COMISSÃO DE CONSTITUIÇÃO E JUSTIÇA E DE CIDADANIA

PROJETO DE LEI Nº. 84, DE 1999
(Apensos os projetos de lei do Senado nºs 76/2000 e 137/2000)

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

Autor: Deputado Luiz Piauhylino

Relator: Deputado Regis de Oliveira

I – Relatório

O projeto de lei nº. 84/1999, de autoria do ilustre deputado Luiz Piauhylino, fruto do trabalho realizado por um grupo de juristas renomados, **tipifica os crimes cometidos na área da informática e estabelece suas penalidades e outras providências**.

O Código Penal Brasileiro foi instituído **pelo Decreto-lei nº. 2.848, de 07 de dezembro de 1940.**

Naquela época, nem ao menos se cogitava na rede mundial de computadores, **conhecida como "internet**".

Com o surgimento da internet no início dos anos 90, **pessoas inescrupulosas começaram a praticar crimes, lesando direitos relativos a bens e dados de informática ou utilizando a rede mundial de computadores como meio de execução de outras condutas ilícitas.**

Por força dos princípios da reserva legal e da anterioridade, **os autores dos denominados "crimes cibernéticos" não podem ser penalizados, pois as mencionadas condutas não estão previstas no estatuto repressivo.**

Tal fato gerou a **impunidade desses criminosos**, que provocou o aumento alarmante de infrações desta natureza, com prejuízo imensurável às pessoas físicas e jurídicas.

O presente projeto pretende **preencher a citada lacuna legislativa**, descrevendo, de maneira detalhada, tais delitos e mencionando a pena cabível pela prática desses ilícitos.

De igual forma, **ajusta a legislação brasileira à Convenção de Budapeste de 2001,** tratado internacional que estabeleceu normas no sentido de reprimir condutas criminosas no ambiente da internet.

Em razão da identidade e natureza da matéria, foram apensados ao projeto de lei nº. 84/1999 duas **propostas de iniciativa do Senado Federal, os PLS nºs 76/2000 e PLS 137/200.**

O Senado Federal, após a unificação das propostas, **aprovou o presente projeto, nos termos do substitutivo apresentado.**

Consoante se infere do texto do substitutivo, **os parlamentares optaram por incluir os crimes eletrônicos e suas respectivas punições no Código Penal, Código Penal Militar e na legislação penal esparsa, deixando de lado a idéia inicial de criar uma lei específica disciplinando a matéria**.

Finalmente, o projeto retorna à Câmara dos Deputados, **para apreciação do substitutivo apresentado.**

É o relatório.

II – Voto do Relator

O projeto de lei nº. 84/1999 e os demais apensados **preenchem o requisito da constitucionalidade**, na medida em que estão em consonância com o inciso I, do artigo 22, da Magna Carta, que atribui à União competência privativa para legislar, entre outras matérias, **sobre direito penal e processual penal.**

De igual forma, o instrumento legislativo escolhido, **lei ordinária, é apropriado ao fim a que se destina.**

No que tange à juridicidade, **as proposições estão em conformação ao direito**, porquanto não violam normas e princípios do Ordenamento Jurídico vigente.

No que se refere à técnica legislativa, a proposição principal e os PLS nº. 76/2000 e 137/2000 **não merecem reparo**.

Após a análise do preenchimento dos pressupostos de constitucionalidade, juridicidade e técnica legislativa, **passa-se a apreciar o mérito das propostas.**

No mérito, chega a esta casa legislativa o presente projeto, oriundo do Senado Federal, para análise e discussão, versando precipuamente sobre a criminalização de condutas realizadas a partir de sistemas eletrônicos, digitais e similares.

Inicialmente, para que possa maximizar a compreensão das propostas que deverão fazer parte do presente Projeto, torna-se necessário alguns comentários relacionados à utilização de meios eletrônicos em nossa sociedade, o que permitirá que as alterações e inovações indicadas venham a ter total compreensão por parte dos demais membros desta Casa de Leis, enriquecendo o debate e permitindo o aperfeiçoamento das discussões.

A Internet, a rede mundial de computadores, teve seu início no final da década de 60 quando foi criada a ARPANET, com o intuito de descentralizar dados através de vários computadores interligados, porém a internet tal qual a conhecemos e usamos hoje surgiu no início dos anos 90 quando pesquisadores do CERN (Organização Européia Para a Pesquisa Nuclear) criaram o “world wide web” — o “www” que aparece diante do nome de sites — que, padronizando a exibição de documentos nos computadores, permitiu sua visualização sem que o usuário tivesse necessidade de conhecer profundamente sobre programas de acesso à rede.

Esta facilidade de acesso popularizou a Internet que, até então, estava relegada a fanáticos por computadores, profissionais da área e pesquisadores que necessitavam de rapidez na troca de informações.

Com a popularização da rede mundial de computadores está ocorrendo uma grande revolução na sociedade global: cada vez mais e mais pessoas começam a acessar a Internet e descobrem-se diante de um maravilhoso mundo novo, repleto de possibilidades: ler notícias online, pesquisar, visitar museus virtualmente, procurar emprego.

Conseqüentemente, a utilização de tecnologia nas mais variadas atividades acabou prosperar e uma maior quantidade de pessoas se vale de inúmeros recursos tecnológicos para consecução de suas atividades.

A cada instante, mais pessoas inserem o uso da rede em seu dia-a-dia: aumentando sua produtividade ao estar diretamente em contato com colaboradores e clientes, conhecendo pessoas de todos os cantos do mundo com interesses similares, divulgando seu próprio negócio.

Desta forma, relações pessoais, comerciais, de consumo e de trabalho, entre outras, passam pela rede mundial de computadores, provocando uma revolução jamais vivida pelo mundo até hoje.

A Internet, e outras novas tecnologias que surgiram com o avanço das ciências eletrônicas, proporcionaram uma revolução digital trazendo à classe média brasileira maior facilidade de acesso ao universo dos computadores.

A possibilidade de acesso a estas novas tecnologias trouxe para a sociedade diversos impactos, principalmente na seara do Direito. Antigos conceitos legais tiveram de ser reformulados, revestindo-se de uma roupagem mais moderna, de forma que pudessem se alinhar a estes novos conceitos.

Por outro lado, novas situações jurídicas passaram a exigir dos profissionais do Direito tratamento diferenciado, além de conhecimentos mais específicos sobre as matérias informáticas.

Como conseqüência do que restou exposto, novas condutas, que se valem da tecnologia para a sua consecução, passaram a ser praticadas, agredindo direito de terceiros ou atentando contra o interesse comum.

Algumas dessas ações apresentam adequação legal no ordenamento jurídico pátrio e, por assim dizer, tipificação penal, cabendo-nos fazer distinção quanto aos novos tipos de crimes que passaram comumente a ser chamados de crimes eletrônicos e informáticos.

Muitos ilícitos são perfeitamente enquadráveis no Código Penal pátrio e na legislação penal extravagante, quais sejam aqueles em que a Internet, ou outro ambiente eletrônico, informático ou computacional, é tão-somente o seu meio de execução, motivo pelo qual a tipificação ajusta-se perfeitamente ao ato praticado.

Dentre alguns exemplos de crimes eletrônicos estão à exposição em sites de Internet de fotos pornográficas com crianças ou adolescentes – enquadrando-se no art. 241, do Estatuto da Criança e do Adolescente – pedofilia; e o plágio de textos de terceiros e sua publicação em um site, caso em que há violação ao direito de autor – art. 184, do Código Penal.

Estes crimes, dentre outros, cometidos pelo meio eletrônico, não necessitam de legislação específica, pois já se encontram sob a égide da legislação vigente. Alguns necessitam apenas de ligeiras mudanças, para se adaptarem à sua consumação na Internet.

Mas existem aquelas condutas em que o objeto da ação lesa direito relativo a bens ou dados de informática e estes em sua maioria não encontram tipificação em nosso ordenamento jurídico.

É o caso do acesso indevido de hackers a computador de terceiro, que atualmente não encontra amparo criminal, mas às vezes se tenta qualificar, para esfera cível, como invasão de privacidade.

Em relação aos crimes eletrônicos, interessa-nos destacar que a grande maioria das prisões deles decorrentes foi efetuada ou por flagrante delito ou por confissão do acusado, tudo em decorrência da falta de eficácia e contundência que apresentam as demais provas neles geradas (que em geral são documentos eletrônicos), já que no Direito Penal não se admite presunção de culpa ou autoria para se efetuar a prisão; imprescindível é ter certeza quanto à veracidade dos fatos.

Desta forma, o panorama que se afigura no que diz respeito ao combate dos chamados crimes eletrônicos poderia ser comparado a batalhas em que exércitos se enfrentam numa guerra, dado ao antagonismo de posições com que as forças envolvidas nesta disputa disputam a mesma.

De um lado, a criminalidade organizada que procura agir no submundo da internet, valendo-se de táticas que em muito se assemelham àquelas utilizadas por integrantes de uma força de guerrilha, cooptando a cada dia novos “cybers-guerrilheiros” com conhecimento científico adequado para suas práticas criminosas.

Na outra frente da batalha estão os órgãos policiais, responsáveis pela investigação deste tipo de delito e o Ministério Público, os quais acabam lutando de forma desigual pela inexistência de instrumentos eficazes para vencer a burocracia estatal na obtenção de provas contra os criminosos, principalmente no que diz respeito a regramento legislativo eficaz que permita a obtenção dos meios necessários para uma atuação efetiva e adequada.

Dentre as maiores dificuldades enfrentadas pelos órgãos de repressão a delinqüência digital, podem ser mencionadas aquelas relacionadas à obtenção de informações sobre crimes e criminosos, porque se criou no Brasil uma situação jurídica que dificulta muito a obtenção dos dados necessários para a investigação.

Em qualquer investigação envolvendo um crime praticado pela Internet, é essencial que se tenha uma informação absolutamente essencial que é o endereço I.P., o qual vai permitir a identificação de um computador, levando até o responsável pela ação delituosa.

Ocorre que, por força de reiteradas decisões judiciais, uma Autoridade Policial, somente poderá ter acesso a esse tipo de informação mediante autorização de um juiz de direito.

Há que ser mencionado que, doutrinariamente, pode ser defendida posição contrária a este entendimento uma vez que o endereço I.P. é dado cadastral tal qual um número de telefone de uma residência, o qual pode ser consultado livremente na lista dos assinantes.

Prevalecendo este tipo de entendimento, em inúmeras situações isso pode levar de quatro a seis meses para o fornecimento dos dados, dificultando sobremaneira o trabalho da Autoridade Policial na obtenção de uma simples informação cadastral, que é o centro da investigação.

E os problemas não terminam ai.

É comum no mercado de telecomunicações, uma empresa, uma concessionária pública de telefonia, ceder por locação um endereço I.P. para outra empresa.

Desta forma, quando o juiz deferir a obtenção desta informação, a concessionária informará apenas que o endereço em questão está alocado para outra empresa, sendo necessária nova representação e a repetição de todo o procedimento judicial para serem obtidos os dados.

Ocorre que os dados armazenados pelas concessionárias de telecomunicações e provedores são extremamente voláteis e na maior parte das vezes ocorrendo um grande lapso de tempo para o efetivo rastreamento dos endereços I.P., não raramente, a informação acabará perdida em virtude do seu apagamento.

Por tudo quanto restou exposto, à conclusão inevitável é que os órgãos de repressão não estão dotados de instrumentos adequados para que possam desenvolver um trabalho melhor e fazer frente às “táticas de guerrilha” de que se valem os “cybers-criminosos”.

Fraudes bancárias e financeiras por meio eletrônico saltaram de 5% para 40% do total dos incidentes eletrônicos registrados entre 2004 e 2005, em todo o país. As tentativas de fraudes pela rede mundial de computadores cresceram, apenas naquele ano (2005), 579%. (o dado é do "Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil - www.cert.br).

As armadilhas eletrônicas, tais como o "phishing scam" e os "hoax" - as piadas de má-intenção voltadas para obtenção de vantagem ilícita, acabaram por se tornarem práticas comuns, auxiliando no desenvolvimento da chamada “engenharia social", conjunto de práticas criminosas cujo único objetivo é apenas a obtenção indevida de informações de vítimas.

Hoje são inúmeras as possibilidades de “ganho fácil” para os criminosos digitais, principalmente porque, a maior parte de suas vítimas não são afetas ao uso adequado dos recursos computacionais que diariamente utilizam, tornando-se assim presa fácil numa batalha feroz travada numa arena digital.

Fato comum entre os usuários de informática no país é a utilização do chamado “software pirata”, o qual não permite atualização e correções e acaba por permitir que seu utilizador acabe por se tornar mais uma vítima de criminosos.

E é exatamente neste panorama de verdadeira "guerra cibernética" que desponta, após longa tramitação, que incluiu aprovação interna em Comissões - de Educação, Ciência e Tecnologia, e Constituição e Justiça - o projeto, que teve propositura originária da Câmara Federal, e ao qual se acham apensados e com ele unificados outros dois projetos contendo mesma matéria (de iniciativa do Senado Federal - PLS 76/2000 e PLS 137/2000), voltado, finalmente, para o tratamento e definição dos crimes eletrônicos, habilitando-se como primeira norma brasileira de definição específica do crime cibernético.

A iniciativa - de criminalização das condutas eletrônicas - provê, finalmente, os órgãos repressivos do Estado, de arsenal compatível com a necessidade de enfrentamento de condutas surgidas muito depois da edição dos Códigos Penais.

De se destacar o fato de que os códigos brasileiros já estão sendo aplicados no que diz respeito aos crimes comuns praticados por meio eletrônico, restando às condutas que surgiram apenas com a disseminação de ferramentas de alta tecnologia.

Todavia, ainda que a Lei brasileira venha sendo aplicada na prática, não podemos deixar de lado a recomendação de legislação complementar sobre o assunto (como se destaca o Projeto 84/99), com intuito de prover maior celeridade processual e a efetiva repressão aos delitos eletrônicos.

Urge também, a celebração de tratados internacionais que coíbam as condutas criminosas no ambiente da Internet, como, por exemplo, a excelente Convenção de Budapeste de 2001, também conhecida como "Convenção sobre o Cyber crime", bem como uma política mundial para cooperação recíproca, dada à questão que envolve a extraterritorialidade desses crimes.

De nada adianta delegacias especializadas e um Ministério Público disposto a combater os crimes eletrônicos se não temos ferramentas legais e técnicas capazes de combater efetivamente o crime na Internet.

As estatísticas revelam que o Brasil é o País com o maior número de "crackers" especialistas no mundo, sendo relevante o fato da imprensa anunciar que o Brasil é o país onde se dá o maior número de ataques a páginas Web, e isto acontece porque a sensação de impunidade leva o infrator à certeza que mesmo que seja apanhado, dificilmente será condenado, pois, não havendo leis específicas, a analogia não pode ser empregada no campo do direito penal.

O atraso tecnológico no emprego das ferramentas pelo poder público para combater o cyber crime é uma questão de vontade política, vontade esta que se estende à promulgação de novas leis que darão combate efetivo ao crime eletrônico exclusivo.

Enquanto o Brasil espera, o crime na rede não pára e já existe uma distância abissal entre o nosso ordenamento e a rapidez dos "cybers criminosos", sendo certo que a cada dia novas vítimas são feitas tolhidas nesta "batalha digital"

Tudo isso apenas vem confirmar que nossa legislação vigente já não se encontra adequada às necessidades de nossa sociedade, urgindo a sua adequação imediata as novas tecnologias, que são incorporadas a cada dia ao cotidiano do cidadão.

Neste diapasão, o PL nº. 89/03 pode não ser a melhor de todas as ferramentas a ser disponibilizada aos órgãos de investigação de delitos, mas certamente representa um grande avanço na medida em que procura equilibrar as forças envolvidas neste embate de forma a preservar a lei e a ordem num mundo a cada dia mais "digital".

Fato da maior importância é a adequação da legislação penal adjetiva aos mecanismos instituídos a partir do projeto de lei, o que pode ocorrer nesta oportunidade, pois do contrário, a lei substantiva acabará fadada ao fracasso diante de instransponíveis barreiras que acabarão por serem criadas por todos os envolvidos no uso de recursos tecnológicos, tais como concessionárias de telecomunicação, provedores, instituições financeiras e organizações não governamentais.

A nosso talante, a legislação em vigor já abarca cerca de 95% das hipóteses dos crimes praticados na e com o uso da Internet. Os 5% restantes, por mais esforço hermenêutico que se faça, não estão abarcados, porquanto vige em nosso sistema o primado da legalidade – certo que algumas infrações penais digitais próprias (aquelas que somente podem ser praticadas em ambiente de rede), ainda não têm previsão legal, daí a imperiosa necessidade de tipificá-las.

Mas o mais importante é que a tipificação ao se completar, imediatamente surge perfeita harmonia com as recomendações da Convenção de Budapeste, abarcando todas as hipóteses do que lá se contém (acesso ilegal, atentado à integridade dos dados, atentado à integridade do sistema, abuso de dispositivos, falsificação informática, fraude informática, pornografia infantil e infrações à propriedade intelectual e aos direitos conexos).

Corolário disso é que o Brasil poderá subscrever a Convenção incondicionalmente, inserindo-se imediatamente no sistema legal brasileiro as regras procedimentais lá previstas, com a possibilidade da busca e apreensão de dados informáticos, salvaguarda de informações etc.. É um passo consideravelmente grande que se dá, de forma que o Brasil poderá se declarar inserido no que mais moderno existe no tocante ao enfrentamento desses crimes próprios da modernidade, naquilo que a mais atualizada doutrina penal denomina "Terceira Velocidade do Direito Penal".

Nessa linha de raciocínio, as novas condutas tratam de crimes de perigo, mas há que se construir um tipo próprio àquele que cria um programa, a exemplo da hipótese do inciso II, do art. 72, da Lei nº 9.504/97: constituem crimes, puníveis com reclusão de 5 a 10 anos: I (...) 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 e dados usados pelo serviço eleitoral.

A análise ora realizada abarca também os arts. 10 a 15 do Projeto, que tratam das alterações do Código Penal Militar. Contudo, por se tratar de tipos com redações praticamente idênticas às do Código Penal, as considerações ora formuladas servem àquelas alterações.

Para que o presente projeto possa estar na mais perfeita consonância com o ordenamento jurídico vigente, proporcionando assim os meios necessários a criação da legislação necessária para o combate dos delitos perpetrados por meios eletrônicos, passemos a análise do texto de lei que deverá ser objeto de debate por esta Casa Legislativa, sendo diretamente inseridas nos dispositivos descritos as alterações que entendemos necessárias ao aperfeiçoamento deste.

Art.1º Esta Lei 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, e 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.

Art. 2º O Título VIII da Parte Especial do Código Penal fica acrescido do Capítulo IV, assim redigido:

Capítulo IV

DOS CRIMES CONTRA A SEGURANÇA DOS SISTEMAS INFORMATIZADOS

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:

Pena - reclusão, de 1 (um) a 3 (três) anos, e multa.

Parágrafo único. 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.

COMENTÁRIOS:

A redação deste artigo preenche lacuna e harmoniza-se com a Convenção de Budapeste. É a 'invasão de domicílio eletrônico' que o Direito Italiano contempla. Só que lá se inseriu um singelo parágrafo no artigo referente à invasão, equiparando o sistema informático a casa.

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 legalmente e com expressa restrição de acesso, dado ou informação neles disponível:

Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.

Parágrafo único. Se o dado ou informação obtida desautorizadamente é fornecida a terceiros, a pena é aumentada de um terço.

COMENTÁRIOS:

Trata-se de "crime meio" de difícil caracterização, notadamente por não conter a finalidade da norma, o que justificou fosse acrescentada a expressão "legalmente" estabelecendo assim a necessidade da proteção legal do dado, o que evitaria que o "legítimo titular" ficasse com a prerrogativa de "completar" a lei, já que ele pode escrever como quiser a sua "autorização", que uma vez violada, configura em conduta tipificada como crime.

Ação Penal

Art. 285-C. Nos crimes definidos neste Capítulo somente se procede mediante representação, salvo se o crime é cometido contra a União, Estado, Município, empresa concessionária de serviços públicos, agências, fundações, autarquias, empresas públicas ou sociedade de economia mista e subsidiárias."

Art. 3º O Título I da Parte Especial do Código Penal fica acrescido do seguinte artigo, assim redigido:

“Divulgação ou utilização indevida de informações e dados pessoais

154-A. Divulgar, utilizar, comercializar ou disponibilizar dados e informações pessoais ou de pessoas jurídicas 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.

Pena – detenção, de 1 (um) a 2 (dois) anos, e multa.

§ 1º. “Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada da sexta parte.”

§ 2º. Somente se procede mediante representação, salvo se o crime é cometido contra a União, Estado, Município, empresa concessionária de serviços públicos, agências, fundações, autarquias, empresas públicas ou sociedade de economia mista e subsidiárias.

COMENTÁRIOS:

Da maneira como foi redigido o artigo, a ação penal seria, s.m.j., pública incondicionada, ao passo que nos crimes dos arts. 285 - A até C ela é condicionada à representação.

Ademais, o parágrafo único do art. 154, em vigor (violação do segredo profissional) determina que a ação penal seja condicionada à representação.

Dessa forma, para que haja harmonia entre todos os dispositivos citados e não se rompa o princípio da isonomia, conveniente que o art. 154-A também receba a ação penal pública condicionada.

Sugere-se que o dispositivo abarque não somente as informações das pessoas físicas, mas também das jurídicas (empresas etc.), notadamente por se tratar de um bem jurídico também passível de proteção legal.

Art. 4º O caput do art. 163 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) passa a vigorar com a seguinte redação:

“Dano

Art. 163. Destruir, inutilizar ou deteriorar coisa alheia ou dado eletrônico alheio:

....."(NR)

Art. 5º O Capítulo IV do Título II da Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) fica acrescido do art. 163-A, assim redigido:

"Inserção ou difusão de código malicioso

Art. 163-A. Inserir ou difundir código malicioso em dispositivo de comunicação, rede de computadores, ou sistema informatizado.

Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.

Inserção ou difusão de código malicioso seguido de dano

§ 1º Produzir intencionalmente ou vender código malicioso destinado ao uso em dispositivo de comunicação, rede de computadores ou sistema informatizado.

Pena – reclusão de 1 (um) a 3 (três) anos, e multa.

COMENTÁRIOS:

Muitas vezes os "crackers" não inserem e não difundem os Códigos Maliciosos, somente os produzem e vendem. Na forma atual do projeto, corremos sérios riscos em direcionarmos nossas ações aos "laranjas" (meros difusores) e deixarmos escapar os verdadeiros autores intelectuais do delito, ou seja, os programadores dos artefatos maliciosos. Não há razão para a não criminalização da produção intencional e a venda de códigos maliciosos.

Ressaltamos que a redação atual do projeto não é contrária à Convenção de Budapeste, portanto não obsta sua aprovação, mas a não criminalização da conduta descrita implicaria, num curto espaço de tempo, na necessidade da criação de nova norma visando sanar esta omissão.

É feita a correção da omissão, renumerando-se os parágrafos seguintes.

§ 2º 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 – reclusão, de 2 (dois) a 4 (quatro) anos, e multa.

§ 3º 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.

COMENTÁRIOS:

A redação também ajusta o Sistema Penal Brasileiro à Convenção de Budapeste. Ressalva deve ser feita à natureza da pena porquanto na modalidade simples o preceito secundário é de detenção e nas novas hipóteses a pena é de reclusão. Achamos adequada tal solução, notadamente em razão da danosidade difusa das hipóteses dos arts. 163-A. A pena de reclusão permitirá que existam interceptações autorizadas nessas hipóteses, pois a lei nº 9296/96 não autoriza que isso ocorra somente nos crimes de detenção.
Que fique claro que nas novas espécies a ação é penal pública incondicionada, à vista da atual redação do art.167, do CP.

Art. 6º O art. 171 do Código Penal passa a vigorar acrescido dos seguintes dispositivos:

"Art. 171

§ 2º Nas mesmas penas incorre quem:
.....

Estelionato Eletrônico

VII – difunde, por qualquer meio, código malicioso com intuito de devastar, copiar, alterar, destruir, facilitar ou permitir acesso indevido à rede de computadores, dispositivo de comunicação ou sistema informatizado, visando o favorecimento econômico de si ou de terceiro em detrimento de outrem:

§ 3º Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime do inciso VII do § 2º deste artigo, a pena é aumentada de sexta parte."

COMENTÁRIOS:

Resta evidenciado pela Doutrina brasileira que os crimes cometidos por meio eletrônico – definidos como a ação típica, antijurídica e culpável cometida contra ou pela utilização de processamento automático de dados ou sua transmissão - através da rede mundial de computadores podem ser classificados em: Crimes Informáticos Impróprios e Crimes Informáticos Próprios.

Nos primeiros, como já salientado, o instrumento utilizado para a execução da atividade delituosa é que é informatizado, o que não ocorre, todavia,

com o delito propriamente dito (evidencie-se que poderá ocorrer no mundo material).

Os segundos, por outra esteira, crimes da informática em sentido estrito, serão realizados quando o meio eletrônico é *"conditio sine quo non"* para a consumação do delito. Assim, v.g., a transmissão de vírus de computador é uma forma destes crimes.

O Código Penal, datado de 07 de dezembro de 1940, no que tange a esta última modalidade criminosa, é precário e não tipificou qualquer destas condutas ofensivas. Neste diapasão, é imprescindível a reforma neste estatuto legal a fim de disciplinar essas novas ações lesivas ao interesse de toda coletividade. Já em razão dos delitos informáticos impróprios, os tipos penais tradicionais, como enfatizados, abarcam essas condutas sendo possível a punição dos delinqüentes.

Não obstante ser admissível a aplicação da regra penal clássica para estas formas criminosas modernas, faz-se mister o esclarecimento do ponto de vista legal, com escopo de não restar qualquer dúvida acerca destes crimes, com fito impossibilitar o surgimento de teorias que advoguem a impunidade. Desta forma, não pregamos por um "direito penal máximo", defendemos apenas a regulamentação destes delitos praticados através da informática.

Resta evidente a necessidade de inserção na legislação pátria de regramento que permita incriminar os delitos de informática em sentido estrito, sancionando as condutas nas quais o meio eletrônico é efetivamente imprescindível para a consecução do delito, estabelecendo-se, porém, a necessidade da vantagem ilícita em detrimento da vítima.

Desta maneira, de acordo com o modelo dessa proposta de tipificação, tanto as infrações da informática próprias como as impróprias seriam disciplinadas, tornando incontroversos os delitos cometidos contra o sistema informático, não restando lacuna legal em matéria criminal.

Art. 7º Os arts. 265 e 266 do Código Penal passam 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, informação ou telecomunicação, ou qualquer outro de utilidade pública:

..... "(NR)

COMENTÁRIOS:

Na prática, trata-se de repetição do disposto no art.163, modalidade simples. Contudo, é conveniente e oportuno que a redação permaneça como está, porquanto se trata de bem jurídico específico, que merece proteção também específica. Ademais, faz adequação a legislação brasileira à Convenção de Budapeste e permite sua inserção ao sistema legal brasileiro.

"Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático, dispositivo de comunicação, rede de computadores ou sistema informatizado

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: - Pela Supressão deste artigo.
..... "(NR)

COMENTÁRIOS:

A redação que aqui se vislumbra, praticamente repete o que está redigido no art. 163, § 1º do projeto. Isto geraria um conflito aparente de normas quando da análise de um caso concreto, certo que, ao fim e ao cabo, prevaleceria à redação do art. 266 do projeto, porquanto a sanção deste é de detenção de 1 a 3 anos, enquanto o preceito secundário do art. 163, § 1º é de reclusão de 2 a 4 anos. Ou seja, ao invés de auxiliar no combate ao crime digital, neste ponto o projeto prejudicaria os interesses da sociedade. Sugere-se, pois, a rejeição do art. 266 do projeto.

Art. 8º O caput do art. 297 do Código Penal passa a vigorar com a seguinte redação:

"Falsificação ou Alteração de dado informático ou documento público

Art. 297. Falsificar ou alterar, no todo ou em parte, dado informático ou documento público verdadeiro:
....."(NR)

COMENTÁRIOS:

Embora um dos elementos normativos do tipo seja DADO ELETRÔNICO, sua definição não está contemplada no rol preconizado no art.16, do projeto. Ali se vislumbram os conceitos de DADOS INFORMÁTICOS e DADOS DE TRÁFEGO. Sugere-se, pois, que no projeto seja retirada a expressão DADO ELETRÔNICO e a mesma substituída pela expressão DADO INFORMÁTICO de mesma equivalência e já definida no artigo 16 do projeto.

Da forma como foi redigido, o art. 297 não tipifica a adulteração de dado eletrônico. Apenas sua falsificação. Dessa forma, sugere-se que se retome a redação original do projeto, antes de sua análise pelo Senado: “Falsificar ou alterar, no todo ou em parte, dado eletrônico ou documento público verdadeiro (...)”.

Art. 9º O caput do art. 298 do Código Penal passa a vigorar com a seguinte redação:

“Falsificação ou alteração de dado informático ou documento particular

Art. 298. Falsificar ou alterar, no todo ou em parte, dado informático ou documento particular verdadeiro:

.....

.....”(NR)

COMENTÁRIOS:

As considerações do art.297 aqui são repetidas. Sugere-se a seguinte redação: “Falsificar ou alterar, no todo ou em parte, dado informático ou documento particular verdadeiro (...)”.

Art. 10. O art. 251 do Capítulo IV do Título V da Parte Especial do Livro I do Decreto-Lei nº. 1.001, de 21 de outubro de 1969 (Código Penal Militar), passa a vigorar acrescido do inciso VI ao seu § 1º, e do § 4º, com a seguinte redação:

“Art. 251. .....

§ 1º - Nas mesmas penas incorre quem:

.....

Estelionato Eletrônico

VI - difunde, por qualquer meio, código malicioso com intuito de devastar, copiar, alterar, destruir, facilitar ou permitir acesso indevido à rede de computadores, dispositivo de comunicação ou sistema informatizado, visando o favorecimento econômico de si ou de terceiro em detrimento de outrem;

§ 4º - Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada da sexta parte.”

COMENTÁRIOS:

A alteração proposta segue o mesmo diapasão daquela descrita no artigo 6º do presente projeto, motivo pelo qual se justifica a mesma com os mesmos argumentos esposados naquele dispositivo.

Art. 11. O caput do art. 259 e o caput do art. 262 do Capítulo VII do Título V da Parte Especial do Livro I do Decreto-Lei nº. 1.001, de 21 de outubro de 1969 (Código Penal Militar), passam a vigorar com a seguinte redação:

"Dano Simples

Art. 259. Destruir, inutilizar, deteriorar ou fazer desaparecer coisa alheia ou dado informático alheio, desde que este esteja sob administração militar:(NR)

"Dano em material ou aparelhamento de guerra ou dado eletrônico

Art. 262. Praticar dano em material ou aparelhamento de guerra ou dado informático de utilidade militar, ainda que em construção ou fabricação, ou em efeitos recolhidos a depósito, pertencentes ou não às forças armadas:"(NR)

Art. 12. O Capítulo VII do Título V da Parte Especial do Livro I do Decreto-Lei nº. 1.001, de 21 de outubro de 1969 (Código Penal Militar), fica acrescido do art. 262-A, assim redigido:

"Inserção ou difusão de código malicioso

Art. 262-A. Inserir ou difundir código malicioso em dispositivo de comunicação, rede de computadores, ou sistema informatizado, desde que o fato atente contra a administração militar:

Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.

Inserção ou difusão código malicioso seguido de dano

§ 1º Se do crime resulta destruição, inutilização, deterioração, alteração, dificultação do funcionamento, ou funcionamento não autorizado pelo titular, de dispositivo de comunicação, de rede de computadores, ou de sistema informatizado:

Pena – reclusão, de 2 (dois) a 4 (quatro) anos, e multa.

§ 2º Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada da sexta parte."

Art. 13. O Título VII da Parte Especial do Livro I do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), fica acrescido do Capítulo VII-A, assim redigido:

"Capítulo VII-A

DOS CRIMES CONTRA A SEGURANÇA DOS SISTEMAS INFORMATIZADOS

Acesso não autorizado a rede de computadores, dispositivo de comunicação ou sistema informatizado

Art. 339-A. Acessar, mediante violação de segurança, rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso, desde que o fato atente contra a administração militar:

Pena - reclusão, de 1 (um) a 3 (três) anos, e multa.

Parágrafo único. 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.

Obtenção, transferência ou fornecimento não autorizado de dado ou informação

Art. 339-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, desde que o fato atente contra a administração militar:

Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.

Parágrafo único. Se o dado ou informação obtida desautorizadamente é fornecida a terceiros, a pena é aumentada de um terço.

"Divulgação ou utilização indevida de informações e dados pessoais

Art. 339-C Divulgar, utilizar, comercializar ou disponibilizar dados e informações pessoais contidas em sistema informatizado sob administração militar 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.

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

Parágrafo único - Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática de crime, a pena é aumentada da sexta parte.

Art. 14. O caput do art. 311 do Capítulo V do Título VII do Livro I da Parte Especial do Decreto-Lei nº. 1.001, de 21 de outubro de 1969 (Código Penal Militar), passa a vigorar com a seguinte redação:

"Falsificação de documento

Art. 311. Falsificar ou alterar, no todo ou em parte, dado informático ou documento público ou particular verdadeiro, desde que o fato atente contra a administração ou o serviço militar:"(NR)

COMENTÁRIOS:

Vide comentário ao artigo 6º do Projeto.

Art. 15. Os incisos II e III do art. 356 do Capítulo I do Título I do Livro II da Parte Especial do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), passa a vigorar com a seguinte redação:

"CAPÍTULO I

DA TRAIÇÃO

Favor ao inimigo

Art. 356. .....:

.....

II - entregando ao inimigo ou expondo a perigo dessa conseqüência navio, aeronave, força ou posição, engenho de guerra motomecanizado, provisões, dado informático ou qualquer outro elemento de ação militar;

III - perdendo, destruindo, inutilizando, deteriorando ou expondo a perigo de perda, destruição, inutilização ou deterioração, navio, aeronave, engenho de guerra motomecanizado, provisões, dado informático ou qualquer outro elemento de ação militar. (NR)

COMENTÁRIOS:

Alterou-se apenas a expressão DADO ELETRÔNICO por DADO INFORMÁTICO.

Art. 16. Para os efeitos penais considera-se, dentre outros:

I – dispositivo de comunicação: qualquer meio capaz de processar, armazenar, capturar ou transmitir dados utilizando-se de tecnologias magnéticas, óticas ou qualquer outra tecnologia;

II – sistema informatizado: qualquer sistema capaz de processar, capturar, armazenar ou transmitir dados eletrônica ou digitalmente ou de forma equivalente;

III – rede de computadores: o conjunto de computadores, dispositivos de comunicação e sistemas informatizados, que obedecem a um conjunto de regras, parâmetros, códigos, formatos e outras informações agrupadas em protocolos, em nível topológico local, regional, nacional ou mundial através dos quais é possível trocar dados e informações;

IV – código malicioso: o conjunto de instruções e tabelas de informações ou qualquer outro sistema desenvolvido para executar ações danosas ou obter dados ou informações de forma indevida;

V – dados informáticos: qualquer representação de fatos, de informações ou de conceitos sob forma suscetível de processamento numa rede de computadores ou dispositivo de comunicação ou sistema informatizado;

VI – dados de tráfego: todos os dados informáticos relacionados com sua comunicação efetuada por meio de uma rede de computadores, sistema informatizado ou dispositivo de comunicação, gerados por eles como elemento de uma cadeia de comunicação, indicando origem da comunicação, o destino, o trajeto, à hora, a data, o tamanho, a duração ou o tipo do serviço subjacente.

COMENTÁRIOS:

A opção por definir alguns conceitos atende aos interesses daqueles que desconhecem quaisquer denominações. Se de um lado é bom, porquanto suprime grande parcela de discussões (algumas questões preliminares desaparecerão) e se harmoniza com o que de mais moderno se vislumbra nos Tratados e Convenções Internacionais (pois nessas hipóteses há realmente que se definirem conceitos, ante a existência de inúmeros países protagonistas em caso de contenda judicial).

Art. 17. Para efeitos penais consideram-se também como bens protegidos o dado, o dispositivo de comunicação, a rede de computadores, o sistema informatizado. – Supressão do Artigo.

COMENTÁRIOS:

Sugere-se a supressão deste dispositivo, absolutamente desnecessário, pois ao optar pela inclusão dos tipos ao longo do Código Penal – e não por lei

autônoma, o legislador manteve o bem jurídico original. Ex.- no crime de 'dano digital' o bem jurídico ainda é o patrimônio e não o sistema em si. No caso dos crimes de adulteração de documento eletrônico, a fé pública ainda é o bem jurídico tutelado.

Em verdade, há uma concorrência de bens jurídicos: os originais e a 'segurança informática', que tem os requisitos integridade, disponibilidade e confidencialidade contemplados na Convenção de Budapeste. Ademais, da forma como foi lavrado, o art. 17 não contempla o rol previsto no art. 16 do projeto, o que, de certa forma, é paradoxal.

Art. 18. Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.

COMENTÁRIOS:

É interessante ver reafirmado o desejo do Legislador brasileiro em querer enfrentar esse tipo de criminalidade, próprio da modernidade, no que a mais avançada doutrina denomina de "Terceira Velocidade do Direito Penal". Melhor não suprimir o art.18.

Art. 19. O inciso II do § 3º do art. 20 da Lei nº. 7.716, de 5 de janeiro de 1989, passa a vigorar com a seguinte redação:

"Art. 20 .....

.....

§ 3º.....

II – a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas, ou da publicação por qualquer meio.

..... "(NR)

COMENTÁRIOS:

Trata-se da lei que pune o racismo. A redação traz uma ótima novidade para o sistema de repressão aos crimes dessa natureza, situação que já existe na prática, decorrente de alguns Termos de Ajustamentos de Conduta formulados pelos Ministérios Públicos Estaduais e Federal com alguns provedores. Contudo, a própria Convenção de Budapeste permite essa solução e na hipótese de o Brasil subscrevê-la, haveria um bis in idem positivo. Acrescente-

se que tal solução não deve se circunscrever apenas aos crimes de racismo, mas a todos, especialmente nas hipóteses de crimes contra a honra.

Art. 20. O caput do art. 241 da Lei nº 8.069, de 13 de julho de 1990, passa a vigorar com a seguinte redação:

"Art. 241. Apresentar, produzir, vender, receber, fornecer, divulgar, publicar ou armazenar, por qualquer meio de comunicação, inclusive rede mundial de computadores ou Internet, fotografias, imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente:

..... "(NR)

COMENTÁRIOS:

Não são técnicas as expressões "receptar" e "armazenar consigo". Sugere-se "receber" (verbo do art.180, do CP) e apenas "armazenar", pois o "consigo" redundaria em pleonasmo. Ademais, o agente desta conduta nunca teria "consigo", em seu próprio corpo, a informação, mas em seu computador, em sua máquina. Uma arma de fogo pode ser trazida "consigo", nunca o rol de informações do dispositivo, a não ser num "pen drive", num disquete ou em algo similar. Indaga-se: o que seria o "consigo" no meio eletrônico? Desta forma, melhor uso da expressão "armazenar".

Art. 21. O art. 1º da Lei nº 10.446, de 8 de maio de 2002 passa a vigorar com a seguinte redação:

"Art. 1º .....

.....

V – os delitos praticados contra ou mediante rede de computadores, dispositivo de comunicação ou sistema informatizado.

....."(NR) – Supressão do artigo.

COMENTÁRIOS:

Há inquestionável rompimento do Pacto Federativo contemplado na Constituição Federal. Isto porque a redação dá a entender que todas as infrações tratadas no projeto seriam de competência da Justiça Federal.

Preocupa-nos a paulatina inversão dos valores constitucionais, o que novamente se constata no projeto. Em verdade, a regra da Carta Magna é que a competência seja Estadual e o resíduo Federal. Nunca o contrário. Há ingerência das instâncias federais na vida dos Estados.

Ademais, nem a Polícia Federal, nem a Justiça Federal têm condições de dar cabo de tanta demanda. Muito menos a sociedade, especialmente as vítimas e testemunhas, devem se desdobrar para sair de seus rincões para se dirigir às Varas Federais normalmente situadas em grandes centros. Melhor que as regras dos arts. 69 e ss do Código de Processo Penal continuem a definir a competência de cada caso concreto.

Por derradeiro, não é demais lembrar que a redação do art.21 conflita com a redação do art.18, pois se a vontade do legislador é que os órgãos da polícia judiciária (presumem-se as estaduais) estruturem setores especializados, por qual razão deixaria ao exclusivo talante da Polícia Federal o combate aos crimes digitais?

Por fim, se deixar-se apenas e tão somente aos entes federais o combate desses crimes, como os Estados poderão se proteger no caso de serem vítimas de criminosos desse jaez?

Dessa forma, sugere-se a supressão do art. 21.

Art. 22. O responsável pelo provimento de acesso a rede de computadores mundial, comercial ou do setor público, bem como os prestadores de serviço de conteúdo, são obrigados a:

COMENTÁRIOS:

Não somente os provedores de acesso devem ser contemplados nesse dispositivo. Há outros, como os de serviço (não contemplados no art.16 – que deveria definir todos os dispositivos e protagonistas nessa seara tecnológica).

O Projeto somente atribui responsabilidade a provedores de acesso a um sistema informático o que, s.m.j., excluiria a responsabilidade de prestadores de serviço de conteúdo (servidor webmail, homepage, etc). Seria extremamente prejudicial às investigações de crimes cibernéticos tal lacuna em nosso ordenamento jurídico, pois na maioria dos casos investigados somente alcançamos os “dados de acesso” (tráfego) após as informações prestadas por fornecedores de serviço de conteúdo. Certamente, aprovado o Projeto na atual redação, nova proposição legislativa deverá preencher esta lacuna para dotar o Brasil de uma legislação mais eficaz no combate aos crimes de tecnologia e adequar o Brasil aos termos da Convenção de Budapeste. Deve ficar claro na legislação que os prestadores de serviço (acesso e conteúdo) devem adotar todos os esforços para possuírem os meios tecnológicos conhecidos para cumprimento das obrigações previstas no artigo 22, sob pena de esvaziamento desta disposição.

Logicamente, se o dado requisitado for tecnologicamente inviável de ser obtido em determinado momento ou local, nenhum pena deve ser aplicada.

Entretanto, se houver tecnologia nova, ainda não difundida, que permita a obtenção do dado, um tempo razoável deve ser fixado para que o prestador de serviço a adote. Entretanto, caso houvesse tecnologia disponível e, por negligência, o prestador não se atualizou e deixou de cumprir com as obrigações previstas na legislação (art. 22, PLC 89), deve arcar com sua responsabilidade, a ser apurada mediante o devido processo legal.

I – manter em ambiente controlado e de segurança, pelo prazo de três anos, com o objetivo de provimento de investigação pública formalizada, os dados de endereçamento eletrônico da origem, destino, hora, data e a referência GMT da conexão efetuada por meio de rede de computadores e fornecê-los exclusivamente à autoridade investigatória e o Ministério Público mediante requisição;

COMENTÁRIOS:

O prazo de 3 (três) anos é absolutamente razoável.

A requisição de informações cadastrais somente mediante requisição judicial é muito radical. A ordem judicial deve contemplar o próprio conteúdo da informação – o dado sensível e não a informação cadastral, como corolário do disposto no art.5º, XI, da CF.

Na vida prática, fora a rede, quando um ônibus atropela alguém e a respectiva placa é anotada, a Autoridade Policial não necessita solicitar ao Juiz de Direito que determine a remessa do dado cadastral (de quem dirigia o coletivo etc.).

Ademais, há hipóteses em que não se torna necessária a judicialização da demanda, como nos inquéritos civis, oportunidade em que o próprio Promotor de Justiça ou Procurador da República, p.ex. nos casos de improbidade e no cerne do devido processo legal (inquérito civil regularmente instaurado e com acompanhamento do Conselho Superior do respectivo Ministério Público) pode requisitar tanto a informação cadastral quanto o dado para instruir o procedimento.

Sugere-se, pois, que a requisição judicial seja exigida somente quanto ao dado sensível – a própria informação, e não quanto aos cadastros.

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

COMENTÁRIOS:

A determinação de preservação somente após requisição judicial conflita com regra existente na própria Convenção de Budapeste. Em verdade, tanto nos EUA quanto na Europa, quando se constata que em determinado provedor (de qualquer natureza) exista informação necessária ao sucesso da investigação, tanto a Polícia quanto o Ministério Público emitem uma solicitação de preservação diretamente ao provedor, indicando que a partir de tal data, por exemplo, sejam mantidos os arquivos respectivos, para, futuramente, ser emitida a requisição judicial.

Na realidade, trata-se de um alerta para que o dado seja mantido, sob pena de desobediência. A informação sensível somente é entregue mediante requisição judicial, mas a sua manutenção pode ser feita pela Autoridade Policial e pelo Ministério Público, a fim de não se dilua, dada a volatilidade do dado informático.

III – informar, de maneira sigilosa, à autoridade policial ou judicial, informação em seu poder ou que tenha conhecimento e que contenha indícios da prática de crime sujeito a acionamento penal, cuja prática haja ocorrido no âmbito da rede de computadores sob sua responsabilidade, ressalvada a responsabilização administrativa, civil e penal da pessoa jurídica, sem exclusão das pessoas físicas, autoras, co-autoras ou participes do mesmo fato.

COMENTÁRIOS:

Não é técnico o uso da expressão ‘denúncia’, própria da petição inicial de uma ação penal pública – condicionada ou não, pelo Ministério Público. Também não é técnico o uso da expressão perpetração, mas prática.

Se permanecer restrito aos casos “de que tenha recebido” a informação, não transforma o provedor no garantidor de que trata o art. 13, § 2º, alínea ‘a’, do CP. A Convenção de Budapeste espera que todo e qualquer provedor (de acesso, de serviço etc.) seja um ente co-responsável pelo que trafega em seus sistemas, e não um mero “alcagüeta digital”, que repassa informações criminosas. Tanto que o art. 13, item 2, da mesma Convenção sugere a responsabilidade penal da pessoa jurídica (do “ente moral” provedor) e não apenas de seus responsáveis.

No Brasil, tal modalidade de imputação (à pessoa jurídica) vem preconizada na Magna Carta nos arts. 173, § 5º (para atos praticados contra a

ordem econômica e financeira e contra a economia popular) e 225, § 3º (crimes contra o meio ambiente), certo que o último dispositivo constitucional foi regulamentado pelo art. 3º, da Lei nº. 9.605/98, permitindo que empresas poluidoras possam ser acusadas em ação penal. Ora, no caso dos crimes digitais, nossa C.F. não teria como antever o surgimento da Internet, de forma que os "entes morais" provedores – de acesso ou de outras modalidades, pudessem ser alcançados pela justiça criminal. Contudo, perder a oportunidade de em Lei Ordinária exigir deles maior responsabilidade no combate aos crimes cibernéticos, é deixar que uma "chance de ouro" se esvaia.

Como foi formulada, a redação restringe esse dever de vigilância aos crimes de ação pública incondicionada, afastando de sua abrangência infrações de grande ofensividade, como as condutas que o próprio projeto contempla: arts. 285-A, 285-B, 163-A, 163, dentre outros já existentes no Código Penal e legislação extravagante, de ação pública condicionada ou até mesmo privada, mas de relevância.

§ 1º Os dados de que cuida o inciso I deste artigo, as condições de segurança de sua guarda, a perícia à qual serão submetidos e a autoridade competente responsável por requisitar a perícia, bem como as condições para que sejam fornecidos e utilizados, serão definidos nos termos de regulamento, preservando-se sempre a agilidade na obtenção destas informações e o sigilo na sua manipulação.

COMENTÁRIOS:

O Estado não realiza auditorias, notadamente as agências do Sistema Criminal, mas perícias.

Conflita com a atual redação do art. 159, § 6º, do CPP, dada pela Lei nº 11.690/2008, motivo pelo qual é proposta a sua adequação mediante as alterações apontadas no próprio parágrafo primeiro.

Por outro lado, a obtenção de informações necessárias ao bom andamento das investigações e o sigilo na divulgação das mesmas deverá ser assegurado, o que certamente implicará na adoção de medidas que permitirão que as Autoridades envolvidas possam agilizar suas ações.

A morosidade decorrente da obtenção das informações necessárias por parte das Autoridades competentes implica numa sensação de impunidade, colocando em risco a eficácia da lei.

Desta forma, os órgãos policiais, o Ministério Público e o Poder Judiciário deverão adotar medidas que permitam a agilização na obtenção de tais informações, o que poderá ser levado a cabo com a edição de regulamento que

estabeleça as normas para a requisição, manipulação, periciamento e armazenamento de tais dados.

§ 2º O responsável citado no *caput* deste artigo, independentemente do ressarcimento por perdas e danos ao lesado, estará sujeito ao pagamento de multa variável de R$ 2.000,00 (dois mil reais) a R$ 100.000,00 (cem mil reais) a cada requisição, aplicada em dobro em caso de reincidência, que será imposta pela autoridade judicial, considerando-se a natureza, a gravidade e o prejuízo resultante da infração, assegurada a oportunidade de ampla defesa e contraditório.

§ 3º Os recursos financeiros resultantes do recolhimento das multas estabelecidas neste artigo serão destinados ao Fundo Nacional de Segurança Pública, de que trata a Lei nº 10.201, de 14 de fevereiro de 2001, assegurada à distribuição igualitária entre os Estados membros, na forma de regulamento.

COMENTÁRIOS:

Em respeito ao pacto federativo, objeto de considerações anteriores, os recursos devem ser distribuídos em igualdade de condições para os Estados, o que deverá ser objeto de regulamento que definirá os critérios que deverão nortear esta distribuição.

Art. 23. Esta Lei entrará em vigor cento e vinte dias após a data de sua publicação.

Diante do exposto, o voto é pela constitucionalidade, juridicidade, adequada técnica legislativa e, no mérito, **pela aprovação do PL nº. 89/2003 e PLS nº. 76/2000 e 137/2000, nos termos do substitutivo apresentado**.

Sala da Comissão, em 05 de outubro de 2010.

Deputado Regis de Oliveira
Relator

SUBSTITUTIVO
(ao PLS 76/2000, PLS 137/2000 e PLC 89/2003)

Substitua-se o projeto pelo seguinte:

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.

O **Congresso Nacional** decreta:

Art. 1º Esta Lei 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.

Art. 2º O Título VIII, da Parte Especial do Código Penal, fica acrescido do Capítulo IV, assim redigido:

"Capítulo IV

DOS CRIMES CONTRA A SEGURANÇA DOS SISTEMAS INFORMATIZADOS

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:

Pena - reclusão, de 1 (um) a 3 (três) anos, e multa.

Parágrafo único. 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.

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 legalmente e com expressa restrição de acesso, dado ou informação neles disponível:

Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.

Parágrafo único. Se o dado ou informação obtida desautorizadamente é fornecida a terceiros, a pena é aumentada de um terço.

Ação Penal

Art. 285-C. Nos crimes definidos neste Capítulo somente se procede mediante representação, salvo se o crime é cometido contra a União, Estado, Município, empresa concessionária de serviços públicos, agências, fundações, autarquias, empresas públicas ou sociedade de economia mista e subsidiárias."

Art. 3º O Título I, da Parte Especial do Código Penal, fica acrescido do seguinte artigo, assim redigido:

"Divulgação ou utilização indevida de informações e dados pessoais

Art. 154-A. Divulgar, utilizar, comercializar ou disponibilizar dados e informações pessoais ou de pessoas jurídicas 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:

Pena – detenção, de 1 (um) a 2 (dois) anos, e multa.

§ 1º. 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.

§ 2º. Somente se procede mediante representação, salvo se o crime é cometido contra a União, Estado, Município, empresa concessionária de serviço público, agências, fundações, autarquias, empresas públicas ou sociedade de economia mista e subsidiárias."

Art. 4º O caput do art. 163, do Código Penal, passa a vigorar com a seguinte redação:

"Dano

Art. 163 - Destruir, inutilizar ou deteriorar coisa alheia ou dado eletrônico alheio:

....."

Art. 5º O Capítulo IV, do Título II, da Parte Especial, do Código Penal, fica acrescido do art. 163-A, assim redigido:

"Inserção ou difusão de código malicioso

Art. 163-A. Inserir ou difundir código malicioso em dispositivo de comunicação, rede de computadores, ou sistema informatizado:

Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.

Inserção ou difusão de código malicioso seguido de dano

§ 1º. Produzir intencionalmente ou vender código malicioso destinados ao uso em dispositivo de comunicação, rede de computadores ou sistema informatizado.

Pena – reclusão de 1 (um) a 3 (três) anos, e multa.

§ 2º. 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 – reclusão, de 2 (dois) a 4 (quatro) anos, e multa.

§ 3º. 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."

Art. 6º O art. 171, do Código Penal, passa a vigorar acrescido dos seguintes dispositivos:

"Art. 171. .....
.....

§ 2º Nas mesmas penas incorre quem:
.....

Estelionato Eletrônico

VII – difunde, por qualquer meio, código malicioso com intuito de devastar, copiar, alterar, destruir, facilitar ou permitir acesso indevido à rede de computadores, dispositivo de comunicação ou sistema informatizado, visando o favorecimento econômico de ou de terceiro em detrimento de outrem.

§ 3º. Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime previsto no inciso VII, do § 2º, deste artigo, a pena é aumentada de sexta parte."

Art. 7º Os arts. 265 e 266, do Código Penal, passam 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, informação ou telecomunicação, ou qualquer outro de utilidade pública:
....."

Art. 8º O caput do art. 297, do Código Penal, passa a vigorar com a seguinte redação:

"Falsificação ou Alteração de dado informático ou documento público

Art. 297 – Falsificar ou alterar, no todo ou em parte, dado informático ou documento público verdadeiro:
....."

Art. 9º O caput do art. 298, do Código Penal, passa a vigorar com a seguinte redação:

"Falsificação ou alteração de dado informático ou documento particular

Art. 298 – Falsificar ou alterar, no todo ou em parte, dado informático ou documento particular verdadeiro:

....."

Art. 10. O art. 251, do Capítulo IV, do Título V, da Parte Especial do Livro I, do Código Penal Militar, passa a vigorar acrescido do inciso VI ao seu § 1º, e do § 4º, com a seguinte redação:

"Art. 251. .....

§ 1º Nas mesmas penas incorre quem:

.....

Estelionato Eletrônico

VI - Difunde, por qualquer meio, código malicioso com o intuito de devastar, copiar, alterar, destruir, facilitar ou permitir o acesso indevido à rede de computadores, dispositivo de comunicação ou a sistema informatizado, visando o favorecimento econômico de si ou de terceiro em detrimento de outrem.

.....

§ 4º 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."

Art. 11. O caput do art. 259 e o caput do art. 262, do Capítulo VII, do Título V, da Parte Especial do Livro I, do Código Penal Militar, passam a vigorar com a seguinte redação:

"Dano Simples

Art. 259 - Destruir, inutilizar, deteriorar ou fazer desaparecer coisa alheia ou dado informático alheio, desde que este esteja sob administração militar:

....."

Dano em material ou aparelhamento de guerra ou dado eletrônico

Art. 262 - Praticar dano em material ou aparelhamento de guerra ou dado informático de utilidade militar, ainda que em construção ou fabricação, ou em efeitos recolhidos a depósito, pertencentes ou não às forças armadas:"

Art. 12. O Capítulo VII, do Título V, da Parte Especial do Livro I, do Código Penal Militar, fica acrescido do art. 262-A, assim redigido:

"Inserção ou difusão de código malicioso

Art. 262-A. Inserir ou difundir código malicioso em dispositivo de comunicação, rede de computadores, ou sistema informatizado, desde que o fato atente contra a administração militar:

Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.

Inserção ou difusão de código malicioso seguido de dano

§ 1º Se do crime resulta destruição, inutilização, deterioração, alteração, dificultação do funcionamento, ou funcionamento não autorizado pelo titular, de dispositivo de comunicação, de rede de computadores, ou de sistema informatizado:

Pena – reclusão, de 2 (dois) a 4 (quatro) anos, e multa.

§ 2º 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."

Art. 13. O Título VII, da Parte Especial, do Livro I, do Código Penal Militar, fica acrescido do Capítulo VIII, assim redigido:

"CAPÍTULO VII-A

DOS CRIMES CONTRA A SEGURANÇA DOS SISTEMAS INFORMATIZADOS

Acesso não autorizado à rede de computadores, dispositivo de comunicação ou sistema informatizado

Art. 339-A. Acessar, mediante violação de segurança, rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso, desde que o fato atente contra a administração militar:

Pena - reclusão, de 1 (um) a 3 (três) anos, e multa.

Parágrafo único. 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.

Obtenção, transferência ou fornecimento não autorizado de dado ou informação

Art. 339-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, desde que o fato atente contra a administração militar:

Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.

Parágrafo único. Se o dado ou informação obtida desautorizadamente é fornecida a terceiros, a pena é aumentada de um terço.

Divulgação ou utilização indevida de informações e dados pessoais

Art. 339-C. Divulgar, utilizar, comercializar ou disponibilizar dados e informações pessoais contidas em sistema informatizado sob administração militar 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:

Pena – detenção, de 1 (um) a 2 (dois) anos, e multa.

Parágrafo único. 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."

Art. 14. O caput do art. 311, do Capítulo V, do Título VII, do Livro I, da Parte Especial, do Código Penal Militar, passa a vigorar com a seguinte redação:

"Falsificação de documento

Art. 311. Falsificar ou alterar, no todo ou em parte, dado informático ou documento público ou particular verdadeiro, desde que o fato atente contra a administração ou o serviço militar:

....."

Art. 15. Os incisos II e III, do art. 356, do Capítulo I, do Título I, do Livro II, da Parte Especial, do Código Penal Militar, passam a vigorar com a seguinte redação:

"CAPÍTULO I

DA TRAIÇÃO

Favor ao inimigo

Art. 356. .....
.....

II - entregando ao inimigo ou expondo a perigo dessa conseqüência navio, aeronave, força ou posição, engenho de guerra motomecanizado, provisões, dado informático ou qualquer outro elemento de ação militar;

III - perdendo, destruindo, inutilizando, deteriorando ou expondo a perigo de perda, destruição, inutilização ou deterioração, navio, aeronave, engenho de guerra motomecanizado, provisões, dado informático ou qualquer outro elemento de ação militar."

Art. 16. Para os efeitos penais considera-se, dentre outros:

"I – dispositivo de comunicação: qualquer meio capaz de processar, armazenar, capturar ou transmitir dados utilizando-se de tecnologias magnéticas, óticas ou qualquer outra tecnologia;

II – sistema informatizado: qualquer sistema capaz de processar, capturar, armazenar ou transmitir dados eletrônica ou digitalmente ou de forma equivalente;

III – rede de computadores: o conjunto de computadores, dispositivos de comunicação e sistemas informatizados, que obedecem a um conjunto de regras, parâmetros, códigos, formatos e outras informações agrupadas em protocolos, em
nível topológico local, regional, nacional ou mundial através dos quais é possível trocar dados e informações;

IV – código malicioso: o conjunto de instruções e tabelas de informações ou qualquer outro sistema desenvolvido para executar ações danosas ou obter dados ou informações de forma indevida;

V – dados informáticos: qualquer representação de fatos, de informações ou de conceitos sob forma suscetível de processamento numa rede de computadores ou dispositivo de comunicação ou sistema informatizado;

VI – dados de tráfego: todos os dados informáticos relacionados com sua comunicação efetuada por meio de uma rede de computadores, sistema informatizado ou dispositivo de comunicação, gerados por eles como elemento de uma cadeia de comunicação, indicando origem da comunicação, o destino, o trajeto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente."

Art. 17. Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.

Art. 18. O inciso II, do § 3º, do art. 20, da Lei nº. 7.716, de 5 de janeiro de 1989, passa a vigorar com a seguinte redação:

"Art. 20 .....
.....

§ 3º.....
.....

II – a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas, ou da publicação por qualquer meio.
....."

Art. 19. O caput do art. 241, da Lei nº. 8.069, de 13 de julho de 1990, passa a vigorar com a seguinte redação:

"Art. 241. Apresentar, produzir, vender, receber, fornecer, divulgar, publicar ou armazenar, por qualquer meio de comunicação, inclusive rede mundial de computadores ou Internet, fotografias, imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente:
....."

Art. 20. O responsável pelo provimento de acesso a rede de computadores mundial, comercial ou do setor público é obrigado a:

"I – manter em ambiente controlado e de segurança, pelo prazo de três anos, com o objetivo de provimento de investigação pública formalizada, os dados de endereçamento eletrônico da origem, destino, hora, data e a referência GMT da conexão efetuada por meio de rede de computadores e

fornecê-los exclusivamente à autoridade policial e ao Ministério Público, mediante requisição;

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

III – Levar ao conhecimento, de maneira sigilosa, da autoridade policial ou judicial, informação em seu poder ou que tenha ciência e que contenha indícios da prática de crime sujeito a acionamento penal, cuja prática haja ocorrido no âmbito da rede de computadores sob sua responsabilidade, ressalvada a responsabilização administrativa, civil e penal da pessoa jurídica, sem exclusão das pessoas físicas autoras, co-autoras ou partícipes do mesmo fato.

§ 1º Os dados de que cuida o inciso I, deste artigo, as condições de segurança de sua guarda, a perícia à qual serão submetidos e a autoridade competente responsável por requisitar a perícia, bem como as condições para que sejam fornecidos e utilizados, serão definidos nos termos de regulamento, preservando-se sempre a agilidade na obtenção destas informações e o sigilo na sua manipulação.

§ 2º O responsável citado no *caput* deste artigo, independentemente do ressarcimento por perdas e danos ao lesado, estará sujeito ao pagamento de multa variável de R$ 2.000,00 (dois mil reais) a R$ 100.000,00 (cem mil reais) a cada requisição, aplicada em dobro em caso de reincidência, que será imposta pela autoridade judicial, considerando-se a natureza, a gravidade e o prejuízo resultante da infração, assegurada a oportunidade de ampla defesa e contraditório.

§ 3º Os recursos financeiros resultantes do recolhimento das multas estabelecidas neste artigo serão destinados ao Fundo Nacional de Segurança Pública, de que trata a Lei nº. 10.201, de 14 de fevereiro de 2001, assegurada à distribuição igualitária entre os Estados membros."

Art. 21. Esta Lei entra em vigor cento e vinte dias após a data de sua publicação.

Sala da Comissão, em 05 de outubro de 2010.

Deputado Regis de Oliveira
Relator