

ALEXANDRE MAGALHÃES DE MATTOS

ADVOGADO, PÓS-GRADUADO EM DIREITO INTERNACIONAL PELA ESA-OAB/RJ, PÓS-GRADUADO EM DIREITO EMPRESARIAL PELA UNESA, PROFESSOR UNIVERSITÁRIO. PÓS-GRADUADO EM *DESKTOP PUBLISHING* PELA LM UNIVERSITY. PÓS-GRADUADO EM ANÁLISE DE SISTEMAS PELA PUC-RJ E ANALISTA DE SISTEMAS PELA FACULDADE NUNO LISBOA.

A LEI 84-D E AS ALTERAÇÕES NO CÓDIGO PENAL

SUMÁRIO

1. INTRODUÇÃO	3
2. HISTÓRICO	4
2.1 A evolução dos tipos penais nos crimes relacionados a informática	4
2.2 O nascimento da internet	5
2.3 O início das invasões de sistemas	6
3. DIREITO COMPARADO	7
3.1 A necessidade de se alterar a legislação pátria, o Código Penal.	9
3.2 Perigos vindos do Brasil.....	10
4. NOMENCLATURAS UTILIZADAS	11
4.1 Classificação dos crimes na área da informática	11
5. O PROJETO DE LEI 84-D	14
6. JURISPRUDÊNCIA	17
CONCLUSÃO	19
REFERÊNCIAS	19

1. INTRODUÇÃO

Esta monografia versa sobre a atual situação brasileira quanto aos crimes praticados na *internet* e o Projeto de Lei nº 84-D que altera o Código Penal, dispendo sobre os crimes cometidos na área de informática e suas penalidades.

Como o Brasil ainda não possui uma legislação específica sobre crimes na área de informática, não existe um código ou uma lei que puna, especificamente, crimes relacionados com fraudes, furtos, roubos ou pornografia através da *internet*, com isso, os operadores do direito utilizam-se do Código Penal Brasileiro, promulgado em 7 de dezembro de 1940 e que teve sua Parte Geral alterada em 11 de julho de 1984, ao Estatuto da Criança e do Adolescente, promulgado em 13 de julho de 1990, e a demais Leis existentes no ordenamento jurídico nacional.

Esta monografia constitui-se de uma pesquisa empírica e exploratória, pois analisa a atual legislação referente aos crimes cometidos na área de informática e, como a falta de uma legislação específica, causa lacunas jurídicas que não são puníveis atualmente. É parcialmente bibliográfica, ao buscar, em trabalhos e livros publicados, alguns dos conceitos que são utilizados no ordenamento jurídico vigente e também parcialmente explicativa, ao comentar as evoluções dos crimes na área da informática, quando compara a atual legislação com a legislação proposta.

Como se trata de um tema parcialmente inédito, a maioria das fontes foram pesquisadas na *internet*.

A principal fonte, o projeto de Lei 84-D, está disponível no Congresso Nacional, pois este se encontra na Comissão de Educação do senado, sendo apenas aguardado o encaminhamento para a sanção presidencial.

Buscou-se, para elaborar a monografia, com o estudo em bibliografias da área, o que é muito escasso pois, como dito, o tema é parcialmente inédito por isso as principais fontes são textos jurídicos acessados através da *internet* assim como palestras ministradas na área.

Foi feita uma apresentação histórica detalhada no primeiro capítulo visando explanar a evolução dos tipos penais nos crimes relacionados a informática no Brasil e no mundo assim como é descrito como ocorreu o nascimento da *internet* e o início das invasões de sistemas informatizados.

No segundo capítulo foi realizada uma pesquisa no ordenamento jurídico de outros países, pesquisa esta feita através de livros publicados e de acesso ao endereço eletrônico dos poderes legislativo e judiciário de outras nações. Neste capítulo também é feita uma explanação da necessidade de se alterar a legislação pátria, o Código Penal, assim como, ao final, é demonstrado através de reportagens os perigos vindos do Brasil pela falta de uma legislação específica.

O terceiro capítulo é dedicado a explanar as diversas nomenclaturas utilizadas por nossos operadores do direito a respeito dos crimes praticados na área da informática assim como também é feita a distinção quanto a classificação dos mesmos como próprios ou impróprios. Ao final do capítulo são trazidos alguns dos tipos penais que são utilizados em nosso ordenamento jurídico e que descrevem crimes na área de informática.

O quarto capítulo é dedicado a explanar o Projeto de Lei 84-D, sua criação, tramitação em nossas casas legislativas e a atual situação do mesmo. Algumas impressões de operadores do

direito a respeito do referido projeto são apresentados ao final do capítulo inclusive com relação a se sanar as atuais lacunas no ordenamento jurídico brasileiro.

No quinto capítulo são apresentados alguns julgados de alguns dos tribunais superiores brasileiros visando demonstrar a atualidade e pertinência do tema proposto nesta monografia.

2. HISTÓRICO

2.1 A evolução dos tipos penais nos crimes relacionados a informática

Até meados da década de 1970, os sistemas de informações se baseavam em grandes centros computacionais compostos por equipamentos que ocupavam uma grande área física, cujo valor de aquisição era praticamente impossível para um usuário doméstico. Apenas grandes corporações e órgãos governamentais tinham recursos monetários suficientes para adquirir e manter uma rede de computadores apta a realizar seus processamentos de dados.

Frise-se que era muito custoso e complexo a transmissão de dados entre locais distintos de uma mesma corporação. Nesta época, por exemplo, como o departamento de contabilidade de uma empresa não possuía computadores em cima de mesas nem os funcionários desse departamento tinham o conhecimento necessário para operar tais equipamentos, os dados que deveriam ser processados eram enviados ao Centro de Processamento de Dados da empresa, (CPD). No CPD, estes dados eram manipulados pelos digitadores e, após a digitação dessa massa de dados, os programadores e os analistas de sistemas eram os responsáveis por transformar, através de programas em linguagem de computador, aquelas informações em relatórios que seriam utilizados pelo departamento em questão.

A primeira arquitetura de redes de computadores comerciais do mercado a permitir a transmissão de dados para o meio externo, ou seja, para fora das corporações, foi a SNA, *System Networking Architecture* (Sistema de Arquitetura de Redes). Até essa época, a questão de segurança da informação se baseava apenas no furto ou roubo físico de componentes de um CPD. Os terminais de dados, onde se introduziam as informações dessa época, eram terminais escravos, ou seja, não havia periféricos como unidades de disquetes ou de CD-ROM, nos quais se pudesse utilizar uma mídia para copiar os dados que eram processados no computador central. Outra forma de se introduzir os dados em um sistema computacional era através de cartões perfurados utilizando-se uma máquina semelhante a uma máquina de escrever que perfurava em um cartão de papel a informação que se desejava que fosse inserida em um computador. Também era possível introduzir os dados nos computadores através de fitas ou discos magnéticos, já pré-gravados em outro sistema computacional. Após serem enviados aos computadores, esses dados podiam ser armazenados em unidades de fita, parecidas com as antigas fitas de rolo de música.

Até o advento da arquitetura SNA havia a certeza de que ninguém poderia invadir os sistemas de dados, pois esses só eram acessados pelos funcionários da empresa, assim sendo, esses dados estavam a salvo das cópias não autorizadas. A segurança se baseava na proteção do equipamento, pois apenas danos físicos ao *hardware* (equipamento), poderiam comprometer a funcionalidade e a segurança dos sistemas.

Portanto, até há pouco mais de duas décadas bastava um cadeado, correntes reforçadas no portão, vigias diurnos e noturnos ou um cão feroz para manter as informações de uma empresa protegidas contra intrusos.

Mesmo assim, essas informações só poderiam ser roubadas ou furtadas se fossem obtidas através de relatórios impressos ou se fossem gravadas em fitas magnéticas, ou seja, o furto ou o roubo das informações só poderia se realizar caso o pretendente a criminoso se prontificasse a carregar, literalmente, em baixo dos braços, o produto de sua ação criminosa.

Com o início da transmissão de dados através de linhas telefônicas comuns utilizando-se um equipamento chamado *modem*, iniciou-se uma nova era na questão da segurança dos dados. Sendo assim as grandes corporações da época preocupavam-se apenas em manter a integridade da transmissão das informações pelas linhas telefônicas, que eram analógicas, para que fossem transmitidos de uma localidade a outra sem erros. Como os equipamentos da época custavam alguns milhares de dólares, era praticamente impossível se ter um sistema computacional em uma residência e, assim sendo, apenas grandes corporações, empresas públicas civis e militares, eram capazes de possuir equipamentos computacionais e a invasão em sistemas de dados computacionais era assunto apenas para filmes de ficção científica ou de espionagem no mais clássico estilo da guerra fria entre as potências comunistas e capitalistas.

2.2 O nascimento da *internet*

De acordo com a UNESCO, a *internet*, ou ciberespaço, é um novo ambiente tecnológico humano que permite diversas formas de expressão de idéias, informações e transações econômicas. Ela é constituída por dois elementos: o primeiro seria o de pessoas de todos os países com suas diversas culturas e línguas, em suas várias idades e ocupações profissionais distintas que a alimenta com informações e, o segundo, seria uma rede global de computadores interconectados por infraestruturas de telecomunicação possibilitando o abastecimento de informações processadas e transmitidas digitalmente. Essas informações disponíveis na *internet* circulam de uma forma anônima e não regulamentada, ignorando fronteiras nacionais e, na maioria das vezes, escapando de legislações e jurisdições nacionais.

Pode-se dizer que, o que hoje é conhecido como *internet*, se originou na *Advanced Research Project Agency* (ARPA), uma agência do *Department Of Defense* (DOD), do governo dos Estados Unidos, na década de 60 quando se faziam pesquisas e experimentos a procura de uma solução capaz de implementar a interoperabilidade entre diferentes fabricantes de computadores. Deste trabalho surgiu a rede ARPANET que se tornou operacional em 1969 e a sua expansão ficou conhecida como *internet*. A *Defense Advanced Research Project Agency* (DARPA) sucedeu a ARPA em 1971 e assumiu o controle da ARPANET.

Sabe-se que as universidades norte americanas são famosas por suas pesquisas e pelo incentivo que a iniciativa pública e a privada dão a essas instituições de ensino para criarem e desenvolverem projetos e soluções com viabilidade comercial. Assim sendo, em 1975 quase todos os centros de pesquisas das mais importantes universidades dos EUA já estavam interligados através de uma grande rede de computadores, favorecendo assim a troca de informações entre os mais diversos centros de pesquisas dessas instituições de ensino, destacando-se pela costa leste as universidades de Harvard, Massachusetts, Illinois e Lincoln. Pela costa oeste as universidades de UCLA e Stanford e no meio oeste americano a universidade de Utah. Assim como as universidades, também estavam conectados a essa rede os centros de pesquisas das duas maiores empresas de informática da época, a IBM e a Burroughs, todos eles pesquisando e desenvolvendo em conjunto o que passou a se chamar de *internet*.

Essa *internet* ficou conhecida como *intenet 1* e foi, na realidade, idealizada como uma arma de guerra para ser utilizada durante um conflito nuclear. Ela era uma via de informações que possibilitaria que, se uma cidade fosse destruída e fosse necessária a reconstrução de uma fábrica ou de uma companhia telefônica os engenheiros, arquitetos, físicos e demais profissionais envolvidos nessas construções não precisariam se deslocar até o local da construção para fazer os projetos e cálculos necessários para tais construções, tudo isso seria feito através dos diversos centros de pesquisas espalhados nos EUA.

Um clássico exemplo disso é o caso dos atentados de 11 de setembro nos EUA. Provavelmente, os responsáveis pelos atentados imaginaram que danificando ao máximo as Torres Gêmeas o sistema financeiro norte-americano entraria em colapso pois lá se localizava a sede do *CitiGroup*, as principais corretoras de valores que atuam nas bolsas de valores do mundo e inúmeras empresas ligadas a esse setor. Ao contrário do que se imaginava, essas empresas não se abalaram muito pois,

através da *internet*, a maioria de seus dados estavam armazenados a salvo em outros locais e isso possibilitou que essas empresas continuassem atuando ininterruptamente.

Com o advento dos computadores domésticos, no final da década de 1970 e início da década de 1980, computadores esses que eram vulgarmente chamados de micros, e a possibilidade de transmissão de dados também por linhas telefônicas, iniciou-se um período de ataques e invasões indiscriminadas aos sistemas computacionais. A indústria cinematográfica norte-americana ilustrou essa preocupação com filmes como *War Games*, no qual um jovem acessou acidentalmente o computador de guerra do sistema de defesa norte-americano. Este jovem costumava ajudar os demais alunos de sua escola secundária alterando suas notas de provas através de seu microcomputador conseguindo a aprovação de todos no final do curso. Na maioria desses casos, sempre se retratava a figura de um invasor de sistemas computacionais sigilosos com a de um jovem adolescente com espinhas no rosto.

2.3 O início das invasões de sistemas

Um dos primeiros registros de invasão de sistemas de dados ocorreu em 1983 quando um adolescente de Nova Iorque, fazendo-se passar por um cliente da indústria de refrigerantes PEPSI, acessou os computadores dessa empresa através de seu microcomputador caseiro e fez com que 2 caminhões carregados de refrigerantes fossem fazer a entrega de um pedido de compra em um bar inexistente no meio do deserto de *Mojade*.

Atualmente, uma das maiores preocupações das empresas está nos alardeados vírus de computadores, capazes de inutilizar equipamentos e sistemas por inteiro. Uma observação deve ser feita a respeito deste tópico específico. Existem três tipos de arquivos indesejados que podem danificar um equipamento, são eles, Vírus, Cavalo-de-Tróia e Verme, mas acabam todos sendo chamados pelos leigos como vírus.

Um vírus de computador é um pequeno programa que se auto-insere dentro de um programa benigno, ali permanecendo até que seja disparado, em uma data específica, causando danos e falhas no equipamento. Alguns dos mais conhecidos são: o Sexta-feira 13, que ocorre sempre quando há no calendário a ocorrência do dia 13 em uma sexta-feira, e o Michelangelo, que tem o seu código ativado no dia do aniversário deste mestre renascentista, dia 6 de março. O que caracteriza um vírus de computador é o fato desse pequeno programa ao ser ativado causar uma falha geral no sistema como, por exemplo, apagando todos os dados armazenados no computador.

Um Cavalo de Tróia é um programa que parece ter alguma função real, tal qual um jogo ou utilitário, entretanto ele está, na verdade, executando outra função sem que o usuário perceba. Após algum período de atividade o Cavalo de Tróia pode enviar informações que coleta no sistema para fora do equipamento usando o *e-mail*, correio eletrônico, do proprietário do computador. Diferentemente dos vírus, o Cavalo de Tróia procura informações específicas.

Finalmente, mas não tão menos devastador, há o verme, que é muito parecido com um vírus, porém não causa danos específicos aos sistemas de computador. Eles geralmente causam processamentos ininterruptos, congelamento das funções do computador, páginas impressas a mais no final de um relatório ou o envio de *e-mail* para endereços errados ou não desejados.

Conforme se percebe, com o passar dos anos, o crime na área da informática evoluiu de um simples furto ou roubo de um equipamento, *hardware*, ou de informações sigilosas impressas em formulários contínuos, no qual o delinqüente tinha que, necessariamente estar no local onde desejava atuar, para crimes mais sofisticados, praticados virtualmente, sendo que o sujeito ativo não necessita mais estar fisicamente no local de atuação da sua prática delituosa para consumir o fato.

Um dos crimes mais comuns cometidos atualmente nos ambientes das redes de computadores ocorre quando do recebimento de mensagens não solicitadas, os chamados *spams*. Atualmente

esses *spams* vem adicionados de programas anexados à própria mensagem de *e-mail*. Uma vez abertos esses arquivos anexos, eles instalam programas espíões no computador do destinatário da mensagem, do tipo cavalo de tróia (*spyware*), que permite que o agente criminoso tenha acesso remoto a todo o sistema do computador atacado. Um tipo específico desses programas espíões, o *keylogger*, tem capacidade para registrar qualquer tecla pressionada pelo usuário do computador infectado, bem como alguns movimentos do mouse, e enviar esses dados (por e-mail) para o agente criminoso que opera um computador remoto, tudo sem o conhecimento da vítima. Esse tipo de programa permite capturar informações críticas, como senhas e números de contas bancárias.

Um tipo de estelionato eletrônico que teve um incremento muito grande no ano de 2003, e começo deste, foi o conhecido como *phishing scam*. Nesse tipo de fraude os e-mails têm na indicação da origem um remetente aparentemente confiável, a exemplo de uma instituição bancária, um órgão do governo, uma administradora de cartão de crédito ou um conhecido *site* de comércio eletrônico. A mensagem falsa contém uma solicitação de informações pessoais ou um atalho (*link*) para um endereço falso onde deve ser preenchido um formulário. No *site* falso, a pessoa é solicitada a fornecer número do cartão de crédito, dados de contas bancárias e números de documento de identidade, entre outros. De posse desses dados, os estelionatários (*phreakers*) transferem os recursos das vítimas para suas próprias contas.

Com relação ao sujeito ativo dos verbos do tipo utilizado para classificar as práticas delituosas na área da informática, muito se fala na figura do *hacker*, mas uma explicação deve ser dada a respeito do tema. Os *hackers* são os sujeitos que invadem sistemas computacionais, mas não roubam informações nem danificam os computadores. Para eles basta o desafio técnico de superar as ferramentas de segurança de um sistema. Alguns são chamados de *hackers* éticos pois, depois que superam as barreiras encontradas, deixam um alerta para o administrador do sistema computacional poder consertar a falha de segurança, esses alertas são geralmente acompanhados do endereço eletrônico do *hacker*, o *e-mail*, para que o administrador possa localizá-lo. Outro sujeito é o *lamer* que é um pretense *hacker*, mas sem conhecimento técnico para superar as defesas das redes. Ele perde muito tempo tentando acessar um sistema computacional, sempre sem sucesso. Há também os *crackers* que, por suas vez, são aqueles que invadem e danificam os sistemas que encontram ou realizam atos considerados ilegais, como roubar senhas e informações sigilosas. Mais perigosos ainda há os *phreakers* que são considerados os grandes criminosos virtuais, pois roubam senhas de cartões de crédito, senhas bancária para fraudarem contas bancárias fazendo transferências para contas de terceiros. Finalmente, temos a figura dos *trackers*, que formam a polícia da *internet* e que tem no CERT/CC a sua base operacional.

3. DIREITO COMPARADO

Por ser a informática uma ciência exata, que muda conceitos e valores de forma rápida, alguns países já verificaram a necessidade de se possuir uma legislação específica para combater os crimes que ocorrem nesta área. Esses países inseriram em seus diplomas legais modificações a fim de disciplinar e combater as novas modalidades delitivas que surgiram com o advento do acesso a *internet*.

Escreve René David sobre direito comparado:

O Direito Comparado desempenha um papel parecido ao da história. Ao estudioso de um direito nacional proporciona a perspectiva necessária para perceber adequadamente as linhas mestras deste direito. Coloca em relevo o caráter contingente, acidental, de certas normas ou instituições... significa ao mesmo tempo sair do 'ghetto' jurídico nacional e compreender as ordens jurídicas internacionais.

Em Portugal, no ano de 1991, foi publicada a Lei n° 109, que dispõe sobre a criminalidade na área da informática. O Código Penal Português, Decreto-lei n° 48/95 passou a prever dois tipos penais relacionados à informática sendo o primeiro deles inserido no capítulo reservado aos

crimes contra a reserva da vida referindo-se especificamente a devassa por meio da informática. O segundo delito foi incluído no capítulo destinado aos crimes contra o patrimônio em geral dispondo sobre a fraude através da informática e das comunicações.

Na Itália, o Código Penal Italiano sofreu alterações através da Lei nº 547 de 1993 que acrescentou quinze preceitos incriminadores referentes a crimes praticados na área da informática, contando com algumas figuras essenciais como a sabotagem, o acesso ilegal, a violação de segredo e do sigilo de dados, a falsificação e a fraude e violação dos direitos do autor que desenvolve programas de computador. O envio de vírus também é previsto na legislação italiana, punindo-se a conduta do agente que os difunde. Também a conduta dos *crackers* e dos *phreakers* é disciplinada no crime de acesso ilegal a sistemas de informática ou de telecomunicações.

Nos Estados Unidos a Lei 18 U.S.C., de 1998, disciplina a fraude e as atividades relacionadas a computadores prevendo penas de multa e de prisão, tutela as comunicações de dados tipificando como crime a conduta de quem as intercepta ou revela, tipifica o acesso ilícito de comunicações e dados armazenados, e tipifica a exploração infantil através da *internet* punindo essas condutas com pena de multa e prisão, que podem variar de cinco a quinze anos de detenção.

Na Inglaterra, o *Computer Misuse Act*, de 1990, disciplinou várias condutas criminosas ligadas à informática como a obtenção de acesso não autorizado a sistemas de informação e permitiu o rastreamento do tráfico de informações na *internet* pelos serviços de segurança do país.

No Canadá considera-se o acesso não autorizado, os danos a dados, o furto de telecomunicações, a violação de direito de programas de computador e a fraude através de cartão de crédito como crimes puníveis no âmbito da *internet*. Com diversas leis versando sobre esse tema, sendo a mais atual datando de 2001 e com a *Fact Sheet No. 14* tipificando todas as condutas possíveis, verifica-se que através dos dispositivos de lei números 342.1, 430 e 326 que os crimes nessa área podem ser punidos pela RCMP, *Royal Canadian Mounted Police* (Real Polícia Montada Canadense), com penas de multa e de até 10 anos de prisão.

Na Áustria, com a lei de reforma do Código Penal, de 22 de dezembro de 1987, passou-se a se prever os delitos de destruição de dados, Artigo 126 e a fraude eletrônica, Artigo 148.

Na França a Lei nº 88-19 de 05 de janeiro de 1988 dispõe sobre o acesso fraudulento a sistema de elaboração de dados, Artigo 462-2; sabotagem, Artigo 462-3; destruição de dados, Artigo 462-4; falsificação de documentos eletrônicos, Artigo 462-5 e uso de documentos informatizados falsos, Artigo 462-6.

Na Alemanha a lei federal IuKDG, *Informations- und Kommunikationsdienste-Gesetz*, de 1997 disciplinou o uso dos serviços de comunicações, instituiu a fraude contra os serviços de armazenamento de dados e assinatura digital, puniu a transmissão de material pornográfico por meio da *internet*, através de seus oito artigos e parágrafos. As punições previstas vão de pagamentos de multas a até prisão sem direito a fiança.

Percebe-se que a Alemanha é um dos países que introduziu há mais tempo algum tipo de mudança em sua legislação penal. Essa característica de se estar a frente das mudanças no mundo jurídico, leva a um curioso fato histórico. No final do século XIX, um cidadão alemão foi preso acusado de furto de energia elétrica. Os advogados do acusado, entretanto, observaram que não existia na legislação penal alemã tal delito, pois a energia elétrica não tinha *status* de coisa, e somente coisa poderia ser passível de furto. O tribunal, acatando o princípio “*nulla poena nullum crimen sine legge*” absolveu o réu ao entender que a lei penal não permite interpretação análoga. Com isso, o legislador alemão providenciou logo um dispositivo legal que tipificasse como crime o furto de energia elétrica, pois sem a mesma, aqueles que viessem a desviar a energia elétrica ficariam impunes.

3.1 A necessidade de se alterar a legislação pátria, o Código Penal.

A sociedade brasileira vive um período no qual as facilidades e avanços tecnológicos, que surgiram com o advento do computador, são irreversíveis. Juntamente com esses avanços tem-se, também, o surgimento de novos tipos e situações penais até então não tipificados nos códigos e legislações.

Essa lacuna jurídica faz crescer na sociedade um sentimento de impunidade com relação aos chamados criminosos da *internet*. Por não se ter uma legislação específica sobre crimes na área da informática, tem-se observado um aumento desse tipo de prática delituosa, podendo afetar o cidadão não só em seu aspecto econômico-financeiro como também sua incolumidade física, seus bens patrimoniais, suas informações profissionais e pessoais armazenados em bancos de dados de empresas públicas e privadas. Frise-se também o fato de ainda não possuímos uma legislação específica sobre crimes na área de informática, não existe um código ou uma lei que puna, especificamente, crimes relacionados com fraudes, furtos, roubos ou pornografia através da *internet*, com isso, os operadores do direito utilizam-se do Código Penal Brasileiro, promulgado em 7 de dezembro de 1940 e que teve sua Parte Geral alterada em 11 de julho de 1984, do Estatuto da Criança e do Adolescente, promulgado em 13 de julho de 1990, e a demais leis existentes no ordenamento jurídico nacional.

Sabe-se que em dezembro de 2003, a imprensa nacional noticiou que a justiça brasileira havia condenado o primeiro brasileiro por crimes na *internet*, Guilherme Amorim de Oliveira Alves, de 19 anos, que fora sentenciado a passar 6 anos e 4 meses na prisão por invadir, entre outros *sites*, as páginas dos quatro maiores bancos do País – Caixa Econômica Federal, Banco do Brasil, Itaú e Bradesco – Processo 001.03.101766 no TJMS. Também neste caso, como nos demais ocorridos, o acusado foi apenado pelo Artigo 18 da Lei 7.492/92 que versa sobre crimes contra o sistema financeiro e não por um crime cometido pela *internet*.

Já o Jornal da Globo de 13 de setembro de 2004 noticiou que:

Uma pesquisa revela que oito em cada dez *crackers* são brasileiros.

Americanos estão com a atenção voltada para o crime virtual no Brasil, é que aqui moram pelo menos quatro pessoas que invadiram o site do Exército americano em novembro do ano passado.

Os *crackers* – internautas que invadem sites com a intenção de causar algum dano – destruíram informações do banco de dados das Forças Armadas. O governo americano investigou o caso e mandou as evidências para a Polícia Federal que agora cuida do caso.

O anonimato da rede mundial de computadores facilita a ação de criminosos. Só no ano passado, a Polícia Federal brasileira investigou quase seiscentos crimes cometidos pela *internet*. A expectativa é que esse número suba para mil este ano. Segundo especialistas, as fraudes financeiras que utilizam a rede já causam mais prejuízos no Brasil do que assaltos a bancos, como informa o delegado federal Paulo Quintiliano. “A falta de uma legislação realmente dificulta em alguns casos o trabalho da polícia”.

A pedofilia lidera os crimes cometidos pela *internet*. Dois terços dos casos descobertos pela polícia são páginas de exploração sexual infantil.

Atualmente, manipular dados sem permissão, obter acesso indevido ao meio eletrônico ou sistema informatizado, introduzir vírus em computadores, clonar telefones celulares, falsificar cartão de crédito são atos criminosos, só que ainda não há lei brasileira que os considere como tais.

As alterações propostas na legislação penal são necessárias pois, de acordo com os institutos IBOPE e *NetRatings*, dados referentes a setembro/2003, o brasileiro é um dos povos que mais se utiliza dos serviços bancários *on-line* e, conseqüentemente, passam muito tempo nos *sites* das instituições financeiras. Esses dois institutos verificaram que quarenta e sete por cento dos internautas domiciliares brasileiros utilizam sites financeiros, número superior ao Reino Unido com quarenta e seis vírgula oito por cento, EUA com quarenta e dois vírgula quatro por cento, Espanha com trinta e nove vírgula seis por cento e Itália com vinte e seis vírgula sete por cento.

O índice de utilização de serviços bancários pela *internet* por brasileiros é inferior apenas ao índice da França, com cinquenta e três vírgula oito por cento. Há de se frisar que países como EUA, Inglaterra e França já possuem em seus ordenamentos jurídicos sanções específicas contra crimes nessa área.

Os mesmos institutos também verificaram que o tempo utilizado pelos brasileiros em conexões financeiras pela *internet*, o chamado tempo *on-line* médio, em *sites* financeiros é de uma hora e um minuto, superando todos os outros países citados, como a França com cinquenta e seis minutos e os EUA com cinquenta e cinco minutos.

Ademais, uma vez sancionada a Lei 84-D/99, o Brasil será um dos poucos países do mundo a possuir uma legislação adequada para incriminar tais condutas do gênero. A atual ausência de uma lei específica serve de estímulo para que os crimes nessa área continuem. Com as alterações aprovadas, os criminosos eletrônicos deverão migrar para outros países que não tenham legislação específica e, segundo estudos realizados pelo advogado e deputado Luiz Piauhyllino (PTB-PE) a ocorrência de crimes digitais poderá diminuir em torno de cinquenta por cento no Brasil. Também com essa aprovação, as penas previstas para os delitos irão variar de um mês a cinco anos de detenção e, dependendo do caso, os agravantes poderão em muito desestimular tais práticas delitivas.

3.2 Perigos vindos do Brasil

Segundo a empresa IDC Brasil, a quantidade de fraudes que ocorrem no Brasil são alarmantes. De um universo de 290 pequenas e médias empresas, quase sessenta por cento mencionaram a ocorrência de vírus em seus servidores nos últimos doze meses. Ainda de acordo com a pesquisa realizada por essa empresa, os incidentes de segurança no Brasil cresceram setenta e um por cento apenas no primeiro semestre de 2004. Em 2003 havia crescido cento e dezessete por cento em relação a 2002.

O tipo de ocorrência que mais cresceu, percentualmente, foi a fraude, que aumentou oitocentos e cinquenta e seis por cento no primeiro semestre de 2004 passando de 142 fraudes nos primeiros seis meses de 2003 para 1358 até outubro de 2004.

Ainda de acordo com mesma pesquisa, os vírus ainda são as maiores ameaças aos computadores. Foram notificados 16,4 mil vírus, o que representa um aumento de mais de cinquenta por cento com relação a 2003. Em segundo lugar estão os Cavalos de Tróia que tiveram 16,1 mil incidentes reportados, um aumento de cento e trinta e seis por cento em relação ao mesmo período de 2003. O número das mensagens eletrônicas indesejadas, os *spams*, aumentou cinquenta e dois por cento, passando de 261,5 mil para 399,4 mil.

Outra empresa do setor de segurança de redes de computadores, a norte-americana Pest Patrol, identificou até julho de 2004 cerca de 22,7 mil programas que roubam informações pessoais e alteram as configurações dos programas de navegação na *internet*, os *browsers*. Ainda de acordo com esta empresa, a gigante do setor, a Microsoft, revelou que um único vírus, o MSBlast, infectou mais de 9,5 milhões de computadores no mundo, no período compreendido entre os meses de setembro de 2003 e setembro de 2004.

Em 1999, um vírus de computador demorava 12 horas para infectar até 10 mil computadores na *internet*. No caso do vírus *Slammer*, de 2002, foi necessário apenas uma hora para infectar a mesma quantidade de equipamentos.

Atualmente estima-se que, 4 horas seja o tempo necessário para um *e-mail* percorrer toda a grande rede de computadores, a *internet*. Ou seja, em 4 horas é possível se “bater à porta” de todas as caixas postais, de todos os usuários no mundo. Esse cálculo foi explorado no filme O Exterminador do Futuro partes II e III, quando o andróide T2, interpretado pelo ator Arnold Schwarzenegger, comenta que, após a informação de “destruir os humanos” é inserida na *skynet*

(rede militar americana no filme), 4 horas é o tempo que demora para que todos os sistemas de computadores militares do mundo entrem em colapso e passem a considerar os humanos seus alvos primários.

Finalmente, segundo a empresa londrina de consultoria em risco digital, a mi2g Intelligence Unit, de um total de 125 mil ataques a computadores em todo o mundo, o Brasil é o responsável por 95,5 mil deles, ou seja, setenta e seis vírgula dois por cento. Em seguida vem a Turquia, com 14,7 mil ataques, ou seja, onze vírgula oito por cento. Também, de acordo com relatórios da mesma empresa, os invasores brasileiros se especializaram nos mais diversos crimes virtuais que vão desde roubo de dados e identidade, a fraudes com cartão de crédito, pirataria e vandalismo on-line, já que o Brasil não possui uma legislação com punições específicas para esses tipos de delitos.

4. NOMENCLATURAS UTILIZADAS

Com o passar dos anos e, pela falta de uma padronização, diversas nomenclaturas foram e são utilizadas para qualificar o tema. Dentre elas pode-se encontrar Crimes de Computador, Crimes via *Internet*, Crime Informático, Delitos Praticados por Meio da *Internet*, Crime praticado por meio da informática, Crimes Tecnológicos, Crimes na *Internet* e Crimes Digitais. De todas as nomenclaturas apresentadas a que mais se aproxima do tema é Crimes de Informática visto que engloba todo o sistema da informática e não apenas a *internet*. Assim, os crimes praticados através da *internet* são espécie dos crimes de informática, ficando este com uma abrangência maior. Assim sendo, 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 os perpetrados através do computador. Inclui-se então neste conceito os delitos praticados através da *internet*, pois o pressuposto para acessar a rede de computadores que compõe a *internet* é a utilização de um computador.

Da mesma forma que ainda não há um consenso no ordenamento jurídico pátrio sobre a nomenclatura a ser utilizada para esses tipos de delitos, também o conceito de crime de informática não possui ainda um consenso. Para Ferreira, crime de informática é toda ação típica, antijurídica e culpável contra ou pela utilização de processamento de dados ou sua transmissão.

O professor Araujo Junior conceitua como sendo uma conduta lesiva, dolosa, a qual não precisa, necessariamente, corresponder à obtenção de uma vantagem ilícita, porém praticada sempre com a utilização de dispositivos habitualmente empregados nas atividades de informática.

Diferentemente, para Rodrigues da Costa, é todo aquele procedimento que atenta contra os dados, que o faz na forma em que estejam armazenados, compilados, transmissíveis ou em transmissão, pressupondo assim dois elementos o *software*, programa, e o *hardware*, equipamento.

Já Correia entende que são crimes relacionados às informações arquivadas ou em trânsito por computador, sendo esses dados acessados ilicitamente e usados para ameaçar ou fraudar com a utilização de um meio eletrônico.

Finalmente Bittencourt Brasil salienta que não há diferença no conceito de crime comum e crime de informática e o que os separa é a utilização do computador para alcançar e manipular o seu sistema em proveito próprio ou para lesionar alguém.

4.1 Classificação dos crimes na área da informática

Na doutrina brasileira, tem-se asseverado que os crimes na área de informática podem ser próprios ou impróprios. Os próprios são aqueles que só podem ser praticados através da informática e surgiram com a evolução dos sistemas computacionais e a facilidade e disponibilidade que passaram a ter com o passar do tempo. São tipos penais novos e escassos de legislação o que os

tornam atípicos e de difícil punição como, por exemplo, a violação de e-mail, o vandalismo ou alteração de informações em *homepages*, o dano em arquivos ou sistemas computacionais causados pelo envio de vírus e etc. No dizer de Damásio, aqueles que sejam praticados por computador e se realizem ou se consumem também em meio eletrônico. Neles, a informática (segurança dos sistemas, titularidade das informações e integridade dos dados, da máquina e periféricos) é o objeto jurídico tutelado.

Já os crimes impróprios na área da informática são aqueles que podem ser praticados de qualquer forma, sendo que o sujeito ativo utiliza eventualmente o sistema computacional, ou seja, o computador é um meio, um instrumento para a execução do crime. Nisto estariam inclusos os delitos que violam os bens jurídicos já protegidos em nosso ordenamento tais como o patrimônio e a honra.

Ferreira divide os crimes de informática em duas categorias: na primeira os atos são dirigidos contra o sistema de informática, divididos em atos contra o computador e atos contra os dados ou programas de computador. Na Segunda categoria estão os atos cometidos por intermédio do sistema de informática que podem ser contra o patrimônio, conta a liberdade individual e contra a propriedade imaterial.

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

Muñoz Conde ensina que:

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

Como exemplo, pode-se afirmar que o crime de homicídio praticado por meio do computador (delito impróprio), deverá ser punido nos mesmos moldes do Artigo 121 do Código Penal. A proposição é de Damásio e, embora de difícil consumação nos dias atuais, não é hipótese de todo inverossímil num futuro próximo. Trata-se de caso em que um habilidoso *cracker* invade a rede de computadores de um hospital altamente informatizado, mudando as prescrições médicas relativas a um determinado paciente, substituindo drogas curativas por substâncias letais ao organismo deste ou alterando as dosagens do medicamento prescrito pelo médico, com o fim deliberado de produzir efeito letal. Ao acessar o terminal de computadores, um enfermeiro não percebe a alteração indevida e, inadvertidamente, administra o medicamento em via intravenosa, provocando a morte do paciente. Incidirá, nesta hipótese, o Código Penal e o processo será de competência do tribunal do júri da comarca onde se situar o hospital, aplicando-se nesse aspecto a teoria da atividade.

De igual modo, aplica-se o tipo do Artigo 155, § 4º, inciso II, do Código Penal (furto qualificado pela destreza) ao *cracker* que, violando o sistema de senhas e de segurança digital de um banco comercial, conseguir penetrar na rede de computadores da instituição financeira, dali desviando para a sua conta uma determinada quantia em dinheiro.

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

Algumas premissas legais e doutrinárias tradicionais não permitem a aplicação da legislação penal em condutas delituosas cometidas através de um computador. O argumento mais aceito é baseado no princípio da reserva legal, Artigo 1º do Código de Processo Penal e Artigo 5º, XXXIX da Constituição Federal, que obriga que a legislação tipifique determinado fato como criminoso, uma vez que, sem lei, não há crime.

É clássica, nesse sentido, a referência à conduta do agente que, valendo-se de um microcomputador, obtém acesso à máquina da vítima e ali introduz, por transferência de arquivos, um vírus de computador, que acaba por provocar travamento dos programas instalados no aparelho atingido.

Sabe-se que o crime de dano, previsto no Artigo 163 do Código Penal, consuma-se quando se dá a destruição, a deterioração ou a inutilização de coisa alheia. Mas, um programa de computador, um *software*, não é e nem deve ser considerado como coisa.

Ou, por outra, figure-se como exemplo um indivíduo que invade um sistema e copia um programa de computador. Sabe-se que um *software* tem um valor econômico. Mas não pode ser considerado como *res furtiva*, para enquadrar-se como objeto de crime patrimonial, já que a simples cópia do programa não retira a coisa da esfera de disponibilidade da vítima.

Em qualquer dos casos, para a adequação típica será necessário, certamente, um esforço interpretativo e pode-se objetar com o argumento de que não se admite analogia em Direito Penal, levando à conclusão de que esses fatos seriam atípicos.

Alguns tipos penais, que descrevem crimes na área de informática, já existem e, como exemplo pode-se citar:

- a) o Artigo 10 da Lei Federal nº 9.296/96, que considera crime, punível com reclusão de 2 a 4 anos e multa, “realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo de Justiça, sem autorização judicial ou com objetivos não autorizados em lei” .;
- b) o Artigo 153, §1º-A, do Código Penal, com a redação dada pela Lei Federal nº 9.983/2000, que tipifica o crime de divulgação de segredo: “Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública”, punindo-o com detenção de 1 a 4 anos, e multa;
- c) o Artigo 313-A, do Código Penal, introduzido pela Lei nº 9.983/2000, que tipificou o crime de inserção de dados falsos em sistema de informações, com a seguinte redação: “Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano”, punindo-o com pena de reclusão, de 2 (dois) a 12 (doze) anos, e multa;
- d) o Artigo 313-B, do Código Penal, introduzido pela Lei nº 9.983/2000, que tipificou o crime de modificação ou alteração não autorizada de sistema de informações, com a seguinte redação: “Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente”, cominando-lhe pena de detenção, de 3 (três) meses a 2 (dois) anos, e multa;
- e) o Artigo 325, §1º, incisos I e II, introduzidos pela Lei nº 9.983/2000, tipificando novas formas de violação de sigilo funcional, nas condutas de quem “I – permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública” e de quem “II – se utiliza, indevidamente, do acesso restrito”, ambos sancionados com penas de detenção de 6 meses a 2 anos, ou multa;
- f) o Artigo 12, *caput*, §§1º e 2º, da Lei Federal nº 9609/88, que tipifica o crime de violação de direitos de autor de programa de computador, punindo-o com detenção de 6 meses a 2 anos, ou multa; ou com pena de reclusão de 1 a 4 anos e multa, se o agente visa ao lucro;
- g) o Artigo 2º, inciso V, da Lei Federal nº 8.137/90, que considera crime “utilizar ou divulgar programa de processamento de dados que permita ao sujeito passivo da obrigação tributária possuir informação contábil diversa daquela que é, por lei, fornecida à Fazenda Pública”; e
- h) o Artigo 72 da Lei nº 9.504/97, que cuida de três tipos penais eletrônicos de natureza eleitoral.

Art. 72. Constituem crimes, puníveis com reclusão, de cinco a dez anos.

I — obter acesso a sistema de tratamento automático de dados usado pelo serviço eleitoral, a fim de alterar a apuração ou a contagem de votos;

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

A professora Ferreira, no capítulo *A criminalidade informática*, do livro *Direito e Internet – Aspectos Jurídicos Relevantes* de Newton De Lucca diz que:

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

Portanto, entende-se que tais tipificações esparsas não resolvem o problema da criminalidade na *internet*, do ponto de vista do direito objetivo mas, na realidade, revelam a preocupação do legislador infraconstitucional de proteger os bens relacionados a informática e de assegurar, na esfera penal, a proteção a dados de interesse da Administração Pública e do Estado democrático, bem como a privacidade do indivíduo no âmbito da *internet*.

5. O PROJETO DE LEI 84-D

Em 24 de fevereiro de 1999, o deputado federal Luiz Piauhyllino (PTB-PE), apresentou um projeto de lei chamado de PL-84/1999 que dispunha sobre os crimes cometidos na área de informática. Este foi aprovado em sua respectiva casa e recebeu parecer favorável da CCTCI (Comissão de Ciência e Tecnologia, Comunicação e Informática), da CCJC (Comissão de Constituição e Justiça e de Cidadania) e da CSPCCO (Comissão de Segurança Pública e Combate ao Crime Organizado) sendo encaminhado ao Senado Federal em 12 de novembro de 2003. Nesta casa o projeto recebeu a designação de PLC 89/2003, recebeu parecer e emendas do Senador Marcelo Crivela, tendo sido aprovado em 24 de agosto de 2004 pela CE (Comissão de Educação) aguardando a pauta para ser encaminhado a sanção presidencial.

As alterações propostas no Código Penal por este projeto de lei visam resguardar os bens jurídicos que ainda não possuem uma proteção efetiva no ordenamento jurídico vigente, tais como o acesso indevido ou sem autorização a sistemas informatizados, informações ou base de dados armazenados em meio eletrônico, a criação e difusão de vírus eletrônico, a pornografia infantil na *internet*, a interrupção de transmissão de dados entre outros.

Dentre as várias inovações trazidas por este projeto ao nosso ordenamento jurídico, pode-se destacar que será qualificado o que vem a ser meio eletrônico e sistema informatizado, assim como os objetos que fazem parte de cada um desses contextos.

O projeto também visa combater, não apenas, as malas diretas eletrônicas que são abastecidas com a cópia não autorizada dos dados de pessoas e que são armazenadas em empresas ou órgãos públicos e privados, como também, a venda de CDs de computador com dados de terceiros para empresas de mala direta. Assim também estará se alcançando os indivíduos que coletam dados de terceiros e os fornecem indiscriminadamente às empresas que criam as malas diretas eletrônicas, conhecidas como *spams*. Com isso os endereços eletrônicos e os e-mails, estarão protegidos e só poderão ser divulgados mediante autorização expressa de seu possuidor

Outro aspecto interessante do projeto é o fato deste punir os *hackers*, os *crackers*, os *phreakers* ou todo e qualquer indivíduo que tente acessar dados ou informações bastando apenas que estes não tenham a devida permissão para o acesso.

O projeto pretende terminar com uma das lacunas em nossa legislação, lacuna esta relacionada aos criadores e difundidores de vírus de computador. Percebe-se que, para o projeto de lei, o simples usuário de computador que difunde um vírus eletrônico, sem saber que o está fazendo, não será punido pois, para que ocorra a punibilidade será preciso a intenção de destruir, inutilizar, modificar ou dificultar o funcionamento de um sistema computacional.

Atualmente a nova tecnologia de acesso a *internet*, conhecida como *internet* sem fios ou Wi-Fi, que prevê o acesso a dados e informações utilizando-se a telefonia móvel celular assim como os PDAs, que são pequenos computadores de bolso estará também protegida pois o projeto terminará com mais esta lacuna de nossa legislação quanto a falta de punibilidade relativa a fraude contra o acesso a *internet* utilizando a telefonia móvel ou os cartões inteligentes.

Um dos assuntos mais citados quando se fala de crimes pela *internet* é a fotografia de cena de sexo explícito ou pornografia envolvendo criança ou adolescente. Esta prática delitiva que, atualmente, pelo Estatuto da Criança e do Adolescente, Artigo 241, ou pelo Código Penal, Artigo 218, são reprimidos com pena de reclusão de 1 (um) a 4 (quatro) anos, com a nova legislação, além da pena base já prevista, o indiciado deverá pagar uma multa e sua pena base será aumentada de metade até dois terços em tendo sido o crime cometido por meio de rede de computadores.

Finalmente cabe salientar as figuras da “falsidade informática” e da “sabotagem informática” que o projeto trará ao nosso ordenamento jurídico e, que foram incluídas no Senado Federal, após parecer do Senador Marcelo Crivela. Essas duas figuras trarão inegáveis avanços e tornarão o Brasil o país com uma das legislações mais atualizadas em relação às novas espécies de crimes cometidos pela *internet*.

Incorrerá no tipo penal de “falsidade informática” todo aquele que “de qualquer forma interferir no tratamento informático de dados, com o fito de obter, para si ou para outrem, vantagem indevida de qualquer natureza, induzindo a erro os usuários ou destinatários” (*caput*). Com isso se combaterá as fraudes eletrônicas através de *e-mail*, sendo suficiente, o simples envio de uma mensagem eletrônica falsa, com a finalidade de obter vantagem indevida, mediante a indução do operador ou usuário do computador a erro.

Já a “sabotagem informática”, combaterá aqueles que atuam inundando uma rede de computadores por meio do envio massivo de *e-mails*, impedindo assim o tráfego de demais usuários na rede, assim como daqueles que enviam programas específicos para romper a conexão entre o computador de um usuário com o seu provedor de acesso a *internet*.

Sobre o Projeto de Lei 84-D, a advogada e professora da Faculdade de Direito da Universidade Presbiteriana Mackenzie, Abrusio diz que:

Esse projeto visa acrescentar nova redação para tipos penais já existentes em nosso sistema criminal. O PL nº 84-D trará a previsão de condutas hoje não presentes em lei, tais como a disseminação de vírus, a invasão de sistemas e outros delitos relacionados aos meios eletrônicos. Não há dúvidas de que essa alteração na legislação brasileira, fará com que a sociedade em geral, por intermédio de profissionais especializados, amplie o número de processos relacionados aos crimes pela *internet*.

Corroborando com a idéia de Abrusio, Martinelli (2004), ao comentar o Projeto de Lei 84-D explica que “até o momento presente, só constituem crime as invasões seguidas de danos. Pelo projeto de lei, a simples invasão já poderá incriminar o autor e passam a ser crimes a criação, o desenvolvimento e o armazenamento de vírus”.

Após examinar os diversos projetos de lei que tramitam no Congresso Nacional, o advogado Colares (2004), membro da Unidade de Direito da Tecnologia da Informação da Martorelli Advogados e consultor do Porto Digital enfatiza que “o Projeto de Lei nº 84/99, é o que melhor procura suprir a necessidade preeminente que urge em nossa sociedade da tipificação penal de condutas que lesam dados ou bens de informática”.

A autora Castro, na segunda edição de sua obra “Crimes de informática e seus aspectos processuais”, inseriu um capítulo sobre os projetos de lei que estão em tramitação tanto na Câmara dos Deputados quanto e no Senado Federal. A respeito do PLC 84/99 ela tece os seguintes comentários:

O Projeto de Lei 84/99 prevê sete tipos penais, a saber: dano a dado ou programa de computador, acesso indevido ou não autorizado, alteração de senha ou mecanismo de acesso a programa de computador ou dados, obtenção indevida ou não autorizada de dados ou instrução de computador, violação de segredo armazenado em computador, criação, desenvolvimento ou inserção de dados ou programas de computador com fins nocivos e veiculação de pornografia através da rede de computadores.

Excetuando-se o último tipo, todos os outros protegem os dados, informações e programas do computador, tratando-se de crimes de informática próprios, posto que só podem ser praticados com o auxílio da informática.

O projeto tipificou a veiculação de pornografia, não prevendo, no entanto, a pedofilia na rede, esta sim, muito mais grave e nociva do que a pornografia já encontrada em bancas de jornal e locadoras de vídeos.

A maioria dos crimes deste projeto são apenados com detenção, a única exceção é a criação, desenvolvimento ou inserção de dados nocivos, cuja pena é de 1 a 4 anos de reclusão. Tal opção dificulta a investigação, uma vez que a interceptação telefônica é cabível apenas nos crimes punidos com reclusão. Assim, o juiz não poderá quebrar o sigilo das comunicações telemáticas, o que pode prejudicar e até mesmo impedir a apuração da autoria do delito.

Domeneghetti (2004), consultor e diretor da área jurídica da empresa E-Consulting, empresa voltada exclusivamente a assessoria de empresas que sofrem com fraudes eletrônicas publicou um artigo chamado “Espionagem digital com base no PL 84/99”. Neste artigo, voltado a empresários e profissionais da área tecnológica, ele comenta as inovações que serão trazidas ao nosso ordenamento jurídico pelo PL 84-D e, ao compará-lo com a Lei 9.279/96 assim finaliza “Em que pese o fato do PL tipificar condutas já previstas em lei, como a difusão de vírus criado para destruir, ou da pornografia infantil, o fato é que ele conseguiu tapar um espaço que ainda havia em nossa legislação, deixado pela Lei 9.279/96”.

Ao se buscar a opinião dos membros do judiciário sobre o PLC 84-D, o rebuscado artigo “Crimes de informática”, do Promotor de Justiça do Estado da Bahia, Aras, além de fazer um excelente apanhado sobre essa nova área do direito, também é favorável ao projeto ao comentar:

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

Há todavia tipos com sanções menos graves, como o crime de que se cuida no art. 11 do PLC 84/99, de obtenção indevida ou não autorizada de dado ou instrução de computador, com pena de três meses a um ano de detenção e, portanto, sujeito, em tese, à competência do Juizado Especial Criminal.

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

Finalmente, o juiz Reinaldo Filho, no artigo “O Projeto de Lei sobre os crimes tecnológicos (PL 84/99)” publicado pelo Centro Brasileiro de Estudos Jurídicos da Internet, faz um completo apanhado sobre a evolução dos crimes na área da informática e elogia o projeto não só por criar tipos penais novos mas também por estar a frente de seu tempo. Além de comentar todos os artigos que o projeto de lei se propõe a alterar, Reinaldo Filho ainda comenta as emendas feitas no Senado que visaram aprimorar e atualizar o projeto de lei tornando-o um dos mais modernos no ordenamento jurídico mundial:

O projeto, na versão aprovada pelo Plenário da Câmara criava os seguintes tipos penais, cometidos contra sistemas informáticos ou por meio deles: a) acesso indevido a meio eletrônico

(art. 154-A); b) manipulação indevida de informação eletrônica (art. 154-B); c) pornografia infantil (art. 218-A); d) difusão de vírus eletrônico (art. 163, par. 3º.); e e) falsificação de telefone celular ou meio de acesso a sistema informático (art. 298-A) (3). O projeto também elaborava os conceitos legais de “meio eletrônico” e “sistema informatizado”, para efeitos penais (art. 154-C). Além disso, produzia as seguintes alterações em figuras penais já existentes: a) acrescentava a “telecomunicação” no tipo penal de *atentado contra a segurança de serviço de utilidade pública* (art. 265 do CP) e no de *interrupção ou perturbação de serviço telegráfico ou telefônico* (art. 266 do CP); b) estendia a definição de *dano* do art. 163 do CP (crime de dano), por meio da equiparação à noção de “coisa” de elementos de informática como “dados”, “informação” e “senha”, sob a nova rubrica do dano eletrônico (acrescentando o par. 2º., incs. I e II); c) equiparava o cartão de crédito a documento particular no tipo *falsificação de documento particular*, acrescentando um parágrafo único ao art. 298 do CP, sob a rubrica de falsificação de cartão de crédito; e d) permitia a interceptação do fluxo de comunicações em sistema de informática ou telemática, mesmo para crimes punidos apenas com detenção, por meio do acréscimo de um par. 2º ao art. 2º. da Lei 9.296, de 24 de julho de 1996 (esta regula a interceptação das comunicações telefônica, informática e telemática). Durante sua tramitação, como o projeto original não contemplava algumas condutas já previstas em legislações de outros países, algumas emendas criaram novas figuras delituais, tais como os crimes de falsidade informática (art. 154-C) e de sabotagem informática.

Com essas explicações verifica-se a importância e a abrangência do referido projeto de lei que, mesmo com uma falha apontada por Castro, mostra-se como um avanço e um marco no direito penal pátrio.

6. JURISPRUDÊNCIA

Por se tratar de um tema relativamente novo, ainda são poucos os julgados de segundo grau de nossos tribunais que abordam temas como vírus de computador, fraude pela *internet*, pedofilia pela *internet* e demais assuntos relacionados a essa área.

Quatro julgados serão apresentados por se tratarem de temas interessantes abordados pelos tribunais.

No primeiro deles se perceberá a concessão parcial ao pedido de *habeas corpus* a um cidadão que, ao receber imagens pornográficas de crianças, agradece ao remetente das mesmas.

PENAL E PROCESSUAL PENAL. DIVULGAÇÃO DE FOTOS PEDÓFILAS NA INTERNET. PRISÃO PREVENTIVA. PRESSUPOSTOS E REQUISITOS LEGAIS. PROVA DA EXISTÊNCIA DO CRIME. CONVENIÊNCIA DA INSTRUÇÃO CRIMINAL.

1. O recebimento, pelo paciente, em seu e-mail pessoal, de material fotográfico de conteúdo pornográfico envolvendo crianças, seguido do envio de entusiástica mensagem de agradecimento ao remetente, constitui indício da prática do crime tipificado no art. 241 do Estatuto da Criança e do Adolescente (“Fotografar ou publicar cena de sexo explícito ou pornográfica envolvendo criança ou adolescente”), não se justificando o pedido de trancamento prematuro do inquérito policial por ausência de autoria.
2. Considerada a excepcionalidade de que deve revestir-se a prisão preventiva, como um mal necessário em face do princípio constitucional de inocência, é imprescindível que o magistrado, ao decretá-la, justifique a sua necessidade à vista de um dos seus pressupostos legais (art. 312 - CPP) - no caso, para a conveniência da instrução criminal -, concreta e objetivamente, em face dos fatos autos, não bastando a repetição dos dizeres da lei, ao enumerá-los.
3. Concessão parcial da ordem de *habeas corpus*. Desconstituição do decreto de prisão preventiva.

Processo: HC 2003.01.00.029307-6/MT; TRF 1ª Região

Relator: Des. Federal Olindo Menezes

Órgão Julgador: TERCEIRA TURMA

Publicação: 31/10/2003 DJ p.36

No segundo exemplo tem-se a famosa “contaminação por vírus de computador”. A ação de indenização proposta por Renata Ferreira em face da empresa Distribuidora Paulista de Produtos e Serviços Ltda., iniciou-se depois da autora ter recebido um disquete com um suposto vírus de computador da ré. Por não ter apresentado a materialidade do fato a mesma teve a ação julgada improcedente na 2ª instância.

AÇÃO DE INDENIZAÇÃO. Alegada utilização de disquete contaminado por vírus, no computador da pessoa jurídica, causando dano ao sistema. Não apresentação do disquete. Contestação específica das rés. Inexistência de prova da contaminação, porque não exibido o disquete. Perícia unilateralmente produzida. Inutilidade. Ação improcedente. Apelação provida em parte, apenas para redução da honorária.

Processo: AC 108.150-4/6-00; TJ/SP

Relator: Des. Federal Olindo Menezes

Órgão Julgador: 4ª C.D.Priv.

Publicação: j. 15/02/2001, v.u.

No próximo exemplo tem-se o caso de uma empresa que alega o caso fortuito por ter lançado o nome de um consumidor no cadastro negativo do SPC visto que sua base de dados estaria infectada por um tipo de vírus de computador.

PROCESSO CIVIL E CIVIL. APELO ADESIVO. AMPLITUDE. INDENIZAÇÃO POR DANOS MORAIS. CADASTRO NEGATIVO DO SPC. VÍRUS DE COMPUTADOR. CASO FORTUITO. INEXISTÊNCIA. CONDUTA PREVISÍVEL E EVITÁVEL. MAJORAÇÃO DA CONDENAÇÃO ANTE AS PECULIARIDADES DA CASO EM APREÇO. (...) A infecção de computador por vírus, ante o rápido desenvolvimento tecnológico da informática, inclusive com o aparecimento da rede de computadores “internet”, é hipótese bastante previsível e também evitável, com os modernos mecanismos de defesa, os quais devem ser empregados por todos aqueles que trabalham com referidas máquinas e com grandes bases de dados, sendo a inexistência de tal proteção, derivando de tal infeção o irregular cadastro negativo do SPC, conduta negligente, afastada, assim, a hipótese de caso fortuito. Deve-se majorar a verba de ressarcimento, tendo em vista a hipótese em análise, observando o binômio punição/compensação, quando se nota que a atitude ilícita da instituição perdurou por mais de dois anos, com a imputação indevida ao cadastro do autor de mais de 500 protestos.

Processo: AC 281.733-6; TJ/MG

Relator: Juiz Dorival Guimarães Pereira

Órgão Julgador: 3ª Câmara Cível

Publicação: j. 16/06/1999, v.u.

Nesta última, o *habeas corpus* de número, 2003.01.00.042372-9, negado pela QUARTA TURMA do TRF da 1ª Região, em 14/01/2004, o Ministério Público Federal assim se manifestou com relação a libertação do responsável pelo envio de arquivos de computador com o intuito de fraudar contas bancárias de usuários que acessam sites de bancos através da internet:

A situação do réu (MIGUEL VIANA SANTOS NETO), contudo, é completamente diversa dos demais posto que (*sic*) seu papel na organização criminosa é bastante superior aos outros requerentes, não apenas no faturamento, mas sobretudo na importância decisória e na prática dos atos que lhe competiam. Era ele quem confeccionava e aperfeiçoava programas *TROJAN*, além de prestar assistência técnica mediante pagamento de valores variados. Confessou que utilizava *e-mails* para prática de delitos por meios eletrônicos. Sua libertação, nessa fase inicial da ação penal, significará o retorno de operação da quadrilha porque um de seus ‘cérebros’ voltará a agir por estar (*sic*) em liberdade, até mesmo para ajudar no ganho a ser repassado àqueles que não possam trabalhar momentaneamente.

Processo: HC 2003.01.00.042372-9; TRF 1ª Região

Relator: Des. I'talo Fioravanti Sabo Mendes

Órgão Julgador: Quarta Turma

Publicação: 22/12/2003 DJ p.12

CONCLUSÃO

Conforme pôde-se observar, a lacuna jurídica que há no ordenamento nacional acerca dos crimes na área da informática, faz crescer na sociedade brasileira um sentimento de impunidade com relação aos chamados criminosos da *internet* e, a cada dia que passa, os noticiários informam sobre novas quadrilhas envolvidas nessa prática delituosa e cada vez mais são apresentadas atuações das polícias estaduais e federal para se combater tais atos criminosos. Verificou-se que o Brasil é um dos países nos quais mais ocorrem os acessos a *internet* e, conseqüentemente onde tem ocorrido um aumento desse tipo de prática delituosa. Apresentou-se um pequeno apanhado da legislação de países desenvolvidos e em vias de desenvolvimento sobre esse conturbado tema e comentou-se quão atual está a legislação de tais países.

Foram apresentados alguns julgados recentes de tribunais superiores para demonstrar como os crimes na área da *internet* estão sendo tratados por esses tribunais nos dias de hoje.

Conclui-se que a nova legislação, o Projeto de Lei 84-D, que está prestes a ser encaminhado para sanção presidencial suprirá, senão todas, a maioria das lacunas do ordenamento jurídico pátrio quanto aos crimes praticados na área da *internet*, fazendo com que os criminosos eletrônicos migrem para outros países que não tenham legislação específica, que a sociedade brasileira sintase protegida contra tais delitos e que o Brasil esteja a frente das demais nações nesse tema com uma legislação eficiente e atual.

REFERÊNCIAS

- ABRUSIO, Juliana Canha. *Os hackers e os tribunais*. Infojus, [s.l.], março 2004. Disponível em: <http://www.infojus.com.br/webnews/noticia.php?id_noticia=2109&>. Acesso em: 16 set. 2004
- ARAS, Vladimir. *Crimes de informática. Uma nova criminalidade*. Jus Navigandi, Teresina, outubro 2001. Disponível em: <<http://www1.jus.com.br/doutrina/texto.asp?id=2250>>. Acesso em: 18 set. 2004.
- ARAÚJO JUNIOR, João Marcello de. *Computer-crime*, In CONFERÊNCIA INTERNACIONAL DE DIREITO PENAL, 1988, Rio de Janeiro. *Anais...* Rio de Janeiro, PGDF, 1988. p. 461. Disponível em <http://www.vieiraceneviva.com.br/download/Palestra_Comunicacao_Eletronica_UNOPAR.ppt> Acesso em: 21 abr. 2004
- BITTENCOURT BRASIL, Angela. *Informática Jurídica – O Ciber Direito*. Rio de Janeiro: Forense, 2000, p.133-134.
- _____, Angela. Crimes de Computador. Avocati Locus, [s.l.], fevereiro 2000. Disponível em: <<http://www.advogado.com/internet/zip/crimesdecomputador.htm>>. Acesso em: 22 abr. 2004.
- BRITO, Eduardo Valadares de. *Crimes na Internet*. Infojus, [s.l.], janeiro 1999. Disponível em: <http://www.infojus.com.br/webnews/noticia.php?id_noticia =552&>. Acesso em: 21 abr. 2004
- BRITO, Paulo. *Pirataria*. Capítulo da obra Microcomputador - curso prático. São Paulo: RGE, 1984, v. 1, p. 57-58.
- CALMON, Beatriz Senra. *Crimes na Internet*. Rio de Janeiro: Associação de Bancos no Estado do Rio de Janeiro, 2004.
- CASTRO, Carla Rodrigues Araújo de. *Crimes de informática e seus aspectos processuais*. Rio de Janeiro: Lumen Juris, 2001.
- CERT/CCC, CERT® *Coordination Center*, foi criado em 1988 e é um centro de especialistas em segurança de *internet* localizado no Instituto de Engenharia de Software, um centro de pesquisas e desenvolvimento do governo norte-americano dirigido pela Universidade *Carnegie Mellon* em Pittsburgh, EUA. Disponível em: <<http://www.cert.org>>. Acesso em: 22 abr. 2004.

- COLARES, Rodrigo Guimarães. *Cybercrimes: os crimes na era da informática*. Jus Navegandi, Teresina, outubro 2002. Disponível em <<http://www1.jus.com.br/doutrina/texto.asp?id=3271>>. Acesso em: 16 set. 2004.
- CORREIA, Gustavo Testa. *Aspectos Jurídicos da Internet*. São Paulo: Saraiva, 1999, p. 42.
- _____, Gustavo Testa. *Aspectos Jurídicos da Internet*. São Paulo: Saraiva, 1999, p. 43.
- DAMÁSIO, Evangelista de Jesus. Palestra de abertura in: *I Congresso Internacional do Direito na era da Tecnologia da Informação*, nov. 2000. Recife-PE: Auditório do TRF da 5ª Região.
- DOMENEGHETTI, Caio. *Espionagem digital com base no PL 84/99*. SUCESU-ES, Vitória, fevereiro 2004. Disponível em: <http://www.sucesues.org.br/documentos/index.asp?cod_noticia=434>. Acesso em: 10 nov. 2004.
- DAVID, René. *Los Grandes Sistemas Jurídicos Comtemporaneos*. Madrid: Aguillar, 1973, pg. 9.
- FERREIRA, Ivete Senise. *Novas Fronteiras do Direito na Era Digital*. São Paulo: Saraiva, 2002, p. 146-153.
- _____, Ivete Senise. *Os Crimes da Informática*, In Estudos em Homenagem a Manoel Pedro Pimentel. São Paulo: RT, 1992, p.141-142.
- _____, Ivete Senise. *A criminalidade informática*. Capítulo do Livro “*Direito e Internet – Aspectos Jurídicos Relevantes*”. São Paulo: EDIPRO, 2000, p. 207.
- GOUVÊA, Sandra. *O Direito na era Digital*. Rio de Janeiro: Mauad, 1997.
- MACHADO, Eduardo de Paula. *Novas Fronteiras da Criminalidade: Os crimes tecnológicos*. Boletim IBCCrim, São Paulo, ano 7, nº 81, ano 7, agosto de 1999.
- MACHADO, Daniel. *Formas para tornar sua rede mais segura*, RTI, São Paulo, ano 5, nº 53, out. 2004.
- MARTINELLI, João Paulo Orsini. Aspectos relevantes da Criminalidade na Internet. Jus Navegandi, Teresina, junho 2000. Disponível em <<http://www1.jus.com.br/doutrina/texto.asp?id=1829>>. Acesso em: 21 abr. 2004.
- MIRANDA, Marcelo Baeta. Abordagem dinâmica aos crimes via internet. Jus Navigandi, Teresina, dezembro 1999. Disponível em: <<http://www1.jus.com.br/doutrina/texto.asp?id=1828>>. Acesso em: 22 abr. 2004.
- MUÑOZ CONDE, Francisco & GARCIA ARÁN, Mercedes. *Derecho penal. Parte general*. 3. ed. Valencia: Tirant lo Blanch Libros, 1998, p. 281/282.
- _____, Francisco & _____, Mercedes. *Derecho Penal. Parte General*. 3. ed. Valencia: Tirant lo Blanch Libros, 1998, p. 18.
- PADRÃO, Ana Paula. Habilidade para o mal. Jornal da Globo, Rio de Janeiro, 13 set. 2004. Disponível em <<http://jg.globo.com/JGlobo/0,19125,VTJ0-2742-20040913-61398,00.html>>. Acesso em 14 set. 2004.
- PINHEIRO, Reginaldo Cezar. *Os crimes virtuais na esfera jurídica brasileira*. Boletim IBCCRIM. São Paulo, v.8, n. 101, p. 18-19, abril, 2001.
- REINALDO FILHO, Demócrito. *O Projeto de Lei sobre os crimes tecnológicos (PL 84/99)*. CBEJI, São Paulo, junho 2004. Disponível em: <<http://www.cbeji.com.br/br/novidades/artigos/main.asp?id=3018>>. Acesso em: 10 nov. 2004.
- RODRIGUES, Miguel Angel Davara. Crime Informático. SAPO, Portugal, [s.d.]. Disponível em <<http://canais.sapo.pt/tecnologia/dhc/>>. Acesso em 21 abr. 2004
- RODRIGUES DA COSTA, Marco Aurélio. *Crimes na informática e seus aspectos jurídicos*. 1995. 55 f. Monografia (Mestrado em Direito) - PUC-RS.
- SCAGLIA, Alexandre. Não há crime sem lei, *Information week Brasil*, São Paulo, ano 6, nº 102, jan. 2004.
- UNESCO. Disponível em: <http://www.unesco.org/cybersociety/cyberspace_spec.htm>. Acesso em: 21 abr. 2004.

VALIM, Carlos Eduardo. País lidera acesso a sites governamentais, *Information week Brasil*, São Paulo, ano 6, nº 105, fev. 2004.

War Games — Jogos de Guerra (1983). MGM/UA. O adolescente David, gênio da informática, ao tentar copiar um jogo de computador de uma empresa acidentalmente conecta seu microcomputador ao sistema informatizado do *NORAD* — *North American Aerospace Defense Command*, de defesa antiárea dos Estados Unidos, e quase dá início à terceira guerra mundial; www.netlaw.de/gesetze/iukdg.htm - *Site* com as leis referentes ao Ministério da Informação e Comunicação do governo da Alemanha.

www.rcmp.ca - *Site* da Real Polícia Montada do Canadá.

www.tj.sp.gov.br - *Site* do Tribunal de Justiça do Estado de São Paulo

www.tjmg.gov.br - *Site* do Tribunal de Justiça do Estado de Minas Gerais

www.trf1.gov.br - *Site* do Tribunal Regional Federal da 1ª Região

www.usdoj.gov - *Site* do Departamento de Justiça do governo dos Estados Unidos.