Daniella D'Arco Garbossa*

RESUMO

Trata-se de trabalho que analisa os modernos crimes, praticados por meio de computadores, ou contra computadores, dados e sistemas computacionais. Busca-se avaliar o que existe hoje no ordenamento jurídico pátrio que permita a punição do infrator. Mas, mais do que isso, procura avaliar o projeto de lei atualmente em trâmite no Congresso Nacional Brasileiro que pretende inserir no Código Penal, bem como em leis extravagantes, condutas típicas que respondam aos modernos ataques, possibilitando a subsunção de fatos que hoje ficam sem punição, para que não se viole o princípio da legalidade, de extrema importância no Direito Penal moderno.

Palavras-chave: Crimes Informáticos. Projeto de Lei 76/00.

ABSTRACT

This is a work that examines the modern crimes committed by means of computers, or against computers, computer systems and data. We seek to evaluate what are today the national criminal laws that permit the punishment of the offender. But more than that, it seeks to assess the bill currently pending in Brazilian Congress who wants to enter the Brazilian Penal Code, as well as extravagant laws, typical behaviors that respond to modern attacks, allowing the subsumption of facts that are today without punishment, lest they don't violate the principle of legality, of paramount importance in modern criminal law.

Keywords: Computer Crimes. Bill 76/00.

* Advogada, Especialista em Direito Penal, Mestre em Direito na Sociedade da Informação, Professora Universitária.

1. Introdução

Este estudo tem por escopo tratar dos crimes que acompanham a evolução tecnológica. Trata-se dos crimes informáticos, virtuais, cibernéticos, ou qualquer outra designação que se pretenda dar.

Buscaremos, antes de mais nada, dar um panorama geral do que seria a internet e qual a sua importância para a atual sociedade, já que se trata do meio onde ocorrem as mais variadas condutas ilícitas, como transferência de valores, crimes contra a honra, sabotagem, entre outros.

Ingressando especificamente no tema proposto, traremos alguns conceitos de crimes informáticos, bem como as diferentes classificações propostas.

Traremos, também, algumas questões que apresentam dificuldades para a punição desses crimes, especialmente com relação à identificação do sujeito ativo, ao tempo e ao local do crime e à competência.

Por fim, traremos as alterações na legislação atualmente em vigor pretendidas pelo Projeto de Lei do Senado Federal n. 76/00, que busca tipificar o que denomina de crimes virtuais.

2. Internet

Não podemos ingressar no tema "cibercrimes" ou crimes informáticos, sem antes trazer, ao menos, noções acerca da internet. É o que passamos, inicialmente, a fazer.

A internet é o meio de comunicação mais significativo da atual sociedade, por alguns denominada "Sociedade da Informação" ou "Sociedade do Conhecimento" ou "Sociedade Virtual", entre outras designações.

O surgimento da internet deu-se nos anos 60, nos Estados Unidos, a partir de uma estratégia militar, foi o início da Era da Informação[1]. A idéia de rede interligada surgiu para proteger computadores do governo norte-americano após um ataque nuclear, sendo certo que até o surgimento da Rede Minitel, na França, a internet era utilizada apenas nas áreas militar e universitária, quando passou a ser utilizada também para o comércio[2].

No conceito trazido pelo Ministério da Ciência e Tecnologia do Brasil, internet é um *"sistema de redes de computadores – uma rede de redes – que pode ser utilizado por qualquer pessoa, em qualquer parte do mundo, onde haja um ponto de acesso, e que oferece um amplo leque de serviços básicos, tais como correio eletrônico, acesso livre ou autorizado a informações em diversos formatos digitais, transferência de arquivos"*[3].

Faz parte da internet a teia global, conhecida como 'www' – *World Wide Web*, que nada mais é que um *"enorme conjunto de documentos e serviços...organizados em forma de páginas de hipertexto, em que cada página é identificada por um URL"*[4] (grifos do autor).

Nos dizeres de Marco Antonio Zanellato, a internet é *"uma cadeia mundial de redes de computadores públicos ou privados, ligados uns aos outros por equipamentos informáticos heterogêneos e que fornecem os mais variados serviços"*[5]. Para ele, são três os elementos que caracterizam a internet: *"(a) é uma cadeia de redes (réseau de réseaux); (b) em escala mundial; (c) cujos equipamentos informáticos expressam a mesma linguagem e utilizam as mesmas técnicas para fazer circular a informação"*[6].

Este conceito de internet como um conjunto de redes interligadas surgiu apenas na década de 80, quando foi estabelecido o padrão IP/TCP[7], que significa protocolo de internet e protocolo de controle de transmissão[8].

A internet é fruto da evolução tecnológica proporcionada pela sociedade de massa, sendo certo que as informações são passadas para um número absolutamente

[1] Manuel Castells. **A Sociedade em Rede volume 1 – A Era da Informação: Economia, Sociedade e Cultura: inclusão e exclusão**, p. 82.

[2] Augusto Eduardo de Souza Rossini. **Brevíssimas Considerações sobre Delitos Informáticos**, pp. 133-134.

[3] BRASIL. MINISTÉRIO DA CIÊNCIA E TECNOLOGIA, Livro Verde, p. 171.

[4] Ibidem, p. 178.

[5] **Condutas Ilícitas na Sociedade Digital**, pp. 169-170.

[6] Ibidem, pp. 169-171.

[7] Augusto Eduardo de Souza Rossini, op. cit., p. 134.

[8] BRASIL. MINISTÉRIO DA CIÊNCIA E TECNOLOGIA, op., cit., p. 176.

indeterminado de pessoas em curtos espaços de tempo. Mas não é só. Além de facilitar a comunicação entre as pessoas e possibilitar a disseminação rápida de informações, a internet ainda facilita muito a vida de quem possui acesso a um computador a ela conectado.

Hoje é possível que o indivíduo, sem sair de casa, troque correspondências, arquivos, idéias, comunique-se em tempo real, faça pesquisas, utilize serviços e compre produtos[9]. Existem, inclusive, diversos serviços estatais que são prestados pela internet. É possível, por exemplo, inscrever-se na Previdência Social pela internet, além de muitas outras facilidades que a internet oferece para o cotidiano do ser humano.

Assim, é a internet uma rede mundial de computadores, que facilita ao extremo o relacionamento entre diversas pessoas, físicas ou jurídicas, seja no sentido pessoal ou comercial.

Fato é que a internet permite a rápida comunicação, envio de mensagens e arquivos, transmissão de textos, ofertas de produtos ou serviços, compras, pesquisas etc., mas também permite a prática de condutas ilícitas, pois, como não poderia ser diferente, tudo aquilo que surge para facilitar a vida e a convivência humana, também é acompanhado de práticas contrárias ao Direito.

3. O Surgimento de Novos Bens Jurídicos na Nova Sociedade

Desde que o mundo é mundo, todo avanço social vem acompanhado de prejuízos, e na Sociedade da Informação, com a intensificação do uso da internet, não poderia ser diferente.

A transmissão de dados via internet não é totalmente segura. São freqüentes as notícias que se tem a respeito de invasores da rede, que conseguem acessar dados pessoais das pessoas, com os mais variados objetivos, colocando em risco a transmissão de informações.

Não é outro o entendimento de Liliana Minardi Paesani, ao afirmar:

> a questão que levanta maior polêmica é, sem dúvida, a circulação internacional de informações. A circulação dos antecedentes, idéias e fundamentos constitui o fenômeno conhecido pelo nome de 'fluxo de dados transfronteiras', que tem provocado a preocupação das grandes organizações internacionais. Na busca das mais várias soluções, tentam proteger primeiramente as idéias e antecedentes de caráter pessoal e, em seguida, os problemas jurídicos ligados a questões econômicas importantes[10].

Ainda para a autora, a informação tornou-se um novo bem jurídico, que deve ser tutelado pelo Direito, são as suas palavras:

> a informação, para poder ser valorada e valorizada, é submetida a tratamentos sofisticados. Pode ser guardada, manipulada como um objeto, cedida ou até subtraída ilicitamente [...] A problemática relacionada ao uso, lícito ou ilícito da informação e da Informática, sua difusão e circulação, tem levantado problemas e questões novas à luz do Direito: são problemas a que os juristas, inicialmente reticentes, não puderam omitir-se, dada a relevância econômica e social do fenômeno[11].

Observamos, portanto, que na nova sociedade surgem questões até então não reguladas pelo Direito, mas que não podem ser ignoradas, tendo em vista que a disseminação da internet provocou profundas mudanças em todos os ramos do Direito, não apenas com relação às informações.

Assim, no novo contexto social, a informação adquire um valor importante, da mesma forma que os demais instrumentos e bens informáticos. Segundo Marco Antonio Zanellato, trata-se do conceito de valor agregado, já que "*os bens informáticos não valem pelo que eles são, mas sim pelo valor que eles adicionam à vida de alguém, de uma*

[9] Marco Antonio Zanellato, op. cit., pp. 169-171.

[10] **Direito de Informática. Comercialização e Desenvolvimento Internacional do *Software***, p. 32.

[11] Ibidem, p. 26.

empresa, do Poder Público, etc. Ou seja, o valor está atrelado à utilidade agregada, que se adiciona ao processo"[12].

Na seara do Direito Penal, o uso da internet veio acompanhado de diversas condutas capazes de causar lesões aos mais diversos bens jurídicos. Nesse sentido, conforme lembra Alexandre Jean Daoun, "*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"*[13].

Em vista disso, surgem diversas discussões a respeito da possibilidade ou não de se amoldarem as condutas praticadas no meio virtual aos tipos penais já existentes. Com relação àquelas condutas que não se amoldam, não há que se falar em punição, o que violaria o princípio da legalidade.

Assim, surgem diversos projetos de lei buscando tratar da matéria, trazendo a tipificação de delitos praticados no ambiente virtual. Trataremos de um projeto de lei em específico, que pretende a tipificação de diversas condutas, que denomina como "crimes virtuais".

Antes de adentrarmos na análise deste projeto, importante trazer alguns conceitos básicos para que se compreenda o conceito desta nova modalidade delitiva.

4. Crimes Informáticos

Inicialmente, ressaltamos que, apesar de inúmeras ocorrências envolvendo atividades ilícitas pela internet, ainda não se chegou a um consenso a respeito do conceito de delito informático. A própria denominação que se confere a essa espécie de crime não é uniforme, há quem fale em criminalidade mediante computadores, criminalidade do computador, delito informático, criminalidade da informática, delitos cibernéticos, cibercrimes, entre outros. Entretanto, a denominação "delitos informáticos" é mais abrangente, incluindo todas as condutas praticadas a partir de sistemas informáticos, seria, na verdade, o gênero, enquanto os demais, como o delito cibernético, seriam espécies[14].

Para Augusto Eduardo de Souza Rossini, o melhor conceito de delito informático é o da Organização para a Cooperação Econômica e Desenvolvimento da Organização das Nações Unidas, que assim o define: "*o crime de informática é qualquer conduta ilegal não ética, ou não autorizada, que envolva processamento automático de dados e/ou transmissão de dados"*[15].

Vale trazer à baila o conceito de crime de computador nas palavras de Paulo Marco Ferreira Lima:

> [...] temos que crimes de computador são qualquer conduta humana (omissiva ou comissiva) típica, antijurídica e culpável, em que a máquina computadorizada tenha sido utilizada e, de alguma forma, facilitado de sobremodo a execução ou a consumação da figura delituosa, ainda que cause um prejuízo a pessoas sem que necessariamente se beneficie o autor ou que, pelo contrário, produza um benefício ilícito a seu autor, embora não prejudique a vítima de forma direta ou indireta[16].

Já para Carla Rodrigues Araújo de Castro:

> Crime de informática é aquele praticado contra o sistema de informática ou através deste, compreendendo os crimes praticados contra o computador e seus acessórios e perpetrados através do computador. Inclui-se neste conceito os delitos praticados através da Internet, pois pressuposto para acessar a rede é a utilização de um computador.
> Tal qual a nomenclatura, o conceito de crime de informática também não é uniforme. Para Ivette Senise Ferreira, crime de

[12] **Condutas Ilícitas na Sociedade Digital**, p. 167.

[13] **Os novos crimes de informática.** Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=1827>. Acesso em 08 de outubro de 2006.

[14] Augusto Eduardo de Souza Rossini, op. cit., pp. 137-138.

[15] Ibidem, p. 139.

[16] **Crimes de Computador e Segurança Computacional**, p. 31.

> informática é toda ação típica, antijurídica e culpável contra ou pela utilização de processamento automático e/ou eletrônico de dados ou sua transmissão[17].

Quando essas condutas podem ser subsumidas a um tipo penal existem na legislação pátria, não encontramos qualquer problema. É possível enquadrarmos um crime no Código Penal ou em leis extravagantes quando a internet é apenas seu meio de execução. Estes são os crimes eletrônicos, crimes da internet, crimes digitais, crimes cibernéticos ou *cybercrimes*, como, por exemplo, a exposição na internet de fotografias pornográficas envolvendo menores, que se subsume ao artigo 241, do Estatuto da Criança e do Adolescente, ou a publicação não autorizada de textos em um site, que se enquadra no artigo 184, do Código Penal[18].

Diversos crimes podem ser praticados a partir da internet, que nada mais é que o meio utilizado para a sua execução. Como ocorre na hipótese de crimes contra a honra, crime de ameaça, violação de comunicações, entre outros. Nestas hipóteses o agente pode enviar mensagens eletrônicas para a vítima ameaçando-a ou injuriando-a, ou para terceiros, caluniando ou difamando o ofendido. Em outras palavras, quando o meio executório para a prática do delito é escrito ou alguma forma de divulgação, é possível a utilização da internet para a sua prática.

Apenas a título de exemplo, a internet pode até ser utilizada para a prática de um crime de homicídio doloso, caso o agente, por exemplo, intencionalmente, interfira na programação de um aparelho em funcionamento na unidade de terapia intensiva (UTI), desligando-o e causando a morte do paciente[19].

O problema aparece quando a conduta praticada não encontra tipificação legal, vez que lesiona o bem informação, cuja proteção jurídico-penal é reclamada pela sociedade atual, conforme já ressaltado. Tais práticas, conhecidas como crimes informáticos puros, não encontram correspondência na legislação penal pátria[20].

5. Classificação dos Crimes Envolvendo Computadores

Alguns estudiosos propõem classificações dos crimes praticados por meio de computadores, utilizando ou não a internet, sendo as mais importantes aquelas que consideram o crime informático como de meio, método ou fim e que os dividem em puros e mistos, conforme se verá adiante.

Conforme Augusto Eduardo de Souza Rossini os delitos informáticos puros ocorrem quando o agente visa especificamente ao sistema de informática, ou seja, *software, hardware*, dados e sistemas e meios de armazenamento, nesta hipótese a conduta visa somente ao sistema informático da vítima. Como exemplos, podem ser citadas as condutas dos *hackers* e *crackers* e as violações ao *software.*

Já os delitos informáticos mistos são aqueles em que o computador é mera ferramenta para a ofensa a outros bens jurídicos que não sejam do sistema de informática. Como exemplo, podemos citar o estelionato, a ameaça, os crimes contra a honra, o homicídio (a partir da mudança pela internet de rotas de aviões, entre outros)[21].

Seguindo essa mesma linha de bem jurídico lesionado, Mário Furlaneto Neto e José Augusto Chaves Guimarães trazem os crimes informáticos puros, mistos e comuns[22]. No crime informático puro o objeto do crime é apenas o sistema de computador, seria um atentado físico ou técnico ao equipamento e seus componentes, incluindo dados, sistemas, *softwares e hardwares*. Já no crime informático misto o uso da internet é condição sem a qual a conduta criminosa não se efetiva, mas cujo bem jurídico não é o informático, seria a hipótese da transferência ilícita de valores em uma *homebanking.* Por fim, o crime informático comum é aquele em que a internet é apenas o meio executório para a prática de um crime previsto na legislação

[17] **Crimes de Informática e seus Aspectos Processuais**, p. 9.
[18] Rodrigo Guimarães Colares, op. cit.
[19] Mário Furlaneto Neto; José Augusto Chaves Guimarães, op. cit., p. 71.
[20] Rodrigo Guimarães Colares, op. cit.
[21] Op. cit.
[22] Op. cit., p. 69.

penal, é o caso da divulgação em sites de fotografias pornográficas envolvendo crianças e adolescentes, que tipifica o delito previsto no artigo 241, do Estatuto da Criança e do Adolescente.

Outra classificação dos crimes virtuais leva em consideração se o uso da tecnologia informática é método, meio ou fim da atividade criminosa. Na verdade, essa classificação segue a mesma linha daquela que divide os crimes informáticos em puros e mistos, apenas alterando sua denominação. O crime informático será tido como de método quando o agente utilizar a tecnologia eletrônica para a obtenção de um resultado ilícito; serão de meio quando a tecnologia for o meio de execução da conduta criminosa; e serão de fim quando as condutas forem dirigidas contra a entidade física do objeto ou máquina eletrônica ou seu material, com o objetivo de danificá-lo[23].

Em outras palavras, o crime informático será crime meio quando praticado em ambiente virtual para se chegar ao crime fim, que pode ser um crime de furto, estelionato, entre outros. A internet é o meio que facilita a prática do crime, como nos casos de transferência de quantias em dinheiro para as contas de criminosos. Nesta hipótese, estamos diante dos crimes praticados com o computador, ou seja, crimes comuns em que o computador funciona apenas como meio.

O crime informático será de fim quando praticado contra o computador, ou seja, contra as informações e programas nele contidos, nesta hipótese o computador é o objeto do crime[24]. Os atos do agente são praticados contra um sistema de informática, por qualquer motivo que seja, são ações que atentam contra o próprio material informático, como suportes lógicos ou dados dos computadores.

Paulo Marco Ferreira Lima traz a classificação dos crimes de computador segundo a proposta de Ulrich Sieber[25]:

1. Crimes econômicos, que incluem: fraude por manipulação de um computador contra um sistema de processamento de dados; espionagem informática; furto de tempo; intrusão de sistemas; ofensas tradicionais;

2. Ofensas aos direitos individuais, consistentes em: uso incorreto de informação; obtenção ilegal de dados e posterior arquivo das informações; revelação ilegal e mau uso de informações; dificultar a distinção da obtenção, arquivamento ou revelação de dados; e

3. Ofensa aos direitos supra-individuais, que seriam: ofensas contra interesses estaduais e políticos; ofensas contra a integridade humana.

Ainda Paulo Marco Ferreira Lima traz outra classificação, agora com base em Marc Jeager, que denomina tais crimes com fraude informática[26]:

1. Fraudes propriamente ditas, envolvendo: fraudes da matéria corporal ou dos *hardwares*; fraudes no nível do *input* de dados; fraudes no nível do tratamento dos programas e dados; fraude no nível do *output* de dados; e

2. Atentados à vida privada.

6. Alguns Tipos de Condutas

São diversas as ações ilícitas que podem ser praticadas no meio virtual.

A Organização das Nações Unidas, no Oitavo Congresso sobre Prevenção de Delito e Justiça Penal, realizado em Havana, em 1990, publicou uma relação com os seguintes crimes informáticos: fraudes cometidas mediante manipulação de computadores (com manipulação de dados de entrada ou saída, ou de programas de informática); falsificações informáticas (alteração de documentos computadorizados, uso do computador para falsificação de documentos); danos ou modificações de programas ou dados computadorizados (criação de vírus para aderir a programas legítimos e propagar-se a outros programas informáticos; gusanos, semelhantes ao vírus, mas para se infiltrar em programas de dados para modificá-lo ou destruí-lo, sem regenerar-se; bomba lógica ou cronológica, para destruição ou modificação de dados em momento futuro; acesso não autorizado a sistemas de serviços, incluindo sabotagem e

[23] Ibidem, p. 70.
[24] Ibidem, p. 69.
[25] Op. cit., pp. 36-40.
[26] Op. cit., pp. 40-41.

espionagem informáticas; *hackers*, que se aproveitam das falhas nos sistemas de segurança para terem acesso a programas e órgãos de informações; reprodução não autorizada de *softwares*)[27].

No Décimo Congresso sobre Prevenção de Delito e Tratamento do Delinquente, realizado em Viena, em 2000, a Organização das Nações Unidas relacionou outros tipos de delitos, como a espionagem industrial, para descoberta de segredos comerciais, técnicas e estratégias; sabotagem de sistemas; sabotagem e vandalismo de dados; pesca ou averiguação de senhas secretas; estratagemas, para buscar acesso a sistemas geralmente restritos; pornografia infantil; jogos de azar; fraudes, especialmente contra consumidores; lavagem de dinheiro, sendo o comércio eletrônico novo meio pra transferência eletrônica de valores e mercadorias[28].

Marco Antonio Zanellato relaciona algumas práticas ilícitas costumeiras na internet. Traremos algumas delas na seqüência.

A primeira delas refere-se aos chamados *cookies*, que registram as informações prestadas pelo usuário, bem como todos os cliques que ele faz num determinado site, prática essa normalmente utilizada por sites de comércio, para que conheçam os gostos de seus usuários. O problema surge quando esses *cookies* passam a ser utilizados por espiões, ou quando é utilizado sem controle e conhecimento do usuário, ou, ainda, quando essas informações são vendidas a outras empresas sem o consentimento do usuário[29].

Já os "*spywares são programas espiões que enviam informações do computador do usuário da rede para desconhecidos*"[30]. A diferença entre os *spywares* e os *cookies* consiste no fato de que estes são plantados por um *website*, enquanto que aqueles são introduzidos por um programa *freeware*, na verdade eles roubam as informações do computador do usuário. Normalmente o usuário instala o programa sem nem saber do que se trata e, a partir daí, o programa obtém informações que estão no computador ou que passam por ele, como as digitadas no teclado[31].

Há, também, os *spammings*, que consistem no envio de mensagens eletrônicas, especialmente publicitárias, não solicitadas, os *spams*. O problema dessas mensagens, além de serem enviadas sem solicitação do destinatário, é que enchem a caixa eletrônica do usuário, além de envolverem práticas desleais e comércio incontrolado de informação.[32].

Outro problema que se verifica com relação aos *spams*, é a invasão da privacidade do usuário da internet, já que

> os *spammers*, com suas baterias de e-mails indesejados, costumam usar um truque sujo para acompanhar os passos das pessoas na rede. Eles anexam um *cookie* com um número único aos *e-mails* em HTML e, a partir daí, espionam clique por clique dos destinatários, sem que eles sequer desconfiem do que está acontecendo. Para ter uma idéia do alcance desse perigo, basta dizer que listas brasileiras com 100.000 endereços de *e-mails* são oferecidos pela internet, a qualquer pessoa, por 50 reais[33] (grifos do autor).

Nos Estados Unidos, o *Can-Spam Act* prevê o crime de enviar por correio eletrônico mensagem comercial com informação falsa ou enganosa. No Brasil, essa prática pode ser enquadrada no artigo 67 do Código de Defesa do Consumidor[34]. Em 2002 foi apresentado pelo deputado Ivan Paixão o Projeto de Lei n. 6.210/02, trazendo limitações ao envio de *spams*[35].

Outra prática indevida e muito utilizada na internet consiste nos *hoaxes*, que é o envio de e-mails de conteúdo alarmante ou falso, normalmente constando como remetentes empresas importantes ou órgãos governamentais, na maioria das vezes acompanhadas de vírus. O objetivo dessas

[27] Mário Furlaneto Neto; José augusto Chaves Guimarães, op. cit., pp. 70-71.
[28] Ibidem, p. 71.
[29] Marco Antonio Zanellato, op. cit., pp 171-184.
[30] Ibidem, p. 187.
[31] Ibidem, mesma página.
[32] Ibidem, pp. 189-190.
[33] Ibidem, p. 192.
[34] Ibidem, p. 197.
[35] Ibidem, pp. 201-202.

mensagens é alarmar a população, espalhando desinformação[36].

Outra espécie de programa espião é o *sniffer*, parecido com os *spywares*. Trata-se de um programa rastreador, usado para penetrar no *hardware* de computadores conectados à internet, objetivando a busca de determinado tipo de informação, é um verdadeiro atentado à privacidade dos usuários da rede[37].

O cavalo de tróia também é um programa espião e, uma vez instalado no computador, permite o "roubo" de informações, arquivos e senhas do usuário. Normalmente o usuário recebe e-mails com o arquivo anexado e, quando abre o arquivo, instala-se o cavalo de tróia no computador do usuário e

> na maioria das vezes, tal programa ilícito vai possibilitar aos hackers o controle total de 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. É um verdadeiro procedimento de invasão informática[38].

Produzem danos semelhantes ao cavalo de tróia os *backdoors*, programas que podem ser abertos em razão de defeitos de fabricação ou falhas no projeto dos programas, o que pode ser acidental ou propositalmente[39].

Já os vírus, podem ser espalhados de diversas maneiras, a partir da instalação de programas de procedência duvidosa, com a utilização de disquetes ou CDs infectados, com a abertura de arquivos, entre outros. Os vírus podem destruir totalmente os programas e arquivos do computador, podendo exercer controle total sobre a máquina. O vírus pode permanecer encubado, reproduzindo e infectando outros computadores, até que um evento qualquer seja capaz de acordá-lo, o que normalmente ocorre em uma data específica[40].

De acordo com Carla Rodrigues Araújo de Castro:

> Vírus é um programa estranho ao sistema do computador capaz de copiar e instalar cópias a si próprio, resultando na realização de tarefas não solicitadas e destruindo arquivos e seus correspondentes dados. Ao lado dos vírus existem os *worm* e *trojans*. *Worms* são programas que se propagam de um sistema para o outro sem a interferência do usuário infectado, dividem-se em: *worm* de Internet e *worm* de IRC. O *worm* destrói diversos arquivos do computador. Por fim, os *trojans*, também chamados de *cavalos de tróia* ou *backdoors*, são programas enviados para computador alheio associados a uma música, desenho ou piada[41].

O objetivo dos vírus é destruir arquivos. Diante da falta de previsão legal desta figura criminosa, a conduta somente poderá ser punida se a destruição dos arquivos implicar em um prejuízo econômico para a vítima[42].

Vale ressaltar que a grande maioria das condutas praticadas por meio de computador, utilizando-se ou não a internet, além dessas acima explicitadas, não encontram qualquer correspondência na atual legislação, impedindo a punição dos criminosos.

Por exemplo, há condutas voltadas contra um determinado computador que visam a tomar conhecimento de todos os dados e informações nele constantes, sejam eles de qualquer natureza. Se tais informações puderem ser apreciadas economicamente, ou seja, se possuírem um valor de mercado, poderá restar tipificado o crime de furto.

Entretanto, caso os arquivos que o agente venha a subtrair não possuam valor econômico, a conduta restará impune. É o caso daquele que invade o computador de um usuário e subtrai-lhe diversos arquivos, como trabalhos de faculdade, fotografias, enfim, diversos arquivos pessoais, sem qualquer conteúdo econômico. Nesse sentido também é o entendimento de Carla Rodrigues Araújo de Castro quando afirma que "*para a*

[36] Ibidem, pp. 202-203.
[37] Ibidem, p. 203.
[38] Ibidem, p. 204.
[39] Ibidem, p. 205.
[40] Ibidem, p. 206.
[41] Op. cit., pp. 27-28.
[42] Op. cit., p. 28.

configuração do delito é necessário que o objeto subtraído possua valor econômico. Assim, se o agente subtrai arquivo sem valor, como, por exemplo, uma foto de família, não haverá crime"[43].

Com relação à transferência ilícita de valores, a partir da manipulação de dados eletrônicos, Paulo Marco Ferreira Lima defende que esta conduta não se enquadra nem no crime de furto mediante fraude nem no crime de estelionato. E isso porque, para que haja a fraude, em uma ou outra hipótese, é necessário que a vítima seja enganada, e a fraude, no caso, é contra máquinas mecânicas ou informáticas, que não podem ser enganadas. Somente as pessoas podem ser enganadas[44]. Nas palavras do autor:

> [...] o engano é um estado psicológico consistente em uma representação mental que não responde à realidade; resulta impensado aceitar a possibilidade desta representação mental equivocada em uma máquina. É que não podem ser enganados aqueles que carecem de capacidade de equivocar-se: que não é capaz de conhecer, não é capaz de errar, em tal direção, como uma máquina carece do sentido da realidade, impossível é afirmar que atua em forma errônea por ação do sujeito ativo[45].

7. Sujeito Ativo

É importante mencionar as diferenças entre as diversas espécies de sujeitos ativos nos crimes informáticos. A designação comum dos sujeitos ativos refere-se a *hacker, cracker, lamer, pheakers, cardes* e *cyberterrorists*.

Muito se confunde entre as figuras do *hacker* e do *cracker*, havendo, inclusive, situações em que se trocam esses termos.

Segundo Marco Antonio Zanellato,

> cabe fazer uma distinção entre *hacker* e *cracker*, ao menos para efeito de repressão penal de suas condutas, na medida em que as dos primeiros seriam menos nocivas do que as do segundo, de modo a merecerem tratamento legal diferenciado...Os *crackers* dirigem suas ações, habitualmente, à destruição de sistemas informáticos, inserindo neles *vírus, Cavalos de Tróia, sniffers, spywares* etc. São, portanto, mais perigosos do que os *hackers* ou meros intrusos informático [46] (grifos do autor).

O *hacker* é aquele que possui alta habilidade técnica para lidar com sistemas de computação ou comunicações em rede; enquanto que o *cracker*, ou pirata digital, é o especialista em sistemas informatizados que invade sistemas alheios, sem autorização[47].

Como bem lembra Marco Antonio de Barros, a denominação *hacker*, em inglês, significa "fuçador" [48] . E, realmente, sua intenção é apenas fuçar em determinado sistema.

Os invasores reúnem-se e tiram proveito de várias máquinas comprometidas. Os *hackers* tiram proveito de redes e sistemas operacionais vulneráveis[49].

Nos dizeres de Paulo Marco Ferreira Lima, *"Os* hackers *são, em regra, invasores dos sistemas eletrônicos que, por espírito de emulação, estariam desafiando seus próprios conhecimentos técnicos e a segurança de sistemas informatizados de grandes companhias e organizações governamentais*"[50] (grifos do autor).

Os *crackers*, por sua vez, "*adulteram programas e dados, furtam informações, valores e praticam atos de destruição deliberada. São os autores das grandes fraudes eletrônicas, causando expressivos prejuízos a vários usuários, instituições e, enfim, toda a coletividade"*[51].

Já o *lamer*, que também possui conhecimentos em informática, mas não tão

[43] Op. cit., p. 26.
[44] Op. cit., p. 143.
[45] Op. cit., p. 146.
[46] Ibidem, p. 208.
[47] BRASIL. MINISTÉRIO DA CIÊNCIA E TECNOLOGIA, op. cit., p. 168.
[48] **Tutela Punitiva Tecnológica**, p.283.
[49] **"Vírus digitais vão ficar ainda piores", diz especialista.** Notícia veiculada no Jornal Folha online em 10 de agosto de 2006. Disponível em: <http://www1.folha.uol.com.br/folha/informatica/ult124u20442.shtml>. Acesso em 08 de outubro de 2006.
[50] Op. cit., p. 72.
[51] Paulo Marco Ferreira Lima. Op. cit., p. 76.

profundos, busca espalhar vírus e vangloriar-se de seus feitos[52].

Há também os *pheakers*, especialistas em telefonia que, segundo Paulo Marco Ferreira Lima

> atacam no sentido de fraudar sistemas de telecomunicação (mormente linhas telefônicas convencionais e celulares, fazendo uso desses meios gratuitamente ou às custas de terceiros), facilitam o ataque aos sistemas a partir de acesso externo, tornando impossível sua identificação e prejudicando o rastreamento de ataques informáticos[53].

Os cardes são aqueles "criminosos que se apropriam do número de cartões de crédito, obtidos através de invasão de listas eletrônicas constantes nos sites de compras efetivadas pela Internet, ou de outros meios ilícitos para realizar toda a espécie de compras"[54] (grifos do autor).

Por fim, existem os cyberterrorists, cuja atividade ilícita consiste em desenvolver vírus de computador e as denominadas bombas lógicas para sabotar computadores e provocar a queda do sistema de grandes provedores, impossibilitando o acesso de usuários e causando grandes prejuízos econômicos[55].

Com relação à autoria dos delitos praticados a partir de sistemas informáticos, o grande problema é que, no mundo virtual, é mais difícil a identificação dos agentes desses crimes. Por exemplo, no site de relacionamentos Orkut existem diversas comunidades com flagrante caráter criminoso, que difamam ou caluniam as pessoas, ou mesmo praticam incitação ao crime ou apologia de crime ou criminoso.

Conforme notícia veiculada pela Folha de São Paulo no dia 27 de setembro de 2006, o Orkut retirou do ar dez comunidades que faziam apologia a diversos tipos de crime, em razão da propositura de uma ação cautelar pelo Ministério Público do Rio de Janeiro. Para que os criadores de tais comunidades sejam punidos é necessário que a empresa forneça seus dados[56], o que nem sempre ocorre.

No Rio de Janeiro foi identificada a adolescente, de 17 anos, que criou no site Orkut a comunidade "Liberdade pro Samuka", traficante preso no Rio de Janeiro[57].

A dificuldade em se identificar o autor da conduta criminosa existe porque no ambiente virtual raramente as pessoas informam seus dados corretos, até em razão da dificuldade em se verificar sua autenticidade. Assim, utilizam nicknames e dados identificatórios inverídicos, especialmente se tiverem a intenção de praticar ilícitos. Dessa forma, aquela pessoa fica conhecida no meio virtual da forma em que se apresenta, o que nem sempre condiz com a realidade.

Ainda que seja possível identificar o computador utilizado para aquela prática delituosa, é possível que não se chegue ao agente da conduta, já que pode ter se utilizado de computadores de acesso público, cujo estabelecimento não faça registro de usuários; ou, ainda, o computador pode ter apenas programas piratas instalados, registrados em nome de pessoas que podem nem existir, aparecendo, novamente, os dados inverídicos, dificultando ainda mais o conhecimento da autoria da conduta delituosa.

A respeito da dificuldade de identificação do sujeito ativo do crime virtual, vale transcrever a lição de Marco Antonio de Barros:

> Além da necessária destreza no agir, nem sempre será simples a tarefa de identificação da autoria. É que os atos lesivos podem ser praticados sob a camuflagem do anonimato ou de um *nickname* (apelido de identificação). Ademais, se não houver aposição de assinatura digital, a imputação de fato atentatório contra a honra e a consideração a quem

[52] Marco Antonio de Barros. Op. cit., p. 283.
[53] Op. cit., p. 77.
[54] Paulo Marco Ferreira Lima. Op. cit., pp. 77-78.
[55] Paulo Marco Ferreira Lima. Op. cit., p. 78.

[56] **Orkut retira dez páginas do ar por apologia ao crime.** Folha de São Paulo online. Disponível em: <http://www1.folha.uol.com.br/folha/informatica/ult124u20669.shtml>. Acesso em 08 de outubro de 2006.
[57] **Adolescente vai parar na delegacia por apologia ao tráfico no Orkut.** Folha de São Paulo online, 20 de setembro de 2006. Disponível em: <http://www1.folha.uol.com.br/folha/informatica/ult124u20628.shtml>. Acesso em 08 de outubro de 2006.

> supostamente deva ser atribuída a autoria ficarão sujeitas ao reforço de outros elementos de prova, ante a possibilidade de aposição de nome diverso de quem efetivamente seja o autor da imputação[58] (grifos do autor).

8. Tempo e Local do Crime

Outra dificuldade que se apresenta é a questão do tempo e do local do crime. Grande parte dos delitos informáticos são transfronteiras, transnacionais, ou seja, o agente pode estar, por exemplo, no Brasil e invadir o sistema informático de uma empresa que está situada no Canadá e os prejuízos ocorrerem no Japão. Como fica a questão do local do crime? E com relação ao tempo do crime? Quem será o Estado competente para processar e julgar o sujeito?

O meio virtual não possui espaço físico, não está delimitado geograficamente e seu acesso é muito dinâmico.

Há uma dificuldade em se descobrir que um crime foi praticado pelo meio virtual, principalmente em se descobrir quem foram os seus autores, de modo que as investigações se prolongam no tempo, o que pode prejudicar a punição dos criminosos, em razão do decurso do prazo prescricional.

Como bem lembra Marco Antonio de Barros:

> Ainda considerando o caráter transnacional da rede, existe outra questão que pode ser aqui levantada, visto que não existe um tratado internacional que a regulamente. Trata-se do problema da fixação da competência do juízo para processar e julgar um crime ocorrido na rede. Como na Internet não há fronteiras, se um crime contra a honra de uma pessoa foi perpetrado em um estado da federação ou em outro país, sua transmissão virtual propagará seus efeitos para todo o mundo. Pode ser que a vítima se encontre em outra unidade da federação ou país, e ali venha a tomar conhecimento do crime. E aí: o juízo competente seria o local onde o texto foi enviado pelo autor do fato aos computadores dos provedores que hospedam as páginas, ou seria o juízo da jurisdição em que se encontrava o ofendido, uma vez que o crime se consuma no momento em que se toma conhecimento da ofensa?[59].

Nas palavras de Paulo Marco Ferreira Lima:

Para Carla Rodrigues Araújo de Castro, a questão do local do crime informático, na hipótese de ultrapassar a fronteira do Estado, deve ser regido por aqueles princípios contidos no Código Penal, quais sejam, territorialidade, nacionalidade, defesa, justiça penal universal, representação.

Realmente, para que se estabeleça se o Brasil será competente para processar e julgar determinado crime informático, somente se utilizando mesmo desses princípios norteadores da aplicação da lei penal no espaço.

Se assim não fosse, de nenhuma outra forma seria justificada a aplicação da lei penal brasileira ao fato.

Entretanto, vale ressaltar que, sendo o caso de extraterritorialidade condicionada, deverão ser respeitados os requisitos trazidos no artigo 7º, parágrafos 2º ou 3º, do Código Penal.

Com relação à competência, de se seguir as regras trazidas pelo Título V, do Código de Processo Penal, lembrando sempre a competência da Justiça Federal. Ressalte-se que o simples fato de a Polícia Federal intervir nas investigações, nos termos da Lei n. 10.446/02, não desloca a competência para processar e julgar o infrator da Justiça Estadual.

9. Aspectos Processuais

É importante ressaltar alguns aspectos processuais dos crimes praticados no meio virtual.

Com relação àquelas pessoas vítimas de ofensas praticadas por e-mail ou páginas virtuais, vale dizer que devem procurar preservar a prova. Sim, porque no ambiente virtual as páginas podem ser alteradas e não haverá qualquer vestígio da prática daquele

[58] Op. cit., p. 292.

[59] Op. cit., p. 292.

crime, o que poderá dificultar a investigação e a própria punição do ofensor[60].

Sendo os crimes informáticos materiais, ou seja, que deixam vestígios, necessário que se proceda à realização da perícia, hipótese em que o perito deverá informar ao juiz o equipamento, os programas e arquivos, enfim tudo que se mostrar necessário para comprovar a prática do crime e, até mesmo, em que consistiu a prática criminosa[61]. De qualquer forma, sempre será necessária a busca e apreensão do computador utilizado para a prática do crime[62].

Por óbvio, a perícia deverá ser realizada por profissional habilitado, com conhecimentos em informática e sistemas de comunicação.

Vale dizer que os provedores de acesso à internet, assim como os hospedeiros de sítios devem manter registro, cadastro e identificação de todos os seus usuários, o que facilitará em muito a investigação criminal, sempre em busca da verdade real. Entretanto, atualmente, não há qualquer norma legal que obrigue a tais condutas dos provedores.

Também é importante para a investigação criminal que as casas que possibilitam o acesso à internet, como os conhecidos *cybe-cafés* mantenham cadastro de todas as pessoas que utilizaram seus computadores, nele fazendo constar o horário e a máquina utilizada pelo usuário.

10. O Projeto de Lei n. 76/00, do Senado Federal

Conforme consta em seu artigo 1º, este projeto pretende a alteração do Código Penal, do Código Penal Militar, do Código de Processo Penal, do Código de Defesa do Consumidor, da Lei que trata da interceptação telefônica e da Lei n. 10.446/02, que possibilita a intervenção da Polícia Federal nas investigações de crimes de repercussão interestadual ou internacional, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra dispositivos de comunicação ou sistemas informatizados e similares.

Passemos, então, à análise de referido projeto de lei.

O Código Penal, de acordo com o projeto, passará a vigorar acrescido de alguns artigos e com novas redações para determinados artigos, além da inclusão de novas qualificadoras e de normas penais explicativas.

> Dano por difusão de vírus eletrônico ou digital ou similar
> Artigo 163-A. Criar, inserir ou difundir vírus em dispositivo de comunicação, rede de computadores, ou sistema informatizado, com a finalidade de destrui-lo, inutilizá-lo, deteriorá-lo, alterá-lo ou modificar-lhe o funcionamento.
> Pena: reclusão de um a três anos e multa.
> Parágrafo único. A pena é aumentada de sexta parte, se o agente se vale de nome suposto ou da utilização de identidade de terceiros para a prática do crime.
>
> Capítulo VII-A – Da Violação de Rede de Computadores, Dispositivo de Comunicação ou sistema informatizado
> Acesso indevido a rede de computadores, dispositivo de comunicação ou sistema informatizado
> Artigo 154-A. Acessar indevidamente, rede de computadores, dispositivo de comunicação ou sistema informatizado.
> Pena: reclusão de dois a quatro anos e multa.
> § 1º Nas mesmas penas incorre quem, indevidamente, permite, facilita ou fornece a terceiro meio não autorizado de acesso a rede de computadores, dispositivo de comunicação ou sistema informatizado.
> § 2º Somente se procede mediante representação, salvo se o crime é cometido contra a União, Estado, Município, empresa concessionária de serviços públicos, agências, fundações, autarquias, empresas públicas ou sociedade de economia mista e suas subsidiárias.

[60] Marco Antonio de Barros. Op. cit., p. 291.
[61] Carla Rodrigues Araújo de Castro. Op. cit., p. 114.
[62] Ibidem mesma página.

> § 3º A pena é aumentada de sexta pare, se o agente se vale de nome suposto ou da utilização de identidade de terceiros para a prática de acesso.
> § 4º Nas mesmas penas incorre o responsável pelo provedor de acesso à rede de computadores, dispositivo de comunicação ou sistema informatizado, que permite o acesso a usuário sem a devida identificação e autenticação ou que deixa de exigir, como condição de acesso, a necessária identificação e regular cadastramento do usuário.
> § 5º No crime previsto no caput ou na hipótese do § 4º deste artigo, se o crime é culposo:
> Pena: detenção de seis meses a um ano e multa.

O parágrafo 4º busca fazer com que os provedores de acesso à rede de computadores mantenham controle de seus usuários, o que facilitará sobremaneira a investigação de eventuais crimes futuros, a partir da identificação do agente.

Essa nova figura delituosa fará com que os provedores sejam responsáveis por aqueles a quem concede acesso. Não é dizer que serão responsáveis caso seus usuários venham a praticar condutas ilícitas, mas serão responsáveis caso não tenham procedido corretamente ao cadastro deles. É uma forma de tentar cercar o usuário "na fonte". Em outra palavras, aquele que pretende cadastrar-se em um provedor para a prática de condutas ilícitas simplesmente, pensará duas vezes, pois o provedor terá que cadastrá-lo para poder liberar o seu acesso.

É claro que essa norma não será capaz de impedir a prática do crime pelo usuário, que poderá valer-se de dados de terceiros ou fantasiosos, mas já é uma forma de dificultar esse acesso. Tanto isso é verdade que em seu artigo 21 o projeto de lei permite ao provedor a utilização de meios aptos a verificar a autenticidade das informações prestadas pelo usuário quando de seu cadastro.

> Obtenção, manutenção, transporte ou fornecimento indevido de informação eletrônica ou digital ou similar
> Artigo 154-B. Obter indevidamente dado ou informação em rede de computadores, dispositivo de comunicação ou sistema informatizado.
> Pena: detenção de dois a quatro anos e multa.
> § 1º Nas mesmas penas incorre quem mantém consigo, transporta ou fornece dado ou informação obtida indevidamente em rede de computadores, dispositivo de comunicação ou sistema informatizado.
> § 2º Se o dado ou informação obtida indevidamente é fornecida pela rede de computadores, dispositivo de comunicação ou sistema informatizado ou em qualquer outro meio de divulgação em massa, a pena é aumentada em um terço.
> § 3º Somente se procede mediante representação, salvo se o crime é cometido contra a União, Estado, Município, empresa concessionária de serviços públicos, agências, fundações, autarquias, empresas públicas ou sociedade de economia mista e suas subsidiárias.

O parágrafo único do artigo 154-B nada mais é que um crime de receptação específico. Pune aquele que mantém consigo, transporta ou fornece dado ou informação obtida indevidamente em rede de computadores, dispositivo de comunicação ou sistema informatizado. Trata-se de norma especial, que afasta a aplicação da norma geral, qual seja, o artigo 180, do Código Penal.

Assim, somente será aplicado o artigo 180, do Código Penal na hipótese de a conduta praticada pelo agente não for nenhuma dessas previstas no artigo 154-B, parágrafo 1º, mas encontrar previsão no artigo 180, vez que a norma geral somente é aplicável na hipótese de a conduta não se subsumir à norma especial.

Os crimes de acesso indevido à rede de computadores, dispositivo de comunicação ou sistema informatizado e obtenção, manutenção, transporte ou fornecimento indevido de informação eletrônica ou digital ou similar são de ação penal pública condicionada à representação do ofendido, salvo quando cometidos contra entes públicos ou equiparados.

E isso porque são situações que podem representar prejuízo para as vítimas, pois a prática desses crimes demonstram a

vulnerabilidade de seus sistemas, o que poderá prejudicá-los com relação à confiabilidade de seus usuários e clientes.

Desta forma, tornar este fato público poderá causar mais prejuízo do que o já causado pelo criminoso.

Não concordamos com essa solução adotada pelo projeto, uma vez que não se trata de um interesse meramente privado, essas condutas criminosas não violam apenas as vítimas diretas, mas agridem toda a coletividade, pois muitos têm seus dados pessoais nos sistemas das vítimas e poderão sofrer prejuízo com essa violação.

> Dispositivo de comunicação, sistema informatizado, rede de computadores, identificação de usuário, autenticação de usuário, provedor de acesso e provedor de serviço, dados de conexões realizadas
> Artigo 154-C. Para os efeitos penais considera-se:
> I – dispositivo de comunicação: o computador, o computador de mão, o telefone celular, o processador de dados, os meios de armazenamento de dados eletrônicos ou digitais ou similares, os meios de captura de dados, ou qualquer outro meio capaz de processar, armazenar, capturar ou transmitir dados utilizando-se de tecnologias magnéticas, óticas ou qualquer outra tecnologia eletrônica ou digital ou similar;
> II – sistema informatizado: equipamento ativo da rede de comunicação de dados com ou sem fio, a rede de telefonia fixa ou móvel, a rede de televisão, a base de dados, o programa de computador ou qualquer outro sistema capaz de processar, capturar, armazenar ou transmitir dados eletrônica ou digitalmente ou de forma equivalente;
> III – rede de computadores: os meios físicos e lógicos através dos quais é possível trocar dados e informações, compartilhar recursos, entre máquinas, representada pelo conjunto de computadores, dispositivos de comunicação e sistemas informatizados, que obedecem de comum acordo a um conjunto de regras, parâmetros, códigos, formatos e outras informações agrupadas em protocolos, em nível topológico local, regional, nacional ou mundial, este nível conhecido como internet, ou quanto ao proprietário, privado ou público;
> IV – identificação de usuário: os dados de identificador de acesso, senha ou similar, nome completo, data de nascimento e endereço completo e outros dados que sejam requeridos no momento do cadastramento de um novo usuário de rede de computadores, dispositivo de comunicação ou sistema informatizado;
> V – autenticação de usuário: procedimentos de verificação e conferência da identificação do usuário, quando este tem acesso a rede de computadores, dispositivo de comunicação ou sistema informatizado, realizado por quem torna disponível o acesso pelo usuário;
> VI – provedor: o prestador de serviços de acesso à rede de computadores e o prestador de serviços relacionados a esse acesso;
> VII – dados de conexões realizadas: aqueles dados aptos à identificação do usuário, os endereços eletrônicos de origem das conexões, a data, o horário de início e término e a referência GMT dos horários, relativos à cada conexão realizada pelos equipamentos de uma rede de computadores.

O artigo 154-C trata-se de uma norma penal explicativa, já que traz determinados conceitos, como dispositivo de comunicação, sistema informatizado, entre outros.

Essa norma é necessária, entendemos, por dois motivos. O primeiro deles, e o mais importante, para que se limite a aplicação da norma penal incriminadora, respeitando-se o princípio da legalidade, impedindo que, no caso concreto, amplie-se em demasia a aplicação da norma penal, deixando a critério do juiz entender se se trata ou não, por exemplo, de dispositivo de comunicação, sob pena de configurarem-se tipos penais abertos.

Em segundo lugar, porque os temas relacionados à informática são muito novos e exigem conhecimento específico. Dessa forma, com a própria lei trazendo os conceitos

facilitará a aplicação das normas penais pelos juízes, e a própria investigação criminal.

Violação ou divulgação indevida de informações depositadas em banco de dados

Artigo 154-D. Violar, divulgar ou tornar disponíveis, para finalidade distinta daquela que motivou a estruturação do banco de dados, informações privadas referentes, direta ou indiretamente, a dados econômicos de pessoas naturais ou jurídicas, ou a dados de pessoas naturais referentes a raça, opinião política, religiosa, crença, ideologia, saúde física ou mental, orientação sexual, registros policiais, assuntos familiares ou profissionais, além de outras de caráter sigiloso, salvo nos casos previstos em lei, ou por decisão da autoridade competente, ou mediante expressa anuência da pessoa a que se referem ou de seu representante legal.

Pena: detenção de um a dois anos e multa.

§ 1º A pena é aumentada de sexta parte, se o agente se vale de nome suposto ou da utilização de identidade de terceiros para a prática do crime.

§ 2º Se o crime ocorre em rede de computadores, dispositivo de comunicação ou sistema informatizado, ou em qualquer outro meio de divulgação em massa, a pena é aumentada de um terço.

§ 3º Não constitui violação do dever de sigilo a comunicação, às autoridades competentes, de prática de ilícitos penais, abrangendo o fornecimento de informações de acesso, hospedagem e dados de identificação de usuário, quando constatada qualquer conduta criminosa.

Ao punir a violação ou a divulgação das informações privadas constantes em bancos de dados, pretende-se coibir uma prática comum nos dias atuais, consistente na formação de bancos de dados e posterior fornecimento das informações colhidas para finalidade diversa daquela que motivou a criação do banco de dados.

Com a punição dessa conduta busca-se restaurar direitos fundamentais tão agredidos nesta nova Sociedade da Informação, quais sejam, a intimidade e a vida privada.

Visando a acabar com a discussão sobre a possibilidade ou não de uma transferência ilícita de valores operada a partir de uma *homebanking* configurar ou não furto qualificado pela fraude ou estelionato, o projeto pretende acrescentar nova qualificadora no artigo 155, que prevê o crime de furto:

> Artigo 155. (...)
> § 4º A pena é de reclusão de dois a oito anos e multa se o crime é cometido:
> V – mediante uso de rede de computadores, dispositivo de comunicação ou sistema informatizado ou similar.

É claro que não se aplicará a qualificadora apenas aos crimes de transferência ilícita de valores através do ambiente virtual, mas sim a qualquer conduta que configure o crime de furto, tendo, para a sua prática, o agente se valido da utilização da rede de computadores, dispositivo de comunicação ou sistema informatizado ou similar.

Dessa forma, será punido com maior rigor aquele que se vale de meio que dificulte a sua identificação e posterior punição.

Ainda, o projeto pretende a inclusão no Título II, da Parte Especial do Código Penal, que trata dos crimes contra o patrimônio do seguinte artigo:

> Artigo 183-A. Para os efeitos penais, equiparam-se à coisa o dado ou informação em meio eletrônico ou digital ou similar, o bit ou a menor quantidade de informação que pode ser entendida como tal, a base de dados armazenada, dispositivo de comunicação, a rede de computadores, o sistema informatizado, a senha ou similar ou qualquer meio que proporcione acesso aos anteriormente citados.

Dessa forma, atendendo aos reclamos da nova sociedade, o projeto busca proteger novo bem jurídico que atualmente agregou-se ao patrimônio, qual seja, a informação e os dados digitalizados.

Assim, ainda que não tenham um valor de mercado, que não possam ser economicamente mensurados, o projeto pretende a proteção desses bens. Por exemplo,

a senha de acesso do usuário a determinado sistema, por si mesma, não tem qualquer valor, mas ela representa um valor. Ou seja, de posse da senha o agente poderá passar-se pelo usuário e praticar condutas ilícitas contra o próprio usuário ou em nome dele. Trata-se do valor adicionado que mencionamos anteriormente.

Com essa equiparação da informação ou de qualquer dado a coisa, aquele que subtrair do computador do usuário arquivos pessoais, como fotografias ou cartas, sem qualquer valor econômico por si mesmos, poderá ser responsabilizado.

O projeto também pretende a alteração da redação dos artigos 265 e 266 e inclui novos tipos penais:

> Atentado contra a segurança de serviço de utilidade pública
> Artigo 265. Atentar contra a segurança ou o funcionamento de serviço de água, luz, força, calor, informação ou telecomunicação, ou qualquer outro de utilidade pública.
> Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático, dispositivo de comunicação, rede de computadores ou sistema informatizado
> Artigo 266. Interromper ou perturbar serviço telegráfico, radiotelegráfico, telefônico, telemático, informático, de dispositivo de comunicação, de rede de computadores, de sistema informatizado ou de telecomunicação, impedir ou dificultar-lhe o restabelecimento.
> Difusão maliciosa de código
> Artigo 266-A. Difundir, por qualquer meio, programa, conjunto de instruções ou sistema informatizado com o propósito de levar a erro ou, por qualquer forma indevida, induzir alguém a fornecer, espontaneamente ou por qualquer meio, dados ou informações que facilitem ou permitam o acesso indevido ou sem autorização, à rede de computadores, dispositivo de comunicação ou a sistema informatizado, ou a obtenção de qualquer vantagem ilícita.
> Pena: reclusão de um a três anos.
> § 1º A pena é aumentada de sexta parte, se o agente se vale de nome suposto ou da utilização de identidade de terceiros para a prática de difusão maliciosa.
> § 2º É isento de pena o agente técnico ou o profissional habilitado que, a título de resposta a ataque, de frustração de invasão ou burla de proteção do sistema, de interceptação defensiva, de tentativa de identificação do agressor, de exercício de forense computacional e de práticas gerais de segurança da informação manipula código malicioso detectado, em proveito próprio ou de seu preponente e sem risco para terceiros.

O projeto acresce o parágrafo único ao artigo 298, que prevê o crime de falsificação de documento particular

> Artigo 298 (...)
> Falsificação de cartão de crédito ou débito ou qualquer dispositivo eletrônico ou digital ou similar portátil de captura, processamento, armazenamento e transmissão de informações
> Parágrafo único. Equipara-se a documento particular o cartão de crédito ou débito ou qualquer outro dispositivo portátil capaz de capturar, processar, armazenar ou transmitir dados, utilizando-se de tecnologias magnéticas, óticas ou qualquer outra tecnologia eletrônica ou digital ou similar.
> Falsificação de telefone celular ou meio de acesso a rede de computadores, dispositivo de comunicação ou sistema informatizado
> Artigo 298-A. Criar ou copiar, indevidamente, ou falsificar código, seqüência alfanumérica, cartão inteligente, transmissor ou receptor de rádio freqüência ou telefonia celular, ou qualquer instrumento que permita o acesso a rede de computadores, dispositivo de comunicação ou sistema informatizado.
> Pena: reclusão de um a cinco anos e multa.

Com essas alterações, o projeto pretende punir a conduta daquele que “clona” cartões de

crédito ou números de telefone celulares, práticas tão comuns nos dias de hoje.

No capítulo dos crimes contra a honra, o projeto pretende incluir o seguinte artigo:

> Artigo 141-A. As penas neste Capítulo aumentam-se em dois terços caso os crimes sejam cometidos por intermédio de rede de computadores, dispositivo de comunicação ou sistema informatizado.

Entendemos que essa causa de aumento de pena se justifica por dois motivos. O primeiro deles é em relação à dificuldade de se identificar o sujeito ativo do crime. Assim, aquele que se vale de meio que permita a sua ocultação para a prática de crime deverá ter a sua pena aumentada.

O segundo deles é em razão da maior lesão que a ofensa à honra por meio virtual poderá causar ao ofendido. Fato é que uma vez colocada uma informação na internet ela se propaga, passa por e-mails, sítios etc., dificultando sua total retirada. Assim, é possível que uma ofensa pela praticada pela rede hoje, daqui há dez anos ainda esteja circulando pelo ambiente virtual, de modo que a lesão ao ofendido é muito maior, a publicidade que se dá à ofensa é muito maior, justificando o aumento da pena.

Com a inclusão do artigo 356-A ao Código Penal, o projeto pretende punir o provedor que, com sua conduta, dificulta a investigação criminal e a punição do criminoso. Confira-se:

> Artigo 356-A. Deixar de manter os dados de identificação de usuário e os dados de conexões realizadas por seus equipamentos, de valor probatório, aptos à identificação do usuário quando da ocorrência de crime, pelo prazo de três anos contados a partir da data de conexão, aquele que é o responsável pelo provedor de acesso à rede de computadores.

Podemos observar que o projeto pretende responsabilizar mais duramente aquele que se utiliza de identificação inverídica ou se utiliza de identificação de terceiros para a prática desses crimes. E isso porque é muito mais fácil ocultar-se no ambiente virtual e em sistemas de computador e caso o agente se utilize de tais expedientes dificultará em muito a investigação criminal, já que busca justamente esconder-se, causando até transtornos para a pessoa de cuja identidade se utiliza.

O projeto faz as mesmas alterações no Código Penal Militar, ou seja, essas condutas criminosas introduzidas no Código Penal são crimes militares impróprios.

Na Lei n. 9.296/96, o projeto acrescenta o parágrafo 2º no artigo 2º, que traz os requisitos autorizadores da interceptação telefônica:

> § 2º O disposto no inciso III do *caput* não se aplica quando se tratar de interceptação do fluxo de comunicações em rede de computadores, dispositivo de comunicação ou sistema informatizado.

Isto significa que, para que seja autorizada a interceptação de comunicações do fluxo de comunicações em rede de computadores, dispositivo de comunicação ou sistema informatizado, ou seja, interceptação telemática,, não é necessário que o crime seja apenado com reclusão.

Essa alteração é louvável. E isso porque diversos são os crimes praticados em meio virtual que são punidos com detenção. Por exemplo, o crime de ameaça é punido com detenção e pode ser praticado a partir do envio de e-mails pelo agente à vítima. O mesmo ocorre com relação aos crimes contra a honra, salvo a injúria preconceituosa.

As alterações que o projeto pretende no Código de Processo Penal são as seguintes:

Acrescenta o inciso IV no artigo 313, que autoriza a decretação da prisão preventiva nos crimes dolosos:

> Artigo 313. (...)
> IV – punidos com detenção, se tiverem sido praticados contra rede de computadores, dispositivo de comunicação ou sistema informatizado, ou se tiverem sido praticados mediante uso de rede de computadores, dispositivo de comunicação ou sistema informatizado.

Como já tivemos a oportunidade de mencionar, o projeto prevê a necessidade de cadastrar-se o usuário no provedor que permite o acesso a uma rede de computadores, bem como traz o prazo de cento e vinte dias, após a entrada em vigor da lei, para que os usuários atuais providenciem ou revisem sua identificação e cadastro junto ao provedor pelo qual acessa a rede.

Ainda, o projeto prevê a responsabilidade do provedor para que seja identificado e cadastrado o usuário, bem como possibilita-lhe a utilização de meios aptos a verificar a autenticidade das informações fornecidas pelo usuário.

O artigo 22 do projeto prevê as obrigações dos provedores de acesso a uma rede de computadores.

Caso o provedor não cumpra a determinação legal relativa ao cadastro e identificação de seus usuários, poderá ser responsabilizado criminalmente.

Já na Lei n. 10.446/02, que prevê a possibilidade de intervenção da Polícia Federal em investigações de crimes internacionais ou interestaduais, o projeto acrescenta, em seu artigo 1º, outra justificativa para essa intervenção:

> Artigo 1º. (...)
> V – os delitos praticados contra ou mediante rede de computadores, dispositivo de comunicação ou sistema informatizado.

Por fim, no Código de Defesa do Consumidor, o projeto acrescenta o parágrafo único no artigo 9º, que trata do dever do fornecedor de produtos e serviços potencialmente nocivos ou perigosos à saúde ou segurança informar, de maneira ostensiva e adequada, a respeito da sua nocividade ou periculosidade, sem prejuízo da ação de outras medidas cabíveis no caso concreto:

> Artigo 9º. (...)
> Parágrafo único. O mesmo se aplica à segurança digital do consumidor, mediante a informação da necessidade do uso de senhas ou similar para a proteção do uso do produto ou serviço e para a proteção dos dados trafegados, quando se tratar de dispositivo de comunicação, sistema informatizado ou provimento de acesso a rede de computadores ou provimento de serviço mediante o uso dela.

Com essa alteração, o projeto pretende adequar a proteção do consumidor nos termos da nova sociedade, com a predominância dos meios virtuais, também utilizados para práticas consumeristas. Assim, o projeto transfere para o fornecedor do produto ou serviço a responsabilidade de informar ao consumidor sobre a necessidade de sua segurança no ambiente virtual. Justifica-se essa disposição na medida em que o consumidor poderá efetuar comprar a partir do estabelecimento virtual do fornecedor, devendo, para tanto, estar seguro.

São essas as alterações que o projeto pretende, buscando amoldar as diversas legislações penais e processuais aos contornos da nova sociedade.

Uma crítica que podemos tecer a este projeto é a falta de previsão de determinadas condutas na modalidade culposa. E isso porque é bem possível, por exemplo, a disseminação de vírus e o perdimento de informações importantes por meio de negligência, imprudência ou imperícia.

Um usuário desatento poderá, por exemplo, instalar programas maliciosos ou espiões no computador de outra pessoa ou de sua empresa, ou poderá enviar via e-mail vírus que acabou de receber. São situações em que era possível prever o resultado, mas que o usuário, negligente, imprudente ou imperito, não previu.

Um exemplo concreto que podemos dar trata-se da perda avaliada em US$ 38 bilhões (trinta e oito bilhões de dólares) causada por um erro de digitação. O técnico, ao reformatar um drive no departamento de finanças do Alasca, nos Estados Unidos, apertou uma sequencia errada de botões e apagou um disco com dados avaliados no valor mencionado. O técnico imperito, em nosso entendimento, apagou informações de uma conta relacionada a petrolíferas, uma das maiores fontes de renda do estado. Além de reformatar, também apagou o disco com a cópia de segurança. Essa falha gerou um gasto de US$ 200 mil (duzentos mil dólares), e isso porque havia um terceiro *backup* das informações, consistente

em trezentas caixas de papel, o que levou setenta pessoas a digitalizarem novamente as informações, tais pessoas trabalharam durante dois meses, vinte e quatro horas por dia[63].

Imaginemos que não existisse mais o arquivo com os papéis, a perda não seria de apenas duzentos mil dólares, mas seria muito maior. Não seria o caso de punir, a título de culpa, a conduta do técnico? Entendemos que sim.

Podemos observar que o prejuízo foi decorrente de uma conduta culposa, no caso por imperícia, já que se tratava de técnico no assunto.

Trata-se de bem cuja proteção é reclamada pela sociedade e, sendo possível a punição de condutas culposas capazes de lesar esse bem, deverá haver a punição do sujeito.

Entretanto, não podemos negar a boa técnica do projeto de lei em questão, apesar deste esquecimento de previsão da modalidade culposa.

Fato é que, com o constante ingresso dos meios informáticos na vida das pessoas, especialmente a internet, chegamos a um ponto em que é extremamente necessária a proteção penal a esses novos bens jurídicos (informações, dados, sistemas informáticos, programas etc.), sob pena de deixar os usuários da rede de computadores desprotegidos.

Na sociedade atual é praticamente impossível retirar da vida das pessoas o uso dos sistemas de informática, por isso é mister a proteção desses novos bens jurídicos pelo Direito Penal.

11. Conclusões

A partir deste breve estudo, podemos tecer os seguintes comentários à guiza de conclusão:

1. Na atual sociedade, a Sociedade da Informação, surgem novos bens jurídicos, como a informação e os dados eletrônicos e digitais, cuja proteção pelo Direito Penal é reclamada, já que os sistemas informáticos ingressaram na vida das pessoas para as mais variadas práticas.

2. Os novos bens jurídicos não possuem valor econômico por si mesmos, mas são capazes de gerar valores. Trata-se do conceito de valor adicionado, é o valor que as informações e os dados representam.

3. É mister a tipificação de novas condutas, para que seja proporcionada a segurança das relações cibernéticas e a realização da personalidade humana no espaço cibernético.

4. Os delitos praticados a partir da rede de computadores podem ou não necessitar do uso do computador, hipóteses em que serão puros ou mistos.

5. Sendo delitos informáticos mistos, em que o uso de sistemas de computadores podem facilitar a sua execução, atualmente podem ser amoldados aos tipos penais existentes, pois poderiam ser praticados de outra forma, por outro meio.

6. Já os delitos informáticos puros, ou seja, aqueles dirigidos contra o próprio sistema de computadores, o *hardware* e o *software*, como, por exemplo, a disseminação de vírus, não encontram qualquer tipo penal correspondente na legislação atualmente em vigor, de modo que não podem ser punidos, sob pena de violação ao princípio da legalidade.

7. O meio virtual possibilita a ocorrência de diversos ilícitos. Assim, urge a proteção jurídica do novo bem da modernidade, a segurança informática, o que abarcaria o sigilo da transmissão de dados e arquivos, a privacidade do usuário, entre outros.

9. A legislação penal deve atender aos anseios da sociedade. É o que pretende o Projeto de Lei do Senado Federal n. 76/00, que pretende a inclusão na legislação de crimes virtuais, buscando a punição daqueles que praticam o que classificamos como crimes informáticos puros.

10. É necessária a criação da modalidade culposa de determinados tipos penais previstos no projeto, pois é possível que uma conduta negligente, imprudente ou imperita seja capaz de causar graves danos e sérios prejuízos a uma empresa ou a uma pessoa física.

11. Realmente, diante do atual quadro é mais que necessária a criação de uma

[63] Disponível em: <http://tecnologia.terra.com.br/interna/0,,oi1495914-ei4805,00.htm>. Acesso em: 20 de março de 2007, às 15:20hs.

legislação penal adequada à prevenção e repressão de crimes praticados a partir de sistemas informáticos, com ou sem a utilização da internet, sob pena de ignorar-se a evolução tecnológica e deixar vítimas desprotegidas.

12. Dificuldades surgirão na investigação criminal. Mas já pensando nisso, especialmente com relação à identificação da autoria, o mencionado projeto de lei pretende obrigar os provedores de acesso à internet a manterem cadastro de identificação de seus usuários. Pretende, inclusive, punir criminalmente aqueles que não o fizerem, seja por uma conduta dolosa ou culposa.

13. Outra dificuldade que se apresenta com relação aos crimes informáticos refere-se à competência para julgá-los, pois são crimes transnacionais. Diante disso, é mister a aplicação dos princípios relativos à lei penal no espaço, previstos no Código Penal quando trata da extraterritorialidade da lei penal. Assim, verificando-se ser o caso de aplicar-se a legislação penal brasileira, a competência para processar e julgar o agente deverá ser estabelecida de acordo com as regras constantes no Código de Processo Penal.

14. O projeto de lei tratado neste trabalho resume as condutas típicas que atualmente não encontram punição na legislação penal em vigor.

15. É realmente imprescindível a criação de tipos penais que correspondam às condutas ilícitas que acompanham a evolução tecnológica, sob pena de o Estado deixar os usuários da rede de computadores desprotegidos.

REFERÊNCIAS

ALVES, Roque de Brito. **Globalização do crime.** *in* IBCCRIM, São Paulo, v. 8, n. 88, p. 6, mar/00.

AFONSO, Carlos. **Internet para todos – tão perto e tão longe.** Disponível em: < http://www.comciencia.br/reportagens/socinfo/info12.htm>. Acesso em 07 de outubro de 2006.

ÂNGELO, Fernanda K. **Brasil lidera ranking mundial de hackers e crimes virtuais.** Notícia veiculada no Jornal Folha de São Paulo em 19 de novembro de 2002. Disponível em: <http://www1.folha.uol.com.br/folha/informatica/ult124u11609.shtml>. Acesso em 08 de outubro de 2006.

BARRETO, Juliana. **"Vírus digitais vão ficar ainda piores", diz especialista.** Notícia veiculada no Jornal Folha online em 10 de agosto de 2006. Disponível em: <http://www1.folha.uol.com.br/folha/informatica/ult124u20442.shtml>. Acesso em 08 de outubro de 2006.

BARROS, Marco Antonio de. Tutela Punitiva Tecnológica. In PAESANI, Liliana Minardi (coord.) **O Direito na Sociedade da Informação.** São Paulo: Atlas, 2007, pp. 275/300.

_____; ROMÃO, César Eduardo Lavoura. Internet e Videoconferência no Processo Penal. Brasília: **Revista CEJ**, n. 32, jan/mar, 2006, pp. 116-125.

BRASIL, MINISTÉRIO DA CIÊNCIA E TECNOLOGIA. **Sociedade da Informação no Brasil – Livro Verde.** Brasília, setembro, 2006.

CABETE, Eduardo Luiz Santos. **Direito Penal e Globalização.** *in* IBCCRIM, São Paulo, v. 7. n. 84, p. 4, nov/99.

CASTELLS, Manuel. [trad. Roneide Venancio Majer] **A Sociedade em Rede volume 1 – A Era da Informação: Economia, Sociedade e Cultura: inclusão e exclusão.** 9 ed. rev. e ampliada. São Paulo: Paz e Terra, 2006.

CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus Aspectos Processuais.** 2 ed. rev., ampl. E atualizada. Rio de Janeiro: Lumen Juris, 2003.

COLARES, Rodrigo Guimarães. **Cibercrimes – Os Crimes na Era da Informática.** Disponível em: <http://conjur.estadao.com.br/static/text/11500,1>. Acesso em 08 de outubro de 2006.

COSTA, Carlos José de Castro. **Crimes Virtuais.** Disponível em: <http://www.itaperuna.com.br/direito/direito2.htm>. Acesso em 08 de outubro de 2006.

DAOU, Alexandre Jean. **Os novos crimes de informática.** Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=1827>. Acesso em 08 de outubro de 2006.

DOTTI, René Ariel. **A Globalização e o Direito Penal.** *in* IBCCRIM, São Paulo, v. 7, n. 86, p. 9, jun/00.

FURLANETO NETO, Mário; GUIMARÃES, José Augusto Chaves. Direito da Informática. Crimes na Internet: elementos para uma reflexão sobre a ética informacional. **Revista CEJ**, n. 20. Brasília, jan/mar, 2003, pp. 67-73.

GASINO, Wilson. **O "Esquecedor" e a Sociedade da Informação.** Disponível em: < http://www.hottopos.com.br/videtur9/esquece.htm>. Acesso em 07 de outubro de 2006.

GONÇALVES, Fernando Moreira. **Justiça Penal e Globalização.** *in* IBCCRIM. São Paulo, v. 8, n. 100, p. 16, mar/01.

LIMA, Paulo Marco Ferreira. **Crimes de Computador e Segurança Computacional.** Campinas: Millennium, 2006.

OLIVEIRA, Edmundo. **Globalização da Justiça Penal Nacional.** *in* IBCCRIM, São Paulo, v. 11, n. 136, pp. 10/11, mar/04.

PAESANI, Liliana Minardi. **Direito de Informática. Comercialização e Desenvolvimento Internacional do *Software*.** 5 ed. São Paulo: Atlas, 2005.

PRADO, Luiz Carlos Delorme. **Globalização: Notas sobre um conceito controverso.** Disponível em: <http://www.ie.ufrb/br/prebisch/pdfs/17.pdf>. Acesso em 18/03/07, às 15:00.

ROSSINI, Augusto Eduardo de Souza. Condutas Ilícitas na Sociedade Digital. In **Caderno Jurídico***:* Escola Superior do Ministério Público de São Paulo: Imprensa Oficial do Estado de São Paulo. Ano 2, n. 4, jul/02, pp. 131/142.

SANTOS, Celeste Leite dos. Cartão de crédito e manipulação da assinatura digital. In **Revista Jurídica**. Ano 3, n. 2. São Paulo: Escola Superior do Ministério Público de São Paulo: Imprensa Oficial do Estado de São Paulo, jul/dez, 2004, pp. 133/156.

VOGT, Carlos. **Informação e Simulacro.** Disponível em <http://www.comciencia.br/reportagens/socinfo/info01.htm>. Acesso em 07 de outubro de 2006.

SOUZA, Luciano Amaro de. **Expansão do Direito Penal e Globalização.** São Paulo: Quartier Latin, 2007.

ZANELLATO, Marco Antonio. Brevíssimas Considerações sobre Delitos Informáticos. In ***Caderno Jurídico***. São Paulo: Escola Superior do Ministério Público de São Paulo: Imprensa Oficial do Estado de São Paulo. Ano 2, n. 4, jul/02, pp. 164/228.

Adolescente vai parar na delegacia por apologia ao tráfico no Orkut. **Folha de São Paulo online,** São Paulo, 20 de setembro de 2006. Disponível em: <http://www1.folha.uol.com.br/folha/informatica/ult124u20628.shtml>. Acesso em 08 de outubro de 2006.

Orkut retira dez páginas do ar por apologia ao crime. **Folha de São Paulo online,** São Paulo. Disponível em: <http://www1.folha.uol.com.br/folha/informatica/ult124u20669.shtml>. Acesso em 08 de outubro de 2006.

PF prende quadrilha que vendia remédios controlados pela internet. **Folha de São Paulo online,** São Paulo, 26 de julho de 2006. Disponível em: <http://www1.folha.uol.com.br/folha/cotidiano/ult95u124387.shtml>. Acesso em 08 de outubro de 2006.

PF prende 45 suspeitos de desvio de dinheiro pela web. **Folha de São Paulo online,** São Paulo, 23 de agosto de 2006. Disponível em: <http://www1.folha.uol.com.br/folha/informatica/ult124u20490.shtml>. Acesso em 08 de outubro de 2006.

Polícia Federal inicia operação para combater crimes na internet. **Folha de São Paulo online,** São Paulo, 12 de setembro de 2006. Disponível em: <http://www1.folha.uol.com.br/folha/informatica/ult124u20582.shtml>. Acesso em 08 de outubro de 2006.