Falar sobre a evolução da informática; Identificar os tipos de crimes praticados na rede e mostrar as leis existentes, bem como a falta de leis que regulam os diversos delitos praticados na rede.

O tema escolhido é, indubitavelmente, um dos temas mais palpitantes e problemáticos da atualidade, ante sua surpreendente expansão na sociedade e seus reflexos nas atividades humanas, contratuais e extracontratuais prodigiosas do

avanço tecnológico, que impulsiona o progresso materiais, gerado de utilidades e de enormes perigos à integridade da vida humana.

Os crimes de informática servem para identificar essa nova revolução criminosa advinda do uso do computador conectado à rede. A falta de uma lei brasileira sobre crimes cibernéticos tornou possível driblar a própria legislação já existente. É necessária uma urgente reforma da legislação penal e a existência de um novo ramo, denominado Direito cibernético, para regulamentar e tornar o acesso da justiça mais rápido e eficaz, facilitando as investigações, o acesso aos provedores, agilizando a identificação e punição dos ciberdelinquentes responsáveis pela propagação da rede mundial dos delitos praticados por ela.

Por fim, demonstrar-se-á que os internautas também possuem um papel importante na contribuição para o combate deste crime, denunciando sempre, pois assim facilitará chegar aos infratores.

Para a manufatura do presente trabalho serão utilizados os métodos de abordagem indutivo e dedutivo. Serão utilizados também, quando necessários os métodos de procedimento histórico, comparativo, monográfico, estatístico, tipológico e funcionalista.

## 2 EVOLUÇÃO DA INFORMÁTICA

Ao longo da evolução, a sociedade descobriu o uso de importantes ferramentas, que marcaram a história do homem, como o fogo, a roda, a escrita, a energia elétrica e a imprensa. No entanto, apenas no Século XX que se presenciou uma grande revolução no campo das descobertas, surgindo uma tecnologia que somente os mais ousados ficcionistas e futurólogos conseguiram prever.

O final deste século trouxe uma nova organização dos modos de produção e negócios e, conseqüentemente, da economia, da sociedade e da política. Primeiro foi a revolução agrícola, depois a revolução industrial, e por fim a revolução tecnológica, ou revolução da informática.

Com relação ao assunto Alves (1993, p.17) afirma que:

A ciência é uma função da vida. Justifica-se apenas enquanto órgão adequado à nossa sobrevivência. Uma ciência que se divorciou da vida perdeu a sua legitimação. Esta afirmação deve ser levada em conta em relação às três revoluções técnico-científicas que avançam no século atual: a quântica, a informática e a biomolecular.

Bastos, (1989, p. 62) assevera que: "A evolução tecnológica torna possível uma devassa na vida íntima das pessoas, insuspeitada por ocasião das primeiras declarações de direitos".

Repisa-se que a velocidade da evolução tecnológica da área de informática é espantosa quando comparada com outras ciências.

Durante algum tempo a evolução dos computadores foi caracterizada por gerações de acordo com a base do hardware: válvulas transistores e circuitos integrados, ou seja, primeira, segunda e terceira gerações. Chegou-se ainda a falar em quarta geração, quando a integração era muito grande e até mesmo numa quinta com a inteligência artificial.

Prado Junior, (2001, p. 371-372), afirma que:

O ENIAC (Electronic Numerical Integrator and Calculator), desenvolvido entre 1939 e 1946, é, por muitos, considerado como o primeiro computador eletrônico digital embora não possuísse programa armazenado. Na verdade, o primeiro equipamento a operar com programa armazenado foi o ÉDSAC (Electronic Delayed Storage Automatic Computer), tornado operacional em 1949. O EDVAC (Electronic Discrete Variable Automatic Computer), desenvolvido de 1946 a 1951, também operava com programa armazenado. O UNIVAC (Universal Automatic Computer) foi lançado em 1951 pela RemingtonRand e vendido em larga escala por já se acreditar no valor comercial do computador de programa armazenado.

Kaku (2001, p. 42-44), por sua vez, situa a evolução do computador em três fases, sendo elas:

A primeira fase foi dominada pelo desajeitado, mas poderoso computador mainframe, em que a IBM, a Burroughs, a Honeywell e outras foram pioneiras; nesse período os computadores eram grandes e caros e apenas os considerados "iniciados" se comunicavam com a máquina poderosa. A segunda fase se iniciou no começo da década de 1970 com os engenheiros da Xerox PARC que, ao perceber o poder do computador, investiram na construção do primeiro PC (Personal Computer), em 1972. E avançaram muito mais projetando interfaces homem-máquina baseadas em figuras, os ícones, que, apontados pela seta de um mouse faziam os computadores funcionarem. A terceira fase é a da computação onipresente.

Com relação ao assunto, Oliveira Júnior (2001, p. 51) dispõe que:

Na década de 50 surgiu o primeiro computador de grande porte. Tratava-se de uma máquina caríssima, composta de 18 mil válvulas de 16 tipos distintos. Sua altura chegava aos 30 metros, que acabava por consumir 140 Kws de energia. Com o passar dos tempos o tamanho dessas maravilhas tem diminuído progressivamente assim também como o preço. Estima-se que hoje existam milhares dessas máquinas espalhadas em todo o mundo, sendo que a maioria delas esteja interligadas à "Net" formando todo um complexo conjunto de sistemas interligados simultaneamente.

Com a grande evolução dos povos e da sociedade, foi observado então além do surgimento do computador, o surgimento da Internet posteriormente.

Cumprе esclarecer que na atualidade, a informática se transforma em tecnologia da informação, que denomina-se de "TI", ou seja esta tecnologia integra os seus emergentes e modernos recursos. Denomina-se TI como o conjunto dos recursos tecnológicos e computacionais para guarda de dados, geração e uso da informação e de conhecimentos. Está fundamentada nos *hardware* e seus dispositivos e periféricos; *software* e seus recursos; sistemas de telecomunicações; e gestão de dados e informações.

Com relação aos sistemas de telecomunicações e seus respectivos recursos são eles subsistemas especiais do Sistema de Informação global das empresas, tais como, os recursos de satélites, fibra ótica e linhas específicas de comutação de dados.

A gestão de dados e informações são as atividades de guarda e recuperação de dados e níveis e de controle de acesso às informações. Essa gestão requer um completo plano de contingência e um plano de segurança de dados e informações.

Na era do processamento de dados, os usuários eram tímidos, hesitantes, indecisos e superficialmente envolvidos com tecnologias. Na fase da informática os usuários já se posicionam como responsáveis pelos sistemas e estão mais engajados nos processos que utilizam tecnologias.

Ainda com relação ao surgimento da Internet, cumpre trazer algumas ponderações. Segundo Ramalho Terceiro (2004, p. 58):

A INTERNET teve sua origem embrionária em plena guerra fria como arma militar norte-americana de informação. A ideia consistia em interligar todos as centrais de computadores dos postos de comando estratégicos americanos, precavendo-se, pois, de uma suposta agressão russa. Sendo atacado um desses pontos estratégicos, os demais poderiam continuar funcionando autonomamente, auxiliando e fornecendo informações a outros centros bélicos.

No entanto, a Internet, na sua feição atual, é uma "criança" em fase do crescimento bastante acelerado, que ela vem-se passando.

Conforme Aras (2001, p. 51):

A principal *interface da Internet*, é a WWW — *World Wide Web* surgiu na década de 1990. Sucede, porém, que o Código Penal em vigor no Brasil (parte especial) data de 7 de dezembro de 1940. Naquela época, mal havia telefones e rádios nas residências. A televisão ainda não havia sido inventada. A disseminação dos computadores pessoais é, no plano da História, um fenômeno recentíssimo. No Brasil, data da década de 1990 e, ainda assim, apenas os integrantes das classes A, B e C têm suas máquinas domésticas, fazendo surgir, no dizer do professor CHRISTIANO GERMAN uma nova classe de excluídos: os *unplugged*, constituindo um proletariado *off line* ao lado de uma elite *online*.

No ano 2000, a atividade econômica na internet cresceu 58% nos EUA. Durante muitos anos, o acesso à Internet ficou restrito à instituições de ensino e pesquisa. A partir da década de 80, os microcomputadores passaram a custar menos e se tornaram mais fáceis de usar.

Portanto, sendo assim Barros (2004, p. 61), preceitua que:

O que de mais moderno existe em informática é a Internet. A rede das redes, como é chamada, propiciou o surgimento de uma nova sociedade, ao mesmo tempo virtual e global. Essa sociedade formada por milhões de pessoas com culturas heterogêneas, tornou possível o aparecimento do admirável mundo virtual. Para acessá-la, basta um computador, um modem, uma linha telefônica comum e um programa de comunicação, isso hoje, pois a tendência é a intensificação do seu uso nos aparelhos eletrônicos domésticos. Na rede, os direitos de expressão e pensamentos são exercidos em sua máxima plenitude. O ciberespaço deu origem a uma nova cultura

baseada na liberdade de informação dos cidadãos, rompendo barreiras e unificando os costumes, afetando o relacionamento dos indivíduos da comunidade.

Hoje, qualquer pessoa pode se conectar à Internet, basta se associar a um provedor de acesso.

As informações são muito mais acessíveis do que há alguns anos atrás. As criações artísticas, literárias, científicas podem ser expressas em códigos digitais, possibilitando assim a troca rápida de informações.

Atualmente, a Internet é um enorme avanço tecnológico, que contribuiu para as comunicações, ciência, cultura, política, educação e comércio mundiais. Em poucos segundos recebemos milhares de informações que levaríamos meses para conseguir buscando em livros, revistas e jornais.

Sendo assim, Aias (2001, p. 51) dispõe que:

As implicações dessa poderosa máquina no dia-a-dia dos indivíduos são marcantes. Situa-se no campo das relações pessoais, volteiam na seara da Sociologia e da Filosofia, avançam na interação do indivíduo com o Estado (a chamada cidadania digital, *e-gov* ou governo eletrônico), refletem no Direito Civil (ameaças a direitos de personalidade) e no Direito do Consumidor (responsabilidade do provedor de acesso à Internet) e acabam por interessar ao Direito Penal.

A internet, graças aos fatores de economia, velocidade 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.

Conforme Miranda (1999, p. 37):

A cada minuto, milhões de computadores interligam-se por meio das linhas telefônicas no mundo inteiro, fazendo circular bilhões e bilhões de informações que se traduzem em movimentação financeira, intercâmbio cultural e inter-relacionamento pessoal entre pessoas e instituições de todas as partes e das mais variadas culturas. Esta progressiva dependência, obviamente, está trazendo em seu rol uma série de reflexos no mundo jurídico, na medida em que vão surgindo questões ainda carentes de regulamentação que, de maneira poliédrica, tem desafiado doutrinadores dos variados campos das Ciências Humanas, que paradoxalmente vão buscar nos nichos tecnológicos respostas para muitas de suas dúvidas. (...) A velocidade com que a tecnologia tem avançado e se popularizado tem sido bem maior que a legislação preventiva, o que é preocupante.

A Internet é uma interligação simultânea de computadores de todo o planeta, constituindo forma e fonte de poder, sendo seu domínio e disponibilidade de uso um patrimônio econômico, político e cultural, em razão do valor estratégico proporcionado pela informação.

Nesse sentido, Martinelli (2000, p. 46), preceitua:

A corrida tecnológica permitiu, também, a evolução dos meios de comunicação, que se consolidaram como imprescindíveis ao mundo globalizado. As pessoas têm à sua disposição diversas maneiras de se comunicarem, fazendo das distâncias meros obstáculos superáveis. Uma nova mentalidade emergiu desta nova via de comunicação. As pessoas hoje podem enviar mensagens em tempo real para outras, conversar em grupo, como se estivessem em reuniões, expressar suas ideias sem censura, comprar sem aparecer na loja, e praticar atos inimagináveis no passado. A partir dessa nova cultura instalada pelo casamento entre tecnologia e comunicação, novas maneiras de praticar atos ilícitos também vieram com a correnteza. Crimes anteriormente realizados com armas, pelo contato pessoal, agora encontram meios alternativos, onde as distâncias não representam barreiras, os agentes permanecem sentados diante de um computador e a violência é dispensada.

A Internet é um universo de informações que está cada vez mais presente e imprescindível em nossas vidas e em nossas profissões, quer seja nos locais de trabalhos ou nos lares das pessoas. Esse mundo virtual de informações cresce em progressão geométrica e em proporções gigantescas, onde muitas entidades e serviços dependem do seu uso. Entretanto, as novas tecnologias ainda são um privilégio de uma minoria da população.

Barros (2003, p. 61) expressa que:

Com a informação instantânea, *essa tecnologia deixa o mundo menor*. São trocas de informações, compra de produtos, assinatura de revistas, reservas de hotéis, fechamento de negócios, divulgação e publicação de comunicações, modificando as rotinas sociais e culturais do homem, trazendo novos desafios à humanidade, como aqueles atribuídos às práticas criminosas.

Portanto, a vida depende cada vez mais do mundo virtual. É a tecnologia rompendo fronteiras, com as suas virtudes e vicissitudes que marcam a nova era.

Vale salientar que a 10 (dez) anos atrás Oito milhões de brasileiros acessavam a internet. Em dois anos esse número chegou na faixa dos quinze milhões. Em 2009 segundo pesquisas realizadas pelo IBOPE 62,3 milhões de brasileiros acessam a internet. Contudo os benefícios da modernidade e celeridade alcançados com a rede

mundial trazem, na mesma proporção, a prática de ilícitos penais que vêm confundindo não só as vítimas como também os responsáveis pela persecução penal.

Desta feita, com a popularização da Internet, ao mesmo tempo em que ela fornece inúmeras facilidades aos usuários, também torna-se um grande atrativo para o criminoso virtual. Os efeitos negativos que esta revolução, vai provocar, mal começaram a serem percebidos.

O comércio eletrônico começou a expandir-se a velocidades inimagináveis, milhares de transações "*on Une*" são efetivadas instantaneamente por pessoas e empresas em diversas áreas do mundo.

Miranda (1999, p. 37) preceitua:

O que mais tem atemorizado, desde os sociólogos até os profissionais da polícia é o crescimento em progressão geométrica do uso da Internet. Sua quase absoluta falta de controle e a forma totalmente dispersa de sua expansão, está criando espaços na rede exclusivamente para atividades criminosas, unindo os ideais ou interesses de uma minoria, excitando a motivação delitiva, tais como crimes de ódio, terrorismo e parafilias.

Futuramente, os criminosos ultrapassarão a capacidade dos organismos policiais em capturá-los, pois prevalecem da forma revolucionária do espaço cibernético, provido de regras sociais ou éticas, limitados somente por suas habilidades técnicas e o anonimato permitido pela Internet, que atrapalha na identificação da autoria.

### **3 CRIMES NA INTERNET**

Com o advento desta nova mídia, ao par de trazer incontáveis benefícios ao irreversível processo de globalização vivido pela sociedade neste final de Século, conduz em seu ventre o germe de uma nova delinquência, em razão do refinamento que norteia a ação dos seus praticantes.

Segundo Ferreira (2000, p. 207-237):

O surgimento dos crimes informáticos remonta, no entender de Ulrich Sieber, da Universidade de Würzburg, à década de 1960, época em que apareceram na imprensa e na literatura científica os primeiros casos de uso do computador para a prática de delitos, constituídos, sobretudo, por manipulações, sabotagens, espionagem e uso abusivo de computadores e sistemas, denunciados em matérias jornalísticas. Somente na década

seguinte é que se iniciariam os estudos sistemáticos e científicos sobre essa matéria, com emprego de métodos criminológicos, analisando-se um limitado número de delitos informáticos que haviam sido denunciados, entre os quais alguns casos de grande repercussão na Europa por envolverem empresas de renome mundial.

A partir de 1980 (...) o aumento de ações criminosas que passaram a incidir em manipulações de caixas bancárias, pirataria de programas de computador, abusos nas telecomunicações etc., revelando vulnerabilidade que os criadores do processo não haviam previsto.

Acrescente-se, ainda, o delito de pornografia infantil na rede, igualmente difundido na época.

Essa criminalidade, conta com as mesmas características da informatização global, todos os países fazem uso da informatização, assim a delinquência correspondente, ainda que em graus distintos, integrantes de vários níveis sociais e económicos já têm acesso aos produtos informatizados.

A criminalidade informática, é um fenómeno surgido no final do século XX, designa todas as formas de conduta ilegais realizadas mediante a utilização de um computador, conectado ou não a uma rede, que vão desde a manipulação de caixas bancários, à pirataria de programas de computador, passando por abusos nos sistemas de telecomunicação.

Uontcrme Ramalho Terceiro (2002, p.58):

A criminalidade informática preocupa o mundo e tem reclamado definições. Para a OECD — *Organization for Economic Cooperation and Development*, o crime de computador é "qualquer comportamento ilegal, aéctico ou não autorizado envolvendo processamento automático de dados e, ou transmissão de dados", podendo implicar a manipulação de dados ou informações, a falsificação de programas, a sabotagem eletrônica, a espionagem virtual, a pirataria de programas, o acesso e/ou o uso não autorizado de computadores e redes.

Diante da popularização e do fácil acesso ao microcomputador, muitos indivíduos utilizam a Internet, jovens na sua maioria, como meio para praticar delitos das mais variadas espécies, causando enormes prejuízos a Bancos ou Instituições Financeiras através de desvios em seu erário, bem como divulgando de material pornográfico ou de carácter discriminatório.

No Brasil já foram identificados vários casos de delitos via Internet e estes se aliaram de tal forma às novas tecnologias que até o crime organizado trabalha com rede de computadores.

Carvalho (2001, p.51) aduz que: "Há crimes novos, contemporâneos da formação da rede mundial de computadores, mas estão acontecendo, pela "net",

delitos já de muito tempo conhecidos da sociedade, só que agora perpetrados com o requinte do "bit".

Existem os que utilizam a Internet como biblioteca do crime, dirundindo práticas criminosas, na medida em que são disponibilizados, ao alcance de qualquer pessoa medianamente equipada, meios para a prática de ilícitos, por iniciativa de alguns e conivência de outros que pregam uma "liberdade total" na Web.

Delitos que ofendem interesses relativos ao uso, à propriedade, à segurança ou à funcionalidade de computadores e equipamentos periféricos, redes de computadores e programas de computador. Infrações que atinjam redes de computadores ou a própria Internet ou que sejam praticados por essas vias. Estes são crimes à distância.

### 3.1 ESPÉCIES DEPRIMES NA INTERNET

Martinelli (2000, p.46) dispõe que são estes os crimes na internet

Fraudes, leilões, compra e venda de mercadorias, uso de senhas alheias na conexão com provedores de acesso, pirâmides, trabalhos em casa com promessa de altos ganhos e utilização de senhas falsas na utilização de serviços "on-line" pagos. A pornografia infantil, crimes contra a honra que aparecem na Internet, pelas "home pages" e por correio eletrônico. Na primeira, os gerenciadores das páginas recebem uma quantia dos usuários (através de depósito ou cartão de crédito), que dispõem de um acervo de fotos e vídeos. Na segunda, o material é distribuído de um usuário a outro, diretamente. Atos que denigrem a integridade moral das pessoas através da injúria, da calúnia ou da difamação, utilizando a Internet como maneira de difusão de ofensas, por imagens, ou palavras. O racismo é a divulgação da aversão a determinados grupos de pessoas, muitas vezes incitando à violência, seja pela etnia, pela religião, pela nacionalidade, através de "home pages" ou correio eletrônico. A interceptação de correspondência eletrônica é a difusão de programas de computador pela grande rede, sem a autorização dos detentores de direitos sobre eles. Os crimes de pirataria. A difusão de obras literárias, jornalísticas, musicais, entre outras.

O anonimato permitido pela estrutura virtual, que caracteriza a rede, dificulta a identificação do autor. Ocorre essa barreira porque o trabalho fica restringido à manipulação dos dados digitais. Mais um problema converte ao flagrante, praticamente impossível de ser obtido, pois o resultado vem muito depois do início da execução ou a vítima toma conhecimento do fato após longo intervalo de tempo porque não experimenta o prejuízo instantaneamente.

A determinação dos lugares em que o crime foi executado e gerou resultados, assim como a definição da materialidade, da autoria e da culpabilidade acabam por dificultar ainda mais os procedimentos investigativos.

Aras (2001, p.51), *relata* que:

Os cibecriminosos em geral cometem infrações de várias espécies, como a prática na qual o internauta se apropria de domínios virtuais registrados em nome de terceiros. Outra conduta corriqueira é "sequestro" que consiste em inserir alteração no endereço de uma determinada página para conduzir o internauta a outro site. Tem também os programas intrusos que servem para vasculhar a intimidade de internautas. Existem aqueles que abrem brechas de segurança em sistemas, permitindo a instalação de uma espécie de janela virtual no computador da vítima e que pode ser aberta ao alvitre do hacker para fins ilícitos. Não são incomuns os casos de perseguição ou ameaças digitais, por via telemática.

Rossini (2002, p. 180-210), cita, algumas condutas, como sendo crimes da informática, veja:

(...)

d) hoaxes, como sendo emails que possuem conteúdos alarmantes e falsos, geralmente apontando como remetentes empresas importantes ou órgãos governamentais, como as correntes ou pirâmides, hoaxes típicos que caracterizam crime contra a economia popular, podendo, ainda, estarem acompanhadas de vírus;

(...)

f) trojan horses ou cavalos de tróia, que, uma vez instalados nos computadores, abrem suas portas, tornando possível a subtração de informações, como senhas, arquivos etc.

(...) Embora o usuário possa recebê-lo de várias maneiras, na maioria das vezes ele vem anexado a algum e-mail. Este vem acompanhado de mensagens bonitas que prometem mil maravilhas se o arquivo anexado for aberto. Uma vez aberto o arquivo, o trojan horse se instala no computador do usuário. Na maioria das vezes, tal programa ilícito vai possibilitar aos hackers o controle total da sua máquina. Poderá ver e copiar todos os arquivos do usuário, descobrir todas as senhas que ele digitar, formatar seu disco rígido, ver a sua tela e até mesmo ouvir sua voz se o computador tiver um microfone instalado.

Portanto, verifica-se que delito eletrônico, em sentido amplo, é qualquer conduta criminógena ou criminal, cuja realização tem o emprego da tecnologia eletrônica como método, meio ou fim e, em um sentido estrito, qualquer ato ilícito penal em que os computadores, suas técnicas e funções desempenham um papel como método, meio ou fim.

Cumprindo ainda trazer à baila a relação de tipos de delitos informáticos publicada pela Organização das Nações Unidas (ONU) no Oitavo Congresso sobre Prevenção

de Delito e Justiça Penal, celebrado em Havana, Cuba, em 1990. A relação reconheceu os seguintes delitos:

1. Fraudes cometidas mediante manipulação de computadores, caracterizadas por:

- a) manipulação de dados de entrada, também conhecida como subtração de dados;
- b) manipulação de programas, modificando programas existentes em sistemas de computadores ou enxertando novos programas ou novas rotinas;
- c) manipulação de dados de saída, forjando um objetivo ao funcionamento do sistema informático, como, por exemplo, a utilização de equipamentos e programas de computadores especializados em decodificar informações de tarjas magnéticas de cartões bancários ou de crédito;
- d) manipulação informática, técnica especializada que aproveita as repetições automáticas dos processos do computador, apenas perceptível em transações financeiras, em que se saca numerário rapidamente de uma conta e transfere a outra.

2. Falsificações informáticas:

- a) como objeto, quando se alteram dados de documentos armazenados em formato computadorizado;
- b) como instrumento, quando o computador é utilizado para efetuar falsificações de documentos de uso comercial, criando ou modificando-os, com o auxílio de impressoras coloridas a base de raio laser, cuja reprodução de alta qualidade, em regra, somente pode ser diferenciada da autêntica por perito.

3. Danos ou modificações de programas ou dados computadorizados, também conhecidos como sabotagem informática, ato de copiar, suprimir ou modificar, sem autorização, funções ou dados informáticos, com a intenção de obstaculizar o funcionamento normal do sistema, cujas técnicas são:

- a) vírus, série de chaves programadas que podem aderir a programas legítimos e propagar-se a outros programas informáticos,
- b) gusanos, análogo ao vírus, mas com objetivo de infiltrar em programas legítimos de programas de dados para modificá-lo ou destruí-lo, sem regenerar-se;
- c) bomba lógica ou cronológica, requisitando conhecimentos especializados já que requer a programação para destruição ou modificação de dados em um certo momento do futuro;
- d) acesso não-autorizado a sistemas de serviços, desde uma simples curiosidade, como nos casos de hackers, piratas informáticos, até a sabotagem ou espionagem informática;
- e) piratas informáticos ou hackers, que aproveitam as falhas nos sistemas de segurança para obter acesso a programas e órgãos de informações; e
- f) reprodução não-autorizada de programas informáticos de proteção ilegal, causando uma perda económica substancial aos legítimos proprietários intelectuais.

Posteriormente, no Décimo Congresso sobre Prevenção de Delito e Tratamento do Delinquente<sup>20</sup>, celebrado em Viena, entre os dias 10 e 17 de abril de 2000, a ONU publicou um comunicado à imprensa, relacionando outros tipos de delitos informáticos, praticados por meio do computador, quais sejam:

- a) Espionagem industrial: espionagem avançada realizada por piratas para as empresas ou para o seu próprio proveito, copiando segredos comerciais que abordam desde informação sobre técnicas ou produtos até informação sobre estratégias de comercialização;

- b) Sabotagem de sistemas: ataques, como o bombardeiro eletrônico, que consistem no envio de mensagens repetidas a um site, impedindo assim que os usuários legítimos tenham acesso a eles. O fluxo de correspondência pode transbordar a quota da conta pessoal do titular do e-mail que as recebe e paralisar sistemas inteiros. Todavia, apesar de ser uma prática extremamente destruidora, não é necessariamente ilegal;
- c) Sabotagem e vandalismo de dados: intrusos acessam sites eletrônicos ou base de dados, apagando-os ou alterando-os, de forma a corromper os dados. Podem causar prejuízos ainda maiores se os dados incorretos forem usados posteriormente para outros fins;
- d) Pesca ou averiguação de senhas secretas: delinquentes enganam novos e incautos usuários da internet para que revelem suas senhas pessoais, fazendo-se passar por agentes da lei ou empregados de provedores de serviço. Utilizam programas para identificar senhas de usuários, para que, mais tarde, possam usá-las para esconder verdadeiras identidades e cometer outras maldades, como o uso não autorizado de sistemas de computadores, delitos financeiros, vandalismo e até atos de terrorismo;
- e) Estratagemas: astuciosos utilizam diversas técnicas para ocultar computadores que se parecem eletronicamente com outros para lograr acessar algum sistema geralmente restrito a cometer delitos. O famoso pirata Kevin Mitnick se valeu de estratagemas em 1996, para invadir o computador da casa de Tsutomu Shimomura, expert em segurança, e destruir pela internet valiosos segredos de segurança;
- f) Pornografia infantil: a distribuição de pornografia infantil por todo o mundo por meio da internet está aumentando. O problema se agrava ao aparecer novas tecnologias como a criptografia, que serve para esconder pornografia e demais materiais ofensivos em arquivos ou durante a transmissão;
- g) Jogos de azar: o jogo eletrônico de azar foi incrementado à medida que o comércio brindou com facilidades de crédito e transferência de fundos pela rede. Os problemas ocorrem em países onde esse jogo é um delito e as autoridades nacionais exigem licenças. Ademais, não se pode garantir um jogo limpo, dado as inconveniências técnicas e jurisdicionais para sua supervisão;
- h) Fraude: já foram feitas ofertas fraudulentas ao consumidor tais como a cotização de ações, bônus e valores, ou a venda de equipamentos de computadores em regiões onde existe o comércio eletrônico;
- i) Lavagem de dinheiro: espera-se que o comércio eletrônico seja um novo lugar de transferência eletrônica de mercadorias e dinheiro para lavar as ganâncias do crime, sobretudo, mediante a ocultação de transações;

Portanto, nota-se que com a rede mundial, modificou-se hábitos e costumes, combinando comportamentos tradicionais com o acesso à informação e cultura, se tornou assim um rico campo para as mais vastas atividades ilícitas.

Neste sentido Ferreira (2000, p. 207) afirma que:

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

Com todo o exposto, verifica-se a existência do crime de informática propriamente dito, aparecendo o computador como meio e meta, podendo ser objetos de tais delitos o computador, seus periféricos, os dados ou o suporte lógico da máquina e as informações que guardar, bem como o computador como o meio de execução, para a consumação do crime-fim.

A cultura da Internet tradicionalmente requer ou permite que o internauta assuma uma identidade virtual. Em geral, os cibernavegantes ocultam suas identidades sob apelidos ou *nicknames*, e alguns utilizam *e-mails* virtuais, providência que torna ainda mais difícil a identificação do usuário.

Um dos grandes problemas da criminalidade *on Une* é justamente o da identificação do autor do fato ilícito, muito mais do que a determinação da materialidade. Não são impossíveis situações delitivas em que uma pessoa se faça passar por outra, mediante o uso indevido de senhas pessoais em sistemas informatizados, podendo, em casos mais graves e bem raros, ocorrer o "furto de identidade", que consiste em alguém assumir durante certo tempo a identidade de outro internauta na grande rede, com evidentes implicações pessoais.

Castro (2001, p. 52) estabelece que:

A criação e desenvolvimento de vírus surgiu com a informática, aquele que se dedica a estudar novas formas de atacar o computador alheio, sem no entanto enviar os vírus, não pode ser punido. A conduta de quem os envia, só poderá ser punida se causar dano patrimonial ao destinatário, pois quem envia um vírus e destrói arquivos e programas causando prejuízo financeiro, estará incurso nas sanções do artigo 163 do Código Penal. Todavia, quem destrói arquivo sem valor econômico, não se adequa na figura prevista pelo legislador, sendo fato atípico. O mesmo ocorre com a sabotagem e o vandalismo virtual, quem acessa um site e nele insere palavras ou textos "pichando" as páginas ou quem recria uma página da rede por algum tempo também não responderá por esta ação. O uso desautorizado do computador, conhecido como furto de uso ou de tempo, não é crime, assim, quem utiliza o equipamento alheio sem pedir autorização do proprietário, quem usa provedor de terceiro para acessar a Internet, não pode sequer ser processado criminalmente. Da mesma forma, o acesso não autorizado em redes, a alteração e/ou destruição de senhas para ingresso em sistemas, intranet e Internet também não são puníveis.

Embora a impunidade atinja um número razoável de condutas, não pode-se afirmar que tudo na rede é permitido.

Sendo assim, Miranda (1999, p. 37) afirma:

O estelionato, a lavagem de dinheiro, os crimes contra a honra, discriminação, os crimes do colarinho branco, furto a modalidade conhecida

por "salami slicing" (fatiamento de salame, em que o ladrão faz regularmente transferências eletrônicas de pequenas quantias de milhares de contas para a sua própria, muitas vezes camuflada por campanhas de arrecadação de donativos de modo a não despertar suspeitas), serviços subtraídos, o contrabando, a pornografia infantil, parafilia, invasões de privacidade, apologia de crimes, violações à propriedade intelectual ou industrial, violações à Lei do Software, pixações em sites oficiais do governo, vandalismo, sabotagem, dano, propagação de vírus de computador, a pirataria em geral, espionagem, tráfico de armas e drogas, lesões a direitos humanos (terrorismo, crimes de ódio, racismo, etc), destruição de informações, jogos ilegais, dentre inúmeros outros, apenas para explicitar a complexidade da matéria tratada, são exemplos de infrações que são investigadas por nossa polícia, podendo seus autores serem processados e condenados.

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 na Internet.

O ilícito eletrônico ou informático, mesmo que não previsto em lei penal, pode ensejar reparação cível. 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 pecuniária.

### 3.2 CLASSIFICAÇÃO DOS CRIMES NA INTERNET

Como fator criminógeno, a informática possibilita não só o cometimento de novos delitos. Existem os crimes cometidos com o computador e os cometidos contra o computador, isto é, contra as informações e programas nele contidos, conforme demonstrar-se-á.

Corrêa (2000, p. 43) afirma que: "(...) no contexto dos denominados "crimes digitais", ou seja, todos aqueles relacionados às informações arquivadas ou em trânsito por computadores, sendo esses dados, acessados ilicitamente, usados para ameaçar ou fraudar".

Assim, pode-se dizer que os crimes cometidos contra o computador, ou seja, contra as informações e programas nele contidos, bem como contra as informações ou dados em trânsito por computadores, com o dolo específico de ameaça e de fraude, não abordando aqueles crimes praticados com o computador, mas cujo bem protegido pelo ordenamento jurídico é diverso, como por exemplo, a pedofilia, furto, etc.

Cumprasseverar que não existe consenso na classificação dos delitos de informática, mas existem várias maneiras de conceituar tais condutas, conforme ver-se-á a seguir.

Sendo assim, Ferreira (2000, p. 207) preceitua:

Existem duas categorias de crimes informáticos: a) os crimes cometidos contra um sistema de informática, seja qual for a motivação do agente; b) os crimes cometidos contra outros bens jurídicos, por meio de um sistema de informática. No primeiro caso, temos o delito de informática opropriamente dito, aparecendo o computador como meio e meta, podendo ser objetos de tais condutas o computador, seus periféricos, os dados ou o suporte lógico da máquina e as informações que guardar. No segundo caso, o computador é apenas o meio de execução, para a consumação do crime-fim, sendo mais comuns nesta espécie as práticas ilícitas de natureza patrimonial, as que atentam contra a liberdade individual e contra o direito de autor.

Neste mesmo sentido Gomes (2001, n. 1) assinala que:

Os crimes informáticos dividem-se em crimes contra o computador; e crimes por meio do computador, em que este serve de instrumento para atingimento da meta optata. O uso indevido do computador ou de um sistema informático (em si um fato "tipificável") servirá de meio para a consumação do crime-fim. O crime de fraude eletrônica de cartões de crédito serve de exemplo.

Desta feita, verifica-se que a Rede Mundial de Computadores, é apenas mais um meio para a realização de uma conduta delituosa. Se antes, os delitos, tais como, a pornografia infantil era consumada através de vídeos e fotografias, hoje também se consuma através dos *sítes*. Portanto, verifica-se que modificou-se apenas a forma, mas a essência do crime permanece a mesma.

Deste modo, a caracterização do delito praticado por meio do computador dependerá da análise do caso concreto, devendo a conduta do delinquente informático se submeter em norma prevista na legislação em vigor do país onde o delito for cometido.

Para Pinheiro (2001, p. 18-19) os crimes na internet classificam em:

Virtuais puros, mistos e comuns. O crime virtual puro seria toda e qualquer conduta ilícita que tenha por objetivo exclusivo o sistema de computador, pelo atentado físico ou técnico ao equipamento e seus componentes, inclusive dados e sistemas. Crime vi-lual misto seria aquele em que o uso da internet é condição sine qua non para a efetivação da ccnduta, embora o bem jurídico visado seja diverso do informático, como, por exemplo, as transferências ilícitas de valores em uma homebanking ou no cnamado salamislicing, onde o cracker retira de milhares de contas correntes, diariamente, pequenas quantias que correspondem a centavos e as transfeie para uma única conta. Embora esses valores sejam ínfimos para o correntista, que, na maioria das vê vezes, nem se dá conta do furto, representam para o cibercriminoso uma expressiva quantia em seu montante.

Assim sendo, verifica-se que os crimes na internet são chamados de puros e impuros. São puros ou próprios, aqueles que sejam praticados por computador e se realizem ou se consumem também em meio eletrônico. Neles, a informática é o objeto jurídico tutelado. Já os crimes eletrônicos impuros ou impróprios são aqueles em que o agente se utiliza do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço real, ameaçando ou lesando outros bens, não-computacionais ou diversos da informática.

Portanto, crime virtual comum seria utilizar a internet apenas como instrumento para a realização de um delito já tipificado na lei penal.

Ferreira (2000, p. 210) define crime de informática como sendo: "toda ação típica, antijurídica e culpável, cometida contra ou pela utilização de processamento automático de dados ou sua transmissão".

Com relação ao assunto Rossini (2002, p. 140) afirma que: "o crime de informática é qualquer conduta ilegal não-ética, ou não-autorizada, que envolva processamento automático de dados e/ou transmissão de dados".

Verifica-se assim que, existem delitos informáticos puros, em que o sujeito visa especificamente ao sistema de informática em todas as suas formas, incluindo *software*, *hardware*, dados e sistemas, bem como meios de armazenamento, e delitos informáticos impuros, em que o computador é a ferramenta para a ofensa a outros bens jurídicos que não exclusivamente os do sistema informático.

#### 4 OS CRIMINOSOS DIGITAIS

Os crimes de computador são cometidos por pessoas cuja ocupação profissional implica o uso cotidiano de microcomputadores, não estando excluída, a possibilidade de serem perpetrados por meros diletantes.

Embora no *underground* cibernético, as diferentes designações ainda façam algum sentido e tenham importância, o certo é que, hoje, para a grande maioria das pessoas, a palavra *hacker* serve para designar o criminoso eletrônico, o ciberdelinqüente.

Para Martineli, (2000, p. 46):

O agente criminoso da informática revela-se diferente dos demais pela utilização plena do intelecto e dos conhecimentos técnicos. Não há emprego de armas tradicionais e inexistente contato com a vítima, pois todos os procedimentos acontecem à distância.

Fraga (2001, p. 374) traz algumas considerações sobre quem seria o sujeito ativo que pratica os delitos na internet:

- a) o inside hacker. indivíduo que tem acesso legítimo ao sistema, mas que o utiliza indevidamente ou exorbita do nível de acesso que lhe foi permitido, para obter informações classificadas. Em geral, são funcionários da empresa vítima ou servidores públicos na organização atingida;
- b) o outsider hacker, que vem a ser o indivíduo que obtém acesso a computador ou a rede, por via externa, com uso de um modem, sem autorização.

Os agentes dos delitos possuem características similares uns de outros são geralmente indivíduos que possuem um mesmo nível intelectual, social e econômico.

O perfil do criminoso, baseado em pesquisa empírica, indica jovens, inteligentes, educados, com idade entre 15 e 32 anos, do sexo masculino, magros, caucasianos, audaciosos e aventureiros, com inteligência bem acima da média e movidos pelo desafio da superação do conhecimento, além do sentimento de anonimato, que bloqueia seus parâmetros de entendimento para avaliar sua conduta como ilegal, sempre alegando ignorância do crime e, simplesmente, uma brincadeira. Preferem ficção científica, música, xadrez, jogos de guerra e não gostam de esportes, sendo que suas condutas geralmente passam por três estágios: o desafio, o dinheiro extra, e, por fim, os altos gastos e o comércio ilegal.

Pode-se ainda chegar à conclusão de que existem três categorias, a primeira categoria de pessoas dos 15 aos 17 anos de idade, ou seja, inimputáveis, nesta classe se encontram adolescentes hackers que praticam desde ilícitos de pouca expressão, tais como, montam páginas na Internet, pegam na própria rede fotos de pornografia infantil, etc, até ilícitos de maiores consequências, tais como, receitas de bombas, crimes raciais, etc.

Na segunda categoria estão as pessoas com um conhecimento mais profundo em computação, aqueles na média dos 17 anos aos 25 anos de idade, que geralmente tentam obter pequenas vantagens com arrimo nos ilícitos cometidos, compra de CDs com números de cartões de créditos falsos, etc.

Enquanto a terceira categoria são aqueles que usam a rede para nocivamente difundir ideais Fascistas, Nazistas, praticam crimes financeiros, portanto, esta é a categoria mais perigosa.

Portanto, verifica-se que as condutas do delinquente 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, como se pode perceber, dificulta sobremaneira, especialmente quando se trata de menores inimputáveis, que o cyber-criminoso seja surpreendido em flagrante ou mesmo que se suspeite dele.

Cumprir mencionar que, não é difícil identificar a máquina que praticou os crimes através da Internet, posto que todo computador possui um número, o problema é saber quem utilizou o computador para cometer o ilícito. Quanto às empresas, estabelecimentos de ensino, casa de amigos, Lan-houses, Cyber Cafés e outros locais em que o uso é feito por diversas pessoas, a investigação pode ser infrutífera.

Ademais a vítima conta com o Direito Processual Penal, como por exemplo, a busca e apreensão do computador, para que seja adiante periciado, interrogatório do acusado, entre outras medidas.

Neste sentido o Colendo Supremo Tribunal Federal, mostrando a necessidade da perícia técnica nestes casos manifestou:

Crime de Computador: publicação de cena de sexo intanto-juvenil (ECA -art. 241), mediante inserção em rede BBS/INTERNET de computadores, atribuída a menores: tipicidade: prova pericial necessária à demonstração da autoria: HC deferido em parte. (STF - HC nº 76689/PB - Ministro Sepúlveda Pertence).

Assim, crer que estamos diante de uma atitude criminosa que jamais será desvendada é no mínimo inconsequente.

#### 4.1 FORMAS DE ATUAÇÃO DOS CRIMINOSOS

Favorecido pela possibilidade de anonimato da internet e pela ausência, em muitos países, de legislações específicas, o mercado de crimes na Internet tornou-se um dos mais lucrativos do mundo. Cumprir ressaltar que a pedofilia movimentou milhões de dólares por ano e expõe crianças indefesas a abusos que nem mesmo adultos suportariam.

Ao contrario do que muitos podem pensar, os crimes vinuais estão diretamente ligados ao mudo real. Cumpre ressaltar que no caso da pedofilia na Internet para que as imagens sejam disponibilizadas na web, crianças e adolescentes foram abusados e explorados sexualmente.

Rossini (2002, p. 180-210), cita, dentre outras condutas, vejamos:

- a) spamming, como forma de envio não-consentido de mensagens publicitárias por correio eletrônico a uma massa finita de usuários da rede, conduta esta não oficialmente criminal, mas antiética;
- b) cookies, a quem chama "biscoitinhos da web", pequenos arquivos de textos que são gravados no computador do usuário pelo browser quando ele visita determinados sites de comércio eletrônico, de forma a identificar o computador com um número único, e obter informações para reconhecer quem está acessando o site, de onde vem, com que periodicidade costuma voltar e outros dados de interesse do portal;
- c) spywares, como programas espiões que enviam informações do computador do usuário da rede para desconhecidos, de maneira que até o que é teclado é monitorado como informação, sendo que alguns spywares têm mecanismos que acessam o servidor assim que usuário fica on-line e outros enviam informações por e-mail;
- (...)
- e) sniffers, programas espiões, assemelhados aos spywares, que, introduzidos no disco rígido, visam a rastrear e reconhecer e-mails que circundam na rede, de forma a permitir o seu controle e leitura;

Sabe-se que vários fatores contribuem de forma avassaladora para a prática dos diversos e novos delitos praticados na rede, um dos grandes fatores é a globalização.

Neste sentido Blum (2000, p. 117) assinala que:

A reprimenda à criminalidade praticada com o emprego de meios eletrônicos, notadamente os que avançam na rede mundial de computadores, terá de ser acionada por todos os povos civilizados e essa perspectiva deriva, com certeza, do próprio fenômeno da globalização.

Os agentes de delitos praticados na rede utilizam sua criatividade para inovar sempre, criando a cada dia um novo método de atuação.

Para Ferreira, (2000, p. 210) a conduta do agente criminoso revela:

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

Infelizmente, a legislação brasileira é extremamente confusa, não havendo uma clara caracterização dos crimes realizados na Internet.

## 5 A LEGISLAÇÃO BRASILEIRA NOS CRIMES DE INFORMÁTICA

A criminalidade na rede, caracterizada pela dificuldade de investigação, piova e aplicação aa loi penal, pelo caráter transnacional e ilimitado dessas condutas, o que pode gerat conflitos de falta de legislação específica, bem como de Direito Internacional, ejn aecortência da competência da jurisdição sancionadora.

Valirn (2000, p. 115) diz que:

O grande problema ao se trabalhar com o conceito de jurisdição e territorialidade na Internet reside no caráter internacional da rede. Na Internet não existem fronteiras e, portanto, algo que nela esteja puulicado estará em todo o mundo. Como, então, determinar o juízo competente para analisar um caso referente a um crime ocorrido na rede?

Um dos maiores problemas enfrentado pela sociedade é a falta de uma legislação específica que tipifique os crimes praticados na rede, carece de uma Lei própria, pois muitos delitos ainda se utilizada da analogia para a punição do infrator. Além da competência para julgar os delitos, uma vez que este atinge diversas fronteiras.

Segundo Fraga (2001, p. 366):

Em 1986, (...) publicou o relatório denominado *Computer-Related Crime: Analysis of Legal Policy*, no qual abordou o problema da criminalidade informática e a necessidade de tipificação de certas condutas, como fraudes financeiras, falsificação documental, contratação de *software*, interceptação de comunicações telemáticas, entre outras.

O Brasil sendo um Estado democrático de Direito, conforme prevê o art. 1º da Constituição Federal de 1988, necessariamente aplicam-se em seu território os princípios da legalidade e da anterioridade da lei penal.

O art. 5º, inciso XXXIX, da Constituição Federal, estabelece, entre as liberdades públicas, a garantia de que: "não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal", bem como o art. 1º do Código Penal, por sua vez, estatui que: "Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal".

Tais dispositivos traduzem, no direito positivo, os velhos princípios gerais do *nullum crimen sine lege* e *núlla poena sine lege*.

Conde (1998, p. 281-282) diz que:

A tipicidade é a adequação de um fato cometido à descrição que desse fato tenha feito a lei penal. Por imperativo do princípio da legalidade, em sua vertente do *nullum crimen sine lege*, somente os fatos tipificados na lei penal como delitos podem ser considerados como tais.

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

Por sua vez, Jescheck (1978, p. 372-373) assevera que:

O conteúdo do injusto de toda classe de delito toma corpo no tipo, para que um fato seja antijurídico penalmente há de corresponder aos elementos de um tipo legal. Esta correspondência se chama tipicidade.

Para que se admita um novo tipo penal no ordenamento brasileiro, é imprescindível que se atendam outras regras constitucionais, no sentido da elaboração legislativa.

Os delitos praticados na internet, a competência é duplamente federal, porque, conforme o art. 22, inciso I, da Constituição Federal de 1988, compete privativamente à União legislar sobre direito penal e, segundo o inciso IV, do mesmo artigo, a União também detém a competência para legislar sobre informática.

A colocação do problema nesses termos tem relevância porque, em tratando de Internet, nos defrontamos com velhos delitos, executados por diferentes modos (muda o *modus operandi*), ao mesmo tempo em que estamos diante de uma nova criminalidade, atingindo novos valores sociais.

Quanto aos velhos delitos, já tipificados no Código Penal não há dificuldades para operar o sistema penal. Utiliza-se as fórmulas e diretrizes do processo penal, basta adequar e modernizar as formas de persecução penal pelos órgãos oficiais, principalmente no tocante à investigação criminal pela Polícia Judiciária, uma vez que os ciberdelinquentes têm grande aptidão técnica.

O Direito brasileiro não oferece solução para condutas lesivas ou potencialmente lesivas que possam ser praticadas pela Internet e que não encontrem adequação típica no rol de delitos existentes no Código Penal e nas leis especiais brasileiras ou nos tratados internacionais, em matéria penal, do qual o Estado brasileiro seja parte.

Para a adequação típica dos crimes ocorridos via internet, será necessário, certamente, um esforço interpretativo e poder-se-á objetar com o argumento de que não se admite analogia em Direito Penal, levando à conclusão de que tais delitos seriam atípicos, ou seja, impunes.

Neste sentido Morreira (2001, p. 5-8) cita o julgado abaixo:

Em acórdão ainda recente, de 27.7.2000, a E. Sexta Câmara Criminal do Tribunal de Justiça do Rio de Janeiro, no julgamento do Habeas Corpus nº 1.916/00, concedeu a ordem para trancar, por falta de justa causa, ação penal intentada pelo Ministério Público contra várias pessoas a quem se imputava a transmissão, pela internet, de fotografias pornográficas que incluíam crianças e adolescentes. A denúncia buscava fundamento no art. 241 do Estatuto da Criança e do Adolescente, que comina pena de 1 a 4 anos de reclusão a quem "fotografar ou publicar cena de sexo explícito ou pornográfico envolvendo criança ou adolescente". (...) Não configurado o tipo delituoso, seria impossível recorrer à analogia para incriminar os denunciados, o que infringiria o princípio da reserva legal e a consequente proibição da analogia in malam partem. A atipicidade resultaria do fato de não se haver utilizado "documento palpável, sensível" — única forma de "publicar", no juízo do relator e da maioria da Câmara. Os denunciados teriam "divulgado" as fotografias; conforme se lê na ementa, porém, "divulgar não é publicar: quem publica, divulga, certamente; mas nem todo aquele que divulga, publica". E isso porque "a divulgação pode ser por qualquer forma, até oral, mas a publicação não prescinde da existência de objeto material corpóreo". Em direito, só se legitima o uso do verbo "publicar" para designar comportamento que empregue "objeto material corpóreo", que se traduza em "impressão ou edição"? Tanto na linguagem comum, quanto na própria do direito, a significação de "publicar" de modo nenhum se prende necessariamente a este ou àquele modo de agir; em especial, ao que se vale de "documento palpável, sensível", de "objeto material corpóreo", menos ainda de instrumento escrito, estampado, impresso. Quem quer que torne pública alguma coisa, seja como for, publica-a. Ao contrário do que pareceu ao eminente relator do acórdão, é perfeitamente possível "publicar um segredo oralmente". (...) para que se configure o tipo do art. 241 do Estatuto da Criança e do Adolescente, não é preciso, em absoluto, que a "cena de sexo explícito ou pornográfico envolvendo criança ou adolescente" seja estampada, impressa, dada a lume em livro, jornal, revista, inserida em "documento palpável", em "objeto material corpóreo". Se a cena é divulgada por outro meio, de tal sorte que a ela possam ter acesso setores indiscriminados do público, pessoas em geral, publicada está ela, e configurado o tipo. Não se exige, na hipótese de efetuar-se a publicação em "documento palpável", em "objeto material corpóreo", que todos, sem exceção, pudessem in concreto ver o livro, o jornal, a revista: bastaria, à evidência, que o veículo da publicação fosse acessível ao público em geral. Com a devida vênia, portanto, na espécie decidida pela E. 6ª Câmara Criminal do Tribunal de Justiça do Rio de Janeiro, ao julgar o Habeas corpus nº 1.916/00, não estava em causa o princípio nullum crimen sine lege, nem era mister, para reconhecer como típica a conduta descrita na denúncia, fazer uso da analogia in malam partem.

Portanto, existem casos em que advogados bem preparados conseguem livrar seus clientes acusados de crimes praticados na rede, alegando que na esfera Penal,

não ser possível fazer analogia, a não ser *in bonan panem*, não há que se falar em realização de diversos delitos pela Internet.

A falta de uma lei brasileira sobre diversos crimes cibernéticos tornou possível driblar a legislação brasileira já existente, portanto, não ser crime, onde faz com que os agentes denunciados estão conseguindo *habeas corpus* facilmente.

Esse é um exemplo das dificuldades exegéticas e dos problemas consequentes no tocante à impunidade e à insegurança jurídica que a falta de leis para diversos crimes de informática acarreta para a coletividade e para o cidadão, respectivamente.

Alguns tipos penais, que descrevem crimes de informática, já existem, como pode verificar no art. 10 da Lei Federal n. 9.296/96, que considera crime, punível com reclusão de 2 a 4 anos e multa, "realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo de Justiça, sem autorização judicial ou com objetivos não autorizados em lei".

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

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

O art. 313-B, do Código Penal, introduzido pela Lei n. 9.983/2000, que tipificou o crime de modificação ou alteração não autorizada de sistema de informações, com a seguinte redação: "Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente", cominando-lhe pena de detenção, de 3 (três) meses a 2 (dois) anos, e multa.

O art. 325, §1º, incisos I e II, introduzidos pela Lei n. 9.983/2000, tipificando novas formas de violação de sigilo funcional, nas condutas de quem "I - permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra

forma, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública" e de quem "II - se utiliza, indevidamente, do acesso restrito", ambos sancionados com penas de detenção de 6 meses a 2 anos, ou multa.

O art. 12, *caput*, §§1- e 2-, da Lei Federal n. 9.609/98, que tipifica o crime de violação de direitos de autor de programa de computador, punindo-o com detenção de 6 meses a 2 anos, ou multa; ou com pena de reclusão de 1 a 4 anos e multa, se o agente visa ao lucro.

O art. 2º, inciso V, da Lei Federal n. 3.137/90, que considera crime "utilizar ou divulgar programa de processamento de dados que permita ao sujeito passivo da obrigação tributária possuir informação contábil diversa daquela que é, por lei, fornecida à Fazenda Pública".

O art. 72 da Lei n. 9.504/97, que cuida de três tipos penais eletrônicos de natureza eleitoral.

Para Ferreira (2000, p. 208) essas leis:

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

Greco (2000, p. 15) assinala que: "Além das repercussões na ideia de soberania e na eficácia das legislações, não se pode deixar de mencionar os reflexos que serão gerados em relação ao exercício da função jurisdicional".

Problemas de soberania, jurisdição e competência estarão cada dia mais presente no cotidiano dos juristas e dos operadores do Direito que se defrontarem com questões relativas à internet.

Desta feita, um crime cometido na Internet ou por meio dela consuma-se em todos os locais onde a rede seja acessível.

Martins (2001, p. 51-52) afirma que:

Toda comunicação eletrônica pública deve ter o mesmo tratamento para efeitos ressarcitórios da comunicação clássica pela imprensa. A desfiguração de imagem por informações colocadas fora da soberania das leis do país ensejaria os meios ressarcitórios clássicos, se alavancada no Brasil.

Como alternativa à fórmula da Lei de imprensa, assinala-se o art. 72 do Código de Processo Penal que estabelece a competência do foro de domicílio do réu, quando não for conhecido o lugar da infração.

Ferreira (2000, p. 213) entende que:

Já se deu a internacionalização da criminalidade informática, devido à mobilidade dos dados nas redes de computadores, facilitando os crimes cometidos à distância. Diante desse quadro, é inispensável que os países do globo harmonizem suas normas penais, para prevenção e repressão eficientes.

No tocante aos crimes à distância, deve-se aplicar a teoria da ubiquidade, que foi acolhida no art. 6º do Código Penal: "Considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado".

Martins (2001, p. 44) afirma que:

O recente fenômeno da universalização das comunicações por computador exige a preparação de uma legislação universal, de controle de todos os países, mediante disciplina jurídica idêntica e com possibilidades de intervenção supranacional de órgãos internacionais e/ou comunitários.

Cumpra ainda citar alguns julgados proferidos pelo Tribunal de Justiça do Rio de Janeiro com relação aos crimes praticados na Internet:

QUEBRA DE SIGILO BANCÁRIO. LEGITIMIDADE DO M.P. PRINCÍPIO DA INDISPONIBILIDADE. RECLAMAÇÃO PROCEDENTE. Reclamação. Decisão que indefere pedido de quebra de sigilos bancário e telefônico e dados de usuário da internet. Crime de furto. Pedido formulado pelo "parquet", após esgotadas todas as diligências possíveis para a apuração dos fatos delituosos, cujo indeferimento torna impossível a aferição necessária. Aplicação da Lei Complementar n. 105/01, que permite a quebra do sigilo, na forma do art. 1º, par. 4º, quando necessária à apuração da ocorrência de qualquer ilícito, em especial nos crimes que arrola nos incisos I a IX, rol meramente exemplificativo, diante da expressão "especialmente" utilizada pelo legislador. Diversamente do entendimento manifestado pela magistrada, as medidas possibilitarão elucidar o delito, e devem »er concretizadas, conferido o respaldo legal. A atribuição para a iniciativa da ação penal e o dever de diligenciar a verdade real, diante de indícios criminosos, compete ao órgão do Ministério Público, diante do primado dos princípios da indisponibilidade e obrigatoriedade. Procedência da Reclamação. (TJRJ. RECLAMAÇÃO - 2007.077.00030. JULGADO EM 18/10/2007. OITAVA CAMARA CRIMINAL - Unanime. RELATORA: DESEMBARGADORA SUELY LOPES MAGALHÃES).

TRANSAÇÃO VIA INTERNET. ESTELIONATO. CONTINUIDADE DELITIVA. Apelação. Crimes de estelionato praticados contra várias vítimas. Ofertas de diversos produtos no sítio Mercado Livre em momentos diversos. Fatos que

caracterizam o crime de estelionato. Contrato de compra e venda pela internet. Depósitos antecipados realizados em contas correntes dos apelantes sem a entrega posterior dos produtos pelos mesmos. Idêntica mecânica delitiva que possibilitou a identificação dos réus, ora apelantes. Pedido de absolvição por insuficiência de provas. Impossibilidade. Prova oral contundente. Reconhecimento de crime único de estelionato, em continuidade delitiva. Falsidade documental caracterizada. Ajuste da dosimetria. Provimento parcial dos apelos. (TJRJ. AC - 2007.050.00686. JULGADO EM 15/05/2007. TERCEIRA CAMARA CRIMINAL - Unanime. RELATOR: DESEMBARGADOR MARCO AURELIO BELLIZZE).

INCITAÇÃO A PRÁTICA DE INFRAÇÃO PENAL. INTERNET. INVESTIGAÇÃO POLICIAL QUEBRA DE SIGILO. C.P.P. POSSIBILIDADE. Reclamação. Sítio de relacionamento Orkut. Investigação policial. Incitação de crimes. Comunidade "Eu sei Dirigir Bêbado" e "Sou Menor Mas Adoro Dirigir". Recusa do representante legal da empresa que administra o sítio de relacionamentos na Internet em prestar informações sobre os membros e criadores das referidas comunidades. Conduta investigada que ostenta potencial para causar perda de vidas humanas, principalmente de jovens, que estariam sendo estimulados a conduzir veículos automotores sem habilitação ou em estado de embriaguez. Indeferimento pelo Juízo Criminal de pedido de requisição de informações e dados cadastrais de membros e criadores das comunidades, sob o fundamento de que a Lei n. 9.296 não autoriza a quebra do sigilo para apuração de crime apenado com detenção. Distinção entre comunicações telefônicas e telemáticas e dados registraes respectivos, estes equiparados a documentos, cuja quebra de sigilo não tem como base a Lei n. 9.296/96, mas sim o Código de Processo Penal. Necessidade da medida. Informações imprescindíveis à investigação. Ponderação de interesses. Proporcionalidade e razoabilidade da medida. Benefícios à coletividade superiores ao desconforto de alguns membros das comunidades investigadas. O direito à intimidade, que não é absoluto, deve ceder em função de interesse de maior dimensão. O direito à intimidade não se presta a impedir a apuração de crime, sob pena de converter-se em garantidor da impunidade. Os princípios constitucionais delimitam a forma e a extensão do controle dos atos pelo Poder Público estabelecendo o equilíbrio de armas entre a defesa e a acusação, mas não impedem a atuação estatal legítima e legal de investigar e punir condutas contrárias à lei penal. Procedência da Reclamação. (TJRJ. RECLAMAÇÃO - 2006.077.00062. JULGADO EM 21/12/2006. TERCEIRA CAMARA CRIMINAL - Unanime. RELATOR: DESEMBARGADOR MARCO AURELIO BELLIZZE).

*FURTO QUALIFICADO. HACKERS. CONTA CORRENTE BANCARIA. FRAUDE INTERNET.* Apelação. Crime de furto mediante fraude em continuidade delitiva. Art. 155, par. 4., inciso II, na forma do art. 71, ambos do Código Penal. Crime de interceptação das comunicações telemáticas em continuidade delitiva. Art. 10 da Lei n. 9.296/96, n/f do art. 71, do Código Penal. Hacker. Concurso material (art. 69 do Código Penal). Apelo defensivo com preliminares de inépcia da denúncia, cerceamento da defesa, incompetência da Justiça Estadual, nulidade dos "grampos telefônicos" e das provas deles derivadas e nulidade do laudo pericial. Alegações meritórias de insuficiência de prova da autoria e de materialidade para a condenação, de capitulação jurídico-penal equivocada do fato, de ocorrência de crime único, de exacerbação da dosimetria da pena sem fundamentação e de ilegalidade da custódia cautelar. Questões preliminares. Rejeição. Denúncia que descreve satisfatoriamente as condutas do apelante, possibilitando-lhe o exercício do direito de defesa. Competência da Justiça Estadual para julgar o feito em que correntista da Caixa Econômica Federal figura como possível lesado ao lado de dezenas de outros lesados correntistas de outras instituições bancárias. Interceptações telefônicas autorizadas pelo Juízo competente. Lícitude da prova. Integridade das provas derivadas. Laudo pericial que, na realidade, foi recepcionado pelo juízo sentenciante como prova documental. Contraditório estabelecido com a formulação de quesitos pela defesa do apelante.

Condenação amparada em mais de um elemento de prova do contundente e coeso conjunto probatório. Suficiência e legalidade das provas. Rejeição das preliminares. Furto x estelionato. Lesados que tiveram valores subtraídos de suas contas. Furto mediante fraude. Hacker. Absorção do crime de interceptação das comunicações telemáticas pelo crime de furto. Se não houve entrega da coisa pelo lesado, mas subtração, a conduta se ajusta ao tipo penal que prevê o crime de furto. Crime de furto mediante fraude e crime de interceptação das comunicações telemáticas. Conduta do agente consistente em criar propaganda falsa em sítio da internet, objetivando atrair usuários para, infectando-se seus computadores com vírus TROJAN (cavalo de tróia), obter os dados bancários e senhas das vítimas, para a consumação da subtração dos valores lá depositados. Se tal conduta, em sua totalidade, consubstancia a fraude que qualifica o furto, não é possível o reconhecimento do crime autônomo do art. 10 da Lei n. 9296/96, o que caracterizaria "bis in idem". Concurso material que resultaria em censura penal desproporcional à gravidade da conduta, de vez que se as subtrações continuadas fossem praticadas mediante o emprego de arma de fogo, conduta mais grave, a pena seria menor que a fixada na sentença. Razoabilidade. Reconhecimento de crime único de furto qualificado pela fraude, em continuidade delitiva. Dosimetria da pena. Pena-base. Circunstâncias judiciais. Fundamentação adequada e suficiente. Princípios da culpabilidade e da individualização da pena. Regime de pena fechado adequado às circunstâncias do caso concreto. Prisão cautelar. Legalidade da custódia cautelar, no curso do processo, reconhecida pela Turma Revisora e pelo E. Superior Tribunal de Justiça. Superveniência de sentença condenatória, inaugurando novo título prisional cautelar. Coerência na manutenção da custódia, agora mais justificada em razão do juízo de certeza exposto na decisão que impôs severa censura penal. Inexistência de fato novo suficiente a afastar o pretérito reconhecimento da presença dos requisitos do art. 312 do Código de Processo Penal. Necessidade da manutenção da custódia cautelar comprovada. Precedente do E. Superior Tribunal de Justiça (HC 54.544/SC, Rei. Min. Gilson Dipp, 5a. Turma, j. 12.6.06, DJ 1.8.06, p. 490): "As peculiaridades concretas das práticas supostamente criminosas e o posto do acusado na quadrilha revelam que a sua liberação poderia ensejar, facilmente, a reiteração da atividade delitiva, indicando a manutenção da custódia cautelar. As eventuais fraudes podem ser perpetradas na privacidade da residência, do escritório ou, sem muita dificuldade, em qualquer lugar em que se possa ter acesso à rede mundial de computadores. A real possibilidade de reiteração criminosa, constatada pelas evidências concretas do caso em tela, é suficiente para fundamentar a segregação do paciente para garantia da ordem pública". Rejeição das preliminares a provimento parcial do recurso defensivo. (TJRJ. AC -2006.050.03841. JULGADO EM 21/12/2006. TERCEIRA CAMARA CRIMINAL - Unanime. RELATOR: DESEMBARGADOR MARCO AURELIO BELLIZZE).

INTERNET. QUEBRA DO SIGILO DE DADOS CADASTRAIS. MAUS TRATOS CONTRA ANIMAIS. LEI N. 9296, DE 1996. INAPLICABILIDADE. RECLAMAÇÃO. SIGILO DE DADOS. PLEITO MINISTERIAL DE REFORMA DA DECISÃO QUE INDEFERIU MEDIDA CAUTELAR DE QUEBRA DO SIGILO DE DADOS CADASTRAIS DE USUÁRIOS DE INTERNET, PARA APURAÇÃO DE CRIMES DE APOLOGIA DE MAUS TRATOS CONTRA ANIMAIS, VEICULADOS PELO SITE DE RELACIONAMENTO ORKUT. INAPLICABILIDADE, IN CASU, DA LEI Nº 9.296/96. MEDIDA RAZOÁVEL E INDISPENSÁVEL PARA IDENTIFICAR OS AUTORES DOS DELITOS E, POR CONSEQUENTE, VIABILIZAR A PERSECUÇÃO CRIMINAL RECLAMAÇÃO A QUE SE DÁ PROVIMENTO.1. Sendo a quebra de sigilo de dados cadastrais de usuários de internet, no caso concreto, medida indispensável eis que se apresenta como a única via capaz de possibilitar a identificação dos autores das infrações penais investigadas, a fim de possibilitar a respectiva persecução criminal -, deve ser ela deferida, até porque o direito à intimidade dos usuários do site de relacionamento ORKUT

deve ceder em função de um interesse maior, coletivo, qual seja, o de apuração de crimes de apologia de fatos delituosos - no caso, específico, de apologia de crime de maus-tratos contra animais -, até porque não se trata de quebra de sigilo de comunicação telemática, mas tão-somente de quebra de dados cadastrais, não havendo, por conseguinte, que se falar em aplicação da Lei nº 0.296/96. 2. Recurso provido. (TJRJ. RECLAMAÇÃO - 2007.077.000304. JULGADO EM 11/12/2007. SEGUNDA CAMARA CRIMINAL - Unanime. RELATOR: DESEMBARGADOR JOSE AUGUSTO DE ARAUJO NETO).

TRANSAÇÃO VIA INTERNET. DESCUMPRIMENTO DO CONTRATO. ESTELIONATO. CARACTERIZAÇÃO. Crimes contra o patrimônio. Estelionato. Artigo 171, "caput", c/c artigos 61, inciso I, e 65, inciso I, do Código Penal. Pena: 2 anos e 6 meses de reclusão, regime fechado, e 90 dias-multa, no valor unitário mínimo legal. Apelo defensivo: a) absolvição, com base no princípio da intervenção mínima do Direito Penal nos crimes contra o patrimônio, e, implicitamente, por tratar-se de "fraude civil"; b) reconhecimento da circunstância prevista no artigo 65, inciso III, letra "d", do Código Penal, com recálculo da pena; c) afastamento da reincidência por não estar comprovada, e, além do mais, foi desrespeitada a Súmula n. 241 do Superior Tribunal de Justiça, pois a agravante foi considerada nas duas primeiras fases da dosimetria da pena; d) fixação do regime aberto, ressaltando que a imposição do fechado não está fundamentada; e) reconhecimento da continuidade delitiva (artigo 71 do Código Penal); f) concessão da substituição da pena de prisão na forma do artigo 44 do Código Penal. Na fase policial o réu confessou detalhadamente as fraudes que aplicava através de anúncios em sítios da internet de fictícias ofertas de vendas de bens, tendo, ao ser interrogado em juízo, transferido a responsabilidade pela não entrega dos bens, mesmo com o recebimento do preço através de depósitos bancários, para terceira pessoa não identificada. O lesado declarou que, ao reclamar com o réu via telefone a não entrega do notebook "comprado" 9 pago, foi pelo mesmo ameaçado de morte. Presentes estão todas as elementares do crime de estelionato, não se tratando de mero descumprimento de contrato de compra e venda. Ao retratar a confissão extrajudicial, afastou o réu a possibilidade de beneficiar-se com a respectiva circunstância atenuante. A reincidência não está configurada, pois a condenação indicada na sentença transitou em julgado em data posterior ao cometimento do crime em julgamento. A exasperação da pena-base está corretamente fundamentada, não se podendo o mesmo dizer quanto à imposição do regime mais severo. Impossível o reconhecimento da continuidade delitiva, inclusive porque já transitou em julgado a condenação no outro processo. O acusado não tem mérito para beneficiar-se do artigo 44 do Código Penal. Apelo parcialmente provido para, afastando a circunstância agravante do artigo 61, inciso I, do Código Penal, definir a resposta penal em 1 ano e 6 meses de reclusão, a ser inicialmente cumprida em regime semi-aberto, e 50 dias-multa, ficando mantidas as demais cláusulas da sentença. (TJRJ. AC - 2007.050.05838. JULGADO EM 29/11/2007. OITAVA CAMARA CRIMINAL - Unânime. RELATOR: DESEMBARGADOR MARCUS QUARESMA FERRAZ).

## 5.1 CRIAÇÃO DE NOVOS TIPOS PENAIIS

A legislação existente e o alerta do Judiciário em brilhantes decisões sobre os crimes realizados na Internet não fazem eco no Congresso Nacional, onde tramitam vários projetos de Lei sobre o assunto, cumprindo destacar o Projeto de Lei Nº 84/99,

que dispõe sobre os Crimes cometidos na área de Informática, suas Denalidades e dá outras providências, veja:

O Congresso Nacional decreta:

(...)

### **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 forma 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; 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 magnética, 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.

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

Criação, desenvolvimento ou inserção em computador de dados ou programa de computador 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 a 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:** 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.

Deputado LUIZ PIAUHYUNO

Assim sendo o referido Projeto de Lei de Crimes Eletrônicos, proposto pelo Senador (PMDB/MG) Eduardo Azeredo, já passou pelo Senado e entrou em caráter de urgência na pauta da Câmara dos Deputados. Se aprovado, pode ser sancionado pelo presidente Luiz Inácio Lula da Silva e entrar em vigor imediatamente. Contudo, a possibilidade preocupa internautas brasileiros, circula na rede uma petição online contrária à aprovação já possui mais de 130 (cento e trinta) mil assinaturas.

A conduta criminosa já está definida em nossa legislação penal em vigor. A internet é apenas uma ferramenta para o cometimento do crime. Explicitamente, os Tribunais Superiores já reconheceram diversos delitos praticados na rede como crime, independentemente do instrumento de que o agente se vale para cometê-lo.

Alguns dos delitos são passíveis de tipificação pela atual estrutura normativa penal, outros ainda são despercebidos. Faz-se necessário que haja uma reforma na legislação criminal, nos âmbitos nacional e internacional, e os órgãos de investigação precisam ser estruturados de maneira a fluírem seus trabalhos no melhor caminho.

Alguns procedimentos vêm sendo tomados, mas, é necessário que estes tenham eficácia, e sejam seguidos, para que não ocorra tanta impunidade.

A proteção da rede é assunto que ganha cada vez mais atenção da sociedade e, por decorrência, dos legisladores. Com toda razão, sobretudo quando novas tecnologias favorecem a prática de crimes dessa natureza.

O Congresso vem lentamente agindo sobre a questão, ele não consegue discutir e aprovar as leis com a necessária celeridade. Não é necessário a confecção de um novo Código Penal, nem tão pouco uma lei que discipline todos os crimes de informática. As leis atuais podem e devem ser aproveitadas.

No entanto, lacunas existem, carecendo o Direito de uma lei que regule o tema e venha a proteger os bens jurídicos ligados a informática, criando novos tipos penais.

Portanto, a falta de legislação específica para punir os crimes digitais é um dos principais problemas para o sistema financeiro brasileiro. O combate aos crimes eletrônicos deveria ser mais efetivo. A legislação brasileira é antiquada e pune os crimes digitais de maneira mais branda do que os crimes físicos, mas que aqueles são tão danosos ao sistema financeiro quanto estes.

Cumprindo ainda ressaltar que o investimento voltado à segurança das instituições financeiras representa, pelo menos, 10% do orçamento total de TI. Em 2007, R\$ um bilhão e quatrocentos mil reais foram aplicados em segurança dentro das instituições financeiras.

Desta feita, enquanto não forem codificadas em Leis, as condutas de crimes digitais devem ser adequadas à legislação positiva existente, onde encontram guarida, ao menos incidental, variando a sua tipificação conforme o bem jurídico agredido.

## **6 PREVENÇÃO DO DELITO**

Repete-se o acesso à informação sempre foi valorizado, constituindo forma e fonte de poder, sendo seu controle patrimônio econômico político e cultural. Contudo, tais benefícios não surgem sozinhos, trazem consigo seu ponto negativo, tais como, os crimes e criminosos digitais, os quais estão aumentando gradativamente por todo o mundo, de forma avassaladora.

Os profissionais de polícia têm grande receio com o crescimento geométrico do uso da Internet, além da dispersão e falta de controle, uma vez que, surge espaço na rede exclusivamente para as atividades criminosas, ou seja, atrelando os ideais ou interesses de uma minoria, daqueles que utilizam da rede para a prática de delitos.

Desta feita, gera uma preocupação que está chamando a atenção da polícia de todo o mundo, especialmente no que diz respeito à coleta de evidências e materialidade dos delitos.

Mais uma vez, a impunidade é garantida pela atuação equivocada das autoridades, o que serve como incentivo à prática do crime.

Ressalta-se que diversas empresas em todo o País têm sido vítimas dos crimes de computadores, e o fato só não é mais grave, porque muitas delas assumem os

prejuízos, encobrindo os delitos, ao invés de ter uma propaganda negativa, além do grupo de criminosos digitais ainda ser pequeno.

Medidas de cunho internacional têm sido planejadas. No Brasil algumas ações efetivas, às vezes um tanto isoladas, vêm sendo desenvolvidas.

A atuação policial em crimes de computador requer investigação especializada e ação efetiva. Há raríssimos policiais no Brasil preparados para combater esses tipos 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.

Neste sentido Miranda (1999, n. 37) preceitua que:

Os raros investimentos que são feitos na área de qualificação em termos digitais restringem-se a 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 a atuação na área digital às Intranets e nas necessidades internas de compilação e consulta instantânea, e a 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 a obtenção de evidências fáticas a partir de apreensões autorizadas.

Cumprir citar que o Estado do Rio de Janeiro já é munido com Delegacia especializada em Repressão aos Crimes da Informática, onde são apuradas as diversas modalidades ilícitas enquadráveis sob a legislação penal atual. A Polícia Federal também está capacitada a atuar nesta área.

Colares (2002, n. 59) afirma que:

A avassaladora maioria das prisões por este delito foi efetuada ou por flagrante de delito ou por confissão do acusado. Isto ocorre devido à falta de eficácia e contundência que apresentam as demais provas neles geradas (que em geral são documentos eletrônicos), já que no Direito Penal não se admite presunção de culpa ou autoria para se efetuar a prisão: imprescindível é ter certeza quanto à veracidade dos fatos.

A Internet propicia, devido a sua rapidez, a possibilidade de ser eliminados a qualquer momento quaisquer vestígios necessários para a comprovação do delito. Tem-se constatado que na maioria das vezes estes delitos ainda permanecem impunes, porque ainda continuam a ser novidade para os mecanismos coercitivos estatais.

O crescimento exponencial da tecnologia e da Internet permite que o cybercriminoso tenha proveito dos avanços da tecnologia. A fim de adequar as ações policiais a esse novo desafio, impõe-se a criação da cultura e formação de policiais visando o policiamento futuro, ou seja, formar, adequar, equipar e treinar os policiais.

O passo inicial e premente é a criação de uma unidade policial especializada em investigação e atos de polícia judiciária para crimes de alta tecnologia, que englobaria os crimes de computadores e outros que aparecerem no rastro do desenvolvimento tecnológico dos próximos anos.

Repita-se a atuação da polícia em crimes de computador requer investigação especializada e ação efetiva. Não existem no Brasil policiais preparados para combater esse tipo de crime, faltando visão, planejamento, preparo e treinamento.

No entanto, policiais do mundo inteiro, já há alguns anos vêm formando os chamados "Cybercops", policiais especialmente treinados para combater tais delitos, sendo revigorante, a maximização da colaboração entre os Países, alertando para o potencial das perdas económicas, ameaças, privacidade dentre outros valores fundamentais.

Verifica-se ainda que a iniciativa privada também colabora com a nova modalidade de investigação policial, com cursos, equipamentos. Diante da necessidade premente de se antecipar ao iminente avanço dos crimes digitais, que como dito, vêm no rastro da nova ordem mundial globalizada.

A Polícia Civil de São Paulo também deu um passo na investigação digital, é a primeira instituição da América Latina a possuir página na Rede Internacional de Dados, qual seja, Internet, com diversas informações sobre a atividade policial desenvolvida, orientações de auxílio ao cidadão, bem como espaço para sugestões e denúncias, além de arquivo com fotos digitalizadas dos criminosos mais procurados pela polícia, e de crianças desaparecidas.

Destarte ainda que, a Polícia Civil de São Paulo, vem, há alguns anos, efetuando investigações de crimes por computadores com sucesso, apesar de não existir atribuição administrativa, existe apenas o embasamento jurídico do Código de Processo Penal no art. 6º e incisos, bem como decisões em inquéritos policiais, recebidos pelo Ministério Público e Juiz Corregedor da Capital.

Desta feita, com todos estes recursos o dia-a-dia tem demonstrado que a investigação de crimes por computador é muito delicada, seja pela falta de experiência

policial, como pela adoção de procedimentos desatualizados para a alta tecnologia empregada.

Atualmente existem mais de 600 milhões de usuários de computadores em todo o planeta, onde deles mais de 190 países, acessam a Internet, através de trocas de dados, sons e imagens, ou seja, com eficiência e rapidez, portanto como o acesso a rede é muito grande dificulta mais ainda a captura dos criminosos e facilita a prática dos delitos.

No entanto, sabe-se que diante da grande tecnologia aplicada, não vai demorar muito para que os criminosos ultrapassem a capacidade de apanhá-los, contando com o auxílio das vantagens da forma revolucionária do espaço cibernético, desprovido de regras sociais ou éticas, limitado apenas pela imaginação dos criminosos e pelas suas habilidades técnicas.

## 6.1 DENÚNCIAS

No Brasil, a maior parte dos crimes de informática refere-se à distribuição de pornografia infantil na web.

Neste sentido, Castro (2000, p. 179), dispõe:

*Em parceria com a Polícia Federal, o Centro de Defesa da Criança e do Adolescente Yves de Roussan (Cedeca/BA) vem desenvolvendo, desde fevereiro de 2001, o rastreamento de sites de pornografia infantil. No ano passado, foram registradas 305 denúncias somente na Bahia, das quais 38 foram apuradas e encaminhadas para a Polícia Federal.*

As denúncias de divulgação de crimes praticados na rede crescem de forma assustadora em todo o mundo e contribuem na investigação criminal.

Castro (2000, p. 178) afirma que:

A Internet Watch Foundation, uma das maiores organizações não-governamentais que luta contra a pornografia virtual, registrou, em 2001, 11.357 denúncias de sites com imagens de pornografia. O resultado foi o fechamento de 3.332 sítios.

Por uma série de dificuldades geralmente de ordem técnica ou legal as denúncias recebidas não têm levado a frequentes ações penais contra os agentes.

Tudo indica que a solução para o problema virá dos próprios usuários da rede. Alguns sites estão voltados para a denúncia de crimes praticados na rede.

O combate aos crimes na internet depende da conscientização da sociedade e da criação de uma legislação específica. Entretanto, logo após a denúncia, no caso dos pedófilos, estes "migram" para outros sites, dificultando o rastreamento e a consequente punição. O Estado está sendo omissivo nesse caso e que pretende propor uma legislação para combater esse tipo de crime.

Com o objetivo de não só receber e repassar denúncias para as autoridades locais, mas também, e de sensibilizar e mobilizar a mídia, em particular, e a população em geral para o tema, capacitar profissionais, monitorar, acompanhar o andamento das providências tomadas após o recebimento das denúncias por telefone.

Castro (2000, p. 178) assevera que:

O número de denúncias de pornografia infantil na Internet é o que percentualmente mais cresce, aumentou 6,66% em 1997, 20% em 1998 e 73,3% em 1999. Também aqui há crianças inocentes usadas por intermediários para a satisfação dos pedófilos.

Deste modo, verifica-se que mesmo esta não sendo a única solução plausível para o combate aos crimes na rede, contribui de grande forma para diminuir a prática de diversos crimes praticados na Internet, havendo-se assim a sociedade se conscientizarem neste sentido.

## CONCLUSÃO

O final deste século trouxe uma nova organização dos modos de produção e negócios e, conseqüentemente, da economia, da sociedade e da política. Primeiro foi à revolução agrícola, depois a revolução industrial, e por fim a revolução tecnológica, ou revolução da informática.

Com a grande evolução dos povos e da sociedade, foi observado então além do surgimento do computador, o surgimento da Internet posteriormente. Hoje, qualquer pessoa pode se conectar à Internet, basta se associar a um provedor de acesso.

A Internet é uma interligação simultânea de computadores de todo o planeta, constituindo forma e fonte de poder, sendo seu domínio e disponibilidade de uso um patrimônio econômico, político e cultural, em razão do valor estratégico proporcionado pela informação.

Com a popularização da Internet, ao mesmo tempo em que ela fornece inúmeras facilidades aos usuários, também torna-se um grande atrativo para o criminoso virtual.

O comércio eletrônico começou a expandir-se a velocidades inimagináveis, milhares de transações "on line" são efetivadas instantaneamente por pessoas e empresas em diversas áreas do mundo.

Futuramente, os criminosos ultrapassarão a capacidade dos organismos policiais em capturá-los, pois prevalecem da forma revolucionária do espaço cibernético, provido de regras sociais ou éticas, limitados somente por suas habilidades técnicas e o anonimato permitido pela Internet, que atrapalha na identificação da autoria dos delitos.

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

Existem os que utilizam a Internet como biblioteca do crime, difundindo práticas criminosas, na medida em que são disponibilizados, ao alcance de qualquer pessoa medianamente equipada, meios para a prática de ilícitos.

Verifica-se que delito eletrônico, é qualquer conduta criminal, cuja realização tem o emprego da tecnologia eletrônica como método, meio ou fim e, em um sentido estrito, qualquer ato ilícito penal em que os computadores, suas técnicas e funções desempenham um papel como método, meio ou fim.

Como fator criminógeno, a informática possibilita não só o cometimento de novos delitos. Existem os crimes cometidos com o computador e os cometidos contra o computador, isto é, contra as informações e programas nele contidos, conforme demonstrar-se-á.

Assim, pode-se dizer que os crimes cometidos contra o computador, ou seja, contra as informações e programas nele contidos, bem como contra as informações ou dados em trânsito por computadores, com o dolo específico de ameaça e de fraude, não abordando aqueles crimes praticados com o computador, mas cujo bem protegido pelo ordenamento jurídico é diverso, como por exemplo, a pedofilia, furto, etc.

Assim sendo, verifica-se que os crimes na internet são chamados de puros e impuros. São puros ou próprios, aqueles que sejam praticados por computador e se realizem ou se consumem também em meio eletrônico. Neles, a informática é o objeto jurídico tutelado. Já os crimes eletrônicos impuros ou impróprios são aqueles em que o agente se utiliza do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço real, ameaçando ou lesando outros bens. não-computacionais ou diversos da informática.

Portanto, crime virtual comum seria utilizar a internet apenas como instrumento para a realização de um delito já tipificado na lei penal.

Os crimes de computador são cometidos por pessoas cuja ocupação profissional implica o uso cotidiano de microcomputadores, não estando excluída, a possibilidade de serem perpetrados por meros diletantes. Os agentes dos delitos possuem características similares uns de outros são geralmente indivíduos que possuem um mesmo nível intelectual, social e econômico.

O perfil do criminoso, baseado em pesquisa empírica, indica jovens, inteligentes, educados, com idade entre 15 e 32 anos, do sexo masculino, magros, caucasianos, audaciosos e aventureiros, com inteligência bem acima da média e movidos pelo desafio da superação do conhecimento, além do sentimento de anonimato, que bloqueia seus parâmetros de entendimento para avaliar sua conduta como ilegal, sempre alegando ignorância do crime e, simplesmente, uma brincadeira. Preferem ficção científica, música, xadrez, jogos de guerra e não gostam de esportes,

sendo que suas condutas geralmente passam por três estágios: o desafio, o dinheiro extra, e, por fim, os altos gastos e o comércio ilegal.

Sabe-se que vários fatores contribuem de forma avassaladora para a prática dos diversos e novos delitos praticados na rede, um dos grandes fatores é a globalização.

Os agentes de delitos praticados na rede utilizam sua criatividade para inovar sempre, criando a cada dia um novo método de atuação.

Um dos maiores problemas enfrentado pela sociedade é a falta de uma legislação específica que tipifique os crimes praticados na rede, carece de uma Lei própria.

Quanto aos velhos delitos, já tipificados no Código Penal e na legislação extravagante, não há dificuldades para operar o sistema penal. Utiliza-se as fórmulas e diretrizes do processo penal, basta adequar e modernizar as formas de persecução penal pelos órgãos oficiais, principalmente no tocante à investigação criminal pela Polícia Judiciária.

O Direito brasileiro não oferece solução para condutas lesivas ou potencialmente lesivas que possam ser praticadas pela Internet e que não encontrem adequação típica no rol de delitos existentes no Código Penal e nas leis especiais brasileiras ou nos tratados internacionais, em matéria penal, do qual o Estado brasileiro seja parte.

Para a adequação típica dos crimes ocorridos via internet, será necessário, certamente, um esforço interpretativo e poder-se-á objetar com o argumento de que não se admite analogia em Direito Penal, levando à conclusão de que tais delitos seriam atípicos.

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

A conduta criminosa já está definida na legislação penal em vigor. A internet é apenas uma ferramenta para o cometimento do crime. Os Tribunais Superiores já reconheceram diversos delitos praticados na rede como crime, independentemente do instrumento de que o agente se vale para cometê-lo.

Desta feita, enquanto não forem codificadas em Leis, as condutas de crimes digitais devem ser adequadas a legislação positiva existente, onde encontram guarida, ao menos incidental, variando a sua tipificação conforme o bem jurídico agredido.

A atuação policial em crimes de computador requer investigação especializada e ação efetiva. Há raríssimos policiais no Brasil preparados para combater esses tipos de crime.

O crescimento exponencial da tecnologia e da Internet permite que o cybercriminoso tenha proveito dos avanços da tecnologia. A fim de adequar as ações policiais a esse novo desafio, impõe-se a criação da cultura de formação de policiais visando o policiamento futuro.

O passo inicial e premente é a criação de uma unidade policial especializada em investigação e atos de polícia judiciária para crimes de alta tecnologia, que englobaria os crimes de computadores.

Desta feita, com todos estes recursos o dia-a-dia tem demonstrado que a investigação de crimes por computador é muito delicada, seja pela falta de experiência policial, como pela adoção de procedimentos desatualizados para a alta tecnologia empregada.

As denúncias de divulgação de crimes praticados na rede crescem de forma assustadora em todo o mundo e contribuem na investigação criminal.

Com o objetivo de não só receber e repassar denúncias para as autoridades locais, mas também, e de sensibilizar e mobilizar a mídia, em particular, e a população em geral para o tema, capacitar profissionais, monitorar, acompanhar o andamento das providências tomadas após o recebimento das denúncias por telefone.

Deste modo, verifica-se que mesmo esta não sendo a única solução plausível para o combate aos crimes na rede, contribui de grande forma para diminuir a prática de diversos crimes praticados na rede, devendo-se assim a sociedade se conscientizar neste sentido.

## REFERÊNCIAS

- ALVES, Rubem A. **Filosofia da ciência**; introdução ao jogo e suas regras. 18 ed. São Paulo: Brasiliense, 1993
- ANDI, Rede. Oficina de Imagens. Pedofilia na Internet vira crime e penas são ampliadas. **Revista Bons Conselhos**, ano 1, v. 5, nov./dez. 2003.
- ARAS, Vladimir. Crimes de informática. Uma nova criminalidade. **Jus Navigandi**, Teresina, ano. 5, n. 51, out. 2001. Disponível em: <<http://www.jus.com.br/doutrina/texto.asp?id=2250>>. Acesso em: 11 abr. 2009.
- BARROS, Lucivaldo Vasconcelos. O crime na era da inform@ção. **Jus Navigandi**, Teresina. ano. 7, n. 61, jan. 2003. Disponível em: <<http://www.jus.com.br/doutrinaAexto.asp?id=3675>>. Acesso em: 11 abr. 2009.
- BASTOS, Celso Ribeiro. **Comentários à constituição do Brasil**. São Paulo: Saraiva, 1989, v. 2.
- BLUM, Renato Opice; Alexandre Daoun. **Cybercrimes**. Artigo em Direito & internet: aspectos jurídicos relevantes. Bauru: Edipro, 2000.
- BRASIL, Angela Bittencourt. **Informática jurídica**: o ciberdireito. Rio de Janeiro: edição da autora, 2000.
- CARVALHO, Ivan Lira de. Crimes na Internet. Há como puni-los. **Jus Navigandi**, Teresina, ano. 5, n. 51, out. 2001. Disponível em: <<http://www.jus.com.br/doutrina/texto.asp?id=2081>>. Acesso em: 11 abr. 2009.
- CASTRO, Carla Rodrigues Araújo de. **Crimes de informática**. Rio de Janeiro: Lúmen júris, 2000.
- CASTRO, Carla Rodrigues Araújo de. Impunidade na Internet . **Jus Navigandi**, Teresina, ano. 6, n. 52, nov. 2001. Disponível em: <<http://www1.jus.com.br/doutrina/texto.asp?id=2327>>. Acesso em: 11 abr. 2009.
- CINTRA JÚNIOR, Weiler Jorge. A Internet como instrumento de criminalidade e de prevenção. **Revista Meio Jurídico**. São Paulo, ano 4, n. 39, nov. 2000.
- COLARES, Rodrigo Guimarães. Cybercrimes: os crimes na era da informática **Jus Navigandi**, Teresina, ano. 6, n. 59, out. 2002. Disponível em: <<http://www1.jus.com.br/doutrina/texto.asp?id=3271>>. Acesso em: 11 mai. 2009.
- CONDE, Francisco Munoz; ARÁN, Mercedes Garcia. **Derecho Penal**, parte general. 3<sup>5</sup>. ed. Valência: Tirant lo Blanch Libros, 1998.
- CORRÊA. Gustavo Testa. **Aspectos jurídicos da internet**. São Paulo: Saraiva. 2000.

COSTA, Cesar da. **Crime computadorizado**: as consequências não previstas no uso do computador. In: INTERFACE, São Paulo, v. 2, n 16, o. 8-12, 1984.

COSTABILE, Henrique. *Combatendo crimes por computação*. **BANAS**. Sao Paulo, v. 25, n. 1182. jul 1978.

DAOUN, Alexandre Jean. Os novos crimes de informática. **Jus Navigandi**, Teresina, ano. 4, n. -f37, dez. 1999. Disponível em: <<http://www.jus.com.fer/doutrina/texto.asp?id=1827>>. Acesso em: 11 abr. 2009.

FERREIRA, Ivete Senise. **Os crimes de informática**. São Paulo: Revista dos Tribunais, 1992.

FERREIRA, Ivete Senise A criminalidade informática. In: **Direito & internet**: aspectos jurídicos relevantes. Bauru: Edipro, 2000.

FRAGA, Luís Eduarde Schoueri. Crimes de informática - a ameaça virtual na era da informação digital, in **Internet**: o direito na era virtual. Rio de Janeiro: Forense, 2001.

GERMAN, Christiano. **O caminho do Brasil rumo à era da informação**. São Paulo: Fundação Konrad Adenauer, 2000.

GOMES, Luiz Flávio, **Atualidades criminais** (1), in [www.direitocriminali.com.br](http://www.direitocriminali.com.br), 20.05.2001. Disponível em: <<http://www1.jus.com.br/doutrina/texto.asp?id=2250>>. Acesso em: 11 abr. 2009.

GRECO, Marco Aurélio. **Internet e direito**. 2- ed., São Paulo: Dialética, 2000.

JESCHECK, Hans-Heinrich. **Tratado de derecho penal**, parte general. Barcelona: Bosch Casa Editorial, 1978.

KAKU, Michio. **Visões do futuro; como a ciência revolucionará o século XXI**. Rio de Janeiro: Rocco, 2001.

LEVY, Pierre. **Cibercultura**. Tradução de Carlos Irineu da Costa. São Paulo: Editora 34, 1999.

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

LUCCA, Newton de & SIMÃO FILHO, Adalberto (coordenadores). **Direito & internet**: aspectos jurídicos relevantes. Bauru: Edipro, 2000.

MARTINELLI, João Paulo Orsini. Aspectos relevantes da criminalidade na Internet. **Jus Navigandi**, Teresina, ano. 4, n. 46, out. 2000. Disponível em: <<http://www.jus.com.br/doutrina/texto.asp?id=1829>>. Acesso em: 11 abr. 2009

MARTINS, Rogério Vidal Gandra da Silva. **Direito e internet**: relações jurídicas na sociedade informatizada. São Paulo: RT, 2001.

MIRANDA, Marcelo Baeta Neves. Abordagem dinâmica aos crimes via Internet. **Jus Navigandi**, Teresina, ano. 4, n. 37, dez. 1999. Disponível em: <<http://www.jus.com.br/doutrina/texto.asp?id=1328>>. Acesso em: 11 abr. 2009.

MOREIRA, José Carlos Barbosa. Pedofilia na internet o estatuto da criança e do adolescente. **Revista Síntese de Direito Penal e Processo Penal**. Porto Alegre: Síntese, n. 8, jun./jul., 2001. v. 2.

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

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

OLIVEIRA JÚNIOR, João Batista Caldeira de. A Internet e os "novos" crimes virtuais. A fronteira cibernética. **Jus Navigandi**, Teresina, ano. 5, n. 51, out. 2001. Disponível em: <<http://www1.jus.com.br/doutrina/texto.asp?id=2097>>. Acesso em: 14 abr. 2009.

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

PINHEIRO, Reginaldo César. **Os crimes virtuais na esfera jurídica brasileira**. São Paulo: IBCCrim, abr. 2001, v. 101.

PRADO JÚNIOR, Arnaldo Corrêa. **O Processo de informatização da Universidade Federal do Pará**. Belém: Editora Universitária UFPA, 2001. v.2.

RAMALHO TERCEIRO, Cecílio da Fonseca Vieira. O problema na tipificação penal dos crimes virtuais. **Jus Navigandi**, Teresina, ano. 6, n. 58, ago. 2002. Disponível em: <<http://www.jus.com.br/doutrina/texto.asp?id=3186>>. Acesso em: 14 abr. 2009.

ROSSINI, Augusto Eduardo de Souza. **Brevíssimas considerações sobre delitos informáticos**. São Paulo: ESMP, jul. 2002. Caderno Jurídico, ano 02, n. 04.

ROVER, Aires José Rover (organizador). **Direito, sociedade e informática**: limites e perspectivas da vida digital. Florianópolis: Fundação Boiteux, 2000.

SCHOUERI, Luís Eduardo (organizador). **Internet**: o direito na era virtual. Rio de Janeiro: Forense, 2001.

VALIN, Celson. **Direito, sociedade e informática**: limites e perspectivas da vida digital. Florianópolis: Fundação Boiteux, 2000.

