PROJETO DE LEI Nº , DE 2005

(Do Sr. Antonio Carlos Mendes Thame)

Dispõe sobre crimes informáticos, alterando o Código Penal e regulando a disponibilidade dos arquivos dos provedores.

O Congresso Nacional decreta:

Art. 1 O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, passa a vigorar com o acréscimo do seguinte Capítulo VII, inserido no Título I da Parte Especial:

"Capítulo VII" (AC)

"DOS CRIMES INFORMÁTICOS" (AC)

"Inserção de dados falsos em sistema de informações" (AC)

"Art. 154-A. Inserir ou facilitar a inserção de dados falsos, alterar ou excluir indevidamente dados corretos ou capturar dados protegidos, nos sistemas informatizados ou bancos de dados públicos ou privados, ainda que por acesso remoto ou mediante uso de meios insidiosos, com o fim de causar dano ou obter vantagem indevida para si ou para outrem:" (AC)

"Pena – reclusão, de dois a doze anos, e multa." (AC)

"Modificação ou alteração não autorizada de sistema de informações" (AC)

"Art. 154-B. Modificar ou alterar arquivo, sistema de informações ou programa de informática sem autorização

ou solicitação de autoridade competente ou do usuário:" (AC)

"Pena – reclusão, de um a três anos, e multa." (AC)

"Modalidade culposa" (AC)

"Parágrafo único. Se o crime é culposo:" (AC)

"Pena – detenção, de três meses a dois anos." (AC)

"Art. 154-C. Nos crimes previstos neste Capítulo:" (AC)

"I – só se procede mediante representação, salvo se cometido contra a União, Estado, Distrito Federal, Município, empresa concessionária de serviços públicos ou sociedade de economia mista; e" (AC)

"II – as penas são aumentadas de um terço até a metade se resulta dano." (AC)

Art. 2º Os art. 61, 313-B, ***caput*** , e 325 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940, passam a vigorar com as seguintes alterações:

Art. 61. .....

I - .....

II - ter o agente cometido o crime:

.....

"m) utilizando-se de arquivo, programa ou base de dados em meio eletrônico ou armazenado em qualquer outro suporte dele oriundo." (AC)

Art. 313-B. .....

"Pena – reclusão, de um a três anos, e multa. (NR)

Art. 325. .....

"Pena - reclusão, de um a três anos, e multa, se o fato não constitui crime mais grave." (NR)

Art. 3º Os provedores de acesso e de conteúdo da internet deverão cadastrar os usuários e manter por cinco anos, à disposição dos órgãos públicos, os registros de acesso e navegação, vinculados aos respectivos endereços estáticos ou dinâmicos de IP (internet protocol) dos terminais utilizados.

§ 1º O cadastro deverá conter o nome completo ou razão social, endereço, número de registro de identidade da pessoa física e número de registro no Cadastro de Pessoa Física ou Cadastro Nacional de Pessoa Jurídica do usuário na Receita Federal.

§ 2º Os provedores de acesso deverão cadastrar seus novos usuários a partir da publicação desta lei e terão o prazo de noventa dias depois da publicação para completar os cadastros de seus antigos usuários.

§ 3º O não atendimento ao disposto no ***caput*** e nos parágrafos anteriores implicará na aplicação de multa à empresa responsável, no valor de R$ 1.000,00 ou o equivalente ao dano causado, se maior, por evento, acrescida de um terço na reincidência.

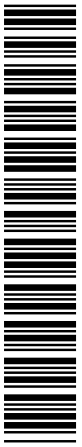
Art. 4º As multas previstas nesta Lei serão impostas pelo órgão gestor de telecomunicações, mediante provocação da autoridade não atendida na solicitação.

Parágrafo único. Os recursos financeiros resultantes do recolhimento de multas estabelecidas nesta Lei serão destinados, 95% ao Fundo Nacional de Segurança Pública – FNSP, de que trata a Lei nº 10.201, de 14 de fevereiro de 2001 e 5% ao Fundo de Fiscalização das Telecomunicações – Fistel, criado pela Lei nº 5.070, de 7 de julho de 1966.

Art. 5º Esta lei entra em vigor na data de sua publicação.

JUSTIFICAÇÃO

Tornou-se rotina para milhões de brasileiros acessar a internet para ler notícias, enviar um e-mail, pagar contas, fazer compras ou participar de uma conversa on line. Embora aparentemente inofensivas tais condutas, elas estão sujeitas ao ataque de hackers, crackers e phreakers, especialistas em invadir sites, capturar senhas e causar danos a bases de dados diversas. Dada a expansão do sistema de telefonia móvel, com acesso à internet, tal risco está onipresente, dispensando até a rede física de computadores.



Embora a diferença entre o mundo real e o virtual, este induz o usuário a ser negligente, pela aparente inofensividade, a não tomar cuidados que adotaria no mundo real. Assim, deixar o computador aberto e logado sem usuário é o mesmo que deixar a porta de casa aberta; abrir um e-mail de remetente desconhecido ou um anexo suspeito é o mesmo que confiar totalmente em estranhos; usar o computador sem antivírus e firewall é o mesmo que dirigir sem cinto de segurança.

Aparecido Francisco (*Número de fraudes e golpes na rede impressiona*) informa que estudo da Universidade de Maryland comprovou custar US$ 21,6 bilhões por ano a empresas norte-americanas o tempo desperdiçado para apagar um spam, praga recebida por 75% dos internautas adultos diariamente. Quase 20.000 mensagens diárias forçam os usuários a gastarem cerca de três minutos com elas. Dos receptores, 14% lêem o conteúdo dos spams, e apenas 4% adquirem algum produto ofertado. Nos Estados Unidos, os golpes via internet causaram prejuízo de US$ 265 milhões aos consumidores no ano passado, segundo levantamento da Federal Trade Commission, órgão regulador do comércio, estimando que as perdas médias por consumidor ficaram em torno de US$ 214 nas transações on line.

No Brasil, segundo país em número de hackers, em 2004 o número de fraudes bancárias e financeiras realizadas via internet cresceu 577%, segundo balanço do Grupo de Resposta a Incidentes para a Internet Brasileira (NBSO), mantido pelo Comitê Gestor da Internet. De 2003 para 2004 houve um aumento de 1% para 5% desse tipo de crime na rede.

Ataques por “cavalos-de-tróia” (Trojan), mecanismos virtuais (spywares = espiões) que induzem o usuário a fornecer informações sigilosas como senhas ou dados bancários, cresceram 1.184% no Brasil entre julho e dezembro do ano passado, segundo levantamento realizado pelas empresas de segurança Winco e Grisoft, contra 293% em países. Identificam-se quinze novos cavalos-de-tróia diários e o dobro nos finais de semana. Durante um ano foram detectados 1.054 modelos de golpes diferentes.

Entre as ocorrências mais freqüentes estão mensagens que afirmam que o usuário está com o nome cadastrado em órgãos de proteção ao crédito (Serasa/SPC), que oferecem ensaios fotográficos de atrizes, que o usuário está sendo traído ou sua empresa está sendo roubada.

Os criminosos estão em ação. No dizer de Patricia Peck (*O crime eletrônico na vida do usuário comum*), nenhuma estratégia de segurança da informação terá êxito, porém, se não incorporar os quatro níveis de controle social do Direito: 1) nível ético, os valores; 2) nível cultural, a educação; 3) nível tecnológico, os processos; e 4) nível legal, as normas.

Deve se aliar o nível legal ao cultural, estabelecendo regras mínimas para a proteção dos interesses dos indivíduos. Tratando-se de algo novo, contudo, as leis parecem não ser ainda suficientes.

O próprio Código Penal já contempla vários crimes cujo meio de execução é a rede mundial de computadores. Dentre os mais comuns, estão os crimes contra a honra (calúnia, injúria e difamação), furto mediante fraude, estelionato, dano, violação de direito autoral, divulgação de segredo, apologia ao crime, falsa identidade e outros que movimentam bilhões de dólares por ano, como a pedofilia, o favorecimento da prostituição associado ao tráfico de seres humanos, o tráfico de drogas e o terrorismo.

Nem sempre a tipificação de uma conduta se torna fácil se não há a adequação perfeita dela com o tipo penal. A diluição do sentimento de reprovabilidade no universo interativo da internet, aliada à cominação de penas leves em certos casos, legitima o acréscimo da alínea *m*) ao inciso II do art. 61 do Código Penal, de forma a tornar uma circunstância agravante genérica o cometimento do crime pela rede mundial de computadores.

A Lei nº 9.983, de 14 de julho de 2000 acrescentou os artigos 313-A e 313-B, além de parágrafos ao art. 325 (violação de sigilo funcional), abordando especificamente o tema, mas restrito aos agentes públicos, visto que inseridos no Capítulo I do Título XI, que trata dos crimes praticados por funcionário público contra a administração em geral. Dessa forma, a mesma

conduta, se praticada pelo particular, não é alcançada pela norma, senão pela via transversa das tipificações comuns (furto, estelionato).

Propõe-se, portanto, a inserção de um Capítulo VII (crimes informáticos) no Título I da Parte Especial, corrigindo a omissão legal, mediante a adaptação dos dispositivos já existentes.

Quanto às penas cominadas nos referidos art. 313-A e 313-B, verifica-se que estão aquém da necessária reprimenda que os delitos em questão merecem. Ora, qualquer crime cometido pela internet tende a potencializar o dano causado, dado o baixo risco para o autor. Entretanto, tratando-se de crimes contra a honra, por exemplo, o risco para a vítima é infinito.

Uma das reclamações mais comuns dos profissionais da persecução criminal refere-se à dificuldade que o próprio ordenamento jurídico traz às investigações. No caso dos crimes de menor potencial ofensivo essa dificuldade se avoluma, diante do rito célere e informal a que estão submetidos os procedimentos respectivos.

Em palestra acerca de *Crimes Informáticos*, proferida no *Information Systems Security Association (ISSA)*, em 27 out. 2004, a Delegada de Polícia Lúcia Lacerda, Diretora da Divisão de Combate aos Crimes de Alta Tecnologia, da Polícia Civil do Distrito Federal, lembrou que o efeito dissuasório e repressivo de um Termo Circunstanciado, procedimento aplicável a tais crimes, é mínimo, quase não produzindo abalo psicológico no infrator, no sentido da reprovabilidade do ato cometido.

A Lei nº 10.259/2001 equiparou os crimes apenados com até dois anos de detenção aos de menor potencial ofensivo conceituados na Lei nº 9.099/1905. de maneira que o resultado imediato da prisão em flagrante do infrator será sua imediata soltura, sem ao menos prestar fiança.

Acreditamos que as proposições em andamento têm um ponto falho em relação às penas, visto que, em quase todas é cominada pena de detenção. Para corrigir a distorção, proponho exasperar a pena dos artigos

mencionados, para reclusão. Incluo, também, a modalidade culposa, à qual, por sua natureza, é cominada pena de detenção.

Outra particularidade quanto à pena de reclusão é que ela confere maior efetividade à persecução criminal. Apenas os crimes apenados com reclusão permitem decretação das prisões temporária e preventiva e a manutenção da prisão em flagrante, bem como a interceptação de comunicações telefônicas e de sistemas de informática e telemática.

Tanto os casos de prisão cautelar como o de interceptação revestem-se de importância crucial para o sucesso das investigações. A segregação possibilita a indicação do corpo de delito e identificação de eventuais comparsas, bem como impede a continuidade delitiva. A interceptação leva à convergência dos indícios para a comprovação de materialidade e autoria, especialmente no caso de concurso de pessoas e pluralidade de vítimas.

De nada adiantaria, porém, criminalizar as condutas, se não se preservassem os indícios e provas do delito. Dessa forma, o Projeto determina aos provedores de acesso o cadastramento dos usuários e preservação dos dados referentes a acesso e navegação por cinco anos, para efetivo rastreamento policial.

O não atendimento à determinação implica o pagamento de multa, a ser aplicada pela agência gestora de telecomunicações, por solicitação da autoridade que verificar a irregularidade, o que confere agilidade ao procedimento e efetivo caráter cogente à norma. A receita decorrente reverterá em benefício do citado órgão gestor e das instituições policiais, visando a coibir a prática criminosa.

Em razão da urgente necessidade de se disciplinar a matéria no tocante aos tópicos enfocados e diante da escalada criminosa na rede mundial de computadores, solicito aos ilustres Pares o apoio para a aprovação do presente Projeto.

Sala das Sessões, em de de 2005.

Deputado Antonio Carlos Mendes Thame

2005.12424.260