



Governos já preparam leis para conter cybercrimes

Sabotagem, roubo de informações armazenadas em arquivos eletrônicos, invasões e fraudes financeiras pela Internet são os crimes da moda.

Recentemente, o ministro da Justiça, José Carlos Dias, reuniu-se com representantes de 32 países em encontro promovido pela Organização dos Estados Americanos (OEA). No encontro foi discutida a elaboração de um instrumento legal único, para todos os países integrantes da OEA, voltado para o combate à criminalidade na Internet. Ficou estabelecido que regras conjuntas deverão ser criadas de maneira compatível com as leis internas de cada país.

No Brasil há dois projetos de lei que tratam dos “cybercrimes” e suas punições. Um deles é projeto de lei 84/99, do deputado Luiz Piauhyllino (PSDB/PE), já aprovado por unanimidade na Comissão de Ciência e Tecnologia da Câmara, aguarda parecer da Comissão de Constituição e Justiça.

O outro (projeto de lei 76/00) foi apresentado pelo senador e ex-ministro da Justiça Renan Calheiros em março e encontra-se na Comissão de Educação do Senado. O prazo para emendas à proposta terminou nesta terça-feira (4/4). *Leia íntegra dos projetos no final da reportagem.*

Os dois projetos definem como crimes a destruição de dados ou sistemas de computação, a apropriação de dados alheios e o uso indevido de dados ou registros sem que seus titulares tenham consentido. São considerados delitos on-line também a modificação ou adulteração de informações, a programação de instruções que ocasionem um bloqueio do sistema, a retirada de informação privada armazenada em base de dados e a divulgação de material pornográfico na rede. As penas previstas variam de 1 mês de detenção a seis anos de reclusão, acrescidos de multa.

O projeto do senador Renan Calheiros é mais específico na determinação das práticas que serão considerados crimes. Pela proposta, é crime a alteração ou transferência de contas representativas de valores, a difusão de material injurioso, o uso da informática para ativar explosivos, alteração de registros de operações tributárias e a sonegação de tributos decorrentes de operações virtuais.

A corrupção de menores e a divulgação de mensagens contrárias aos bons costumes, a interferência em programas relacionados a armamentos, a indução a atos de subversão e a veiculação de mensagens ameaçadoras à soberania nacional também são classificados como crime no texto de Calheiros.

Esse detalhamento do projeto que tramita no Senado é visto com reservas por especialistas. De acordo com o advogado Alexandre Jean Daoun, a proposta do ex-ministro da Justiça, por ser específica e objetiva demais, pode se tornar obsoleta em pouco tempo, dada a rapidez das mudanças que ocorrem no campo da informática.

O advogado Renato Opice Blum, por sua vez, notou que o projeto de lei do Senado não define como crime a navegação desautorizada no site de outras pessoas. Para Blum, a inexistência de punição para a entrada de um hacker num determinado site permite que o direito à privacidade seja desrespeitado.



Os dois advogados entendem que certos cybercrimes já são regulados pela legislação penal em vigor atualmente. Segundo eles, a aplicação do Código Penal aos crimes cometidos na Internet depende da definição de “coisa alheia móvel” (artigo 155 do Código Penal).

Se os dados de computador forem incluídos no conceito de coisa alheia móvel, os cybercrimes serão punidos pela legislação penal em vigor. Assim, a transferência de dinheiro de conta bancária alheia por um hacker que obteve a senha invadindo sites na Internet, seria considerada furto.

Quando o Código Penal foi sancionado (1940), eram considerados “coisa” somente elementos que tivessem existência material (que pudessem ser tocados).

A autora do livro “O Direito na era digital”, Sandra Gouveia, defendeu a regulamentação dos cybercrimes pelas leis já existentes. Segundo parecer de um professor de física (que a autora anexou a seu livro), a materialização das informações digitais é possível mediante a formação de campos magnéticos.

Regulamentação internacional

Pesquisa feita pelo Serviço Federal de Investigações (FBI) dos Estados Unidos, em San Francisco, aponta que os prejuízos financeiros das empresas americanas em função dos “cybercrimes”, em 1999, atingiram o valor de US\$ 266 milhões e afetaram 70% das corporações. Agências governamentais e bancos americanos tiveram a segurança de seus computadores violada.

Em fevereiro deste ano, sites da Internet, como Yahoo!, eBay e Amazon.com, foram invadidos por hackers. O mesmo procedimento utilizado contra esses sites pode ser aplicado a transações “business to business” (entre empresas) e a compras de produtos via Internet.

A secretária da Justiça dos EUA, Janet Reno, publicou um relatório que trata dos “cybercrimes” e sua prevenção, intitulado “A Fronteira Eletrônica: O Desafio de uma Conduta Ilegal Envolvendo o Uso da Internet” (endereço na Web: www.usdoj.gov/criminal/cybercrime).

Segundo Janet, apesar das leis já existentes cobrirem muitos dos crimes on-line nos EUA, a Internet traz “novos desafios”, como a dificuldade de identificação dos “cybercriminosos” e também de definir sua localização (pois em muitos casos eles se encontram em outros países).

Na Internet, qualquer pessoa, inclusive potenciais criminosos, podem permanecer no anonimato porque a estrutura da rede permite a adoção de falsa identidade e o fornecimento de dados pessoais incorretos.

Para Janet, até as provas de crimes na Internet podem ser facilmente alteradas. Por isso, os países em conjunto devem pesquisar meios que assegurem a integridade dessas provas, de maneira que elas sejam reconhecidas no plano internacional.

Em palestra ministrada para o Grupo G8, em 1997, Janet Reno, alertou para a pouca atenção dada pela



comunidade internacional aos “cybercrimes” e sugeriu a formação de um consenso internacional para criar instrumentos de combate a esses crimes.

Confira os projetos que tramitam no Congresso

PROJETO DE LEI DO SENADO 76, DE 2000.

Define e tipifica os delitos informáticos, e dá outras providências.

O CONGRESSO NACIONAL decreta,

Art. 1º Constitui crime de uso indevido da informática:

§ 1º contra a inviolabilidade de dados e sua comunicação:

I – a destruição de dados ou sistemas de computação, inclusive sua inutilização;

II – a apropriação de dados alheios ou de um sistema de computação devidamente patenteados;

III – o uso indevido de dados ou registros sem consentimento de seus titulares;

IV – a modificação, a supressão de dados ou adulteração de seu conteúdo;

V – a programação de instruções que produzam bloqueio geral no sistema ou que comprometam a sua confiabilidade.

Pena: detenção, de um a seis meses e multa.

§2º contra a propriedade e o patrimônio:

I – a retirada de informação privada contida em base de dados;

II – a alteração ou transferência de contas representativas de valores;

Pena: detenção, de um a dois anos e multa.

§ 3º contra a honra e a vida privada:

I – difusão de material injurioso por meio de mecanismos virtuais;

II – divulgação de informações sobre a intimidade das pessoas sem prévio consentimento;

Pena: detenção, de um a seis meses e multa.

§ 4º contra a vida e integridade física das pessoas:

I – o uso de mecanismos da informática para ativação de artefatos explosivos, causando danos, lesões ou



homicídios;

II – a elaboração de sistema de computador vinculado a equipamento mecânico, constituindo-se em artefato explosivo;

Pena: reclusão, de um a seis anos e multa.

§ 5º contra o patrimônio fiscal :

I – alteração de base de dados habilitadas para registro de operações tributárias;

II – evasão de tributos ou taxas derivadas de transações “virtuais”;

Pena: detenção, de um a dois anos e multa.

§ 6º contra a moral pública e opção sexual:

I – a corrupção de menores de idade;

II – divulgação de material pornográfico;

III – divulgação pública de sons, imagens ou informação contrária aos bons costumes.

Pena: reclusão, de um a seis anos e multa.

§ 7º contra a segurança nacional:

I – a adulteração ou revelação de dados declarados como reservados por questões de segurança nacional;

II – a intervenção nos sistemas de computadores que controlam o uso ou ativação de armamentos;

III – a indução a atos de subversão;

IV – a difusão de informação atentatória a soberania nacional.

Pena: detenção, de um a dois anos e multa.

Art. 2º Os crimes tipificados nos §§ 1º a 3º são ações penais públicas condicionadas a representação e os demais ações penais incondicionadas.

Art. 3º Qualquer um desses crimes que venha a ser praticado contra empresa concessionária de serviços públicos, sociedades de economia mista ou sobre qualquer órgão integrante da administração pública terão suas penas aumentadas para dois a seis meses e multa, nos casos dos §§1º e 3º e de um ano e seis meses a dois anos e seis meses e multa nos demais casos.

Art. 4º Caso seja praticado qualquer um dos crimes tipificados nesta Lei como meio de realização ou facilitação de outro crime, fica caracterizada a circunstância agravante qualificadora, aumentando-se a



pena de um terço até a metade.

Art. 5º Todos os crimes por uso indevido de computador estão sujeitos a multa igual ao valor do proveito pretendido ou do risco de prejuízo da vítima.

Art. 6º Esta lei entra em vigor na data de sua publicação.

PROJETO DE LEI 84, DE 1999

(Do deputado Luiz Piauhyllino – PSDB/PE)

Dispõe sobre os crimes cometidos na área de informática, suas penalidades e dá outras providências.

Capítulo I

Dos princípios que regulam a prestação de serviço por redes de computadores

Art. 1º . O acesso, o processamento e a disseminação de informações através das redes de computadores devem estar a serviço do cidadão e da sociedade, respeitados os critérios de garantia dos direitos individuais e coletivos de privacidade e segurança de pessoas físicas e jurídicas e da garantia de acesso às informações disseminadas pelos serviços da rede.

Art. 2º . É livre a estruturação e o funcionamento das redes de computadores e seus serviços, ressalvadas as disposições específicas reguladas em lei.

Capítulo II

Do uso de informações disponíveis em computadores ou redes de computadores

Art. 3º . Para fins desta lei, entende-se por informações privadas aquelas relativas a pessoa física ou jurídica identificada ou identificável.

Parágrafo Único. É identificável a pessoa cuja individuação não envolva custos ou prazos desproporcionados.

Art. 4º . Ninguém será obrigado a fornecer informações sobre sua pessoa ou de terceiros, salvo nos casos previstos em lei.

Art. 5º . A coleta, o processamento e a distribuição, com finalidades comerciais, de informações privadas ficam sujeitas à prévia aquiescência da pessoa a que se referem, que poderá ser tornada sem efeito a qualquer momento, ressalvando-se o pagamento de indenizações a terceiros, quando couberem.

Parágrafo 1º. A toda pessoa cadastrada dar-se-á conhecimento das informações privadas armazenadas e das respectivas fontes.



Parágrafo 2o. Fica assegurado o direito à retificação de qualquer informação armazenada incompleta.

Parágrafo 3o. Salvo por disposição legal ou determinação judicial em contrário, nenhuma informação privada será mantida à revelia da pessoa a que se refere ou além do tempo previsto para sua validade.

Parágrafo 4o. Qualquer pessoa física ou jurídica tem o direito de interpelar o proprietário da rede de computadores ou provedor de serviço para saber se mantém informações a seu respeito, e o respectivo teor.

Art. 6o . os serviços de informações ou de acesso a bancos de dados não distribuirão informações privadas referentes, direta ou indiretamente, a origem racial, opinião política, filosófica, religiosa ou de orientação sexual e de filiação a qualquer entidade, pública ou privada, salvo autorização expressa do interessado.

Art. 7o . O acesso de terceiros não autorizados pelos respectivos interessados a informações privadas mantidas em redes de computadores dependerá de prévia autorização judicial.

Capítulo III

Seção I

Dano a dado ou programa de computador

Art. 8o . Apagar, destruir, modificar ou de qualquer forma inutilizar, total ou parcialmente, dado ou programa de computador, de forma indevida ou não autorizada.

Pena: detenção, de um a três anos e multa.

Parágrafo único. Se o crime é cometido:

I – contra interesse da União, Estado, Distrito Federal, município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;

II – com considerável prejuízo para a vítima;

III – com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;

IV – com abuso de confiança;

V – por motivo fútil;

VI – com uso indevido de senha ou processo de identificação de terceiro;

VII – com a utilização de qualquer outro meio fraudulento.



Pena: detenção, de dois a quatro anos e multa.

Seção II

Acesso indevido ou não autorizado

Art. 9o . Obter acesso indevido ou não autorizado a computador ou rede de computadores.

Pena: detenção, de seis meses a um ano e multa.

Parágrafo 1o . Na mesma pena incorre quem sem autorização, ou indevidamente, obtém, mantém ou fornece a terceiro qualquer meio de identificação ou acesso a computador ou rede de computadores.

Parágrafo 2o . Se o crime é cometido:

I – com acesso a computador ou rede de computadores da União, Estado, Distrito Federal, município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;

II – com considerável prejuízo para a vítima;

III – com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;

IV – com abuso de confiança;

V – por motivo fútil;

VI – com uso indevido de senha ou processo de identificação de terceiro;

VII – com a utilização de qualquer outro meio fraudulento.

Pena: detenção, de um a dois anos e multa.

Seção III

Alteração de senha ou mecanismo de acesso a programa de computador ou dados

Art. 10. Apagar, destruir, alterar, ou de qualquer forma inutilizar, senha ou qualquer outro mecanismo de acesso a computador, programa de computador ou dados, de forma indevida ou não autorizada.

Pena: detenção, de um a dois anos e multa.

Seção IV

Obtenção indevida ou não autorizada de dado ou instrução de computador

Art. 11. Obter, manter ou fornecer, sem autorização ou indevidamente, dado ou instrução de computador.

Pena: detenção, de três meses a um ano e multa.

Parágrafo único. Se o crime é cometido:

I – com acesso a computador ou rede de computadores da União, Estado, Distrito Federal, município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;

II – com considerável prejuízo para a vítima;

III – com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;

IV – com abuso de confiança;

V – por motivo fútil;

VI – com uso indevido de senha ou processo de identificação de terceiro;

VII – com a utilização de qualquer outro meio fraudulento.

Pena: detenção, de um a dois anos e multa.

Seção V

Violação de segredo armazenado em computador, meio magnético, de natureza magnética, optica ou similar

Art. 12. Obter segredos de indústria ou comércio ou informações pessoais armazenadas em computador, rede de computadores, meio eletrônico de natureza magnética, optica ou similar, de forma indevida ou não autorizada.

Pena: detenção, de um a três anos e multa.

Seção VI

Criação, desenvolvimento, ou inserção em computador de dados ou programa de computador com fins nocivos

Art.13. Criar, desenvolver ou inserir dado ou programa em computador ou rede de computadores, de forma indevida ou não autorizada, com a finalidade de apagar, destruir, inutilizar ou modificar dado ou programa de computador ou de qualquer dificultar ou impossibilitar, total ou parcialmente, a utilização de computador ou rede de computadores.



Pena: reclusão, de uma a quatro anos e multa.

Parágrafo único. Se o crime é cometido:

I – contra interesse da União, Estado, Distrito Federal, município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;

II – com considerável prejuízo para a vítima;

III – com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;

IV – com abuso de confiança;

V – por motivo fútil;

VI – com uso indevido de senha ou processo de identificação de terceiro;

VII – com a utilização de qualquer outro meio fraudulento.

Pena: reclusão, de dois a seis anos e multa.

Seção VII

Veiculação de pornografia através da rede de computadores

Art. 14. Oferecer serviço ou informação de caráter pornográfico, em rede de computadores, sem exibir previamente, de forma facilmente visível e destacada, aviso sobre sua natureza, indicando o seu conteúdo e a inadequação para criança ou adolescentes.

Pena: detenção, de um três anos e multa.

Capítulo IV

Art. 15. Se qualquer dos crimes previstos nessa lei é praticado no exercício da atividade profissional ou funcional, a pena é aumentada de um sexto até a metade.

Art. 16. Nos crimes definidos nessa lei somente se procede mediante representação do ofendido, salvo se cometidos contra interesse da União, Estado, Distrito federal, município, órgão ou entidade da administração direta ou indireta, empresa concessionária de serviços públicos, fundação mantidas ou instituídas pelo poder público, serviços sociais autônomos, instituições financeiras ou empresas a que explorem ramo de atividade controlada pelo Poder Público, casos em que a ação é pública incondicionada.

Art. 17. Esta lei regula os crimes relativos à informática sem prejuízo das demais cominações previstas em outros diplomas legais.



Art. 18. Esta lei entra em vigor 30 (trinta) dias a contar da data de sua publicação.

Date Created
04/04/2000