PARECER Nº , DE 2007

Da COMISSÃO DE CIÊNCIA, TECNOLOGIA, INOVAÇÃO, COMUNICAÇÃO E INFORMÁTICA, sobre o Projeto de Lei da Câmara nº 89, de 2003, e Projetos de Lei do Senado nº 137, de 2000, e nº 76, de 2000, todos referentes a crimes na área de informática.

RELATOR: Senador **EDUARDO AZEREDO**

I – RELATÓRIO

Vem a esta Comissão, para exame, o Projeto de Lei da Câmara (PLC) n° 89, de 2003 (n° 84, de 1999, na origem), e os Projetos de Lei do Senado (PLS) n° 137, de 2000, e n° 76, de 2000, todos referentes a crimes na área de informática. Tramitam em conjunto em atendimento ao Requerimento n° 847, de 2005, do Senador Renan Calheiros. Em decorrência do Requerimento n° 848, de 2005, foi extinta a urgência na tramitação do PLC n° 89, de 2003, que havia sido declarada em decorrência da aprovação do Requerimento n° 599, de 2005, de autoria da Senadora Ideli Salvatti.

Em razão da tramitação conjunta, os Projetos de Lei do Senado perderam o caráter terminativo nas comissões.

O PLS n° 137, de 2000, de autoria do Senador Leomar Quintanilha, consiste em apenas um artigo, além da cláusula de vigência, e visa a aumentar em até o triplo as penas previstas para os crimes contra a pessoa, o patrimônio, a propriedade imaterial ou intelectual, os costumes e a criança e o adolescente, na hipótese de tais crimes serem cometidos por meio da utilização da tecnologia de informação e telecomunicações.

O PLS n° 76, de 2000, de autoria do Senador Renan Calheiros, apresenta tipificação de condutas praticadas com o uso de computadores, e lhes atribui as respectivas penas, sem alterar, entretanto, o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal.

Classifica os crimes cibernéticos em sete categorias: contra a inviolabilidade de dados e sua comunicação; contra a propriedade e o patrimônio; contra a honra e a vida privada; contra a vida e a integridade física das pessoas; contra o patrimônio fiscal; contra a moral pública e a opção sexual; e contra a segurança nacional. Tramitou em conjunto com o PLS n° 137, de 2000, por força da aprovação do Requerimento n° 466, de 2000, de autoria do Senador Roberto Freire, por versarem sobre a mesma matéria.

O PLC n° 89, de 2003, de iniciativa do Deputado Luiz Piauhylino, altera o Código Penal (CP) e a Lei n° 9.296, de 24 de julho de 1996, e dá outras providências. Resulta do trabalho do grupo de juristas que aperfeiçoou o PL n° 1.713, de 1996, de autoria do Deputado Cássio Cunha Lima, arquivado em decorrência do término da legislatura. As alterações propostas visam a criar os seguintes tipos penais, cometidos contra sistemas de computador ou por meio de computador: acesso indevido a meio eletrônico (art. 154-A); manipulação indevida de informação eletrônica (art. 154-B); pornografia infantil (art. 218-A); difusão de vírus eletrônico (art. 163, § 3°); e falsificação de telefone celular ou meio de acesso a sistema informático (art. 298-A).

Além dessas modificações, o referido projeto acrescenta o termo "telecomunicação" aos crimes de atentado contra a segurança de serviço de utilidade pública (art. 265) e de interrupção ou perturbação de serviço telegráfico ou telefônico (art. 266); estende a definição de dano do art. 163 para incluir elementos de informática; equipara o cartão de crédito a documento particular no tipo de falsificação de documento particular (art. 298); define meio eletrônico e sistema informatizado, para efeitos penais (art. 154-C); e permite a interceptação do fluxo de comunicações em sistema de informática ou telemática, mesmo para crimes punidos apenas com detenção (art. 2°, § 2°, da Lei n° 9.296, de 24 de julho de 1996).

Tivemos a honra de relatar essas proposições perante a Comissão de Educação (CE), onde foram amplamente debatidas.

Apresentamos relatório e voto pela aprovação do PLS nº 76, de 2000 – por ser esse mais abrangente e mais antigo –, com proveito parcial dos demais, na forma do Substitutivo oferecido, que logrou ser aprovado perante a Comissão, constituindo-se em Parecer, que integra este processado.

Em síntese, o Substitutivo ao PLS nº 76, de 2000, aprovado na Comissão de Educação pretende:

a) inserir no CP os arts. 163-A, para tipificar o crime de *dano por difusão de vírus eletrônico*; 154-A, para definir o delito de *acesso indevido a dispositivo de comunicação*; 154-B, descrevendo o tipo de *manipulação indevida de informação eletrônica*; 154-C, precisando, para os efeitos da lei, os conceitos de *dispositivo de comunicação, sistema informatizado, e outros;* 154-D, para definir o crime de *divulgação de informações depositadas em bancos de dados*; 154-E, incorporando o delito de *não guardar dados de conexões e comunicações realizadas*; e o art. 154-F, tipificando a conduta de *permitir acesso por usuário não identificado e não autenticado*;

b) acrescentar, ainda, no CP, o art. 183-A, para equiparar a "coisa" todo dado ou informação em meio eletrônico, a base de dados armazenada em dispositivo de comunicação e o sistema informatizado, a senha ou qualquer meio que proporcione acesso aos mesmos;

c) alterar o art. 265 do CP, para incluir como objeto do crime de atentado os serviços de informação e telecomunicação;

d) alterar o art. 266 do CP, para prever o crime de interrupção ou perturbação de serviço telemático ou de telecomunicação;

e) acrescentar, no CP, o art. 266-A, para definir o crime de *difusão maliciosa de código*;

f) inserir parágrafo único no art. 298 do CP, para equiparar a documento particular o cartão de crédito ou débito ou

qualquer dispositivo portátil de armazenamento ou processamento de informações;

g) acrescentar o art. 298-A no CP, para definir o crime de *falsificação de telefone celular ou meio de acesso a sistema eletrônico*;

h) inserir o art. 141-A no CP, para estabelecer que os crimes contra a honra terão a pena aumentada de dois terços, se forem cometidos por intermédio de dispositivo de comunicação ou sistema informatizado;

i) alterar o Código Penal Militar, inserindo dispositivos nos moldes dos mencionados nas alíneas *a, b* e *e* acima.

j) no âmbito processual, inserir o § 2º no art. 2º da Lei nº 9.296, de 1996, para permitir a interceptação do fluxo de comunicações em dispositivo de comunicação ou sistema informatizado, ainda que o fato investigado constitua infração penal punida, no máximo, com pena de detenção.

Durante o longo processo de debate sobre a matéria, dentro e fora do Senado Federal, o Substitutivo ao PLS nº 76, de 2000, aprovado na Comissão de Educação, foi aperfeiçoado para ser apresentado à Comissão de Constituição e Justiça (CCJ).

Foram apresentadas, no âmbito da CCJ, duas emendas oferecidas pelo nobre e eminente Senador Flexa Ribeiro, a primeira excluindo a conceituação e aplicação da "defesa digital", sendo retirada pelo autor a Emenda nº 02/CCJ.

Após a audiência pública de 4 de julho, o eminente Senador Valter Pereira apresentou a Emenda nº 03/CCJ, alterando a Lei nº 7.716, de 5 de janeiro de 1989, § 2º do art. 20, que passaria a abranger os crimes de discriminação de raça e de cor cometidos pela divulgação na rede mundial de computadores.

Ainda, em decorrência de alguns questionamentos ocorridos durante a referida audiência pública, o nobre Senador Antônio Carlos Valadares apresentou a Emenda nº 04/CCJ, de redação, que sugeria alteração

do inciso I do art. 21 do Substitutivo, retirando a expressão "aptos à identificação do usuário" e incluindo a expressão "com o estrito objetivo do provimento de investigação pública formalizada".

Embora não cite explicitamente, a Emenda 04/CCJ provocou a emenda de redação aqui realizada pelo Relator, alterando o texto dos dispositivos abaixo, mantendo-os coerentes com o inciso I então alterado:

a. *o inciso III do art. 21, que trata do fornecimento dos dados preservados;*
b. *o inciso IV do art. 21, que trata da preservação imediata de dados de conexões;*
c. *o § 1º do art. 21, que remete para o regulamento o detalhamento dos dados a preservar;*
d. *o art. 22, que define que não há quebra de sigilo no fornecimento de informações autorizado judicialmente.*

A Emenda 04/CCJaltera também o inciso V do mesmo art. 21 do Substitutivo, incluindo a expressão "de acionamento penal público incondicionado", restringindo, assim, os crimes ali citados.

Acolhidas pelo Relator, as Emendas 01, 03 e 04 da CCJ foram incorporadas ao Substitutivo proposto.

Estando o Projeto em pauta na CCJ, pronto para discussão, foram aprovados, em 2 de outubro de 2007, os Requerimentos nºs 1.029 e 1.030, de 2007, solicitando que a matéria fosse analisada pela Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática (CCT) e pela Comissão de Assuntos Econômicos (CAE), respectivamente.

Regimentalmente, estando sobrestada sua tramitação na CCJ, o Projeto passa a tramitar nas duas Comissões, após o que volta à CCJ para decisão terminativa.

Analisadas as sugestões ulteriores, na sua maioria de redação para clareza e concisão, o novo substitutivo, apresentado perante a Comissão de Constituição e Justiça, e já consolidado com as emendas lá recebidas, é o resultado de várias alterações, supressões e inclusões, que passamos a descrever:

a) alterar a ementa da Lei para nela incluir a indicação da alteração da Lei nº 9.296, de 1996, a indicação da alteração do Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), a indicação da alteração da Lei nº 10.446, de 8 de maio de 2002 , (a lei da repressão uniforme pelo DPF), a indicação da alteração da Lei nº 8.078, de 11 de setembro de 1990 (Código do Consumidor), e a indicação de alteração da Lei nº 7.716, de 5 de janeiro de 1989 (Lei Afonso Arinos);

b) incluir um novo art. 1º, para cumprir o que determina o art. 7º da Lei Complementar nº 95, de 26 de fevereiro de 1998;

c) substituir as referências aos termos *"eletrônico"* e *"eletronicamente"* pelas expressões abrangentes *"eletrônico ou digital ou similar"* ou *"eletrônica ou digitalmente ou de forma equivalente"*, respectivamente, em todo o corpo do Substitutivo;

d) no novo art. 154-A do Código Penal, e no seu correspondente novo art. 339-A do Código Penal Militar:
    a. incluir a expressão *"ou sistema informatizado"* no título do artigo;
    b. substituir a expressão *"indevido"* pela expressão *"não autorizado"* e a expressão *"indevidamente"* pela expressão *"sem autorização do legítimo titular, quando exigida"*, ao final do texto;
    c. retirar a expressão *"indevidamente"* do texto do § 1º do artigo;

e) no novo art. 154-B do Código Penal, e no seu correspondente novo art. 339-B do Código Penal Militar:
    a. trocar de posição na oração, a expressão *"dado ou informação obtida"*;
    b. incluir a ação de *"obter"* o dado ou a informação;
    c. substituir a expressão *"indevidamente"* pela expressão *"sem autorização do legítimo titular, quando exigida"*;
    d. incluir a ação de *manter consigo o dado ou a informação obtidos com autorização por prazo definido e que tenha expirado*;

e. incluir a majorante de um terço da pena *se o dado ou a informação obtida indevidamente ou sem autorização são divulgados pela rede de computadores ou qualquer outro meio de divulgação em massa*;

f) modificar as definições constantes do novo art. 154-C do Código Penal, e do seu correspondente novo art. 339-C do Código Penal Militar, como segue:

– na definição de "Dispositivo de Comunicação" incluir a expressão *"os meios de captura de dados eletrônicos ou digitais ou similares"*, substituir a expressão *"digitais"* por *"eletrônicos ou digitais ou similares"* e incluir a expressão *"os receptores e os conversores de sinais de rádio ou televisão digital"*, conhecidos como "*set-top box*";

– na definição de "Sistema Informatizado" substituir a expressão *"eletronicamente"* pela expressão *"eletrônica ou digitalmente ou equivalente"*, incluir a expressão *"capturar"* e suprimir a expressão *"rede de computadores ou internet"*, que passou a ser objeto de definição específica;

– retirar as definições relativas a "*usuário"*;

– incluir a definição de "*Rede de Computadores"*, definindo todas as redes de computadores, locais, regionais, nacionais, mundiais, privadas ou públicas.;

– incluir a definição de *"código malicioso"*, como uma seqüência de operações computacionais que resultem em ação de dano ou em obtenção não autorizada de informações contra terceiro;

– retirar a definição de *"defesa digital"* e todas as referências a ela nos demais artigos, que restringia a legitima defesa em ambiente digital a agente habilitado e outras condicionantes;

– incluir as definições de *"dados informáticos" e "dados de tráfego"*;

g) no novo art. 154-D, *caput*, do Código Penal, e no seu correspondente novo art. 339-D, *caput*, do Código Penal Militar:
   a. incluir, as condutas de *"utilizar"* e de *"comercializar"* sem autorização ou para fim diferente da sua constituição o conteúdo de um banco de dados;
   b. incluir para a decisão de autorizar a divulgação de informações contidas em banco de dados, a expressão *"nos casos previstos em lei,"*;
   c. renumerar o parágrafo único como § 1º e acrescentar o § 2º com a majorante de um terço da pena se o crime ocorre em rede de computadores, dispositivo de comunicação ou sistema informatizado, ou em qualquer outro meio de divulgação em massa;

h) retirar o novo art. 154-E do Código Penal e o seu correspondente novo art. 339-E, do Código Penal Militar, que tratavam da "preservação dos dados de conexões realizadas";

i) incluir o inciso V ao § 4º do art. 155 do Código Penal e acrescentarmos o inciso V do § 6º ao seu correspondente art. 240 do Código Penal Militar, que tratam do crime de *"furto qualificado*";

j) substituir, no título do novo art. 163-A do Código Penal, e no seu correspondente novo art. 262-A do Código Penal Militar, a expressão *"vírus"* por *"código malicioso*";

k) no novo art. 163-A do Código Penal, e no seu correspondente novo art. 262-A do Código Penal Militar:
   a. incluir a conduta de fazer a rede de computadores, o dispositivo de comunicação ou o sistema informatizado funcionar para o agente criminoso sem a autorização do usuário;
   b. incluir em dois parágrafos subseqüentes, os crimes qualificados da intenção de causar dano e o de

realmente produzir resultado danoso, com o correspondente agravamento da pena;

l) alterar a localização do novo tipo de *"difusão de código malicioso"* com objetivo de fraude, o "*phishing*", anteriormente no art. 266-A do Código Penal, ficando melhor codificado no novo art. 171-A (do Título II – Dos Crimes contra o Patrimônio – Capítulo VI – Estelionato e outras Fraudes) e alterar a sua pena, passando de detenção de um a dois anos para reclusão de um a três anos;

m) acrescentar à alteração do art. 266 do Código Penal as expressões *"informático, dispositivo de comunicação, rede de computadores, sistema informatizado"*, para adequação à Lei 9.296, de 1996 e para nele incluir como tipo penal *"o ataque a rede de computadores ou sistema informatizado"*, como o *DoS (Denial-of-Service attack),* o *DDoS (Distributed-Denial-of-Service attack)* e outros equivalentes;

n) substituir no parágrafo único do art. 298 do Código Penal, o acrescentado pelo Substitutivo, a expressão *"armazenamento ou processamento"* pela expressão *"captura, armazenamento, processamento ou transmissão"*;

o) incluir o inciso V ao art. 313 do Decreto-Lei nº 3.689, de 3 de outubro de 1941, Código de Processo Penal (CPP) para a *decretação de prisão preventiva nos crimes dolosos punidos com detenção,* se tiverem sido praticados mediante uso de rede de computadores, dispositivo de comunicação ou sistema informatizado;

p) acrescentar determinação para que a autoridade competente, nos termos de regulamento, estruture órgãos, setores e equipes de agentes especializados no combate à ação delituosa praticada em rede de computadores, dispositivo de comunicação ou sistema informatizado;

q) alterar a Lei nº 10.446, de 8 de maio de 2002, a lei da repressão uniforme, para *possibilitar a atuação da Polícia*

Federal na investigação dos crimes tratados no projeto de lei;

r) acrescentar parágrafo único ao art. 9º da Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor – CDC), *que passa a se aplicar à segurança digital do consumidor*;

s) incluir artigo tratando das obrigações do responsável pelo provimento de acesso a uma rede de computadores, quais sejam:
   a. manter a obrigação da preservação de dados de conexões, retirando a expressão "e comunicações", reduzindo a lista de informações a serem guardadas, e reduzindo o prazo de guarda de "cinco" para "três" anos;
   b. tornar disponíveis à autoridade competente e por autorização expressa da autoridade judicial os dados de conexão no curso de auditoria técnica a que forem submetidos;
   c. fornecer os dados de conexões realizadas quando solicitado pela autoridade competente no curso de investigação e por autorização expressa da autoridade judicial;
   d. preservar imediatamente, após a solicitação expressa da autoridade judicial, no curso de investigação, os dados de conexões realizadas, e outras informações solicitadas por aquela investigação, respondendo pela sua absoluta confidencialidade e inviolabilidade;
   e. informar, de maneira sigilosa, à autoridade competente à qual está jurisdicionado, denúncia da qual tenha tomado conhecimento e que contenha indícios de prática de crime, sujeito a ação penal pública incondicionada, na rede de computadores, sob sua responsabilidade;
   f. informar ao usuário que aquela conexão de acesso à rede de computadores sob sua responsabilidade obedece às leis brasileiras, e que toda comunicação ali realizada será de exclusiva responsabilidade do usuário, perante as leis brasileiras;

g. alertar aos seus usuários, em campanhas periódicas, quanto ao uso criminoso de rede de computadores, dispositivo de comunicação e sistema informatizado;
h. divulgar aos seus usuários, em local destacado, as boas práticas de segurança no uso de rede de computadores, dispositivo de comunicação e sistema informatizado;
i. remeter para regulamento o detalhamento relativo à guarda de dados e outras obrigações;
j. determinar o prazo de transição de cento e oitenta dias para que os dados e procedimentos requeridos estejam disponíveis;
k. definir, respectivamente, a multa pelo descumprimento das obrigações e a destinação dos recursos financeiros resultantes da aplicação da multa;

t) incluir artigo do substitutivo determinando que não constitui violação do dever de sigilo a comunicação, às autoridades competentes, de prática de ilícitos penais, abrangendo o fornecimento de informações de acesso e hospedagem quando constatada qualquer prática criminosa.

Não foram apresentadas emendas nesta Comissão.

II – ANÁLISE

Preliminarmente, cabe mencionar que a matéria está adstrita ao campo da competência privativa da União para legislar sobre direito penal e processual, conforme dispõe o art. 22, I, da Constituição Federal. Neste caso, qualquer membro do Congresso Nacional tem legitimidade para iniciar o processo legislativo.

O tema é atual e merece a devida atenção do Congresso Nacional. Segundo recentes dados divulgados pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (www.cert.br), os códigos maliciosos, classificados como *worm*, representam 40%, ou 51 mil, de todos os incidentes reportados ocorridos na internet no Brasil até setembro de 2007.

Em segundo lugar aparecem as tentativas de fraudes, que chegam a pouco mais de 50 mil e representam 39% dos mesmo incidentes. Segue-lhes os 22 mil incidentes, ou 17%, relativos a leitura simples ou busca, no jargão técnico, *scan*. Em menor volume, mas com mesmo grau de periculosidade ou até maior, os incidentes restantes, são distribuídos em 1.800 ataques de negação de serviço (*DoS - Denial of service*), ou 1,5%, 1.350 ataques a servidores (*aw*), ou 1%, e 200 invasões.

Os números, frise-se bem, podem ser muito maiores, dado que o CERT.br considera apenas as informações reportadas espontaneamente pelos usuários e administradores de redes. Ao todo, o CERT.br recebeu, no ano passado, 197 mil comunicações de incidentes relacionados à internet, alta de 191% em relação a 2005. Este ano já chegam a 129.010 em setembro, mostrando que há uma tendência de ligeira queda, mas o volume é preocupante.

Em relação ao SPAM os números também são preocupantes. Até o momento não foi possível a sua tipificação penal, embora inúmeros projetos de lei estejam em tramitação. Tratando-se de uma mensagem sem autorização prévia, ele é tecnicamente correto como conceito fundamental de uma rede de computadores, mas é perigoso pois é freqüentemente usado como vetor de disseminação de códigos maliciosos de qualquer tipo e objetivo.

Os gráficos abaixo ilustram melhor:

Fonte: http://www.cert.br/stats/incidentes

Os bancos e o comércio continuam os principais alvos, com perdas estimadas em mais de R$ 300 milhões por ano em fraudes virtuais, mas os crimes contra a honra, calúnia, difamação e injúria, incomensuráveis

no mal que provocam, e de difícil ou impossível reparação, são fortes concorrentes aos crimes econômicos, não em volume, mas no aumento relativo, face ao covarde anonimato na rede e à expansão, ou explosão, do uso de computadores no país.

Com esses números, o Brasil ficou, em 2006, na segunda colocação entre os dez países com maior número de incidentes reportados. O líder são os Estados Unidos da América (EUA), com 24,61% dos incidentes, seguido pelo Brasil, com 21,18% deles, e o Canadá, em terceiro lugar, 9,45%.

De acordo com a Comissão Federal de Comércio dos EUA, o custo de crimes de furto pela internet para pessoas físicas e jurídicas no país atinge US$ 50 bilhões por ano. No Reino Unido, o custo para a economia, segundo o Ministério do Interior, foi de US$ 3,2 bilhões nos últimos três anos.

Como se pode observar, trata-se de problema sério e que precisa ser enfrentado pela legislação brasileira.

Materialmente, não vislumbramos inconstitucionalidades ou vícios de juridicidade nos projetos de lei em apreço. No mérito, reiteramos a análise feita por ocasião da apreciação das proposições na Comissão de Educação e na Comissão de Constituição e Justiça, que resultou no Parecer pelo oferecimento do Substitutivo ora examinado.

Tendo sido lido, e estando com sua discussão suspensa, na CCJ, por força dos requerimentos já citados, entendemos que o Substitutivo apresentado àquela Comissão seja acatado e consolidado, por razões de economia processual e celeridade de tramitação, o que fizemos no Relatório que antecede esta Análise deste Parecer.

Nesta CCT recebemos sugestão de apresentar nova emenda ao Substitutivo, incluindo artigo que altera o *caput* do art. 241 da Lei nº 8.069, de 13 de julho de 1990, para passar a vigorar com a seguinte redação, incluindo nele o tipo penal de "manter consigo", que ficaria como segue:

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

A alteração solicitada diz respeito ao Estatuto da Criança e Adolescente – ECA, onde são tipificados os crimes de pedofilia, contra a criança e adolescente, mas não criminaliza a conduta de "manter" ou "guardar" documentos, fotos, vídeos ou qualquer outra referência. Assim a Emenda vem preencher esta lacuna reclamada por quantos tem se interessado pela matéria.

A matéria em exame vem provocando a manifestação continuada de quantos se interessam por ela, em palestras e reuniões técnicas de que temos participado, aqui no Senado ou em associações de classe e de usuários. Temos colhido sugestões e explicado o trabalho que o Parlamento vem desenvolvendo há dez anos.

O Parecer do Relator na Comissão de Constituição e Justiça contem informações e justificação criteriosa de cada uma das determinações do novo Substitutivo.

Mas é importante registrar novamente que embora o Brasil ainda não seja signatário da *Convenção sobre o Cibercrime*, cumpre registrar que podemos ser considerados um país em harmonia com suas deliberações, pois atendemos às recomendações do seu Preâmbulo, como, por exemplo, "a adoção de poderes suficientes para efetivamente combater as ofensas criminais e facilitar a sua detecção, investigação e persecução penal, nos níveis doméstico e internacional e provendo protocolos para uma rápida e confiável cooperação internacional".

A Convenção recomenda procedimentos processuais penais, a guarda criteriosa das informações trafegadas nos sistemas informatizados e sua liberação para as autoridades de forma a cumprir os objetivos relacionados no preâmbulo.

Além disso, trata da necessária cooperação internacional, das questões de extradição, da assistência mútua entre os Estados, da denúncia espontânea e sugere procedimentos na ausência de acordos internacionais específicos, além da definição da confidencialidade e limitações de uso. Define também a admissão à Convenção de novos Estados por convite e a aprovação por maioria do Conselho.

O que é importante sublinhar é a harmonia brasileira com os termos da Convenção, a correspondência entre o que ela recomenda e aquilo

que está sendo proposto nos projetos de lei ao qual oferecemos o presente Substitutivo.

Assim, segundo a Convenção, *a criação de legislação penal em cada Estado signatário deve tratar*:

– *do acesso ilegal ou não autorizado a sistemas informatizados*, objeto do art. 154-A e art. 155 § 4º inciso V do Código Penal e do art.339-A e art. 240 § 6º inciso V do Código Penal Militar;

– *da interceptação ou interrupção de comunicações*, pela inclusão do § 2º ao art. 2º da Lei nº 9.296, de 24 de julho de 1996;

– *da interferência não autorizada sobre os dados armazenados*, objeto do art. 154-D, do art. 163-A e do art. 171-A do Código Penal e do art.339-D, do art. 262-A e do art. 281-A do Código Penal Militar;

– *da falsificação em sistemas informatizados*, objeto do art. 163-A, do art. 171-A, do art. 298 e do art. 298-A do Código Penal e do art. 262-A e do art. 281-A do Código Penal Militar;

– *da quebra da integridade das informações*, objeto do art. 154-B do Código Penal e do art.339-B do Código Penal Militar;

– *das fraudes em sistemas informatizados com ou sem ganho econômico*, objeto do art. 163-A e do art. 171-A do Código Penal e do art. 262-A e do art. 281-A do Código Penal Militar;

– *da pornografia infantil ou pedofilia*, objeto do art. 241 da Lei 8.069, de 1990, Estatuto da Criança e do Adolescente (ECA), alterado pela Lei 10.764, de 2003 e objeto da alteração proposta pelo substitutivo;

– *da quebra dos direitos de autor*, objeto da Lei 9.609, de 1998, (a Lei do Software), da Lei 9.610, de 1998, (a Lei do Direito Autoral) e da Lei 10.695 de 2003, (a Lei Contra a Pirataria);

– *das tentativas ou ajudas a condutas criminosas*, objeto dos § 1º do art. 154-A do Código Penal e do art. 339-A do Código Penal Militar;

– *da responsabilidade de uma pessoa natural ou de uma organização*, objeto de artigo específico do Substitutivo;

– *das penas de privação de liberdade e de sanções econômicas*, objeto das penas de detenção, ou reclusão, e multa, com os respectivos agravantes e majorantes, das Leis citadas e dos artigos do Substitutivo.

Resumindo, a legislação brasileira em vigor já tipifica alguns dos crimes identificados pela Convenção, como os crimes contra os direitos do autor, crimes de pedofilia, crimes de xenofobia e racismo, também objeto de alteração proposta pelo substitutivo, e, caso a caso, cuida de alguns outros já tipificados no Código Penal.

O presente Projeto de Lei, que atualiza o nosso Código Penal, o Código do Processo Penal, o Código Penal Militar, a Lei das Interceptações Telefônicas, a Lei da Repressão Uniforme, o Código do Consumidor, a Lei Afonso Arinos e o Estatuto da Criança e do Adolescente, coloca o Brasil em posição de destaque para que possa tratar e acordar de maneira diferenciada com os países signatários da Convenção de Budapest e outras, inclusive os EUA, país sede das maiores empresas de tecnologia da informação e sede dos maiores provedores de acesso à rede mundial de computadores.

A crescente harmonia com a Convenção da Europa é importante para otimizar a repressão dos crimes de informática, notadamente transnacionais. Essa harmonia facilitará em muito a cooperação judiciária internacional e eventuais extradições.

Assim que as nossas autoridades competentes considerarem adequado, poderemos, com maior efetividade, ser signatários da Convenção sobre o Cibercrime de Budapest, por meio de convite do Comitê de Ministros do Conselho da Europa (art. 37 da Convenção), ou de outras Convenções e Acordos sobre a matéria.

A propósito, em dezembro de 2006 a Comissão de Relações Exteriores e Defesa Nacional do Senado Federal (CRE) aprovou Requerimento de Informações, de nossa autoria, solicitando ao Ministério das Relações Exteriores o posicionamento oficial do Brasil em relação à Convenção, uma vez que ele ainda não é dela signatário. Em seguida fomos recebidos em audiência pelo Senhor Ministro das Relações Exteriores, para tratar, entre outros assuntos, da *Convenção sobre o Cibercrime* e a posição do Brasil.

Posteriormente recebemos em audiência o Senhor Chefe de Cooperação Técnica do Departamento de Problemas Criminais, da Secretaria Geral do Conselho da Europa, que nos informou que sugeriu à Coordenadora Geral contra o Crime Transnacional do Ministério das Relações Exteriores o envio de carta à Secretaria Geral daquele Conselho solicitando o acesso à Convenção pelo Brasil, para, na seqüência, serem ouvidos os Países-Membros.

Havendo aquiescência destes, o Brasil poderá ser convidado a participar como País Membro.

Isso já se mostra necessário pela dificuldade que nossos investigadores e persecutores penais têm tido em relação aos provedores de acesso localizados no exterior.

A propósito da repressão internacional, entendimento recente, de 16 de outubro de 2006, da 3ª Turma do STJ, reforça a tese de que não importa onde é gerada a página da internet, mas sim onde os efeitos do crime são sentidos. Se não há lesão direta a bens, serviços ou interesses da União, a competência para julgar o caso é da Justiça Estadual, mesmo que o crime tenha sido cometido pela internet, por meio de site hospedado no exterior.

Em junho de 2007 participamos da Conferencia sobre o Cibercrime, em Estrasburgo, França, promovida pelo Conselho da Europa, com a participação de quase duzentos especialistas, de 55 países, membros e não membros, signatários da Convenção e convidados, onde pudemos aprofundar no conhecimento da preocupação mundial com a expansão e o não combate ao infocrime.

III – VOTO

Diante do exposto, e considerando a pertinência e importância da solução proposta, somos pela aprovação do Projeto de Lei da Câmara n° 89, de 2003 (n° 84, de 1999, na Câmara dos Deputados), e dos Projetos de Lei do Senado nº 76 e n° 137, ambos de 2000, na forma do novo Substitutivo que ora oferecemos a esta Comissão de Ciência e Tecnologia.

SUBSTITUTIVO

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

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 9.296, de 24 de julho de 1996, o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código do Processo Penal), a Lei nº 10.446, de 8 de maio de 2002, a Lei nº 8.078, de 11 de setembro de 1990 (Código do Consumidor), a Lei nº 7.716, de 5 de janeiro de 1989, e a Lei nº 8.069, de 13 de julho de 1990, 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 9.296, de 24 de julho de 1996, Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código do Processo Penal), a Lei nº 10.446, de 8 de maio de 2002, a Lei nº 8.078, de 11 de setembro de 1990 (Código do Consumidor), a Lei nº 7.716, de 5 de janeiro de 1989, e a Lei nº 8.069, de 13 de julho de 1990, 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 Capítulo V do Título I da Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) fica acrescido do seguinte art. 141-A:

"**Art. 141-A.** As penas neste Capítulo aumentam-se de dois terços caso os crimes sejam cometidos por intermédio de rede de computadores, dispositivo de comunicação ou sistema informatizado."

Art. 3º O Título I da Parte Especial do Código Penal fica acrescido do Capítulo VI-A, assim redigido:

"Capítulo VI-A

DOS CRIMES CONTRA REDE DE COMPUTADORES, DISPOSITIVO DE COMUNICAÇÃO OU SISTEMA INFORMATIZADO

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

Art. 154-A. Acessar rede de computadores, dispositivo de comunicação ou sistema informatizado, sem autorização do legítimo titular, quando exigida:

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

§ 1º Nas mesmas penas incorre quem, permite, facilita ou fornece a terceiro meio não autorizado de acesso a rede de computadores, dispositivo de comunicação ou sistema informatizado.

§ 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 suas subsidiárias.

§ 3º A pena é aumentada de sexta parte, se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática de acesso.

Obtenção, manutenção, transporte ou fornecimento não autorizado de informação eletrônica ou digital ou similar

Art. 154-B. Obter dado ou informação disponível em rede de computadores, dispositivo de comunicação ou sistema informatizado, sem autorização do legítimo titular, quando exigida:

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

§ 1º Nas mesmas penas incorre quem mantém consigo, transporta ou fornece dado ou informação obtida nas mesmas circunstâncias do "caput", ou desses se utiliza alem do prazo definido e autorizado.

§ 2º Se o dado ou informação obtida desautorizadamente é fornecida a terceiros pela rede de computadores, dispositivo de comunicação ou

sistema informatizado, ou em qualquer outro meio de divulgação em massa, a pena é aumentada de um terço.

§ 3º 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 suas subsidiárias.

Dispositivo de comunicação, sistema informatizado, rede de computadores e defesa digital

Art. 154-C. Para os efeitos penais considera-se:

I – dispositivo de comunicação: o computador, o telefone celular, o processador de dados, os instrumentos de armazenamento de dados eletrônicos ou digitais ou similares, os instrumentos de captura de dados, os receptores e os conversores de sinais de rádio ou televisão digital ou qualquer outro meio capaz de processar, armazenar, capturar ou transmitir dados utilizando-se de tecnologias magnéticas, óticas ou qualquer outra tecnologia eletrônica ou digital ou similar;

II – sistema informatizado: o equipamento ativo da rede de comunicação de dados com ou sem fio, a rede de telefonia fixa ou móvel, a rede de televisão, a base de dados, o programa de computador ou qualquer outro sistema capaz de processar, capturar, armazenar ou transmitir dados eletrônica ou digitalmente ou de forma equivalente;

III – rede de computadores: os instrumentos físicos e lógicos através dos quais é possível trocar dados e informações, compartilhar recursos, entre máquinas, representada pelo conjunto de computadores, dispositivos de comunicação e sistemas informatizados, que obedecem de comum acordo a um conjunto de regras, parâmetros, códigos, formatos e outras informações agrupadas em protocolos, em nível topológico local, regional, nacional ou mundial;

IV - código malicioso: o conjunto de instruções e tabelas de informações ou programa de computador ou qualquer outro sistema capaz de executar uma seqüência de operações que resultem em ação de dano ou de obtenção indevida de informações contra terceiro, de maneira dissimulada ou oculta, transparecendo tratar-se de ação de curso normal;

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

comunicação ou sistema informatizado, incluindo um programa, apto a fazer um sistema informatizado executar uma função;

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.

Divulgação ou utilização indevida de informações contidas em banco de dados

Art. 154-D Divulgar, utilizar, comercializar ou disponibilizar informações contidas em banco de dados com finalidade distinta da que motivou o registro das mesmas, incluindo-se informações privadas referentes, direta ou indiretamente, a dados econômicos de pessoas naturais ou jurídicas, ou a dados de pessoas naturais referentes a raça, opinião política, religiosa, crença, ideologia, saúde física ou mental, orientação sexual, registros policiais, assuntos familiares ou profissionais, além de outras de caráter sigiloso, 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.

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

§ 2º Se o crime ocorre em rede de computadores, dispositivo de comunicação ou sistema informatizado, ou em qualquer outro meio de divulgação em massa, a pena é aumentada de um terço.“

Art. 4º O § 4º do art. 155 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), passa a vigorar acrescido do seguinte inciso V:

“**Art. 155.** .....
.....

§ 4º .....
.....

V - mediante uso de rede de computadores, dispositivo de comunicação ou sistema informatizado ou similar, ou contra rede de computadores, dispositivos de comunicação ou sistemas informatizados e similares”.

..... (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:

“**Dano por difusão de código malicioso eletrônico ou digital ou similar**

Art. 163-A. Criar, 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.

Dano qualificado por difusão de código malicioso eletrônico ou digital ou similar

§ 1º Se o crime é cometido com finalidade de destruição, inutilização, deterioração, alteração, dificultação do funcionamento, ou funcionamento desautorizado 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.

Difusão de código malicioso eletrônico ou digital ou similar seguido de dano

§ 2º Se do crime resulta destruição, inutilização, deterioração, alteração, dificultação do funcionamento, ou funcionamento desautorizado pelo titular, de dispositivo de comunicação, de rede de computadores, ou de sistema informatizado, e as circunstâncias demonstram que o agente não quis o resultado, nem assumiu o risco de produzi-lo:

Pena – reclusão, de 3 (dois) a 5 (cinco) anos, e multa.

§ 3º A pena é aumentada de sexta parte, se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime.

Art. 6º O Capitulo VI do Título II do Código Penal passa a vigorar acrescido do seguinte artigo:

“**Difusão de código malicioso**

Art. 171-A. Difundir, por qualquer meio, programa, conjunto de instruções ou sistema informatizado com o propósito de levar a erro ou, por qualquer forma indevida, induzir alguém a fornecer, espontaneamente e por qualquer meio, dados ou informações que facilitem ou permitam o acesso indevido ou sem autorização, à rede de computadores,

dispositivo de comunicação ou a sistema informatizado, com obtenção de vantagem ilícita, em prejuízo alheio:

Pena – reclusão, de um a três anos.

§ 1º A pena é aumentada de sexta parte, se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática de difusão de código malicioso.

Art. 7º O Código Penal passa a vigorar acrescido do seguinte art. 183-A:

"**Art. 183-A.** Para efeitos penais, equiparam-se à coisa o dado, informação ou unidade de informação em meio eletrônico ou digital ou similar, a base de dados armazenada, o dispositivo de comunicação, a rede de computadores, o sistema informatizado, a senha ou similar ou qualquer instrumento que proporcione acesso a eles."

Art. 8º 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)"

"**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:

..... (NR)"

Art. 9º O art. 298 do Código Penal passa a vigorar acrescido do seguinte parágrafo único:

"**Art. 298**. .....

.....

Falsificação de cartão de crédito ou débito ou qualquer dispositivo eletrônico ou digital ou similar portátil de captura, processamento, armazenamento e transmissão de informações.

Parágrafo único. Equipara-se a documento particular o cartão de crédito ou débito ou qualquer outro dispositivo portátil capaz de capturar, processar, armazenar ou transmitir dados, utilizando-se de tecnologias magnéticas, óticas ou qualquer outra tecnologia eletrônica ou digital ou similar.(NR)"

Art. 10. O Código Penal passa a vigorar acrescido do seguinte art. 298-A:

"**Falsificação de telefone celular ou meio de acesso a rede de computadores, dispositivo de comunicação ou sistema informatizado**

Art. 298-A. Criar ou copiar, indevidamente, ou falsificar código, seqüência alfanumérica, cartão inteligente, transmissor ou receptor de rádio freqüência ou telefonia celular, ou qualquer instrumento que permita o acesso a rede de computadores, dispositivo de comunicação ou sistema informatizado:

Pena – reclusão, de um a cinco anos, e multa."

Art. 11. O § 6º do art. 240 do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), passa a vigorar acrescido do seguinte inciso V:

"**Art. 240.** .....

.....

Furto qualificado

§ 6º .....

.....

V – mediante uso de rede de computadores, dispositivo de comunicação ou sistema informatizado ou similar, ou contra rede de computadores, dispositivos de comunicação ou sistema.

..... (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:

Dano por difusão de código malicioso eletrônico ou digital ou similar

Art. 262-A. Criar, 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.

Dano qualificado por difusão de código malicioso eletrônico ou digital ou similar

§ 1º Se o crime é cometido com finalidade de 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.

Difusão de código malicioso eletrônico ou digital ou similar seguido de dano

§ 2º 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, e as circunstâncias demonstram que o agente não quis o resultado, nem assumiu o risco de produzi-lo:

Pena – reclusão, de 3 (dois) a 5 (cinco) anos, e multa.

§ 3º A pena é aumentada de sexta parte se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime.

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

Capítulo VII-A

DOS CRIMES CONTRA REDE DE COMPUTADORES, DISPOSITIVO DE COMUNICAÇÃO OU SISTEMA INFORMATIZADO

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

Art. 339-A. Acessar rede de computadores, dispositivo de comunicação ou sistema informatizado sem autorização do legítimo titular, quando exigida:

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

§ 1º Nas mesmas penas incorre quem permite, facilita ou fornece a terceiro meio não autorizado de acesso a rede de computadores, dispositivo de comunicação ou sistema informatizado.

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

Obtenção, manutenção, transporte ou fornecimento não autorizado de informação eletrônica ou digital ou similar

Art. 339-B. Obter dado ou informação disponível em rede de computadores, dispositivo de comunicação ou sistema informatizado, sem autorização do legítimo titular, quando exigida:

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

§ 1º Nas mesmas penas incorre quem mantém consigo, transporta ou fornece dado ou informação obtida nas mesmas circunstâncias do *caput*, ou deles se utiliza além do prazo definido e autorizado.

§ 2º Se o dado ou informação obtida indevidamente é fornecida a terceiros pela rede de computadores, dispositivo de comunicação ou sistema informatizado, ou em qualquer outro meio de divulgação em massa, a pena é aumentada de um terço.

Dispositivo de comunicação, sistema informatizado e rede de computadores

Art. 339-C. Para os efeitos penais considera-se:

I – dispositivo de comunicação: o computador, o telefone celular, o processador de dados, os instrumentos de armazenamento de dados eletrônicos ou digitais ou similares, os instrumentos de captura de dados, os receptores e os conversores de sinais de rádio ou televisão digital ou qualquer outro meio capaz de processar, armazenar, capturar ou transmitir dados utilizando-se de tecnologias magnéticas, óticas ou qualquer outra tecnologia eletrônica ou digital ou similar;

II – sistema informatizado: o equipamento ativo da rede de comunicação de dados com ou sem fio, a rede de telefonia fixa ou móvel, a rede de televisão, a base de dados, o programa de computador

ou qualquer outro sistema capaz de processar, capturar, armazenar ou transmitir dados eletrônica ou digitalmente ou de forma equivalente;

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

IV – código malicioso: o conjunto de instruções e tabelas de informações ou programa de computador ou qualquer outro sistema capaz de executar uma seqüência de operações que resultem em ação de dano ou de obtenção indevida de informações contra terceiro, de maneira dissimulada ou oculta, transparecendo tratar-se de ação de curso normal;

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, incluindo-se programas, apta a fazer um sistema informatizado executar uma função;

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.

Divulgação ou utilização indevida de informações contidas em banco de dados

Art. 339-D Divulgar, utilizar, comercializar ou disponibilizar informações contidas em banco de dados com finalidade distinta da que motivou o registro das mesmas, incluindo-se informações privadas referentes, direta ou indiretamente, a dados econômicos de pessoas naturais ou jurídicas, ou a dados de pessoas naturais referentes a raça, opinião política, religiosa, crença, ideologia, saúde física ou mental, orientação sexual, registros policiais, assuntos familiares ou profissionais, além de outras de caráter sigiloso, 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.

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

§ 2º Se o crime ocorre em rede de computadores, dispositivo de comunicação ou sistema informatizado, ou em qualquer outro meio de divulgação em massa, a pena é aumentada de um terço.

Art. 14. O 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 Capítulo VIII-A, assim redigido:

Capítulo VIII-A

DISPOSIÇÕES GERAIS

Art. 267-A. Para efeitos penais, equiparam-se à coisa o dado, informação ou unidade de informação em meio eletrônico ou digital ou similar, a base de dados armazenada, o dispositivo de comunicação, a rede de computadores, o sistema informatizado, a senha ou similar ou qualquer instrumento que proporcione acesso a eles.

Art. 15. O Capítulo I do Título VI 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. 281-A, assim redigido:

Difusão de código malicioso

Art. 281-A. Difundir, por qualquer meio, programa, conjunto de instruções ou sistema informatizado com o propósito de levar a erro ou, por qualquer forma indevida, induzir alguém a fornecer, espontaneamente e por qualquer meio, dados ou informações que facilitem ou permitam o acesso indevido ou sem autorização, à rede de computadores, dispositivo de comunicação ou a sistema informatizado, com obtenção de vantagem ilícita, em prejuízo alheio:

Pena – reclusão, de um a três anos.

Parágrafo único. A pena é aumentada de sexta parte, se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática de difusão de código malicioso.

Art. 16. O art. 2º da Lei nº 9.296, de 24 de julho de 1996, passa a vigorar acrescido do seguinte § 2º, renumerando-se o parágrafo único para § 1º:

"Art. 2º

.....

.....

....

§ 2º O disposto no inciso III do *caput* não se aplica quando se tratar de interceptação do fluxo de comunicações em rede de computadores, dispositivo de comunicação ou sistema informatizado." (NR)

Art. 17. O art. 313 do Decreto-Lei nº 3.689, de 3 de outubro de 1941, Código do Processo Penal (CPP), passa a vigorar acrescido do seguinte inciso V:

"**Art. 313.** .....

.....

V – punidos com detenção, se tiverem sido praticados contra rede de computadores, dispositivo de comunicação ou sistema informatizado, ou se tiverem sido praticados mediante uso de rede de computadores, dispositivo de comunicação ou sistema informatizado, nos termos da lei penal.(NR)"

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

Art. 19. 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)"

Art. 20. O art. 9º da Lei nº 8.078, de 11 de setembro de 1990 passa a vigorar com a seguinte redação:

"**Art. 9º** .....

.....

Parágrafo único. O disposto neste artigo se aplica à segurança digital do consumidor, mediante a informação da necessidade do uso de senhas ou similar para a proteção do uso do produto ou serviço e

para a proteção dos dados trafegados, quando se tratar de dispositivo de comunicação, sistema informatizado ou provimento de acesso a rede de computadores ou provimento de serviço por meio dela.(NR)"

Art. 21 O art. 20 da Lei nº 7.716, de 5 de janeiro de 1989, passa a vigorar com a seguinte redação:

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

.....

§ 2º Se qualquer dos crimes previstos no caput é cometido por intermédio dos meios de comunicação social ou publicação de qualquer natureza, inclusive pela criação, manutenção ou divulgação de sítios, páginas, portais ou comunidades na rede mundial de computadores:

.....

§ 3º .....

.....

.....

III – a retirada do sítio, página, portal ou comunidade de conteúdo discriminatório ou preconceituoso.

..... (NR)"

Art. 22 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, fornecer, divulgar, publicar ou manter consigo, por qualquer meio de comunicação, inclusive rede mundial de computadores ou internet, fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente: (NR)"

Art. 23. O responsável pelo provimento de acesso a rede de computadores é obrigado a:

I – manter em ambiente controlado e de segurança, pelo prazo de três anos, com o estrito 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 por esta gerados, cujo fornecimento será feito exclusivamente à autoridade investigatória e dependerá de prévia e expressa autorização

judicial;

II – tornar disponíveis à autoridade competente, por expressa autorização judicial, os dados e informações mencionados no inciso I, no curso de auditoria técnica a que forem submetidos;

III – fornecer, por expressa autorização judicial, no curso de investigação, os dados de que cuida o inciso I deste artigo;

IV – preservar imediatamente, após a solicitação expressa da autoridade judicial, no curso de investigação, os dados de que cuida o inciso I deste artigo e outras informações solicitadas por aquela investigação, respondendo civil e penalmente pela sua absoluta confidencialidade e inviolabilidade;

V – informar, de maneira sigilosa, à autoridade policial competente, denúncia da qual tenha tomado conhecimento e que contenha indícios da prática de crime sujeito a acionamento penal público incondicionado, cuja perpetração haja ocorrido no âmbito da rede de computadores sob sua responsabilidade;

VI – informar ao seu usuário que o uso da rede sob sua responsabilidade obedece às leis brasileiras e que toda comunicação ali realizada será de exclusiva responsabilidade do usuário, perante as leis brasileiras;

VII – alertar aos seus usuários, em campanhas periódicas, quanto ao uso criminoso de rede de computadores, dispositivo de comunicação e sistema informatizado;

VIII – divulgar aos seus usuários, em local destacado, as boas práticas de segurança no uso de rede de computadores, dispositivo de comunicação e sistema informatizado.

§ 1º Os dados de que cuida o inciso I deste artigo, as condições de segurança de sua guarda, a auditoria à qual serão submetidos, a autoridade competente responsável pela auditoria e o texto a ser informado aos usuários de rede de computadores serão definidos nos termos de regulamento.

§ 2º Os dados e procedimentos de que cuida o inciso I deste artigo deverão estar aptos a atender ao disposto nos incisos II , III e IV no prazo de cento e oitenta dias, a partir da promulgação desta Lei.

§ 3º O responsável citado no *caput* deste artigo que não cumprir o disposto no § 2º, 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 verificação ou solicitação, aplicada em dobro em caso de reincidência, que será imposta mediante procedimento administrativo, pela autoridade judicial desatendida,

considerando-se a natureza, a gravidade e o prejuízo resultante da infração.

§ 4º 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.

Art. 24. Não constitui violação do dever de sigilo a comunicação, às autoridades competentes, de prática de ilícitos penais, abrangendo o fornecimento de informações de acesso, hospedagem e dados de conexões realizadas, quando constatada qualquer conduta criminosa.

Art. 25. Esta Lei entrará em vigor sessenta dias após a data de sua publicação.

Sala da Comissão,

, Presidente

, Relator