UNIVERSIDADE FEDERAL DO CEARÁ
FACULDADE DE DIREITO
CURSO DE GRADUAÇÃO EM DIREITO

MARIELLA DE LIMA FASSANARO

CRIMES NA INTERNET:

O PERFIL DO NOVO CRIMINOSO E A DIFICULDADE DE TIPIFICAÇÃO DO DELITO

FORTALEZA
2007

MARIELLA DE LIMA FASSANARO

Crimes na Internet:

O Perfil do Novo Criminoso e a Dificuldade de Tipificação do Delito

Monografia apresentada ao Curso de Graduação em Direito, da Universidade Federal do Ceará (UFC/CE), como requisito parcial para obtenção do grau de Bacharel em Direito.

Orientador: Prof. Dr. Docente Livre Raimundo Hélio Leite

FORTALEZA

2007

Dedico este trabalho à minha

avó, Maria do Carmo, e à

minha mãe, Isabella,

incentivadoras maiores de

todos os projetos e professoras

de todas as coisas.

AGRADECIMENTOS

Ao Professor Raimundo Hélio Leite, pela disponibilidade e parceria no desenvolvimento deste projeto;

A Raimundo Ricci, por me apoiar imensamente, desde sempre;

À minha irmã, Milena, por seu amor e dedicação;

A Bruno Brasil, pelo carinho e companheirismo indispensáveis; e

Aos amigos e colegas de faculdade, pela convivência prazerosa e pela diversão desmedida, e, em especial, a Patricia Machado, pela amizade incondicional.

"O direito não é nada além do mínimo ético."

Georg Jellinek.

RESUMO

Crimes na Internet. O presente estudo monográfico, de natureza exploratória, tem por objeto analisar as conseqüências maléficas do uso da Internet e o novo perfil do criminoso, incluindo suas principais características. Lista e classifica os crimes mais recorrentes para uma melhor compreensão do tema. Centra-se na tentativa de mostrar quão nociva a Internet pode vir a ser, abordando os aspectos relevantes da conduta dolosa para evitar que as armadilhas cibernéticas surtam efeito, através de medidas de prevenção. Expõe algumas das medidas legislativas adotadas no Brasil e no mundo. Procura servir de fonte para eventuais pesquisas acerca do assunto. As hipóteses do trabalho monográfico serão investigadas através de pesquisa do tipo bibliográfica, procurando explicar o problema através da análise da literatura já publicada em forma de livros, revistas, publicações avulsas e imprensa escrita que envolva o tema em análise, bem como documental, através de projetos, leis, normas, resoluções, pesquisas on-line, dentre outros que tratam sobre o tema. Segundo a utilização dos resultados, a pesquisa é pura, tendo por finalidade aumentar o conhecimento do pesquisador para uma nova tomada de posição. Segundo a abordagem, é qualitativa. Quanto aos objetivos, a pesquisa é descritiva, buscando descrever fenômenos, descobrir a freqüência com que um fato acontece, sua natureza e suas características.

Palavras-chave: Crime; Internet; Medidas legislativas.

ABSTRACT

Cybercrimes. The monographic study here presented, exploratory by nature, has the scope of analyzing the harmful consequences provoked by the use of the Internet and the new profile of the outlaw, including its main characteristics. It lists and classifies the most current crimes for a better comprehension of the theme. It is centered on the attempt to show how injurious Internet can become, exploring the relevant aspects of the fraudulent behavior to avoid the occurrence of cybernetic traps through prevention skills. It exposes some legislative measures adopted in Brazil and in other countries and has the intention of being a humble source to eventual researches on the matter. The hypotheses of the monographic work will be investigated through bibliographical research, looking for an explanation for the problem by analyzing previous publications such as books, magazines, detached articles and printing press which involve the theme, as well as document research through projects, rules, resolutions, online material and other means that embrace our work. According to the results utilization, the research is pure, intending to increase the knowledge of the researcher towards a new perspective, a new decision-making possibility. According to the approach, its priority is the quality. About the goals, the research will be describable, intending to expose phenomena, discover how often the certain situation occurs, its nature and characteristics.

Key words: Cybercrimes; Internet; Legislative measures.

SUMÁRIO

1 INTRODUÇÃO

A sociedade moderna e, em especial, os profissionais do Direito têm demonstrado a clara e inequívoca preocupação do homem moderno com os rumos que vem tomando a rede mundial de computadores - a Internet. Apesar de ser, inegavelmente, um marco na divisão da história da humanidade, ao lado de tantos benefícios que propicia, tem também o seu lado nefasto; é, cada vez mais e numa proporção assustadora, instrumento de crime.

Num momento caracterizado pelo fenômeno da globalização, quando a questão tecnológica passa a ser condição *sine qua non* para o desenvolvimento de quase todas as atividades, mormente em se considerando uma realidade de clientes mais exigentes e interativos, cabe refletir sobre a dimensão ética que os novos espaços e suportes informacionais trazem à realidade do profissional da informação, não raras vezes impactando em sua ação. Nesse contexto, estamos nos referindo a um conjunto de compromissos éticos a serem encarados na área informacional.

Se antes, quando a atividade caracterizava-se mais por uma mera troca de informações efetuada por procedimentos pouco complexos, já enfrentávamos as conseqüências da falta de ética e de escrúpulos dos e para com os *internautas*, hoje, com a internet, quando os conceitos passam a ser rediscutidos e, principalmente, quando o volume de informações atinge dimensões nunca antes alcançadas, não se pode mais fugir da reflexão

sobre o aspecto criminal incidente na rede mundial, de modo a revelar um efetivo compromisso ético do usuário e/ou do profissional com a informação em si e com sua própria profissão.

Tal reflexão encontra ainda mais respaldo quando se discute o papel da informação jurídica como um bem social, notadamente ligada a segmentos do Poder Público que, por incumbência principal, devem zelar pelo respeito ao princípio da legalidade. Adequar o avanço tecnológico e a criminalidade, eventualidade e conseqüência dele, à realidade dos tribunais é algo que alcançou níveis de urgência, que não se pode mais evitar falar a respeito ou mesmo agir.

Desse modo, objetiva-se, na presente pesquisa, deslocar-se um tanto da tradicional abordagem da internet como um importante - e valiosíssimo, vale ressaltar - espaço de oferta de informações com agilidade para, em uma visão mais ampla, propiciar a reflexão acerca dos entraves de ordem jurídica a que o uso inadvertido e/ou mal intencionado desse espaço pode levar.

É nosso escopo tentar esmiuçar as particularidades que o assunto carrega consigo. Numa abordagem simples e clara, sem pretensões de ser completa, trataremos de esclarecer o fenômeno em que, infelizmente, se transformou a criminalidade nesse meio de intercomunicação em massa, obviamente criada e desenvolvida somente para acrescer, beneficiar.

Nosso trabalho abordou, inicialmente, os elementos históricos da Internet, o sistema informático e aspectos relevantes da utilização da rede mundial de computadores na contemporaneidade e, em especial, no Brasil, abordando, ainda, a segurança envolvida nas operações.

No segundo capítulo, o foco foi o perfil do novo criminoso, dando ênfase a como o agente delitivo vem atuando no âmbito cibernético, passando à classificação das condutas criminosas – os *cybercrimes* – quanto ao seu potencial ofensivo. Elencamos, ainda, os tipos mais comuns de crimes na Internet. Ressalte-se que não temos a pretensão de identificá-los todos, nem como acompanhar o avanço de tamanho mal. Foi realizada uma rápida abordagem desses crimes quanto à sua transnacionalidade, fugindo dos limites de um único país.

O último capítulo traz as medidas legislativas e preventivas que são comumente adotadas no regulamento pátrio e pelo mundo e uma análise crítica acerca dessas medidas.

Estamos tentando destinar, com a presente pesquisa, um pouco de nossa força de trabalho e vontade de mudança à disposição do combate à conduta maléfica desses delinqüentes. Ainda há, porém, muito a fazer.

2 A INTERNET

Pode-se dizer que a Internet é um importante foro de troca de idéias e de conhecimento, além de se tratar de uma estrutura apta a garantir o fomento de atividades na área de prestação de serviços de utilidade pública e em vários outros segmentos. Na formação de redes de telecomunicações nacionais e mundiais, a Internet é elemento fundamental.

Segundo José de Oliveira Ascensão (2002, p. 69), "a Internet permitiu a experimentação de um tipo de comunicação de âmbito mundial".

Apresentou-se, então, com um caráter atrativo, que levou a que os destinatários nela se empenhassem e adestrassem e, por outro lado, ficassem dependentes desse modo de comunicação. Muito rapidamente, o sistema evolui de um estilo amadorístico e cultural para instrumento de poderosos negócios.

A Internet tornou-se, infelizmente, palco de desvirtuamento de fins. Faremos aqui uma mostra do decurso temporal e como se deu o desenrolar do uso da rede. Também será abordado o sistema informático, a organização das relações entre dados e considerações acerca da codificação digital.

Abordaremos, ainda, os aspectos relevantes no que dizem respeito à utilização da rede mundial de computadores, como, por exemplo, a miscigenação de culturas e compartilhamento de informações e descobertas, tudo ocorrendo numa velocidade espantosa.

Confrontamos, ainda, no maior problema da Internet: a insegurança de algumas operações; falha que não se resolve apenas com o desenvolvimento da tecnologia.

2.1 Elementos Históricos

Se fizermos uma digressão histórica sobre o surgimento da internet, não podemos deixar de mencionar que o projeto *Arpanet*, da Agência de Projetos Avançados (*Arpa*: *Advanced Research Projects Agency*) do Departamento de Defesa norte-americano, confiou, em 1969, à *Rand Corporation* a elaboração de um sistema de telecomunicações que garantisse que um ataque nuclear russo não interrompesse a corrente de comando dos Estados Unidos. Desse modo, como assevera Flávia Rahal (2002, p. 8/9), "a solução aventada foi a criação de pequenas redes locais (*LAN*) nos lugares estratégicos do país e coligadas por meio de redes de telecomunicação geográfica (*WAN*)".

Na eventualidade de uma cidade vir a ser destruída por um ataque nuclear, esse conjunto de redes conexas - a internet, isto é, *inter networking*, coligação entre redes locais distantes, literalmente -, garantiria a comunicação entre as remanescentes cidades coligadas.

Posteriormente, no ano de 1973, Vinton Cerf, do Departamento de Pesquisa avançada da Universidade da Califórnia e responsável pelo projeto, registrou o Protocolo de Controle de Transmissão/Protocolo internet, nosso conhecido de hoje como protocolo *TCP/IP,* que era o código que consentia uma comunicação possível aos diversos *networks* incompatíveis por programas e sistemas para que, entre si, pudessem funcionar sem falhas.

A internet assim decolou, no auge do processo de barateamento das comunicações, e hoje é vista como um meio de comunicação que interliga dezenas, quiçá centenas, de milhões de computadores no mundo inteiro, permitindo o acesso quase ilimitado a uma quantidade de informações praticamente inesgotáveis, anulando toda e qualquer distância de tempo e lugar.

Conforme Mário Furlaneto Neto (2003, p. 67):

> O mais importante elemento detonador dessa verdadeira explosão, que permitiu à internet transformar-se num instrumento de comunicação de massa, a *world wide web* (ou www, w3, web ou, simplesmente, rede mundial), nasceu no ano de 1989, no Laboratório Europeu de Física de altas energias, com sede em Genebra, na Suíça, sob o comando de T. Berners - Lee e R. Cailliau. É composta por hipertextos, ou seja, documentos cujo texto, imagem e sons seriam evidenciados de forma particular e poderiam ser relacionados com outros documentos, permitindo que, com um simples clique no *mouse,* o usuário pudesse ter acesso aos mais variados serviços e informações, sem necessidade de conhecer os inúmeros protocolos de acesso.

O desenvolvimento rápido da área de computadores e de tecnologia de comunicação começou em 1995, quando várias empresas de telecomunicação norte-americanas assumiram o controle de importantes pontos de entroncamento da Internet, passando, finalmente, à utilização comercial da Internet nos Estados Unidos.

Tornou-se internacional quando foram criados acessos a ela também fora dos Estados Unidos e quando as redes existentes na Europa foram ligadas em conjunto.

As primeiras conexões do Brasil foram feitas em 1988, pela Fundação de Amparo a Pesquisa do Estado de São Paulo e pelo Laboratório Nacional de Computação Científica do

Rio de Janeiro, criando-se uma Rede Nacional de Pesquisa em 1989 pelo Ministério da Ciência e Tecnologia.

A utilização comercial da internet no Brasil ocorreu no ano de 1995, facultando-se as empresas denominadas "provedores de acesso" comercializar o acesso à rede mundial de computadores. Desde então, o uso vem crescendo assustadoramente.

Se, por um lado, incontestáveis são os avanços e benefícios que o uso ético da internet trouxe para a propagação da informação, com benefícios incalculáveis em sua divulgação, por outro, têm-se os riscos inerentes à tecnologia da informatização, notadamente os crimes informáticos.

O advento do século 21 veio a consolidar a era virtual, impossível sendo dissociar a Internet das atividades nossas cotidianas.

2.2 O Sistema Informático

A expressão Informática foi criada pelo francês Philippe Dreyfus e surgiu da junção dos vocábulos "informação" e "automática", por analogia do termo inglês *datamation*, em 1962, e é reconhecidamente a tecnologia da informação ou a ciência do uso da informação. É, no dizer de Liliana Paesani (1997, p. 13):

> A ciência do tratamento racional e automático da informação, considerada como suporte dos conhecimentos e comunicações, principalmente por meio de sistemas eletrônicos denominados computadores.

A palavra "informação" deriva do latim *informare*, que significa dar forma, o conteúdo daquilo que permutamos com o mundo exterior ao ajustar-nos a ele, e que faz com que nosso ajustamento seja nele percebido. O processo de receber e utilizar informações é o processo de nosso ajuste às contingências do meio ambiente e de nosso efetivo viver nesse ambiente.

A informação surge da organização das relações entre dados, ou seja, os dados, considerados de forma organizada, adquirem valor e se tornam informação.

"É a coleção de dados que descreve ou integra um corpo de conhecimento", afirma Luís Eduardo Schoueri (2001, p. 103). Para o computador todo dado é informação, seja de registro ou instrução, expressa através de um código digital, dado relacionado ao estado das coisas na realidade circundante. A partir desta realidade, chega-se ao conceito de dado "como a expressão ou conhecimento de um fato isolado", ainda por Schoueri (2001, p. 104). Será aquilo que representar o todo que o compõe de tal modo que o mesmo dado, em um todo diferente, terá significado diferente. É qualquer parte de uma informação ou algo com o poder de trazer alguma informação; que deve ser considerada como preparada para ser processada, operada e transmitida por um sistema de computador ou programa de computador; os dados podem expressar fato, coisas certas ou comandos e instruções, servindo de suporte das informações. No Dicionário Aurélio Buarque de Holanda Ferreira (1998, p. 366) é:

> Representação convencional de fatos, conceitos ou instruções de forma apropriada para comunicação e processamento por meios automáticos; informação em forma codificada.

À coleção de dados ou informações obtidas chamamos Banco de Dados. Os bancos de dados podem conter informações das mais variadas segundo a sistematização dada

por seu criador. Para exemplificar podemos considerar arquivos de conteúdo científico, artísticos, relativos à vida privada de coletividade de pessoas, dentre outros.

O sistema informático, na sua expressão mais popular, que é o computador, é, muitas vezes, apenas um elemento diferenciador da ação humana, quer seja na qualidade de meio para sua execução, quer seja como seu objeto material. Partindo deste prisma, muitas são as tentativas de se classificar as ações que põem em perigo ou lesionam um bem jurídico, tais como delito informático, abuso de informática, crime de computação, delinqüência informática, crimes digitais.

2.3 Aspectos Relevantes

Quando houve a combinação entre dois grandes elementos essenciais ao progresso e desenvolvimento tecnológico, falando de informática e comunicação, fronteiras se abriram através da transmissão de dados de um computador para outro e que, atualmente, demonstra sua força maior no grande emaranhado que é a rede mundial de computadores – a Internet.

Estima-se que pouco mais de doze milhões de brasileiros tenha acesso à internet, segundo dados apurados até o mês de junho de 2006. É um crescimento espantoso de 12,4% em relação à captação de dados feita na mesma época do ano anterior, em junho de 2005.

O Brasil continua liderando o *ranking* de tempo de uso da Internet entre os onze países medidos por pesquisas realizadas recentemente: além de nosso país, Estados Unidos, Japão, Austrália, França, Alemanha, Itália, Espanha, Suécia, Suíça e Reino Unido participaram do apanhado geral de informações. A internet residencial brasileira, turbinada

basicamente pelo aumento do número de usuários de banda larga, apresenta média de conexão de 17h59min.

Segundo o Comitê Gestor da Internet no Brasil[1], o número de domínios <.br> chegou a 858.596 em dezembro, contra 850.228 em novembro. É um aspecto da nossa vida cotidiana que não retroage mais, impossível de assim ser.

Fica difícil, pois, imaginar como seria o desenrolar dos dias sem a integração das pessoas com a informática. Praticamente todo o desenvolvimento econômico de uma nação como a nossa e muitas outras está baseada na tecnologia produzida em seu território e exportada para os demais consumidores.

A liberdade de expressão, tão perseguida pelos idealistas de uma sociedade livre, foi efetivamente alcançada, e hoje incontáveis modalidades para sua utilização são oferecidas pela intercomunicação em massa. Alguns dos recursos são o correio eletrônico, ou *e-mail*, a movimentação de dados (FTP), as páginas eletrônicas (*home pages*) etc.

O crescimento da informação disponível só foi possível em razão de fatos ocorridos no campo do processamento eletrônico de dados e no de computadores. A expansão dessa informação tem se dado em razão da criação dessa enorme Rede Internacional que permite aos computadores compartilhar serviços e comunicar-se diretamente como se fosse

---

[1] Em Nota Conjunta de maio de 1995, o Ministério das Comunicações e o Ministério da Ciência e Tecnologia afirmaram que para tornar efetiva a participação da Sociedade nas decisões envolvendo a implantação, administração e uso da Internet, seria constituído um Comitê Gestor da Internet, que contaria com a participação do MC e MCT, de entidades operadoras e gestoras de espinhas dorsais, de representantes de provedores de acesso ou de informações, de representantes de usuários, e da comunidade acadêmica. O Comitê Gestor foi criado pela Portaria Interministerial de nº 147 , de 31 de maio de 1995. O Comitê Gestor da Internet no Brasil é responsável pela elaboração e coordenação de projetos em áreas de importância fundamental para o funcionamento e desenvolvimento da internet no país. Entre as principais atribuições e responsabilidades do CGI, destacam-se: a proposição de normas e procedimentos relativos à regulamentação das atividades na internet; a recomendação de padrões e procedimentos técnicos operacionais para a internet no Brasil; o estabelecimento de diretrizes estratégicas relacionadas ao uso e ao desenvolvimento da internet no Brasil; a promoção de estudos e padrões técnicos para a segurança das redes e serviços no país; a coordenação da atribuição de endereços internet (IPs) e do registro de nomes de domínios usando <.br>; a coleta, a organização e a disseminação de informações sobre os serviços internet, incluindo indicadores e estatísticas.

parte de uma grande engrenagem. Esse instrumento de comunicação tem atingido proporções sem precedentes.

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

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

O uso do computador é necessário em todos os segmentos econômicos e sociais e, por isso, o direito não poderia ficar ausente a essa nova realidade. A rede mundial de computadores tem servido de instrumento à educação, tornado o computador, na mão de excelentes professores capacitados, um excelente meio de ensino.

No Brasil, advogados e clientes com interesses em decisões do Supremo Tribunal Federal, poderão acessar "site" com fins a obter a íntegra do acórdão desejado; em São Paulo, a Policia Civil aceita ocorrências pelo computador. Enfim, essa rede pode desburocratizar o serviço público e permitir ao cidadão exercer a plenitude de seus direitos.

As compras realizadas na internet vão de CDs a carros, sendo a parte mais visível da era do comércio eletrônico. Diante das várias possibilidades de utilização da internet, pode-se dizer que você é *alguem@algum_lugar*.

Nossa grande motivação é a impunidade crescente e avassaladora. Justifica-se a presente pesquisa pelo seu estimado e necessário valor teórico, social e jurídico, imprescindíveis ao conteúdo de um trabalho científico no âmbito jurídico. Apesar de grande

interesse acerca do tema, o combate à prática dos *cybercrimes* é ínfimo se comparado ao que poderia ser, de fato. A pouca exploração e o escasso esgotamento do assunto tornam esses crimes cada vez mais corriqueiros, tendo como mola propulsora a falta de impunidade.

Na atualidade brasileira, há que se buscar, sem mais delongas, uma alternativa para que se possa resguardar os direitos das vítimas de crimes perpetrados na escala da Internet. A relevância social da pesquisa repousa nas possibilidades de demonstrar quais os caminhos tomados pelo Estado para prover a sociedade de forma eficiente, assim como também incentivar a fiscalização da forma como está sendo feita a repressão ao *cybercrime*. Não se trata apenas de uma questão econômica, e de enorme insensibilidade é tratar qualquer relação humana apenas por este prisma. Quando se sabe que há, dentre outras, violação de privacidade, muito mais está envolvido. Portanto, o proposto até agora não atende suficientemente aos anseios da sociedade, assim como não resguarda direitos.

É praticamente impossível imaginar como seria o desenrolar dos dias sem a integração das pessoas com a informática. Praticamente todo o desenvolvimento econômico de uma nação como a nossa e muitas outras está baseada na tecnologia produzida em seu território e exportada para os demais consumidores. Os crimes na Internet são, pois, um tema importante de ser discutido e debatido. Só assim para maiores esclarecimento, conscientização e educação de todos. Para o olhar e a consciência de alguns, ele é exposto, colocado à mostra, e já está sendo solucionado devidamente. A justificativa, portanto, se dá pelo fato de esta não ser a projeção e imagem da realidade. É preciso evoluir, codificando os crimes e reparando o estrago já feito, prevenindo os eventuais males maiores.

2.4 Segurança na Internet

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

Essa característica é um atrativo à sua utilização intensa, porém devem ser observadas as ressalvas a respeito do assunto.

Em princípio, ao leigo, isto é uma ferramenta sensacional, pois pode obter informações sobre um sem número de assuntos, de qualquer lugar do planeta, independente do horário. Associada a esta facilidade vem uma pequena palavra que nos faz repensar tudo: risco.

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

Verifica-se que não são todos os *sites* que proporcionam recursos de segurança de notório conhecimento, não do modo que se tem divulgado na mídia. Sabe-se que o sistema de compras na internet não é totalmente seguro, fato que traz desconfiança ao usuário quanto a esses mesmos dispositivos de segurança, que são plenamente passíveis de serem burlados.

Devem ser observados, em relação a essa insegurança, dois obstáculos ao comércio eletrônico: a falta de confiança do público no processo das transações *online*, além do lapso temporal existente entre a disponibilização de uma nova tecnologia e a capacidade da

base instalada para suportar essas mudanças. Mas a real questão é se existe, de fato, compatibilidade entre Internet e segurança.

Com a grande expansão da rede mundial de computadores e, conseqüentemente, com a transmissão de documentos e troca de mensagens por meio do computador, se faz necessário criar sistemas que tornem seguras as informações transmitidas, bem como sua autenticidade.

A falta de segurança na internet demonstra sua vulnerabilidade, facilitando o acesso de invasores e dificultando sua identificação. Tais invasões podem se dar contra um usuário comum ou uma empresa, podendo ter conseqüências mais danosas.

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

Demócrito Reinaldo Filho (2003, p. 5) diz que "na área jurídica o maior problema esta relacionado com a aceitação de um documento, petição ou certidão, enviado por computador ou fax, além da verificação da assinatura".

A introdução da criptografia permitiu uma segurança relativa na utilização da assinatura digital. É através dela que se tem permitido assinar o documento, isto é, transmiti-lo com uma assinatura codificada e garantir sua autenticidade, sem possibilidade de adulteração ou falsificação.

Contudo, ainda não é possível se conseguir 100% (cem por cento) de segurança nos dados transmitidos pela rede, mesmo porque, como já foi dito, as formas de tecnologia se diversificam e evoluem a todo tempo.

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

Uma pesquisa nacional sobre segurança da informação foi realizada, e nela foram constatados os seguintes níveis de insegurança concernentes à internet e à intranet: 30% (trinta por cento) das empresas brasileiras sofreram algum tipo de invasão nos últimos dois anos, sendo que 50% (cinqüenta por cento) dos ataques registrados aconteceram há menos de 6 (seis) meses. E o que é mais preocupante: 39% (trinta e nove por cento) dos entrevistados não sabem sequer se foram invadidos. Em 81% (oitenta e um por cento) das empresas invadidas não foi possível quantificar o prejuízo com os problemas de insegurança ocorridos.

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

Dados da mesma pesquisa nacional sobre segurança da informação revelam que os principais inimigos são os próprios funcionários das empresas, demonstrando que 35% (trinta e cinco por cento) dos problemas ocorridos com segurança foram causados propositalmente pelos seus funcionários e apenas 17% (dezessete por cento) por invasores que não são empregados.

Os riscos de invasões são maiores quando o acesso à internet é feito por meio de um "modem" e sem medidas de proteção e controle. Os especialistas chamam a atenção para a importância da elaboração de uma política de segurança corporativa, formalizando procedimentos para o manuseio adequado das informações estratégicas.

É de se ponderar que as empresas não destinam, ainda, investimentos necessários à questão da segurança de seus sistemas, como se verifica na pesquisa realizada.

O orçamento de segurança para 44% (quarenta e quatro por cento) das empresas ainda não é calculado isolado da verba de informática. Mesmo assim, 74% (setenta e quatro por cento) respondeu que esse orçamento aumentou.

Foi verificado que o maior investimento foi realizado por apenas 12% (doze por cento) das empresas - que estão aplicando um milhão de reais por ano.

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

O campo de proliferação de crimes informáticos é extremamente fértil. É possível transferir-se grandes quantidades de dados pessoais para qualquer sistema que esteja conectado na rede. A transferência pode ser interceptada a qualquer momento e os dados podem ser alterados ou suprimidos, gerando muita insegurança.

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

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

3 CONSEQÜÊNCIAS MALÉFICAS DO USO DA INTERNET

Tanta acessibilidade é alvo inconteste de constante preocupação. Apesar dos incontáveis benefícios que a internet propicia, o nefasto é inevitável: é instrumento de crime.

Não tendo sido criada para a viabilização de ações criminosas, a rede sofreu, de fato, desvirtuamento a olhos vistos, e o mal só cresce, desmedido. Novas mentalidade e realidade emergiram, e a correnteza trouxe à tona novas maneiras de cometer atos ilícitos, passíveis da mesma repugnância destinada a qualquer outro crime.

Até, e principalmente, a distância tornou-se obstáculo superável pelo crime. O criminoso de antes precisava do contato pessoal para configurar uma eventual infração. Amiúde, o que ocorre agora é que o mesmo sujeito pode, sentado diante de um computador, ser agente de um ilícito, sendo a violência física dispensada para caracterizá-lo como infrator.

O anonimato propiciado pela internet é um dos grandes entraves para correr atrás do prejuízo, dificultando terrivelmente a identificação da autoria, continuando, assim, a deixar a sociedade desamparada. Surge, então, a urgente necessidade de combater esses crimes.

Alguns dos delitos são passíveis de tipificação pela atual estrutura normativa penal. Outros, infelizmente, ainda são cometidos livremente, sem que haja vestígio de prévia cominação legal. Faz-se necessário que haja uma reforma na legislação criminal, nos âmbitos

nacional e internacional, com cooperação justa e eficiente, e os órgãos de investigação precisam ser estruturados de maneira a fluírem seus trabalhos no melhor caminho.

Há unanimidade quanto à indubitável questão de que a internet é meio novo para execução de crimes velhos, também gerando, obviamente, um aumento descontrolado na dimensão dos delitos e das novidades maléficas, todos agora perpetrados através do *bit*.

A criação e a popularização da internet no Brasil e no mundo fizeram, sim, surgir novos crimes, como invasão de computadores, criação de comunidades virtuais para fazer apologia ao uso de drogas e envio de vírus de computador por e-mail, dentre muitos outros, de gravidade ainda maior.

É ponto pacífico que a lei deve acompanhar as inovações criadas e experimentadas pela sociedade, adaptando-se aos novos tempos, quaisquer que sejam as mudanças representadas pelo decurso temporal. Mas, como na maioria dos sistemas jurídicos que têm a lei como fonte principal (é o caso brasileiro), o processo legislativo é bem mais lento do que os avanços tecnológicos e as conseqüências destes.

No entanto, nem por isso os operadores jurídicos devem cruzar os braços, ficando no aguardo de providências legislativas compatíveis com a modernidade das técnicas criminosas. Se há possibilidade de encaixe da conduta anti-social a um dispositivo legal em vigor, não deve o aplicador do Direito quedar-se em omissão.

Com o surgimento de novos meios de propagação e realização de práticas criminosas, também passam a ser necessárias novas técnicas de investigação policial para tratar especificamente dos chamados *cybercrimes* - crimes cibernéticos ou crimes pela internet. A dificuldade é fazer com que um crime informático passe a ser encarado como crime regular.

Luís Eduardo Schoueri (2001, p. 365/366) afirma que:

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

Quando se obtém, por exemplo, a informação de que um material ilegal está sendo divulgado, o que se tenta fazer é extrair dessa página da internet informações que se possam levar a uma possível autoria daquele material. A partir deste momento, o que se pode fazer é encaminhar a investigação de uma maneira tradicional.

Dependendo do tipo de crime, os procedimentos podem variar. Uma das possibilidades de investigação é consultar o provedor ou o hospedeiro da página na internet para tentar descobrir o responsável pelo crime. O passo seguinte é encaminhar os pedidos de mandado de busca e apreensão ou de prisão ao poder Judiciário, para que se possa prosseguir com as investigações.

Os ataques pela Internet saíram definitivamente da fase de vandalismo e se tornaram uma atividade ilícita lucrativa. Hoje, o chamado *cybercrime* visa a resultados financeiros e se mostra como mais uma ramificação do crime organizado.

Os dados, coletados mundialmente a cada seis meses para mostrar o cenário atual e as tendências de ameaças na Internet, apontam, entre julho e dezembro de 2006, uma diminuição contínua nos ataques mais críticos, que destroem ou danificam dados, e um

aumento nas ameaças "menos agressivas" e invisíveis. Fraudes online e roubo de informações confidenciais dominam o cenário atual. *Bots* e suas redes (*botnets*) e códigos maléficos modulares (que instalam outros softwares depois do ataque inicial) são os métodos de ataque preferidos. Aplicativos e navegadores da *Web* também estão se tornando cada vez mais alvos dos *cybercriminosos*.

Vejamos alguns exemplos: afirmar que alguém cometeu um fato definido como crime, sem que tal seja verdade, configura delito de calúnia (Código Penal, art. 138), tanto quando a difusão é feita oralmente ou pelos caminhos da Internet; atacar, a pedradas, o carro de um desafeto constitui o crime de dano (Código Penal, art. 183), assim como pratica o mesmo delito o indivíduo que invade perniciosamente um equipamento de informática alheio, danificando-lhe a base de dados, como também é considerado praticante de igual ilícito penal a pessoa que apaga, com o ânimo de causar prejuízo a outrem, imagens gravadas em fita de VHS, de difícil ou de impossível recuperação; é estelionatário quem falsifica a assinatura e o valor de um cheque de terceiro para levantar fundos junto a agência bancária, assim como também é estelionatário quem captura, na Internet, os dados de um cartão de crédito titularizado por outra pessoa e a partir destes faz compras nos chamados "magazines virtuais", impondo prejuízo à primeira.

Lege habemos, como se diz em latim. Assim, não há que ser dito que o Judiciário nada pode fazer só pelo fato de determinado crime ter sido perpetrado via Internet.

Não se desconhece, conforme alinhado pouco acima, que o advento dessa nova mídia, a 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 delinqüência, intimamente unida ao que chamamos de macrocriminalidade, dado o refinamento que norteia a ação dos seus praticantes.

Pesquisas apontam que o Brasil está na rota dos crimes envolvendo a internet. De acordo com a Polícia Federal, de cada dez *cybercriminosos* ativos no mundo, oito vivem no Brasil. Além disso, cerca de 2/3 dos responsáveis pela criação de páginas de pedofilia na internet - já detectadas por investigações policiais brasileiras e do exterior - têm origem brasileira. As pesquisas também apontam que, no Brasil, as fraudes financeiras que utilizam internet e correios eletrônicos já superam, em valores financeiros, os prejuízos de assalto a banco.

Para tornar mais eficaz o combate aos crimes cibernérticos, nossos especialistas têm trabalhado como nunca antes. O foco principal é, além de combater, incentivar a pesquisa e o desenvolvimento científicos, com o objetivo de produzir técnicas novas e avançadas de investigação e repressão.

Sendo cada vez mais a internet utilizada para a prática de crimes, nem sempre é fácil encontrar os responsáveis. Às vezes, o trabalho se torna mais difícil ainda, principalmente quando os criminosos hospedam suas informações no exterior.

Nesses casos, as coisas sempre se complicam um pouco mais e, por isso, eles têm utilizado a cooperação internacional, junto com grupos das polícias dos outros países para conseguir efetivar os planos de ação. Estão sempre em contato para possibilitar o combate efetivo aos crimes cibernéticos.

3.1 Sujeitos da Conduta: O Novo Perfil do Criminoso

Como já foi dito anteriormente, ao mesmo tempo em que surge toda esta explosão de serviços e oportunidades que a internet nos disponibiliza, somos obrigados a conviver diariamente com a figura do indivíduo que usa o computador para atos ilegais.

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

José de Oliveira Ascensão (2002, p. 255) explica que:

> 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 inexiste contato com a vítima, pois todos os procedimentos acontecem à distância.

Chegou-se a acreditar que para a prática de tais atividades seria necessário um conhecimento técnico diferenciado, exclusivo. Na verdade, a conclusão a que se chega hoje é que não é preciso ser nenhum conhecedor profundo de tecnologia informática, pois basta o equipamento adequado para entrar na rede e consultar alguns *sites* que têm por escopo orientar os internautas sobre meios eficazes e diversificados de atuar de forma ilícita.

Os *cybercriminosos* são verdadeiros fanáticos pela informática, cujo passatempo preferido é interceptar mensagens digitais e/ou invadir os computadores alheios, descobrindo

segredos e, algumas vezes, até mesmo deixando instituições bancárias, industriais ou militares em verdadeiro pânico.

O espírito de muitos desses criminosos é apenas aventureiro; buscar o limite de sua capacidade intelectual, mostrar ao mundo do que é capaz ou, simplesmente, satisfazer-se com o reflexo de alguma peripécia estampado nos jornais.

Alguns deles são apenas amadores em busca de diversão e emoções fortes. Outros sem embargo, possuem índole diversa; são fraudadores maiores, novos e modernos charlatães que desejam auferir vantagens ilícitas como, por exemplo, surrupiar contas bancárias, ao adentrarem nos sistemas de instituições financeiras, ou roubarem segredos industriais.

Na verdade, a designação *hacker*, comumente usada, não é a única para aqueles que se utilizam do sistema informático de forma inadequada. De forma genérica, o termo designa pessoas que, ligadas à internet, têm conhecimento real de programação e sistemas operacionais; conhecem falhas de segurança nos sistemas, procuram achar novas brechas e dominam o conhecimento da informática, apenas buscando ampliar sua sabedoria a respeito, tudo por uma espécie de desafio. Deve-se distinguir *hacker* de *cracker*:

C*racker* é um hacker do mal. O *hacker* é aquele que usa seus conhecimentos na busca de soluções de situações criadas pelos *crackers*, que se especializam, muitas vezes, em quebrar senhas. Esses últimos são os verdadeiros criminosos, já que invadem sistemas, roubam arquivos, destroem discos rígidos, espalham vírus, fazem espionagem industrial na lavagem de dinheiro sujo internacional etc., tendo em vista a obtenção de benefícios para si ou para outrem, sempre e detrimento de terceiros. Este é o indivíduo nocivo à sociedade digital do novo milênio, pois as policias internacionais e a sociedade ainda não estão preparados para contê-los.

A propósito, o termo *cracker* foi cunhado em 1985 pelos próprios *hackers*, com o inequívoco objetivo de não serem confundidos com aqueles.

No jargão dos iniciados, um jovem que acabou de ganhar um computador e já quer invadir o Pentágono com programas simples, obtidos na Internet, as chamadas "receitas de bolo", é chamado de *lamer* e, além de ser inofensivo (se tiver sorte, é capaz de não destruir seu próprio computador na primeira tentativa), é desprezado por quem entende de informática. Fazem o uso anti-social da rede, apenas para disturbá-la.

Os *pheakers* são os que se utilizam de meios de comunicação através de fraudes, sem pagar pelos serviços.

Leonardo Medeiros Jr. (2002, p. 65) nos ensina que:

> O perfil do criminoso, baseado em pesquisa empírica, indica jovens inteligentes, educados, com idade entre 16 e 32 anos, do sexo masculino, caucasianos, audaciosos e aventureiros, com inteligência bem acima da média, 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.

É possível descrever, esquematizando, as principais características daqueles que praticam crimes por computador na atualidade, porém os dados tomados per ele referem apenas a agentes internos de empresas e não a *crackers* ou *hackers*, mas merecem ser analisados:

a) Idade: 16 a 35 anos;

b) Sexo: masculino, em sua maioria;

c) Função: administrador de alto nível;

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

e) Antecedentes Criminais: nenhum;

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

g) Reações ao ser apanhado: "Isso não é crime"; "Eu não prejudiquei ninguém"; "Todo mundo faz isso"; "Eu apenas tentei demonstrar que era possível ser feito".

Quando se estuda o perfil do delinqüente de informática, inclusive as condutas dos *crackers* e dos *hackers,* diz-se que é inequívoca a idéia de que esses criminosos digitais são *experts*, pois, tendo os sistemas disponíveis, qualquer pessoa pode ser autor do delito de informática, bastando ter conhecimentos de computação, para ser capaz de cometê-los.

Nosso estudo revelou que, através das inumeráveis compilações que circulam pelo mundo da informática, são os crimes dessa espécie cometidos à égide de "*special opportunity crimes*", conforme Louise Shelley (1998, p. 2), quais sejam os crimes afeitos à oportunidade, perpetrados por agentes que tem a sua ocupação profissional ao manuseio de computadores e sistemas, em várias atividades humanas, e em razão dessa ocupação cometem delitos, invariavelmente, contra seus empregadores.

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

Por derradeiro, é de se concluir que as ações tendentes a ameaçar a proteção do bem jurídico podem ser perpetradas por qualquer pessoa, não necessitando ela de nenhum conhecimento especifico profundo, nada absolutamente extraordinário.

3.2 Classificação dos Delitos Praticados na Internet

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

Liliana Paesani (1997, p. 12) explica que:

> Dado é um conjunto de caracteres (letras e/ou números) que, por si só, não transmitem nenhum significado. Na informática, refere-se a dados tudo aquilo que é fornecido ao computador de forma bruta. Quando os dados são vistos dentro de um contexto e transmitem algum significado as pessoas, tornam-se informações. No caso da informática refere-se aos resultados processados que o computador nos dá de volta.

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

O *National Center For Computer Crime Data*[2], dos Estados Unidos, defende a posição de que o Direito Criminal da Informática é concebido para proteger os sistemas de computadores e das comunicações, além da informação.

---

[2] O Centro Nacional para Informações Relativas a Crimes Informáticos é uma organização não governamental dedicada a coletar e disseminar informações estatísticas dos *cybercrimes* e tecnologia de segurança de informações.

Existem inúmeras classificações que são propostas para o estudo da matéria. Contudo, acreditamos que a classificação quanto ao objeto material é o mais recomendado a fazer, visto que acaba englobando as outras existentes. Essa é a classificação mais acertada, a mais sensata.

Dessa forma, segundo o objetivo material dos delitos de informática são:

a) delitos de informática puros;

b) delitos de informática mistos; e

c) delitos de informática comuns.

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

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

Portanto, é crime de informática puro toda e qualquer conduta ilícita que tenha por objetivo exclusivo o sistema de computador, seja pelo atentado físico ou técnico do equipamento e seus componentes, inclusive dados e sistemas.

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

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

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

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

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

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

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

3.3 *Cybercrimes*

Em uma abordagem sobre ilícitos informáticos que violam a privacidade na *web*, cita-se, dentre outras condutas:

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. A partir de 1980, ressalta-se 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;

b) *cookies*, ou "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*;

d) *hoaxes*, como sendo *e-mails* 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;

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;

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, no dizer popular, maravilhas, para o caso de o arquivo anexado ser 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. Considerando-se que boa parte dos computadores é dotada de microfones ou câmaras de áudio e vídeo, observa-se que o cavalo de tróia permite a possibilidade de se fazer escuta ambiente clandestina, arma poderosa nas mãos de criminosos que visam à captura de segredos industriais.

A doutrina juscibernética comparada, mormente a ibero-americana, enriquece ainda mais o debate. Há quem defenda que não há uma definição de caráter universal própria de delito informático, apesar dos esforços dos *experts* que tenham se ocupado do tema, e, enquanto não existe a concepção universal, foram formulados conceitos funcionais atendendo a realidades nacionais concretas.

Desse modo, há autores, como Mário Furlaneto Neto (2003, p. 72), que resgatam um entendimento que diz que:

> Delito eletrônico, em sentido amplo, é qualquer conduta criminal em cuja realização haja o emprego da tecnologia eletrônica como método, meio ou fim e, em sentido estrito, qualquer ato ilícito penal em que os computadores, suas técnicas e funções desempenham um papel como método, meio ou fim.

Complementando sua definição, classifica os delitos eletrônicos em três categorias:

a) Os que utilizam a tecnologia eletrônica como método, ou seja, condutas criminais onde os indivíduos utilizam métodos eletrônicos para obter um resultado ilícito;

b) Os que utilizam a tecnologia eletrônica como meio, ou seja, condutas criminais em que para a realização de um delito utilizam o computador como meio; e

c) Os que utilizam a tecnologia eletrônica como fim, ou seja, condutas dirigidas contra a entidade física do objeto ou máquina eletrônica ou seu material com o objetivo de danificá-lo.

No *Oitavo Congresso sobre Prevenção de Delito e Justiça Penal*, celebrado em Havana, Cuba, em 1990, a Organização das Nações Unidas (ONU) publicou uma relação de tipos de delitos informáticos. 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 o 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 seguranças para obter acesso a programas e órgãos de informações; e

f) reprodução não-autorizada de programas informáticos de proteção legal, causando uma perda econômica substancial aos legítimos proprietários intelectuais.

Posteriormente, no *Décimo Congresso sobre Prevenção de Delito e Tratamento do Delinqüente*, 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, pagando-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: delinqüentes enganam novos e incautos usuários da internet para que revelem suas senhas pessoais, fazendo-se passar por agentes da lei ou empregados de provedores e 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 Tsotomo Shimamura, *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.

A rede mundial, uma sociedade virtual que modificou hábitos e costumes, combinando comportamentos tradicionais com o acesso à informação e cultura, também se tornou motivo de inquietude, um rico campo para as mais variadas atividades ilícitas, criminalidade esta, caracterizada pela dificuldade de investigação, prova e aplicação da lei penal, pelo caráter transnacional e ilimitado dessas condutas, o que pode gerar conflitos de Direito Internacional, em decorrência da competência da jurisdição sancionadora.

Em recente revisão, o Código Penal espanhol foi atualizado pela Lei Orgânica nº11, de 30 de abril de 1999, que contemplou como crimes a pornografia infantil praticada via internet e a posse de material pornográfico relacionado à pornografia infantil.

Como podemos observar, o computador pode ser meio para a prática de delitos previstos na legislação ordinária, como, por exemplo: ameaça (promessa de malefícios futuros); crimes contra a honra praticados via *e-mail* (ofensas à honra objetiva – difamação –, subjetiva – injúria – e a imputação falsa de fato considerado como crime – calúnia); violação de correspondência, considerando-se a confidencialidade da correspondência eletrônica; tráfico de drogas; apologia ao crime; e até mesmo homicídio doloso, na hipótese de uma pessoa, intencionalmente, interferir na programação de um aparelho em funcionamento em um paciente internado na Unidade de Terapia Intensiva (UTI), cujo desligamento venha a lhe

causar a morte, bem como para outras condutas potencialmente danosas, ainda não-disciplinadas pelo Direito Penal.

Importante dizer que a caracterização do delito praticado por meio do computador dependerá da análise do caso concreto, devendo a conduta do delinqüente informático se subsumir em norma prevista na legislação em vigor do país onde o delito for cometido, sendo que a exemplificação neste artigo apresentada não tem o condão de ser taxativa.

Figura não-tipificada pelo Direito Penal brasileiro, o delito de terrorismo praticado com o auxilio da informática é classificado da seguinte forma:

a) terrorismo de Estado: praticado por governantes que, para poder seguir exercendo um controle político sobre seus governados, recorrem ao uso da informática como fator de opressão, de forma a utilizar em seu proveito a informação como poder. Distinguem-se governantes de Estados totalitários daqueles que estão sob o manto de um Estado democrático, que recorrem a essa estratégia para um melhor controle da cidadania. Para alguns tratadistas, essa conduta trata-se de excesso de poder e não de terrorismo, requerendo um contrapeso adequado para que não suscitem abusos contra os cidadãos, ou seja, um adequado controle sobre o controle, como, por exemplo, os desenvolvidos pelo Escritório de Inspeção de Dados da Suécia, a Comissão Federal de Dados da República Federativa da Alemanha e a Comissão Nacional de Liberdades e Informática da França;

b) terrorismo entre Estados: caso em que a teleinformática a serviço de um determinado Estado pode propiciar verdadeiros atentados contra a soberania de outros Estados por intermédio do conhecimento e uso indevido de dados informacionais de caráter confidencial e estratégico, mediante o fluxo de dados transnacionais. Como exemplos, temos eventuais ocupações físicas e destruição parcial ou total de centros de informação, como um quartel militar e uma central nuclear ou química;

c) terrorismo entre particulares: na posição do autor, trata-se de atos de criminalidade em sentido lato, motivados por questões de ordem pessoal, histórica, econômica e religiosa. Cita como exemplo os vírus informáticos, que constituem, em algumas ocasiões, sempre que presente a intenção dolosa de causar um dano, verdadeiros atentados terroristas contra o suporte material e lógico dos computadores com a conseqüente perda de informações e, sobretudo, caracterizando mais prejuízos do que originalmente se pretendia provocar, inclusive financeiro e com perdas de vidas humanas, o que a doutrina tem considerado verdadeiros delitos preterintencionais;

d) terrorismo de particulares contra o Estado: conduta esta mais conhecida na atualidade como realizada por grupos anárquicos de esquerda, de direita, fanáticos religiosos, ecologistas, etc. Geralmente provocam estragos de perdas humanas e materiais. Como exemplos, teríamos a possibilidade de uma invasão física e automatizada a algum centro informático ou a inserção de vírus informáticos, o planejamento e a simulação de atentados por meio de um computador a fim de aperfeiçoar o verdadeiro ataque, a posse de informações confidenciais (fitas, discos magnéticos ou qualquer outro suporte material de informação), ou a ação de roubos e fraudes informáticas para a obtenção de fundos para suas atividades etc.

Encontram-se diversificados os atos ilícitos possíveis por via da grande rede, por isso o trabalho visa a restringir as observações inerentes àqueles que acontecem com maior freqüência e dispõem de maior potencialidade de danos. Simplificando, por fim, os crimes mais comumente cometidos são estes, listados a seguir.

a) fraudes: As fraudes de maior freqüência na Internet são 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 *online* pagos.

Muitas das fraudes partem de propagandas difundidas por *spam*, grupo de mensagens distribuídas a uma grande quantidade de destinatários de forma indiscriminada (o mesmo *spam* pode servir para a propagação de vírus).

b) pornografia infantil: A pornografia infantil talvez seja o crime que mais provoque a repulsa da sociedade. Não há qualquer forma de se aceitar as situações constrangedoras a que crianças são subordinadas para saciar as fantasias de pessoas desequilibradas.

A pedofilia é um fenômeno fora dos padrões comuns toleráveis pela sociedade, encontrando na Internet um veículo para satisfazer virtualmente os seguidores dessa prática.

Esta modalidade aparece na Internet de duas maneiras: pelas *home pages* e por correio eletrônico. Na primeira opção, 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 opção, o material é distribuído de um usuário a outro, diretamente.

c) crimes contra a honra: Consistem nos 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, seja por imagens, seja por palavras.

d) racismo: Outra modalidade criminosa que encontra na Internet as facilidades do anonimato. 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.

São características do racista: o ódio, a desumanização do próximo, a construção do inimigo. Existe a teorização da superioridade em relação a outros grupos.

As *home pages* e os *e-mails* racistas geralmente são identificados por grupos racistas organizados, nunca pelo nome da pessoa que a criou, já que o racismo é crime em quase todos os países.

e) interceptação de correspondência: Consiste este ato no desvio de *e-mails* de uma conta para outra, sendo possível a leitura, a modificação e o uso dos dados contidos, além de impedir que o verdadeiro destinatário possa utilizar-se destes.

A interceptação de correspondência eletrônica é polêmica principalmente quando esta poderia servir como prova e meio de instrumento de investigação de outros crimes.

f) pirataria de *softwares*: É a difusão de programas de computador pela grande rede, sem a autorização dos detentores de direitos sobre eles. Tornou-se comum a prática de *download* de arquivos por meio de *sites* que os oferecem aos seus visitantes, ou por FTP (canal de transmissão de arquivos da Internet).

g) violação de direitos artísticos: Pode-se dizer que se trata de uma modalidade específica entre os crimes de pirataria. Enquadram-se nesses crimes a difusão de obras literárias, jornalísticas, musicais, entre outras.

Como exemplos podem ser citados os arquivos de formato MP3, os textos das agências de notícias, os *e-books* (livros eletrônicos), as fotografias artísticas retiradas de uma página e utilizadas em outra etc.

3.4 A Transnacionalidade dos *Cybercrimes*

Muitos podem ser os objetivos ou as intenções de quem opera a Internet. Algumas delas sabidamente criminosas. Mas, enquanto no campo das intenções, ou da cogitação, nada há que se pode fazer. O problema surge no momento em que a intenção se converte em ação ou conduta e produz resultados de relevância penal.

Dentro da seara criminal, os chamados crimes de concorrência desleal, crimes de estelionato, interceptação de dados, os chamados crimes contra honra (calúnia, injúria e difamação), a pedofilia, a pirataria, dentre tantos outros, todos, passíveis de serem cometidos via Internet.

Ao menos no campo da criminalidade, a Internet traz um gravíssimo problema: o da transnacionalidade, ante a possibilidade que dá ao agente de cometer o delito, remotamente, a partir de um Estado, fazendo-o consumar-se em outro além de suas fronteiras geográficas, bem como a prerrogativa que dá aos delinqüentes de poder utilizar das fronteiras para despistar e conturbar uma investigação, camuflando-se, visando a sua impunidade. Diga-se, ademais, ser a ubiqüidade outra característica marcante nesta prática.

Temos, pois, que a transnacionalidade é, sem dúvidas, a nota mais saliente desta prática, ante a qual os Estados, isolados, têm suas forças reduzidas a uma virtual impotência investigativa, haja vista que tanto a Polícia quanto o Poder Judiciário esbarram nos chamados princípio da Territorialidade e no princípio da Soberania.

Ao mesmo tempo, há que se somar a todos esses empecilhos de ordem prática, as diferenças existentes entre as legislações dos diferentes países que contribuem para acentuar, ainda mais, esta problemática. Basta atentarmos para o fato de uma conduta ser considerada

crime em um país e lícita em outro (aliás, às vezes até em estados de um mesmo país, como ocorre nos Estados Unidos).

Desta feita, os crimes cometidos via internet, por serem delitos praticados à distância e possuírem a seu favor poderosas armas garantidoras da impunidade, apresentam maior eficácia e estando mais a imune à ação do Direito Penal.

Assim, para o combate das manifestações transnacionais, e como já manifestadas nos parágrafos anteriores, materializadas nas diferenças normativas existentes entre as legislações dos diferentes países bem como na dificuldade de investigação, impõe-se a necessidade de cooperação entre os países, cooperação esta cuja necessidade acentua-se na mesma proporção em que se dá o avanço da transnacionalidade na Internet.

Por fim, e na contramão das tendências atuais, acreditamos ser este o ponto mais importante e o qual merece todas as nossas atenções e todos os nossos esforços, visto que é, sem sombra de dúvidas, o mais delicado, de maior complexidade e dificuldade e o que mais problemas trará num futuro próximo.

É necessário pensarmos não apenas no combate interno (dentro de nossas fronteiras) dos crimes cometidos através da internet, mas, também, nos adiantarmos no palco internacional, pois como já se tornou de conhecimento geral, o casamento da criminalidade com a tecnologia tem, de fato, conseguido internacionalizar o crime de maneira ágil, pouco rastreável e quase impune.

4 MEDIDAS ADOTADAS

O Brasil tem hoje um conjunto de leis que são suficientes para que muitas coisas sejam feitas por parte do Poder Público. Existem acordos dos quais o Brasil é signatário e existe o conhecimento sobre a legislação de outros países. Nosso país tem se orientado nesse sentido; é fato. Existem vários projetos de lei sobre esse assunto tramitando no Congresso. Basta que as coisas andem e que haja uma celeridade na aprovação desse arcabouço jurídico.

4.1 Medidas Legislativas

Há a necessidade de a legislação brasileira acompanhar a evolução da criminalidade, já que nosso Código Penal data de 1940. A solução é a reforma desse instituto ou a elaboração de leis extravagantes.

Primeiro ponto importante é a tipificação de determinadas condutas. Por princípio do Direito Penal, só é crime o que está previamente definido em lei. Portanto, as pessoas que praticaram atos pela Internet e que não sejam tipificados, apesar de toda sua reprovação, não poderão ser condenadas.

Mister se faz o acréscimo de uma agravante na Parte Geral do Código Penal. Os crimes cometidos por meio da tecnologia, dificultando as investigações, teriam um aumento nas mesmas regras atuais.

Outro ponto a ser discutido é a pena aplicada a esses crimes. Como em qualquer momento do Direito Penal, a sanção deve ser proporcional à conseqüência do ato. Entre as penas alternativas, poderia ser inclusa a participação do condenado nas investigações de outros delitos tecnológicos (utilização de seu conhecimento no combate ao crime).

Para combater essa nova vertente de crimes está em curso no Congresso Nacional o Projeto de Lei 76/2000, que tipifica condutas como, por exemplo, o acesso indevido a um sistema ou a uma rede de computação, tanto para fins particulares como para fins políticos, comprometendo a segurança nacional. Segue o mencionado Projeto de Lei o princípio da especialidade, dando o caráter de exclusividade às condutas já punidas genericamente no sistema penal tradicional.

Nada obstante, um grave pecado tisna de retrógrada uma proposta que tem o objetivo original de ser avançada: a excessiva previsão de penas privativas de liberdade, em claro descompasso com o Direito Penal moderno, que diante da inegável falência da prisão como instrumento de ressocialização, prega a adoção de penas alternativas (multas severas, prestação de serviço à comunidade, restrições de direitos etc.), bem mais compatíveis com a periculosidade e com o status intelectual de um usuário de computador.

O grande obstáculo, aquele que tem sido praticamente intransponível, que é enfrentado pelo operador jurídico que trava contato com a criminalidade da Internet diz respeito à aplicação da lei penal no espaço. O Código Penal Brasileiro abraça a teoria da ubiqüidade, dizendo, em seu art. 5º, que se considera praticado o crime no lugar em que foi desenvolvida a conduta delinqüencial, assim como o lugar onde se produziu ou deveria

produzir-se o resultado. E lista, no art. 7º, várias hipóteses de aplicação da lei brasileira a crimes cometidos no estrangeiro (ou, ainda, a partir do estrangeiro), aí incluídos os delitos "que, por tratado ou convenção, o Brasil se obrigou a reprimir".

Tome-se como exemplo o fato de ser o Brasil signatário de um tratado internacional que o obriga a reprimir os crimes contra crianças e adolescentes, aqui previstos na Lei 8.069/90. Considerando que o Estatuto da Criança e do Adolescente não tutela apenas os brasileiros, em tese poder-se-ia aplicar ao alienígena veiculante de fotografia pornográfica de criança (*sex pics*) o disposto no art. 241 do diploma menoril, que pune dita conduta com reclusão, de um a quatro anos. Só que o Código Penal Brasileiro lista cinco condições para que tal aplicação seja implementada, e dentre as listadas está a de "entrar o agente em território nacional" e "ser o fato punível também no país em que foi praticado".

Denúncias de crimes cibernéticos podem ser feitas tanto para a Polícia Federal, como para as polícias civis. Já há, para tanto, orientação do Superior Tribunal de Justiça para que os crimes cibernéticos sejam classificados como crimes federais e que, portanto, estão sob a competência da Polícia Federal. Contudo, as polícias civis também investigam e podem e devem continuar investigando esses crimes.

É de ser pensada uma mitigação das exigências do sistema penal brasileiro, para os casos de aplicação da lei nacional aos crimes praticados pela rede mundial de computadores. Será um grande passo para o definitivo e civilizado ingresso do Brasil no processo de globalização que marca a virada do século.

4.2 Medidas Preventivas

Medidas de caráter alheio ao Direito Penal podem ser muito úteis na prevenção à criminalidade virtual. Optamos por destacar algumas delas, a fim de que se possa contribuir para diminuir a incidência desses *cybercrimes*.

Cooperação entre os órgãos de investigação (polícia, Ministério Público) com institutos de tecnologia para a investigação desses delitos – o profissional do Direito não está apto a examinar os aspectos técnicos do crime;

Adoção de sistemas de segurança por parte dos usuários de computadores, tanto nas residências como nas empresas;

A cooperação da vítima na notificação das ocorrências;

Elaboração e promoção de uma conduta ética por parte dos usuários de computadores, a fim de tornar o respeito aos demais parte dessa nova cultura que vem emergindo com a tecnologia;

Imposição de certas medidas de segurança nos setores mais sensíveis (sistema financeiro, órgãos de segurança nacional, autarquias etc.) através de leis;

Participação de *hackers* no desenvolvimento dos sistemas de segurança para computadores – ninguém melhor do que eles para detectar as lacunas que permitem a execução do crime;

Desenvolvimento de *softwares* para controle de conteúdo de *home pages* com materiais impróprios a determinadas faixas etárias, a fim de que os pais possam controlar o contato de seus filhos com a pornografia ou violência;

Desenvolvimento e utilização em larga escala da criptografia. Mensagens criptografadas são escritas em códigos ou cifras, onde somente determinadas pessoas possuem a chave para a sua compreensão. Essa tecnologia aumenta a segurança dos dados transmitidos, garantindo a privacidade das pessoas envolvidas.

5 CONSIDERAÇÕES FINAIS

A Internet é um meio de comunicação jamais visto. Por isso 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.

A evolução da informática proporcionou uma nova dimensão da criminalidade. A tecnologia trouxe um *modus operandi* até então inimaginável para os juristas. O contato direto entre autor e vítima tornou-se apenas virtual e os meios de execução foram simplificados a um simples aparato eletrônico.

Desse modo, questões como a propagação deliberada de vírus informáticos, destruindo sistemas inteiros e levando à impossibilidade de acesso à informação (direito constitucionalmente protegido), não podem mais deixar de ser uma preocupação inerente ao profissional da informação, visto incorporarem-se a seu próprio fazer.

Assim sendo, uma reflexão ética a mais se incorpora ao *métier* desse profissional, qual seja, aquela de buscar, pelas formas que lhe forem legitimamente acessíveis, propiciar que o acesso e a recuperação de informações se façam em moldes consonantes com a estrutura jurídica estabelecida, atuando não apenas como um mero disponibilizador de informações, mas como um valioso colaborador das instâncias jurídicas que visam a garantir tais direitos.

É mais do que notável que a criminalidade tecnológica evolui, assim como a preocupação que ela causa em todos os setores da sociedade. No entanto, as autoridades competentes não acompanham essa caminhada por falta de diversos recursos. Urge a desburocratização na criação dessas leis, que têm o claro fito de serem profiláticas.

Ainda há o problema de arcaísmo das normas vigentes, elaboradas em épocas em que não se imaginavam o estágio em que a criminalidade poderia chegar. Portanto, as leis devem se adaptar à realidade e às necessidades que a modernidade impõe. Deve-se ter cuidado para não criar uma lei específica demais, já que novos delitos surgirão com o progresso tecnológico.

O problema da jurisdição só poderá ser resolvido por uma cooperação entre os países - já que a transnacionalidade é barreira grande demais para ser abarcada por uma única legislação -, por meio de tratados internacionais que regularizem o uso da Internet. As leis de vigência interna em um país não serão suficientes para um mundo onde as barreiras da informação foram todas eliminadas.

Defende-se aqui, portanto, a proporcionalidade na aplicação das leis e, sempre que possível, a substituição da pena privativa de liberdade pelas penas alternativas restritivas de direito (por exemplo, diminuição da pena quando houver negligência por parte da vítima ou a punição somente os crimes dolosos). É preferível investir nas medidas não-penais.

6 REFERÊNCIAS

ASCENSÃO, José de Oliveira. **Direito da Internet e da Sociedade de Informação**. Rio de Janeiro: Forense, 2002.

COSTA, Marco Aurélio Rodrigues da. **Crimes de Informática**. Jus Navigandi, Teresina: ano 1, n. 12, maio 1997. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=1826>.

CUNHA, Celso; CINTRA, Lindley. **Nova Gramática do Português Contemporâneo**. 3. ed. Rio de Janeiro: Nova Fronteira, 2001.

DAOUN, Alexandre Jean. **Os novos crimes de informática**. Jus Navigandi. Teresina: ano 4, n. 37, dez. 1999. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=1827>.

FRIEDMAN, Thomas L. **O mundo é plano: Uma breve história do século XXI**. Rio de Janeiro: Objetiva, 2005.

FURLANETO NETO, Mário. **Crime na internet: Elementos para uma reflexão sobre a ética informacional**. Revista CEJ. Brasília: v. 7, n. 20, p. 67-73, jan/mar, 2003.

LABATON, Stephen. **Exércitos sem alma**. Folha de São Paulo, p. F2-F4. São Paulo: 13 jul. 2005.

MEDEIROS JÚNIOR, Leonardo. ***Hackers*, *crackers*, *pheakers* e *insiders*: O que eles fazem?** Consulex: Revista Jurídica. Brasília: v. 6, n. 121, p. 64-65, jan. 2002.

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

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Décimo Congresso sobre Prevenção de Delito e Tratamento do Delinqüente**. Disponível em: <http://www.onu.org/>.

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

RAHAL, Flávia. **Crimes e Internet: Breves notas aos crimes praticados por meio da rede mundial e outras considerações**. Boletim Ibccrim. São Paulo: v. 9, n. 110, p. 8-9, jan. 2002.

REINALDO FILHO, Demócrito. **Questões técnicas dificultam condenações por crimes cometidos na internet**. Informativo Jurídico Consulex. Brasília: v. 17, n. 49, p. 4-5, 8 dez. 2003.

SCHOUERI, Luís Eduardo. **Internet: O Direito na Era Virtual**. 2. ed. Rio de Janeiro: Forense, 2001.

SHELLEY, Louise. **Crime and Corruption in the Digital Age**. University of New York. New York Press, 1998, New York.

TEIXEIRA, Duda. **Crime e Castigo na Internet**. Isto É Dinheiro. São Paulo: n. 249, p. 52-53, 5 jun. 2002.

Mercadão dos Cosméticos

CERTIFICADO

Certifica que Jacqueline da Silva Pinheiro

concluiu o curso de APERFEIÇOAMENTO DE ESCOVA

Com duração 9 horas

Fortaleza - CE, 09 de JANEIRO de 2007

Certificado

Certifico que Sandra Maria Sousa da Silva,

concluiu o Curso de Reciclagem de Manicure,

com duração de 08 *horas/atividades.*

Fortaleza - Ce, 09 *de* Janeiro *de 200* 7 .

Concludente

Ana Maria de Oliveira
Instrutora de Higiene e Beleza

MERCADÃO DOS COSMÉTICOS