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 aprovado pelo Senado Federal.**

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 não muito incomum 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, ainda que com ressalvas, 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 abrangente 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, propomos as seguintes emendas ao Substitutivo aprovado pelo Senado Federal, submetendo-as à análise e estudos não apenas dos pares dessa Casa, mas também a toda a sociedade, diretamente atingida pelos crimes cometidos nos meios digitais e que clama por uma legislação que atenda aos seus anseios de fim da impunidade de tais delitos.

Emenda Supressiva nº 1

Suprima-se da ementa do Substitutivo do Senado Federal ao PL 84/99 os termos "dispositivos de comunicação", que passa a ter a seguinte redação:

> ***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 ou sistemas informatizados e similares, e dá outras providências.***

Justificativa

Visando, pragmaticamente, afastar críticas ao PL, propõe-se a retirada dos termos "dispositivos de comunicação" de todos os dispositivos do PL.

A existência desses termos levou a interpretação de muitos de que poder-se-ia criminalizar práticas comuns, como desbloqueio de celulares bloqueados, desbloqueio de aparelhos de DVD, permitindo que os mesmos lessem DVD's de todas as regiões, desbloqueio de aparelhos de HDTV, permitindo que os filmes transmitidos por esses aparelhos sejam gravados, ainda que muitos desses aparelhos já possuam essa funcionalidade.

As infrações acima descritas já são tratadas pela Lei de Direitos Autorais, além de refletirem infração a dispositivos contratuais, cuja penalização pecuniária poderá ser obtida no âmbito civil.

Sob os mesmos argumentos, propomos a supressão dos mesmos termos em todos os dispositivos onde citados, nos termos das seguintes ementas:

Emenda Supressiva nº 2

Suprima-se do artigo 1º do Substitutivo do Senado Federal ao PL 84/99 os termos "dispositivos de comunicação", que passa a ter a seguinte redação:

> "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 sistemas informatizados e similares, e dá outras providências."

Emenda Supressiva nº 3

Suprima-se do tipo penal previsto no art. 2º do Substitutivo do Senado Federal ao PL 84/99 os termos "dispositivos de comunicação", que passa a ter a seguinte redação:

> "Acesso não autorizado a rede de computadores ou sistema informatizado"

Emenda Supressiva nº 4

Suprima-se do caput art. 285-A previsto no art. 2º do Substitutivo do Senado Federal ao PL 84/99 os termos "dispositivos de comunicação", que passa a ter a seguinte redação:

> "Art. 285-A. Acessar, mediante violação de segurança, rede de computadores ou sistema informatizado, protegidos por expressa restrição de acesso:"

Emenda Supressiva nº 5

Suprima-se do caput do art. 285-B previsto no art. 2º do Substitutivo do Senado Federal ao PL 84/99 os termos "dispositivos de comunicação", que passa a ter a seguinte redação:

> "Art. 285-B. Obter ou transferir, sem autorização ou em desconformidade com autorização do legítimo titular da rede de computadores ou sistema informatizado, protegidos com expressa restrição de acesso, dado ou informação neles disponível:"

Emenda Supressiva nº 6

Suprima-se do caput art. 163-A previsto no art. 5º do Substitutivo do Senado Federal ao PL 84/99 os termos "dispositivos de comunicação", que passa a ter a seguinte redação:

> "Art. 163-A. Inserir ou difundir código malicioso em rede de computadores ou sistema informatizado:"

Emenda Supressiva nº 7

Suprima-se do § 1º do art. 163-A previsto no art. 5º do Substitutivo do Senado Federal ao PL 84/99 os termos "dispositivos de comunicação", que passa a ter a seguinte redação:

> "§ 1º. Se do crime resulta destruição, inutilização, deterioração, alteração, dificultação do funcionamento, ou funcionamento desautorizado pelo legítimo titular de rede de computadores, ou de sistema informatizado:"

Emenda Supressiva nº 8

Suprima-se do inciso VII do § 2º do art. 163-A previsto no art. 5º do Substitutivo do Senado Federal ao PL 84/99 os termos "dispositivos de comunicação", que passa a ter a seguinte redação:

> "VII – difunde, por qualquer meio, código malicioso com intuito de facilitar ou permitir acesso indevido à rede de computadores ou sistema informatizado."

Emenda Supressiva nº 9

Suprima-se do tipo penal do art. 265 previsto no art. 7º do Substitutivo do Senado Federal ao PL 84/99 os termos "dispositivos de comunicação", que passa a ter a seguinte redação:

> "**Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático, rede de computadores ou sistema informatizado"**

Emenda Supressiva nº 10

Suprima-se do tipo penal do art. 266 previsto no art. 7º do Substitutivo do Senado Federal ao PL 84/99 os termos "dispositivos de comunicação", que passa a ter a seguinte redação:

> "Art. 266. Interromper ou perturbar serviço telegráfico, radiotelegráfico, telefônico, telemático, informático, rede de computadores, de sistema informatizado ou de telecomunicação, assim como impedir ou dificultar-lhe o restabelecimento:"

Emenda Supressiva Parcial nº 11

Suprima-se do inciso VI do art. 251 previsto no art. 10 do Substitutivo do Senado Federal ao PL 84/99 os termos "dispositivos de comunicação", que passa a ter a seguinte redação:

> "VI - Difunde, por qualquer meio, código malicioso com o intuito de facilitar ou permitir o acesso indevido a rede de computadores ou a sistema informatizado, em prejuízo da administração militar."

Emenda Supressiva nº 12

Suprima-se do caput art. 262-A e de seu parágrafo 1º, ambos previstos no art. 12 do Substitutivo do Senado Federal ao PL 84/99, os termos "dispositivos de comunicação", que passam a ter as seguintes redações:

> "Art. 262-A. Inserir ou difundir código malicioso em rede de computadores, ou sistema informatizado, desde que o fato atente contra a administração militar: (...)
>
> "§ 1º Se do crime resulta destruição, inutilização, deterioração, alteração, dificultação do funcionamento, ou funcionamento não autorizado pelo titular de rede de computadores, ou de sistema informatizado: (...)"

Emenda Supressiva nº 13

Suprima-se do caput do art. 339-B, previsto no art. 13 do Substitutivo do Senado Federal ao PL 84/99, os termos "dispositivos de comunicação", que passa a ter a seguinte redação:

> **"Acesso não autorizado à rede de computadores ou sistema informatizado**
>
> Art. 339-A. Acessar, mediante violação de segurança, rede de computadores ou sistema informatizado, protegidos por expressa restrição de acesso, desde que o fato atente contra a administração militar: (...)"

Emenda Supressiva nº 13

Suprima-se do caput do art. 339-B, previsto no art. 13 do Substitutivo do Senado Federal ao PL 84/99, os termos "dispositivos de comunicação", que passa a ter a seguinte redação:

"Art. 339-B. Obter ou transferir, sem autorização ou em desconformidade com autorização do legítimo titular da rede de computadores ou sistema informatizado, protegidos por expressa restrição de acesso, dado ou informação neles disponível, desde que o fato atente contra a administração militar:"

Emenda Supressiva nº 14

Suprima-se do artigo 16 do Substitutivo do Senado Federal ao PL 84/99 o inciso I, que traz o conceito de "dispositivo de comunicação", renumerando-se os demais incisos. Suprimam-se os termos "dispositivos de comunicação" também dos já renumerados incisos II, IV e V.

Emenda de redação nº 15

Ajuste-se a redação do inciso IV do artigo 16 do Substitutivo do Senado Federal ao PL 84/99, alterando-se o termo "dados informáticos" para "dados eletrônicos".

A alteração proposta visa ajustar a redação do conceito previsto nesse inciso aos demais termos contidos nos seguintes artigos, nos quais os termos utilizados, embora refiram-se ao mesmo objeto, são "dados eletrônicos":

- Art. 163, *caput*;

- Tipo penal do artigo 297 do Código Penal e o correspondente *caput* do artigo 297;

- Tipo penal do artigo 298 do Código Penal e o correspondente *caput* do artigo 298;

- Tipo penal do artigo 262, *caput*, do Código Penal Militar e o correspondente caput do artigo 262;

- Artigo 311, *caput*, do Código Penal Militar;

- Artigo 356, inciso II e III, do Código Penal Militar.

Por conseqüência, ajuste-se também a redação do inciso V, já renumerado, deste artigo 16.

Observadas, portanto a Emenda Supressiva nº 14 e as Emendas de Redação nº 15, o artigo 16 do Substitutivo do Senado Federal ao PL 84/99 passa a ter a seguinte redação:

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

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

II – rede de computadores: o conjunto de computadores 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;

III – 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;

IV – dados eletrônicos: qualquer representação de fatos, de informações ou de conceitos sob forma suscetível de processamento numa rede de computadores ou sistema informatizado;

V – dados de tráfego: todos os dados eletrônicos relacionados com sua comunicação efetuada por meio de uma rede de computadores ou sistema informatizado, 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."

Emenda Supressiva nº 16

Suprima-se o art. 17 do Substitutivo do Senado Federal ao PL 84/99, renumerando-se os seus posteriores artigos.

Embora, em alinhamento ao disposto na Convenção de Budapeste, tenha o relator do Substitutivo do Senado Federal tentado esclarecer o objetivo da lei e os bens por ela protegidos, na verdade o que se pretende proteger com essa nova legislação são os proprietários ou titulares dos dados, redes de computadores sistemas informatizados, sejam eles pessoas físicas ou jurídicas, entidades públicas ou privadas, motivo pelo qual sugerimos a supressão do seu artigo 17.

Emenda Supressiva nº 17

Suprima-se do art. 17, já renumerado, do Substitutivo do Senado Federal ao PL 84/99 os termos "dispositivos de comunicação", que passa a ter a seguinte redação:

"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 ou sistema informatizado."

Emenda Supressiva nº 18

O Congresso Nacional, após iniciativa da CPI da Pedofilia, e tendo em vista a relevância dos crimes realizados contra crianças e adolescentes, em especial os crimes relacionados à pedofilia, aprovou a Lei nº 11.829, de 25.11.2008, que alterou a Lei nº 8.069/90 - Estatuto da Criança e do Adolescente (ECA), para *"aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet."*

Sendo assim, ao texto final a ser levado à apreciação do Presidente da República deve-se suprimir os seguintes artigos, pois já abrangidos pela Lei supra mencionada em seus artigos 240, 241 e 241-A.

- Art. 5º do PL 84/99 da Câmara dos Deputados, que trazia alterações ao Código Penal, inserindo o art. 218-A sobre "Pornografia Infantil"

- Art. 20 do Substitutivo do Senado Federal ao PLC 89/03, que trazia alterações no artigo 241 do Estatuto da Criança e do Adolescente.

Emenda Supressiva nº 19

Suprima-se do inciso V, inserido no art. 1º da Lei nº 10.446, de 08 de maio de 2002, tal como previsto no art. 19, já renumerado, do Substitutivo do Senado Federal ao PL 84/99 os termos "dispositivos de comunicação", passando o mesmo a ter a seguinte redação:

"(...) V – os delitos praticados contra ou mediante rede de computadores ou sistema informatizado.

....." (NR)

Sobre esse inciso, importante manifestarmo-nos pela sua manutenção. A Lei nº 10.446/2002, dispõe "*sobre* ***infrações penais de repercussão interestadual ou internacional que exigem repressão uniforme****, para os fins do disposto no inciso I do § 1º do art. 144 da Constituição."*

Note-se que, em seu artigo 1º traz o seguinte: "Art. 1º Na forma do inciso I do § 1º do art. 144 da Constituição, quando houver repercussão interestadual ou internacional que exija repressão uniforme, poderá o Departamento de Polícia Federal do Ministério da Justiça, **sem prejuízo da responsabilidade dos órgãos de segurança pública arrolados no art. 144 da Constituição Federal, em especial das Polícias Militares e Civis dos Estados**, ***PROCEDER À INVESTIGAÇÃO***, dentre outras, das seguintes infrações penais:"

Assim, não vemos inconstitucionalidade no que nela disposto, uma vez que tal lei apenas determina que, nos crimes nela arrolados, a Polícia Federal terá **PROCEDÊNCIA** de investigação, mas não retira das Polícias Civil e militar a competência para atuar e investigar tais crimes.

Ademais, não se tem notícia de qualquer questionamento quanto à constitucionalidade dessa lei em qualquer tribunal desse país.

Dando continuidade a esse parecer, antes de adentrarmos à proposição de supressão de partes do artigo 20, já renumerado, do Substitutivo do Senado Federal ao PL 84/99, tecemos alguns comentários, que visam esclarecer aspectos de extrema relevância quanto ao que nele contido, o que poderá arrefecer potenciais críticas a esse dispositivo e seu conteúdo.

Ressalte-se, inicialmente, que a guarda de log de acesso, prevista no inciso I do artigo 20, já renumerado, do Substitutivo do Senado Federal ao PL 84/99, é essencial para a identificação de autoria de um crime praticado pela internet. Essa informação permite que se localize o local de onde partiu o ataque, recorrendo-se, então à investigação usual, para fim de identificação de quem utilizou aquela máquina no período identificado como o de uso para tal ataque.

O texto desse inciso do PL é claro ao determinar que essa informação ("log de acesso") só será fornecida à AUTORIDADE INVESTIGATÓRIA, mediante PRÉVIA REQUISIÇÃO JUDICIAL, que, por sua vez, servirá para dar provimento à "INVESTIGAÇÃO PÚBLICA FORMALIZADA".

Não há de se falar, portanto, em invasão de privacidade, pois tal informação será utilizada, única e exclusivamente, para a investigação de um **crime já identificado e em fase de investigação pela autoridade competente**.

Por sua vez, o inciso II do artigo 20, já renumerado, refere-se aos "logs de conteúdo", os quais, APENAS APÓS REQUISIÇÃO JUDICIAL serão FORNECIDOS À AUTORIDADE INVESTIGATÓRIA. Tudo que for guardado entre a ordem judicial e o fim da correspondente investigação **deverá ser guardado com absoluta confidencialidade e inviolabilidade pelo provedor de conteúdo** (vide o parágrafo 1º do artigo 20 abaixo, já renumerado, que tratará das condições de segurança dessas informações, as quais deverão ser auditadas):

> *"§ 1º Os dados de que cuida o inciso I deste artigo, **AS CONDIÇÕES DE SEGURANÇA DE SUA GUARDA**, a AUDITORIA à qual serão SUBMETIDOS e a autoridade competente responsável pela auditoria, serão definidos nos termos de regulamento."*

Ressalte-se, ainda, que a Constituição Federal, em seu art. 5º, inciso IV[1], veda o anonimato, vinculando tal vedação à liberdade de pensamento e manifestação. Trata-se de um dos princípios fundamentais da nossa sociedade, cujo respeito aos valores é necessário ao pleno equilíbrio dos direitos e deveres de todos os cidadãos. Conclui-se, portanto, que, ao direito de acesso à internet, deve-se contrapor o dever social de identificação, sob pena de que o anonimato venha a permitir àqueles de má-fé praticarem diversas modalidades de crimes e infrações.

Em relação ao prazo de guarda de "logs de acesso", importante aqui destacar que o prazo proposto está em alinhamento às Recomendações para o Desenvolvimento e Operação da Internet no Brasil do Comitê Gestor da Internet (Item 3.2. Manutenção de Dados de Conexão), norma editada em 19.08.1999, disponível em: http://www.cgi.br/publicacoes/documentacao/desenvolvimento.htm

Nesse sentido, trazemos informações sobre como outros países estão tratando essa questão (cf. artigo 15º da Diretiva 2006/24/CE, da Comunidade Européia).

- 18 meses: Alemanha, Áustria, Grécia, Eslovênia, Polônia

- Holanda: máximo de 18 meses

- 36 meses: Bélgica, Estônia, República Checa.

Sendo assim, propomos a manutenção do artigo 20, já renumerado, com as seguintes supressões.

Emenda Supressiva nº 20

Suprima-se o inciso III do artigo 20, já renumerado, do Substitutivo do Senado ao PL 84/99.

A supressão desse inciso se deve ao fato de que não se pode transferir ao particular competência atribuída aos órgãos das polícias civis e militares, cujas competências estão claramente definidas no artigo 144, da Constituição Federal. As denúncias sobre crimes devem ser endereçadas exclusivamente a esses órgãos, a quem compete fazer juízo de valor sobre o fato que lhes é apresentado. Se para os delegados da polícia civil já há dificuldades em tipificar determinados delitos

[1] IV - é livre a manifestação do pensamento, sendo vedado o anonimato;

realizados nos meios eletrônicos; se os promotores públicos, a quem compete apresentar denúncia sobre tais crimes, também têm essa dificuldade; se aos juízes, que diante de provas e fatos, tal tipificação pode redundar em um processo de interpretação legal, como transferir ao particular essa responsabilidade, expondo-o a toda uma gama de conseqüências por transferir a informação sobre um suposto crime que, posteriormente não se confirma?

Ainda, a leitura desse dispositivo pode levar à interpretação de que, para ter ciência de um delito, haveria o provedor de conteúdo de monitorar seus usuários. Embora o objetivo do texto do Substitutivo aprovado pelo Senado Federal, não seja esse, abrir-se-á a possibilidade de tal interpretação, uma vez que, inclusive por uma precaução legal, antes mesmo de enviar a informação sobre a denúncia, o provedor possivelmente fará um juízo de valor sobre tal denúncia, qualificando-a ou não dentre os tipos penais sujeitos ao acionamento penal público incondicionado. Novamente, estar-se-á transferindo uma competência dos órgãos do poder público a um ente privado (a de julgar), sujeitando-o a toda uma sorte de reflexos negativos em relação à informação enviada ou, se entender não ser o caso aplicável ao dispositivo, não enviada.

Emenda Supressiva nº 21

Suprimam-se os §§ 2º e 3º do artigo 20, já renumerado, do Substitutivo do Senado ao PL 84/99, renumerando-se o parágrafo 1º, que passa a ser o parágrafo único.

Manifestamo-nos pela supressão do parágrafo segundo do artigo 20, já renumerado, do Substitutivo ao PL 84/99, uma vez que o Código Penal, em seu artigo 330, tipifica o crime de Desobediência, assim qualificado como *"Desobedecer a ordem legal de funcionário público"*, já prevendo pena de detenção, de quinze dias a seis meses, e **multa**, a ser aplicada pela autoridade judicial desatendida.

Complementa o Código de Processo Civil que prevê, em seu art. 14:

> *"Art. 14. São deveres das partes e de todos aqueles que de qualquer forma participam do processo: (...)*
>
> *V - **cumprir com exatidão os provimentos mandamentais e não criar embaraços à efetivação de provimentos judiciais**, de natureza antecipatória ou final.*
>
> *Parágrafo único. Ressalvados os advogados que se sujeitam exclusivamente aos estatutos da OAB, **a violação do disposto no inciso V deste artigo constitui ato atentatório ao exercício da jurisdição, podendo o juiz, sem prejuízo das sanções criminais, civis e processuais cabíveis, aplicar ao responsável multa em montante a ser fixado de acordo com a gravidade da conduta e não superior a vinte por cento do valor da causa**; não sendo paga no prazo estabelecido, contado do trânsito em julgado da decisão final da causa, a multa será inscrita sempre como dívida ativa da União ou do Estado."*

Assim, a aplicação da multa no âmbito civil, que eventualmente poderá ser diária, será fixada pelo magistrado com a finalidade específica de compelir, legitimamente, o seu destinatário a cumprir referida ordem, ocorrendo, nesse caso, a descaracterização do crime de desobediência (vide HC 86.254-3/RS, Rel. Min. Celso de Mello, DJ 10.03.06).

Além disso, o parâmetro estabelecido no parágrafo a ser suprimido nos parece inconstitucional, ao ferir os princípios da razoabilidade e da proporcionalidade (este aferível apenas perante o caso

concreto), implicando em vício ao devido processo legal material (art. 5º, LIV, da CF), por estabelecer limites às multas que, observada a quantidade de requisições a serem atendidas, poderá inviabilizar economicamente a empresa solicitada, caso não as atenda, sendo tais multas dobradas, em caso de reincidência. Assim, entendemos que, *"considerando-se a natureza, a gravidade e o prejuízo resultante da infração"*, terá a autoridade judicial desatendida, observando a legislação vigente, tempero ao aplicar eventual multa.

Em decorrência à supressão do parágrafo segundo, suprima-se também o parágrafo terceiro desse artigo.

Observadas as Emendas Supressivas nº 20 e 21, passa o artigo 20, já renumerado a ter a seguinte redação:

> "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 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;
>
> II – preservar imediatamente, após requisição judicial, outras informações requisitadas em curso de investigação, respondendo civil e penalmente pela sua absoluta confidencialidade e inviolabilidade;
>
> **Parágrafo único.** Os dados de que cuida o inciso I deste artigo, as condições de segurança de sua guarda, a auditoria à qual serão submetidos e a autoridade competente responsável pela auditoria, serão definidos nos termos de regulamento."

Por fim, propomos a seguinte emenda, visando reunir parte de texto aprovado por essa Câmara dos Deputados com o texto do art. 163 do Substitutivo do Senado Federal ao PL 84/99, nos seguintes termos e fundamentos.

Emenda Aglutinativa nº 22

Reúnam-se o caput do art. 163 do Substitutivo do Senado Federal ao PL 84/99, ao texto do § 2º mesmo PL tal como aprovado pela Câmara dos Deputados, esclarecendo que ambos se complementam.

Essa emenda aglutinativa tem o objetivo de tornar claro a equiparação de dados eletrônicos a coisa, assim entendido o dado eletrônico, a informação, a base de dados, as senhas ou qualquer outro meio de identificação para acesso a meios eletrônicos ou sistema informatizado.

Com a aglutinação ora proposta, pretende-se inserir no código penal conceitos técnicos da área de informática, tornando mais clara ao Poder Judiciário, aos aplicadores da lei e aos cidadãos comuns a amplitude dessa nova legislação, o que permitirá, por exemplo, confirgurar com mais facilidade, crimes de clonagem de cartões ou mesmo furto de dados.

Aprovada essa Emenda, passará o artigo 4º do Projeto de Lei nº 84, de 1999, a ter a seguinte redação:

Art. 4º O 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:

.....”

§ 2º Equipara-se à coisa:

I – o dado, a informação ou a base de dados presente em meio eletrônico ou sistema informatizado;

II – a senha ou qualquer meio de identificação que permita o acesso a meio eletrônico ou sistema informatizado.

Sala da Comissão, 14 de dezembro de 2010.

Deputado Regis de Oliveira
Relator