COMISSÃO DE CIÊNCIA E TECNOLOGIA, COMUNICAÇÃO E INFORMÁTICA

PROJETO DE LEI Nº 84, DE 1999

(Substitutivo do Senado Federal)

Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), o Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), a Lei nº 7.716, de 5 de janeiro de 1989, a Lei nº 8.069, de 13 de julho de 1990, e a Lei nº 10.446, de 8 de maio de 2002, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra dispositivos de comunicação ou sistemas informatizados e similares, e dá outras providências.

Autor: SENADO FEDERAL

Relator: Deputado EDUARDO AZEREDO

I – RELATÓRIO

Tramita nesta Comissão, em regime de urgência, o substitutivo do Senado Federal ao Projeto de Lei nº 84, de 1999, este aprovado pelo Plenário da Câmara dos Deputados em novembro de 2003. O texto está sujeito à apreciação do Plenário.

O texto original do Projeto de Lei nº 84, de 1999, de autoria do Deputado Luiz Piauhylino, introduzia no Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal – as seguintes tipificações penais:

- **Acesso indevido a meio eletrônico: "**Art. 154-A. Acessar, indevidamente ou sem autorização, meio eletrônico ou sistema informatizado", estabelecendo pena de detenção, de três meses a um ano, e multa;

- **Manipulação indevida de informação eletrônica: "**Art. 154-B. Manter ou fornecer, indevidamente ou sem autorização, dado ou informação presente em ou obtida de meio eletrônico ou sistema informatizado", estabelecendo pena de detenção, de seis meses a um ano, e multa;

- **Difusão de vírus eletrônico:** criação, inserção ou difusão de dado ou informação em meio eletrônico ou sistema informatizado, indevidamente ou sem autorização, com a finalidade de destruí-lo, inutilizá-lo, modificá-lo ou dificultar-lhe o funcionamento;

- **Falsificação de cartão de crédito:** Equiparando-se a documento particular o cartão de crédito ou débito;

- **Falsificação de telefone celular ou meio de acesso a sistema eletrônico:** Art. 298-A. Criar ou copiar, indevidamente ou sem autorização, ou falsificar código, seqüência alfanumérica, cartão inteligente, transmissor ou receptor de radiofreqüência ou de telefonia celular ou qualquer instrumento que permita o acesso a meio eletrônico ou sistema informatizado, estabelecendo pena de reclusão de um a cinco anos, e multa.

- Dano eletrônico: Equiparando à "coisa" "o dado, a informação ou a base de dados presente em meio eletrônico ou sistema informatizado, e a "senha ou qualquer meio de identificação que permita o acesso a meio eletrônico ou sistema informatizado".

- Pornografia infantil: Art. 218-A. Fotografar, publicar ou divulgar, por qualquer meio, cena de sexo explícito ou pornográfica envolvendo criança ou adolescente, estabelecendo pena de reclusão, de um a quatro anos, e multa.

Além dessas novas tipificações penais, o texto também propunha a modificação dos artigos 265 e 266 do Código Penal, que passariam a vigorar com as seguintes redações:

- Atentado contra a segurança de serviço de utilidade pública: "Art. 265 Atentar contra a segurança ou o funcionamento de serviço

de água, luz, força, calor ou telecomunicação, ou qualquer outro de utilidade pública";

- **Interrupção ou perturbação de serviço telegráfico ou telefônico:** Art. 266. Interromper ou perturbar serviço telegráfico, radiotelegráfico, telefônico ou de telecomunicação, impedir ou dificultar-lhe o restabelecimento.

O texto, aprovado pelo Plenário da Câmara dos Deputados em novembro de 2003, foi enviado ao Senado Federal, que optou por oferecer um substitutivo, contendo vinte e três artigos, os quais dispõem de novas tipificações penais, além de obrigações administrativas aos provedores de acesso à Internet, conforme detalharemos a seguir.

Tipificações penais

- **Acesso não autorizado a rede de computadores, dispositivo de comunicação ou sistema informatizado: "**Art. 285-A. Acessar, mediante violação de segurança, rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso". A pena proposta é de reclusão, de 1 (um) a 3 (três) anos, e multa;

- Obtenção, transferência ou fornecimento não autorizado de dado ou informação: "Art. 285-B. Obter ou transferir, sem autorização ou em desconformidade com autorização do legítimo titular da rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso, dado ou informação neles disponível". A pena proposta é de reclusão, de 1 (um) a 3 (três) anos, e multa;

- Divulgação ou utilização indevida de informações e dados pessoais: "Art. 154-A. Divulgar, utilizar, comercializar ou disponibilizar dados e informações pessoais contidas em sistema informatizado com finalidade distinta da que motivou seu registro, salvo nos casos previstos em lei ou mediante expressa anuência da pessoa a que se referem, ou de seu representante legal". A pena proposta é de detenção, de 1 (um) a 2 (dois) anos, e multa;

- **Dano:** Alteração no art. 163 do Código Penal – "Destruir, inutilizar ou deteriorar coisa alheia ou dado eletrônico alheio";

- **Inserção ou difusão de código malicioso:** “Art. 163-A. Inserir ou difundir código malicioso em dispositivo de comunicação, rede de computadores, ou sistema informatizado”, estabelecendo pena de reclusão, de 1 (um) a 3 (três) anos, e multa;

- **Inserção ou difusão de código malicioso seguido de dano: “**Se do crime resulta destruição, inutilização, deterioração, alteração, dificultação do funcionamento, ou funcionamento desautorizado pelo legítimo titular, de dispositivo de comunicação, de rede de computadores, ou de sistema informatizado”, pena de reclusão, de 2 (dois) a 4 (quatro) anos, e multa.

- **Estelionato Eletrônico: “**difunde, por qualquer meio, código malicioso com intuito de facilitar ou permitir acesso indevido à rede de computadores, dispositivo de comunicação ou sistema informatizado. Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte.

- **Atentado contra a segurança de serviço de utilidade pública:** alteração no art. 265 - “Atentar contra a segurança ou o funcionamento de serviço de água, luz, força, calor, informação ou telecomunicação, ou qualquer outro de utilidade pública”;

- **Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático, dispositivo de comunicação, rede de computadores ou sistema informatizado:** alteração no art. 266 - Interromper ou perturbar serviço telegráfico, radiotelegráfico, telefônico, telemático, informático, de dispositivo de comunicação, de rede de computadores, de sistema informatizado ou de telecomunicação, assim como impedir ou dificultar-lhe o restabelecimento.

- **Falsificação de dado eletrônico ou documento público:** Art. 297. Falsificar, no todo ou em parte, dado eletrônico ou documento público, ou alterar documento público verdadeiro;

- **Falsificação de dado eletrônico ou documento particular:** Art. 298. Falsificar, no todo ou em parte, dado eletrônico ou documento particular ou alterar documento particular verdadeiro.

Essas mesmas tipificações penais propostas para o Código Penal Civil são introduzidas no Código Penal Militar – Decreto-Lei nº 1.001, de 21 de outubro de 1969 – por intermédio dos artigos 10 ao 15 do substitutivo.

O artigo 17 do substitutivo define como “bens protegidos” o dado, o dispositivo de comunicação, a rede de computadores, o sistema informatizado, e o 18 estabelece que os órgãos da polícia judiciária estruturarão setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.

É introduzida também uma nova previsão na Lei de combate ao Racismo, de forma a obrigar a “cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas, ou da publicação por qualquer meio” de mensagens de conteúdo discriminatório ou preconceituoso relativo à raça, cor, etnia, religião ou procedência nacional.

O artigo 20 tipifica com penas mais severas a prática de pornografia infantil, e o 21, por sua vez, inclui no rol de competências legais do Departamento de Polícia Federal os “delitos praticados contra ou mediante rede de computadores, dispositivo de comunicação ou sistema informatizado”.

Finalmente, o artigo 22 trata de obrigações para os provedores do serviço de acesso à Internet no Brasil:

- manter em ambiente controlado e de segurança, pelo prazo de 3 (três) anos, com o objetivo de provimento de investigação pública formalizada, os dados de endereçamento eletrônico da origem, hora, data e a referência GMT da conexão efetuada por meio de rede de computadores e fornecê-los exclusivamente à autoridade investigatória mediante prévia requisição judicial. Estes dados, as condições de segurança de sua guarda e o processo de auditoria à qual serão submetidos serão definidos nos termos de regulamento.

- preservar imediatamente, após requisição judicial, outras informações requisitadas em curso de investigação, respondendo civil e penalmente pela sua absoluta confidencialidade e inviolabilidade;

- informar, de maneira sigilosa, à autoridade competente, denúncia que tenha recebido e que contenha indícios da prática de crime sujeito a acionamento penal público incondicionado, cuja perpetração haja ocorrido no âmbito da rede de computadores sob sua responsabilidade.

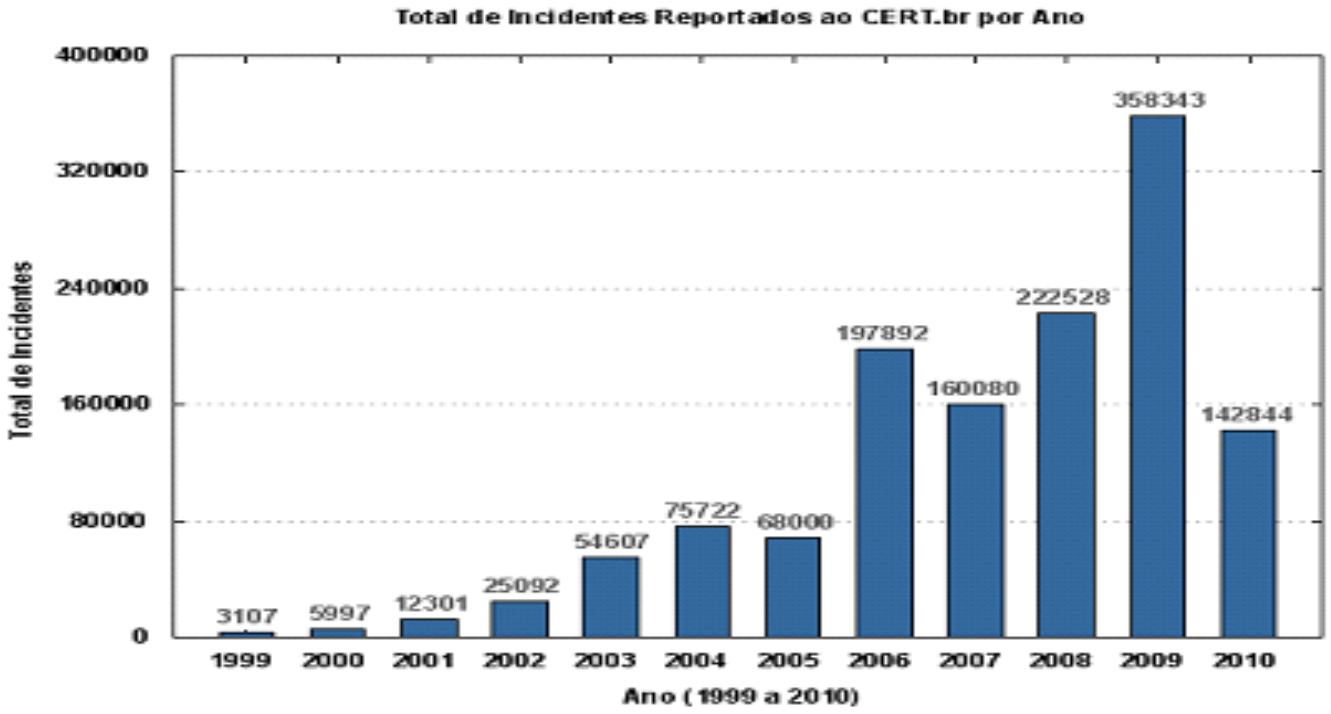
Por fim, a vigência da nova lei é fixada para cento de vinte dias após a data de sua publicação.

O substitutivo do Senado Federal foi distribuído, também, para a apreciação da Comissão de Segurança Pública e Combate ao Crime Organizado e Comissão de Constituição e Justiça.

É o Relatório.

II – VOTO DO RELATOR

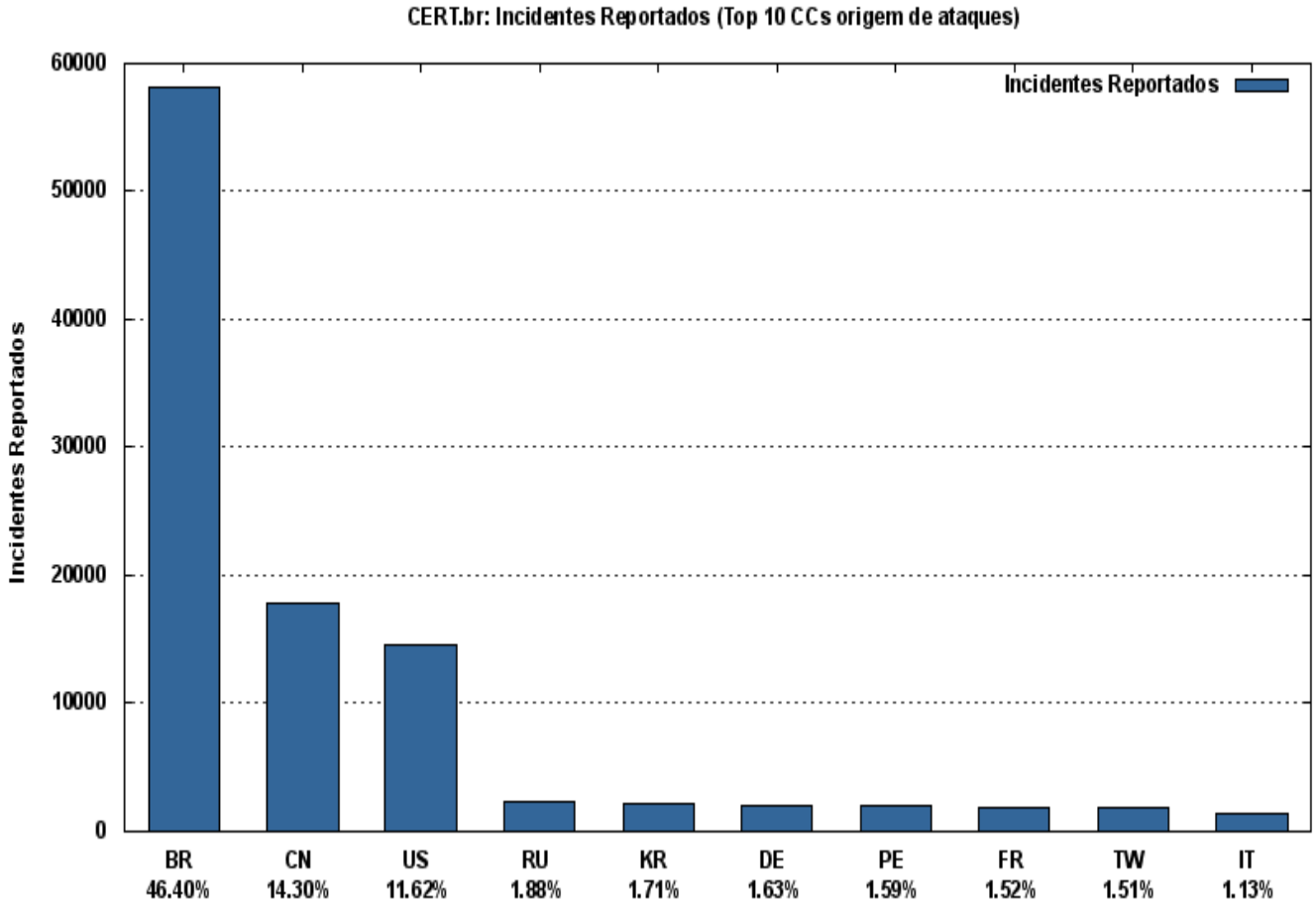
A ocorrência de crimes por meio da Internet – os chamados crimes cibernéticos – vinha se expandindo de forma exponencial até 2009. Em 2010, porém, ocorreu uma redução significativa, conforme mostrado



no gráfico abaixo.

Apesar da queda de incidentes reportados ao CERT.BR - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil – em 2010, o número ainda é elevado e chama a atenção o fato de que os ataques ocorridos na Internet brasileira provêm, em sua maioria, de sistemas localizados fisicamente no próprio Brasil, seguido de China e dos Estados Unidos da América, conforme mostrado abaixo.

Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2010



Os dados acima, provenientes das estatísticas oficiais de incidentes reportados ao CERT.BR mostram uma situação de insegurança na Internet brasileira.

Em âmbito internacional a situação não é diferente. O Relatório de acompanhamento de crimes na Internet de 2010 do FBI – órgão de investigação federal do governo dos Estados Unidos – indica que o número de reclamações recebidas por aquele órgão, aponta que a criminalidade na Internet atingiu, em 2010, um total de 303.809 queixas, o que corresponde ao segundo nível mais elevado em sua série histórica de dez anos.

As fraudes financeiras on-line reportadas ao FBI em 2008 atingiram o montante de US$ 265 milhões. O prejuízo financeiro médio que sofreram os cidadãos americanos vítimas de fraudes on-line foi de U$ 931,00, sendo que esse valor cresce com a faixa etária, mostrando que quanto mais idoso o cidadão, mais susceptível à criminalidade on-line.

Um outro indicador que chama a atenção é o que mostra a evolução das fraudes relacionadas aos cartões de débito e de crédito, que, no ano de 2008, segundo o FBI, totalizaram 9% do total das ocorrências criminosas na Internet.

O relatório do FBI aponta também que as fraudes cibernéticas estão se tornando mais sofisticadas e recomenda atenção, por parte das autoridades públicas, empresas e cidadãos, para o uso consciente da Internet com o emprego de mecanismos eficientes de segurança, pois a criminalidade digital está orientada ao mercado global, e tem na incapacidade dos consumidores de distinguir entre atividades on-line legítimas e fraudulentas uma aliada.

Isso torna evidente que a criminalidade na Internet é uma ameaça grave não só às economias dos países, como impõe prejuízos financeiros significativos aos cidadãos.

Destaque-se, aqui, inclusive, um fenômeno tipicamente brasileiro, que não pode ser desconsiderado neste cenário: trata-se do fato, incontestável, de que os serviços públicos nacionais – da União, dos Estados, dos Municípios – e respectivos órgãos da administração direta e indireta – vão ganhando, cada vez mais, ações e produzindo benefícios públicos e ofertando serviços preponderantemente pela internet.

O e-gov, denominação do programa oficial de serviços eletrônicos da União, produziu facilidades para a população, que ganharam destaque internacional, como, por exemplo, a imensa proporção dos envios de ajuste fiscal - a conhecida declaração anual de imposto de renda, à Receita Federal -, e os acessos aos serviços da Previdência, os serviços de licenciamento de veículos, obtenção de certidões tributárias on-line, entre outros.

O interesse coletivo público da população passa por estas inovadoras aplicações, que se utilizam preponderantemente da Internet e dos sistemas eletrônicos, motivo pelo qual o mesmo interesse público não pode se sujeitar, cada dia mais, à riscos crescentes de craqueamento, invasões, pichações, atentados, sem mínima resposta do aparato repressivo do próprio Estado, que, todos sabemos, deve, por sua vez, agir sob estrita legalidade em matéria penal.

Não se pode deixar, também, de mencionar, aqui, o fato de que o Poder Judiciário brasileiro, através de ações coordenadas, em todo o país, pelo Conselho Nacional de Justiça, e de outras ações locais e regionais, dos Tribunais Federais, do Trabalho, e Estaduais, dá franco prosseguimento à automação judiciária, através da transformação progressiva do processo

judicial, em papel, no processo eletrônico, hoje apoiado pela Lei Federal 11.419/2006, que deu novo ar, de tecnologia da informação, à estrutura de solução de litígios do país.

Sistemas judiciários eletrônicos de grande fator de inovação neste campo – como o PROJUDI (Processo Judicial Eletrônico), o agora recém-lançado pelo CNJ, PJE-Processo Judicial Eletrônico do CNJ, dentre outros – estão começando a transformar a justiça brasileira num cenário de inovação inédita, em que os litígios, os interesses conflituosos das pessoas e empresas, passam a ser processados e decididos pelo emprego de equipamentos eletrônicos, redes de computadores e de telecomunicações e bancos de dados, tendo como usuários os juízes, promotores, advogados, e serventuários da Justiça.

Esse acervo, por óbvio, não pode ser exposto, em razão da sensível ligação que possui com o interesse nacional, à ação impune de pessoas mal intencionadas, exigindo previsão mínima de resposta penal para ações que podem ser interna e externamente aviadas, agora, contra a Justiça eletrônica do país.

Além disso, é importante apontar que o desafio de combater o crime praticado na Internet se impõe a todos os países do mundo, tendo em vista que esse tipo de criminalidade guarda características particulares e diversas das tradicionais que ocorrem no mundo físico, como o caso da extraterritorialidade, da velocidade da consecução, da possibilidade de se “programar” um determinado delito para ocorrer após um determinado período de tempo em áreas geográficas específicas do planeta.

A dificuldade de produção de evidências digitais que permitam às autoridades provar a autoria dos crimes é outro aspecto característico desse problema.

Esse ponto, tratado no projeto de lei alvo deste relatório como fator inédito do cenário da investigação policial brasileira, merece destaque, na medida em que a sofisticação dos meios de implementação das ações criminosas cibernéticas diferem substancialmente dos crimes produzidos, historicamente, no meio físico.

A diferença de utilização de meios criminosos – meios eletrônicos sofisticados, como a implementação e softwares de ruptura de

ambientes protegidos por firewalls, aplicativos maldosos que se utilizam de expertises diferenciadas de programação computacional, astúcia na utilização de sistemas internos e na violação externa de recursos lógicos de segurança da informação – produz novo feitio de criminalidade, cujo estudo ganha corpo em vários locais do mundo civilizado e começa a chegar à academia brasileira: a “engenharia social”, ou, “engenharia do mal”.

Para combate a esta “engenharia” ultra especializada na prática do crime eletrônico, torna-se imprescindível habilitar o Estado brasileiro com ferramentas e conhecimentos igualmente novos, compatíveis com o poder ofensivo especializado das condutas.

A computação forense e a otimização dos Institutos de Criminalística das polícias estadual e federal, através do surgimento de investigações especializadas, com novo foco de preparação dos investigadores, habilitação técnicas dos policiais, recursos de identificação de origens e destinos de ataques cibernéticos, para suporte ao convencimento sobre o crime e sua natureza pelos delegados de polícia, dos técnicos laboratoriais de pesquisa, passam a constituir condição obrigatória da lida com esta nova feição de “elementos materiais” da prova cibernética dos crimes, o corpo de delito do crime eletrônico.

Somente a norma legal, que delimite, administrativamente, esta nova modalidade de preparação dos agentes policiais do Estado, que permita a instituição de cargos, funções, tecnologicamente suportadas, e mesmo a proporcional adequação dos orçamentos estaduais e federais, permitirá que o escopo investigatório se compatibilize com o porte especial desta modalidade criminosa.

Já o campo da extraterritorialidade da lei penal, considerada como a da possibilidade de aplicação da lei de crimes fora da jurisdição de origem, ou, na prática, a situação na qual um delito praticado em um país pode repercutir em outro, se torna especialmente séria, pois a jurisdição penal, em geral, está adstrita às fronteiras geográficas dos países.

A exemplo de realidades conhecidas, que cruzam, também, fronteiras geográficas em razão do porte e das características de suas operações tecnológicas – cite-se, como exemplo, a aviação comercial e militar – os acessos eletrônicos, depois do fenômeno “internet”, não observam,

naturalmente, fronteiras territoriais, sendo comum, na atualidade, a utilização, por nacionais, de redes e facilidades eletrônicas, de outros países.

Para tratar eventos criminosos que esta integração internacional de redes e possibilidades permite, é necessária, mesmo vital, a cooperação internacional, entre polícias e entre autoridades judiciárias, assim como certo nível de uniformidade da legislação penal.

Essa uniformidade precisa se verificar tanto em termos de Direito Material – tipificação de condutas – como em termos de Direito Processual, em face da necessidade de cooperação e atuação rápida das autoridades policiais e judiciais no combate a esse tipo de delito.

Esse contexto evidencia o fato de que a preocupação com a segurança cibernética está crescendo na direta proporção em que crescem os crimes praticados pela Internet. Nos Estados Unidos, por exemplo, o presidente Barack Obama criou um Comando dentro do Departamento de Defesa para se dedicar à guerra eletrônica.

No anúncio do novo órgão, o presidente norte-americano afirmou que “as ameaças virtuais estão entre os maiores desafios enfrentados por seu país”.

Isso é especialmente verdade ao constatarmos que os sistemas de produção e distribuição de energia elétrica, de telecomunicações, os bancos de dados de informações publicas e privadas dos governos, empresas e instituições, os registros de documentos de saúde dependem da perfeita funcionalidade da Internet.

Não é ficção imaginar uma situação em que criminosos virtuais produzam um ataque aos sistemas de gerenciamento de produção e distribuição de energia elétrica, sem bombas, sem armas, apenas com softwares, e coloquem em colapso o fornecimento de energia para a sociedade.

O mercado financeiro é outro exemplo: um ataque virtual pode colocar em colapso o sistema de pagamentos de um país, trazendo prejuízos para a economia nacional.

Além disso, os dados privados dos cidadãos, como registros financeiros, de crédito, de saúde assim como os processos e autos

judiciais estão progressivamente migrando para plataformas digitais em sistemas integrados na Internet. Acessos indevidos a tais sistemas têm o potencial de expor a vida privada de milhões de cidadãos.

Na medida em que todas essas informações pessoais migram do papel para os arquivos digitais, o roubo de identidade, por meio de falsificação de documentos e obtenção de dados pessoais, torna-se um problema ainda mais sério, e não é por outro motivo que multiplicam-se no mundo quadrilhas especializadas nesse tipo de delito, que, com milhões de identidades e números de cartões de crédito roubados, compram mercadorias em uma parte do planeta e os revendem em outros países.

Esses esquemas organizados de crimes cibernéticos estão com estruturas de tal forma sofisticadas que chegam a dispor de equipes com dezenas de consultores encarregados de “proteger” os engenheiros e analistas encarregados de cometer os crimes por intermédio da Internet, conforme mostrado no Painel de Crimes Cibernéticos do Fórum Econômico Mundial de 2009.

Esse quadro torna-se, a cada dia que passa, a cada novo cidadão que é incluído no mundo digital sem que disponha dos requisitos básicos de proteção no ambiente digital, a cada nova escola ou hospital público que se informatiza, a cada tribunal ou instância judicial que passa a operar online, a cada nova transação financeira e comercial eletrônico, mais dramático.

A urgência e a pertinência do texto que estamos analisando, portanto, é diretamente proporcional à dramaticidade da situação verificada na Internet, e não é por outro motivo que os mais avançados e importantes países do mundo estão tratando essa questão com prioridade cada vez mais elevada.

O texto que emanou do Senado Federal, assim como o que foi aprovado pela Câmara dos Deputados em novembro de 2003, aponta soluções para muitos desses desafios, além de estarem alinhados com as disposições previstas nas legislações relativas à matéria que estão sendo introduzidas em muitos países.

É evidente que legislar sobre uma tecnologia tão recente e tão sofisticada e que está produzindo mudanças no comportamento dos

cidadãos em um espaço de tempo tão curto é uma tarefa desafiadora, sobretudo quando levamos em consideração que a nova legislação não deve, em hipótese alguma, criar óbices aos novos paradigmas criados e já amplamente difundidos na sociedade.

A tarefa de legislar sobre Internet, para garantir a segurança dos cidadãos, empresas, governos e instituições não deve, assim, entrar em conflito com as infinitas possibilidades de comunicação permitidas pela rede, não deve interpor modelos de controle ou vigilância sobre os cidadãos, até porque, além de incompatíveis com uma cultura democrática e de liberdade, são absolutamente inócuos.

As amplas possibilidades de difusão do conhecimento e da cultura, assim como a ampliação da liberdade de expressão e da livre manifestação do pensamento de forma anônima, estabelecem novos padrões do exercício da cidadania, e do controle do Estado por parte da sociedade.

Assim, nenhuma disposição legal pode colocar – mesmo que involuntariamente - qualquer restrição a essa realidade. É essa preocupação de tentar aliar esses conceitos aparentemente antagônicos – segurança e liberdade – em prol do interesse público que nos leva a considerar que o texto que apreciamos neste momento precisa de aperfeiçoamentos, tanto para garantir que a liberdade na Internet continue sendo ampla, quanto para ampliar os níveis de segurança dos cidadãos em uma norma que seja perene e não fadada à obsolescência em um curto espaço de tempo.

Entretanto, no estágio atual de tramitação desta proposição, aprovada pelo Plenário do Senado Federal em 2008, como substitutivo ao Projeto de Lei nº 84, de 1999, aprovado pelo Plenário da Câmara dos Deputados, em 2003, as possibilidades de alteração no texto são bastante limitadas. A rejeição de determinados dispositivos do texto é algumas dessas possibilidades regimentais.

Nesse sentido, optamos por propor a supressão de dispositivos do texto que se mostraram controversos, de forma a permitir sua apresentação em outro projeto de lei. Dessa forma propomos a rejeição dos artigos 2°, 3º, 4º,5º, 6º, 7º, 8º, 10º, 11, 12, 13, 14, 16, 17, 20, 21 e 22 presentes no substitutivo do Senado Federal ao PL 84/99.

Diante do exposto, o voto é pela APROVAÇÃO do Substitutivo do Senado Federal, da seguinte forma:

a) Pela aprovação dos artigos 9º, 15, 18 e 19 do Substitutivo do Senado;

b) Pela aprovação da ementa do substitutivo, exceto as expressões “de rede de computadores, ou” e “dispositivos de comunicação ou”;

c) Pela aprovação do art. 1º, exceto as expressões “de rede de computadores, ou” e “dispositivos de comunicação ou”;

d) Pela rejeição dos artigos 2º, 3º, 4º, 5º, 6º, 7º, 8º, 10º, 11, 12, 13, 14, 16, 17, 20, 21 e 22.

Sala da Comissão, em de de 2012.

Deputado EDUARDO AZEREDO
Relator

2012_5013