O PROJETO DE LEI SOBRE CRIMES TECNOLÓGICOS (PL 84/99) - Notas ao parecer do Senador Marcello Crivella

Autor: **Demócrito Reinaldo Filho** Fonte: **Infojus**

O Senador Marcelo Crivella apresentou seu relatório quanto ao PLC 89/2003, na condição de membro da Comissão de Constituição, Justiça e Cidadania do Senado Federal. O projeto em questão, originário da Câmara (PL 84/99), de autoria do Dep. Luiz Piauhylino, altera o Decreto-Lei n. 2.848, de 07 de dezembro de 1940 (Código Penal), dispondo sobre os crimes cometidos no campo da informática e suas penalidades.
Trata-se da superação de mais uma fase da longa caminhada que o projeto vem percorrendo. Só na Câmara dos Deputados passou por 04 comissões temáticas, recebeu várias emendas, apensamentos a outros projetos e substitutivos. Chegou ao Senado no dia 13.11.03, tendo sido enviado para a CCJ no dia seguinte, onde ainda se encontra para ser votado pelos membros da comissão e, em seguida, pelo plenário da casa legislativa.
O projeto tem a virtude de pretender se tornar a primeira lei brasileira que trata de uma maneira ampla e sistematizada dos crimes cometidos através dos meios informáticos (1). Não apenas cria tipos penais novos, mas estende o campo de incidência de algumas figuras já previstas no CP para novos fenômenos ocorrentes nos meios desmaterializados - impossíveis de terem sido previstos pelo legislador de 1940, ano de edição do atual Código Penal. Como se sabe, persistiu uma discussão doutrinária se a legislação brasileira precisava ser reformada ou se ela já satisfazia e era suficiente para punir os comportamentos criminosos que ocorrem nos ambientes desmaterializados, dos sistemas informáticos e das redes telemáticas. Para alguns, os chamados "crimes informáticos" são apenas uma faceta de realidades já conhecidas, crimes e condutas já tipificadas em sua definição material que apenas são cometidos com o auxílio de outros recursos (os elementos informáticos). A grande verdade, porém, é que determinadas condutas surgidas nesses ambientes são inteiramente novas, e não guardam relação ou similitude com tipos já descritos na lei atual, havendo uma necessidade de sua reformulação para "acompanhar os novos tempos - a Era Digital", como ressaltou o Sen. Marcelo Crivella em seu parecer (2). Por isso o projeto de lei em comento cria novos tipos penais, não se limitando a reformular conceitos legais existentes.
O projeto, na versão aprovada pelo Plenário da Câmara (em novembro de 2003), 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 do 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).
O Sen. Marcelo Crivella, muito apropriadamente, entendeu que o projeto necessitava de alguns aperfeiçoamentos. É claro que isso se deve ao longo tempo de maturação que o projeto ficou na Câmara, mas também é fato de que o projeto original não contemplava algumas condutas já previstas em legislações de outros países, como bem lembrou o Senador. Nesse sentido, apresentou algumas emendas criando novas figuras delituais, tais como os crimes de falsidade informática (art. 154-C) e de sabotagem informática, com a emenda relativa a eles assim redigida:

"**Falsidade Informática**

Art. 154-C. Introduzir, modificar, apagar ou suprimir dado ou sistema informatizado, ou, de qualquer forma, interferir no tratamento informático de dados, com o fim de obter, para si ou para outrem, vantagem indevida de qualquer natureza, induzindo a erro os usuários ou destinatários.
Pena - detenção, de um a dois anos, e multa.
Parágrafo único. Nas mesmas incorre quem, com a mesma finalidade, cria, disponibiliza ou divulga comunicação eletrônica falsa.

Sabotagem Informática

Art. 154-D. Introduzir, modificar, apagar ou suprimir dado ou sistema informatizado, ou, de qualquer forma, interferir em sistema informatizado, com o fim de desorientar, embaraçar, dificultar ou obstar o funcionamento de um sistema informatizado ou de comunicação de dados à distância.
Pena - detenção, de um a dois anos, e multa."

O acréscimo dessas duas figuras (4) traz inegáveis avanços ao projeto e o atualiza em relação às novas espécies de crimes informáticos cometidos por meio de **redes eletrônicas**.

A definição do crime de *falsidade informática*, e em especial a subespécie da *comunicação eletrônica falsa* (encapsulada no par. único do art. 154-D), vem em boa hora diante do fenômeno que se tornou a marca cada vez mais comum dos crimes cometidos nos ambientes das redes informáticas: a associação entre fraudadores e *spammers*. A nova faceta de um problema que cada vez mais assola os usuários, o recebimento de mensagens não solicitadas (*spams*), agora vem adicionado às tentativas de fraudes eletrônicas (*scams*). Não se trata somente das tradicionais mensagens eletrônicas enganosas, contendo texto com as famosas "correntes" ou promessas de recompensa. Agora, elas costumam vir adicionadas de "programas maléficos" atachados à própria mensagem de e-mail. Uma vez abertos esses arquivos anexos, eles instalam programas espiões no computador do destinatário da mensagem, do tipo *spyware* ou *trojan* (cavalo de tróia), que permite que o agente criminoso tenha acesso remoto a todo o sistema do computador atacado (5). Um tipo específico desses programas espiões (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 último ano (2003) e começo deste foi o conhecido como *phishing scam*. Nessa subcategoria de fraude através de comunicação eletrônica falsa (*scam*), 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 (6). A nota característica, portanto, dos *phishing scams* é que o estelionatário se faz passar por uma confiável fonte e usa geralmente o endereço de e-mail dessa fonte (ou endereço eletrônico ligeiramente parecido, mas suficiente a confundir o destinatário) ou falseia seu endereço na *Web* (7), prática conhecida como *spoofing*. A mensagem falsa contém uma solicitação de informações pessoais ou um *link* para um endereço falso onde deve ser preenchido um formulário. No *website* 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 (*scammers*) transferem os recursos das vítimas para suas próprias contas (8).

A redação do dispositivo em comento (art. 154-C), a ser introduzido no CP, pretende abarcar todas essas modalidades de fraudes eletrônicas, ao prever que incorre 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*). As fraudes eletrônicas perpetradas por e-mail, ainda que sem a utilização de programas espiões, também não escapam da regulamentação, na medida em que o parágrafo único esclarece que "nas mesmas penas incorre quem, com a mesma finalidade, cria, disponibiliza ou divulga comunicação eletrônica falsa" - na verdade o parágrafo único estabelece a figura do crime de *comunicação eletrônica falsa*, como já observamos acima.

É suficiente, portanto, o simples envio de uma mensagem eletrônica falsa, com a finalidade de obter vantagem indevida, mediante a indução do operador ou usuário de um sistema informático a erro. O artifício ou meio fraudulento necessário à caracterização do crime pode ser exclusivamente a mensagem eletrônica falsa, desde que daí surta um duplo resultado: a vantagem indevida (ilícita) e o prejuízo alheio (da vítima). A consumação propriamente dita exige esses dois elementos (vantagem ilícita e dano patrimonial), mas a figura do crime de *falsidade informática* admite a tentativa, da mesma forma como o estelionato tradicional (do art. 171 do CP). Em outras palavras, aquele que envia mensagem eletrônica falsa, com essa finalidade (a obtenção de vantagem indevida), ainda que não se concretize o prejuízo do destinatário, responde pelo crime na modalidade tentada, até porque, nessa hipótese, a fraude já estaria caracterizada.

Entendemos que a pena prevista para esse tipo de crime está muito atenuada, pois o limite é de 02 anos de detenção (e multa). A *falsidade informática* pode gerar imensos prejuízos patrimoniais para empresas e pessoas físicas, em escala ampliada. Observe-se que para o crime de estelionato tradicional a pena é de reclusão até 05 anos. Não há motivo, portanto, para que sua versão eletrônica tenha previsão de pena mais branda, na medida em que o seu potencial de lesão é muito mais acentuado.

É importante também destacar que a regra do art. 154-C, que se pretende introduzir no CP por meio do projeto, não objetiva e nem tampouco resolveria o problema específico do *spam* - o envio de mensagens não solicitadas. A questão do *spam* deve ser tratada em uma lei específica, contendo uma regulamentação completa e exaustiva sobre o problema, que estabeleça os tipos penais, as exceções (os casos em que se legitima o envio de mensagens comerciais não solicitadas), atribua poderes a agências governamentais para fiscalizar e aplicar multas, contenha previsão das sanções civis e penais, os limites das penas pecuniárias, atribua recompensa a quem prestar informações que auxiliem a desvendar identidades dos criminosos, entre outras medidas. Algumas leis estrangeiras editadas recentemente sobre *spam* têm mais de cem dispositivos (9). Além do mais, a questão do *spam* é objeto de vários projetos que estão tramitando atualmente no Congresso Nacional. O futuro art. 154-C se limita, como se disse antes, ao problema das fraudes eletrônicas, quer sejam elas cometidas com ou sem a utilização de e-mail. Trata-se de uma ferramenta legal para combater os *scammers*, e não propriamente os *spammers*.

A figura do crime de *sabotagem informática*, delineado no descritor normativo do art. 154-D, pretende por sua vez alcançar outras modalidades de crimes informáticos cometidos em rede, a exemplo do conhecido "denial-of-service attack", um tipo de delito que pode resultar em significante perda de tempo e dinheiro para as vítimas, em geral empresas que operam serviços na Internet ou em outras redes de arquitetura aberta.

O principal objetivo nesse tipo de ataque é impossibilitar a vítima (um sistema informático) de ter acesso a um particular recurso ou serviço. Em geral, não somente o operador do sistema atacado fica impossibilitado de fazer uso dele, mas também seus legítimos usuários. Por exemplo, existem *hackers* que atuam inundando uma rede informática por meio do envio de massivos pacotes de informações, impedindo assim o tráfico na rede (ainda que temporariamente) de todos os seus usuários; em outros casos, atuam tentando romper a conexão entre o computador do usuário ao do seu provedor,

obstaculizando o acesso a um serviço prestado por esse último. Em suma, esse tipo de ataque essencialmente visa a desabilitar o computador da vítima ou a rede informática que ela usa para prestar ou receber um serviço. O pior é que esse tipo de ataque pode ser executado com limitados equipamentos contra sofisticados *sites* e sistemas informáticos. Usando um velho e simples PC e uma conexão à Internet de baixa velocidade, um *hacker* consegue incapacitar máquinas e redes informáticas tecnicamente sofisticadas.

Os modos de ataque são os mais variados possíveis, atingindo a velocidade do tráfico de informações na rede, a memória ou espaço em disco do sistema informático ou sua estruturação de dados.

Boa parte dos ataques que se enquadram nessa categoria (*denial-of-service*) são cometidos contra a velocidade de conexão ("banda") da rede. O objetivo, nesse caso, é prevenir o provedor ou mantenedor da rede de se comunicar com outras redes ou sistemas informáticos. Explico: o *hacker* executa seu ataque por meio do estabelecimento de uma conexão com a máquina do servidor-vítima, mas o faz de tal maneira que a conexão não se completa. Nesse meio tempo, ele impede que os usuários legítimos do sistema se comuniquem com o servidor, pois este está ocupado tentando completar a conexão semi-aberta (10). A velocidade da conexão à rede também pode ser afetada por meio do envio de extenso pacote de informações diretamente para ela. Esse tipo de ataque às vezes não ocorre de um único computador, pois ele pode coordenar ou cooptar o ataque simultâneo de muitas outras máquinas contra o servidor ou sistema-vítima.

Outros recursos informáticos podem ser atingidos, como se disse, além da "banda" de conexão à rede. Por exemplo, muitos sistemas são estruturalmente desenhados para processar os dados que os alimentam. Um intruso pode simplesmente alterar seu funcionamento por meio da inclusão de um pequeno programa que não faça absolutamente nada, a não ser reproduzir-se automaticamente, consumindo assim todos os recursos de processamento de dados do sistema-vítima.

Também é comum de o ataque consumir espaço em disco do computador-vítima, colocando arquivos FTP em áreas da rede disponibilizadas aos usuários. Em geral, os servidores se previnem desse tipo de ataque limitando o espaço em disco que pode ser utilizado para a colocação de dados, mas os *hackers* às vezes têm como eliminar esse tipo de controle.

Alguém pode sugerir que esses tipos de ataques a sistemas informatizados já estariam cobertos pela figura do *dano eletrônico*, que a versão original (proveniente da Câmara) já pretendia criar (par. 2o. do art. 163 do CP). Só que esses ataques podem ser feitos sem necessariamente destruir o sistema informático (vítima do ataque) ou sequer alterar sua configuração de dados. Daí que a redação do dispositivo referente ao crime de *sabotagem informática* incrimina o ato que "de qualquer forma, interferir em sistema informatizado, com o fim de desorientar, embaraçar, dificultar ou obstar o funcionamento de um sistema informatizado ou de comunicação de dados à distância".

O parecer do Senador Crivella também estabelece a obrigação de todos os provedores de Internet armazenarem os registros de movimentação de seus usuários, pelo prazo de 03 anos (11). Trata-se de medida inadiável e indispensável para possibilitar a investigação de delitos cometidos na rede mundial. Sem esses registros de conexão e navegação é impossível qualquer investigação criminal de delitos informáticos. O projeto, nesse sentido, segue uma tendência global, pois praticamente todos os países desenvolvidos já incluíram esse tipo de obrigação legal em seus sistemas jurídicos, sobretudo depois que o combate ao terrorismo se tornou assunto de política geral. Essa providência, aliás, já deveria ter sido implementada por via infralegal, através de alguma agência reguladora, a exemplo da Anatel. O Comitê Gestor da Internet (CGI) no Brasil apenas recomenda aos provedores nacionais, dada a ausência de lei nesse sentido, que guardem por até três anos os registros de conexão dos usuários (12).

O parecer ainda faz outros ajustes ao projeto original, como, por exemplo, a eliminação da figura do art. 218-A (pornografia infantil), cuja inclusão não é mais necessária, uma vez que a Lei a Lei 10.764, de 12 de novembro de 2003, já criou esse tipo de delito (por meio do aperfeiçoamento da redação do art. 241 do ECA, que agora já pune a difusão desse tipo de material ilícito na Internet). Além disso, aperfeiçoa a redação do art. 298-A (crime de falsificação de telefone celular ou meio de acesso a sistema informático), de que trata o projeto de lei da Câmara (13), e acrescenta um parágrafo único ao art. 46 do CP, de modo a possibilitar a aplicação de penas restritivas de direito a *hackers*, aproveitando os seus conhecimentos técnicos em cursos de instituições públicas ou outras atividades equivalentes (14).

O parecer do senador Crivella segue para votação na Comissão de Constituição, Justiça e Cidadania do Senado Federal. Caso seja aprovado, a matéria seguirá para a apreciação da Comissão de Educação da Casa. Após análise nesta comissão, ele retornará para a Comissão originária para receber parecer definitivo.

De um modo geral, o parecer promove alterações importantes ao projeto originário da Câmara. É claro que o combate aos *cybercrimes* não se resolverá na sua aprovação. O grande problema desse tipo de crime é que quase sempre é muito difícil determinar sua origem. A identificação do agente responsável direto pelo ato envolve a necessidade de cooperação com o provedor de Internet ou do administrador das *networks* afetadas. É preciso dotar os órgãos policiais e ministeriais com pessoal e meios técnicos para promover o rastreamento desses crimes. Nos EUA, o próprio FBI auxilia na investigação de alguns casos, inclusive possibilitando o contato para pessoas que estão situadas fora daquele país (15). Além disso, é necessário que o nosso país assine tratados de cooperação, que simplifiquem procedimentos de extradição, já que esses crimes são cometidos de maneira transnacional. Apesar disso tudo, a definição legal das práticas criminosas é realmente o primeiro passo na luta contra o problema. Em respeito ao princípio da *legalidade* estrita que impera no campo penal, é imprescindível a descrição de forma antecedente (na lei) para que se possa, então, punir as condutas.

Agora, o que não podemos é retardar ainda mais a aprovação do projeto e, a cada passo, ficar acrescentado novas figuras à sua redação original. É melhor uma lei que não preveja todos os delitos de possível ocorrência no ciberespaço do que nenhuma. A existência de um vácuo na legislação penal dificulta a luta contra os *cybercrimes*. Parece-me que o correto, no momento, reside em apressar a votação do projeto com os crimes já incluídos e analisados nas diversas comissões (tanto na Câmara como no Senado), até porque, nos ambientes das redes de comunicação, novas modalidades de crime surgem a cada dia; é impossível se prever todas elas. A aprovação do projeto é um primeiro passo; no futuro se pode criminalizar outras condutas que forem surgindo. Por exemplo, nos EUA existe uma lei de crimes informáticos há 14 anos, o *Computer Misuse Act* (CMA). O debate que se trava lá no momento é sobre a necessidade de atualizá-la, sobretudo para fazer face aos crimes cometidos em redes informáticas abertas. Mas ela é uma lei básica, que vem servindo (pelo menos até agora) eficazmente.

Precisamos de um estatuto básico sobre crimes informáticos em nosso país, e o projeto originalmente apresentado pelo Dep. Luiz Piauhylino cumpre bem esse papel.

Notas:

(1) Antes dele, apenas a Lei 9.983, de 14.07.2000, havia introduzido no Código Penal Brasileiro a figura qualificada do crime de divulgação de segredo (art. 153, §1º-A), cujo tipo prevê pena de detenção de um a quatro anos e multa para aquele que 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. Essa Lei introduziu, ainda, o chamado "peculato eletrônico", ao acrescentar no Código Penal os artigos 313-A e 313-B, os quais contêm a previsão de punição para o funcionário público que praticar a inserção de dados falsos em sistemas de informações (art. 313-A) - a pena prevista é de reclusão de dois a doze anos e multa -, bem como para aquele que modificar ou alterar sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente (art. 313-B), sendo a pena neste caso de detenção de três meses a dois anos e multa. Também a Lei nº 10.764, de 12.11.2003, alterou a redação do artigo 241 do Estatuto da Criança e do Adolescente, ampliando o descritor normativo do crime de pornografia infantil, para proibir a divulgação e publicação na Internet de fotografias e imagens contendo cenas de sexo explícito envolvendo criança ou adolescente, com pena de reclusão de dois a seis anos, além de multa.
Essas duas leis anteriores, como se vê, trataram de definir de forma isolada tipos específicos de "crimes informáticos", possuindo ambas outros dispositivos que tratam de figuras delitivas que não se incluem nessa denominação. Não foram elaboradas, portanto, com a finalidade de criar um texto sistematizado e geral sobre delitos no campo da informática, objetivo a que se propõe o projeto de lei ora em comento.
(2) Como consta do parecer do Senador, para essas novas condutas ilícitas "não havia remediação hermenêutica possível para inclusão nos dispositivos penais tradicionais".
(3) Essa numeração atribuída a cada um desses crimes é a que o projeto pretende introduzir no Código Penal.
(4) O parecer do Senador Marcelo Crivella modifica o artigo 2º do PLC, que aborda os crimes contra a inviolabilidade dos sistemas informatizados e acrescenta outros na "Seção V do Capítulo VI do Título I do Código Penal". Assim, o atual artigo 154-C do PLC é transformado em 154-E, para que sejam acrescidos os dois novos artigos (o do *crime de falsidade informática* e o do *crime de sabotagem informática*).
(5) Recentemente foi registrado o envio em massa de uma mensagem a internautas brasileiros, oferecendo um produto para aumento do pênis - item tradicional na lista dos *spammers*. Só que tudo não passava de uma farsa, pois a mensagem visava a instalar um arquivo espião no computador do destinatário. O e-mail, supostamente de uma empresa chamada "DoutorPenis.com", vem em português e promete um manual para "aumentar permanentemente o órgão sexual masculino em até 40% do comprimento e diâmetro".
Um "cavalo de tróia", contendo um formulário para inscrição no Big Brother Brasil 4, também circulou intensamente meses atrás no braço brasileiro da Internet.
Outro tipo bastante comum de fraudes eletrônicas são as cometidas por meio do envio de mensagens com ofertas falsas de anti-vírus, mas que na verdade, quando aberto o arquivo anexo, descarregam um *trojan* no computador da vítima.
(6) Através dessa prática de se fazer passar por um banco ou *site* comercial conhecido, os *scammers* conseguem enganar as pessoas com mais facilidade, segundo dados estatísticos. Já existe inclusive uma organização mundial que combate esse tipo específico de prática, o "Anti-Phishing Working Group", cujo site é www.antiphishing.org . O FBI também mantém um serviço que visa a combater fraudes eletrônicas, o "Internet Fraud Complaint Center" - www.ifccfbi.gov .
(7) Todo *site* tem um endereço de localização na Web (a *World Wide Web*), o canal gráfico da Internet.
(8) De acordo com pesquisa digulgada pelo Gartner Group, os *phishing attacks*, embora não sendo uma coisa nova na Internet, explodiram em número nos últimos seis meses. 76% dos ataques registrados foram lançados de outubro de 2003 pra cá. Outros 16% foram executados nos seis meses anteriores, significando que 92% de todos os ataques foram conduzidos no ano passado. Ou seja: embora sendo um tipo de fraude já antiga (em termos de Internet), os *phishing scams* adquiriram uma dimensão preocupante apenas a partir do ano passado. De acordo com essa mesma pesquisa, 57 milhões de cidadãos americanos foram vítimas de tentativas de fraudes desse tipo. De acordo com Avivah Litan, Diretor de pesquisas do Gartner Group, e autor de um estudo baseado na mesma pesquisa, as tentativas de fraudes eletrônicas (*phishing scams*) não são executadas por *hackers* amadores, mas pelo crime organizado, em particular por cartéis de drogas da Europa oriental, que descobriram que o furto de identidade (*identity theft*) e dados pessoais, e a fraude eletrônica em geral, pode ser um "negócio" bastante lucrativo. Ele estima que o prejuízo causado às companhias de cartões de crédito e bancos americanos só ano passado (2003) foi da ordem de US$ 1.2 bilhões. E o pior, nesse tipo de prática, é que os criminosos têm uma chance de uma em 700 de serem pegos, segundo ele avalia. Se os *phishing attacks* continuarem, estima ele, o resultado vai ser um decréscimo na taxa de confiança nas transações comerciais *on line*. A não ser que governos e empresas tomem providências, a taxa de crescimento do comércio eletrônico, que atualmente é de 20% anual, irá decair rapidamente. Ele estima que, pelo ano de 2007, a taxa de crescimento do comércio eletrônico nos EUA caia para 10% ou mais, se essas medidas não forem tomadas. Os dados da pequisa foram divulgados em entrevista publicada no site InternetWeek.com - www.internetwk.com
(9) É o caso da lei americana (o *CAN-SPAM Act*) e da lei australiana (o *Spam Act 2003*).
(10)Para esse tipo de conexão, usa-se o termo *"half-open" connection*.
(11) O parecer traz emenda que acrescenta um parágrafo único ao art. 11 do projeto da Câmara (PLC 89/03).
(12) Tal recomendação está prevista no item 3.2 ("Manutenção de Dados de Conexão") do documento "Recomendações para o Desenvolvimento e Operação da Internet no Brasil", criado pelo Comitê Gestor.
(13) O art. 298-A, proposto pelo projeto, cria o crime de falsificação de telefone celular ou meio de acesso a sistema informático. O parecer sugere emenda para deixá-lo com a seguinte redação:
"Art. 298-A. Criar, copiar, interceptar, usar, indevidamente ou sem autorização, ou falsificar **senha**, código, seqüência

alfanumérica, cartão inteligente, transmissor ou receptor de radiofreqüência ou telefonia celular ou qualquer instrumento que permita o acesso a meio eletrônico ou sistema informatizado.
Pena: reclusão, de um a cinco anos, e multa" .
A redação anterior não era clara sobre a conduta bastante comum da "quebra de senhas", o que demandava um aperfeiçoamento do art. 298-A, agora incluída pelo parecer do Sen. Marcelo Crivella.
(14) A emenda proposta tem a seguinte redação:
"Dê-se ao art. 5o. do Projeto de Lei da Câmara n. 89, de 2003, a seguinte redação:
Art. 5o. O art. 46 do Decreto-Lei n. 2.848, de 7 de dezembro de 1940 - Código Penal, passa a vigorar acrescido do seguinte parágrafo:
"No crime praticado contra ou por meio de meio eletrônico ou sistema informatizado, o juiz poderá aproveitar as habilidades e conhecimentos do condenado para a ministração de cursos ou trabalhos de criação de sistemas informatizados em empresas ou instituições públicas, ou para qualquer tipo de prestação de serviços equivalentes" (NR)"
(15) A página com informações para contato: www.fbi.gov/contactus.htm

Fonte: http://www.ibdi.org.br/index.php?secao=&id_noticia=338&acao=lendo