SENADO FEDERAL

(**) (*) PARECERES
Nº 582 a 586, DE 2008

Sobre o **Projeto de Lei da Câmara nº 89, de 2003** (nº 84/99, na Casa de origem), que *altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal e a Lei nº 9.296, de 24 de julho de 1996, e dá outras providências* (dispõe sobre os crimes cometidos na área de informática, e suas penalidades, dispondo que o acesso de terceiros, não autorizados pelos respectivos interessados, a informações privadas mantidas em redes de computadores, dependerá de prévia autorização judicial). **(Tramitando em conjunto com os Projetos de Lei do Senado nºs 76 e 137, de 2000, nos termos do Requerimento nº 847 de 2005)**

PARECER Nº 582, DE 2008
(Da Comissão de Educação, Cultura e Esporte)

(Somente sobre os Projetos de Lei do Senado nºs 76 e 137, de 2000, que já se encontravam apensados nos termos do Requerimento nº 466, de 2000)

Relator: SENADOR JUVÊNCIO DA FONSECA

I – RELATÓRIO

O Projeto de Lei em epígrafe intenta disciplinar as relações no campo da informática, tipificando condutas e instituindo penas, além de disciplinar o uso de bancos de dados em computador, contendo informações privadas.

Ao Projeto, distribuído a esta Comissão de Educação e à Comissão de Constituição, Justiça e Cidadania, nesta última em caráter terminativo, não foi apresentado emenda no prazo regimental.

Foi apensado para tramitação conjunta o Projeto de Lei do Senado, nº 137, de 2000, do ilustre Senador Leomar Quintanilha, que em sua ementa "Estabelece nova pena aos crimes cometidos com a utilização de meios de tecnologia de informação e telecomunicações".

A esta Comissão de Educação cabe analisar o projeto sob os aspectos técnico e de mérito, sendo a apreciação final na Comissão de Constituição, Justiça e Cidadania.

É o relatório.

(*) Republicado em 27/6/08, para correção na ementa.
(**)Republicado em 7/7/08, para exclusão de página em duplicidade (lista de votação da CE)

II – ANÁLISE

O projeto RENAN CALHEIROS em exame é oportuno, de estrema necessidade e merece um tratamento o mais rápido possível, para que tenhamos definidas as novas figuras tipo do Direito Penal, relacionadas com a informática.

Como diz na sua justificativa o ilustre Senador Renan Calheiros: "o espaço cibernético é um mundo virtual onde os defeitos e os atos ilícitos dos seres humanos se reproduzem com a mesma facilidade como as suas virtudes e suas atividades lícitas."... "Paralelamente a este avanço tecnológico, surgiram novas formas de conduta antisocial, fazendo dos equipamentos de informática meios de delinqüência e de infrações".

A audiência pública promovida por esta Comissão de Educação foi proveitosa. Trouxe-nos elementos novos de enfoque da questão, que resultaram no substitutivo que ao final apresentamos, como aperfeiçoamento da propositura do ilustre Senador Renan Calheiros.

Gostaria de ressaltar a contribuição da Ordem dos Advogados do Brasil, por sua Comissão de Informática do Conselho Federal, que nos propiciou, após frutíferos debates, oferecer este trabalho.

Constata-se de início, que o mundo dos computadores se desenvolveu rapidamente, em tecnologia cada vez mais sofisticada e numa velocidade nunca vistos.

Naturalmente, essa invasão dos computadores na vida da sociedade traz reflexos no mundo jurídico-penal.

Entende-se por crime informático qualquer ação em que o computador seja o instrumento ou o objeto do delito, ou então, qualquer delito ligado ao tratamento automático de dados.

Os maiores problemas enfrentados hoje no combate aos crimes virtuais têm sido buscar a correta tipicidade dentro da legislação vigente, vez que a utilização indevida do computador nas condutas delituosas extrapola em muito os limites existentes, que permitam o enquadramento penal. Embora saibamos da dificuldade da legislação em acompanhar paripassu os avanços dos "cybercrimes", é fundamental que se abandone a idéia fixa de que a carência de legislação específica sobre crimes na Internet seja um impeditivo intransponível para buscar na legislação vigente algumas soluções concretas.

Nessa linha de raciocínio, devemos nos conscientizar de que a Internet é antes de qualquer coisa, um novo meio de comunicação e um novo instrumento para a prática de delitos já tipificados e delitos novos. Via de regra,

qualquer crime de informação previsto na Lei Penal que não distinga o meio, poderá se aplicar à Internet.

Distinguem-se os crimes virtuais entre os delitos informáticos puros, ou seja, aqueles que só podem ser concebidos em face de um sistema informático, ainda não tipificados na legislação brasileira e delitos informáticos impuros, aqueles que podem ser cometidos também fora do universo do computador, encontrando já definição no sistema punitivo atual.

Puros são aqueles em que o sujeito ativo visa especificamente ao sistema de informática, em todas as suas formas. São elementos que compõem a informática o "software", o "hardware", computador e periféricos, os dados e sistemas contidos no computador, os meios de armazenamento externo, tais como fitas, disquetes, etc. São aquelas condutas que visam exclusivamente violar o sistema de informática do agente passivo.

O Crime de Informática Impuro ocorre quando o agente visa a um bem juridicamente protegido diverso da informática, porém, o sistema de informática é ferramenta para a sua consumação.

Atendendo a essa classificação, poder-se-ia incorporar ao Código Penal agravantes pelo uso de sistema de informática, vez que é meio que necessita de capacitação profissional e a ação delituosa por esta via reduz a capacidade da vítima em evitar o delito.

Entendemos ser a presente classificação apta à elaboração da legislação que possa alcançar os delitos de informática, sem contudo correr-se o risco de sobreposição de normas e, assim, também entendemos que é meio hábil à formação de um eficaz Direito Penal de Informática.

O Governo Federal antecipou-se às vulnerabilidades dos delitos informáticos contra as bases de dados da Administração Pública através da Lei nº9983/2000, em que foram tipificados novos ilícitos, próprios dos crimes virtuais puros, ou seja, aqueles que só podem ser concebidos através de um sistema informático. Por essa lei, somente a Administração Pública está protegida na qualidade de vítima desses delitos. O cidadão e a empresa encontram-se desprotegidos. São considerados como possíveis agentes de delito, mas não como vítima de um ilícito penal informático.

Diante desse quadro, surge o projeto Renan Calheiros, em exame, que merece a nossa melhor acolhida, mas com alguns reparos técnico-jurídicos. Contempla tipos penais já existentes no Código Penal e às vezes com apenação menor do que a já prevista, como é o caso da nova tipificação do homicídio, como delito informático. A "alteração ou transferência de contas representativas de valores", já está contemplada no Código Penal, nos artigos 155 (furto) ou 171 (estelionato), também com apenação maior.

Igualmente, o delito "contra a honra e a vida privada", configura-se como delito impuro, já previsto na Lei de Imprensa (nº5.250/69), no Código Eleitoral (Lei nº 3757/65) e nos artigos 138 e 140 do Código Penal. A pena prevista no projeto é menor que nas leis vigentes.

O art. 4º do Projeto, confunde circunstância agravante com qualificadora. São institutos diferentes. O Código Penal Brasileiro utiliza-se de outro critério para a definição de qualificadora.

Além do mais o projeto n.84-A, de 1999, em tramitação na Câmara Federal, com idêntica proposta, mereceu ampla discussão naquela Casa, assim como este PLS aqui no Senado Federal, recomendando que as conclusões de ambas as Casas sirvam para um substitutivo que integre o resultado dos estudos feitos.

O PLS nº 137/2.000, anexo ao presente, de autoria do nobre Senador Leomar Quintanilha, também é oportuno porque pretende penalizar com mais rigor os crimes de informática. É justamente partindo dessa contribuição que procuraremos, com o nosso substitutivo, oferecer uma penalização mais rigorosa para esses crimes, especialmente porque são praticados por pessoas de alta qualificação profissional e inteligência das mais brilhantes, virtudes que deveriam ser colocados para o bem estar da sociedade e não para destruir valores da coletividade.

Por outro lado, deixo de aproveitar e de analisar os dispositivos de preceitos não tipificados como delitos do projeto n.84-A, de 1999, em tramitação na Câmara, preferindo ater o meu relatório à parte específica dos crimes de informática, sem deixar de aproveitar o trabalho elaborado na Câmara Federal e nesta Casa, oferecendo um substitutivo que insere a matéria no Código Penal. Com este objetivo acrescentei o título XI-A ao mesmo código, sob o título "Dos crimes contra os serviços de informática".

A iniciativa me parece correta, visto que uma lei de importância como esta haverá de estar no próprio Código Penal, não em legislação extravagante, de difícil localização. O preceito, para universalizar deve estar no Código.

O Título "DOS CRIMES CONTRA OS SERVIÇOS DE INFORMÁTICA" me parece adequado, diante da definição de "informática" como ciência que estuda o tratamento das informações quanto à sua coleta, armazenamento, classificação, transformação e disseminação.

Concentra o projeto nas informações coletadas, armazenadas e distribuídas pelo sistema computadorizado, que hoje invade as atividades do homem, como instrumento de modernidade técnica. Tais serviços, pela sua importância, devem ser protegidos como um bem da sociedade.

De todos os debates e audiências públicas que se realizaram, chegamos à tipificação de oito delitos de informática. Aguardamos que a discussão nesta Comissão e na de Constituição, Justiça e Cidadania, nossos pares ofereçam novas luzes sobre matéria tão atual e palpitante.

III – VOTO

Ante o exposto, voto pela aprovação do Projeto de Lei do Senado n.76, de 2000, de autoria do nobre Senador RENAN CALHEIROS nos termos do substitutivo anexo e pela rejeição do Projeto de Lei do Senado n°137, de 2.000.

Senador JUVÊNCIO DA FONSECA
Relator

EMENDA Nº 1 – CE (SUBSTITUTIVO)

Altera o Decreto-Lei nº 2848 de 7 de dezembro de 1940 (Código Penal), para tipificar os crimes contra os serviços de informática e dá outras providências.

Art.1º. O Decreto Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), passa a vigorar acrescido do Título XI-A, nos seguintes termos:

TÍTULO XI-A
DOS CRIMES CONTRA OS SERVIÇOS DE INFORMÁTICA

CAPÍTULO I
DOS CRIMES DE INFORMÁTICA

Acesso indevido ou não autorizado a computador.

Art.359-I.- Acessar, indevidamente ou sem autorização, dados ou informações armazenados em computador ou em rede de computadores.

Pena – detenção de seis meses a um ano e multa

Parágrafo único. Na mesma pena incorre quem, nas mesmas condições, obtém ou fornece a terceiro meio de acesso a computador ou rede de computadores.

Alteração de meio de acesso a programa de computador

Art.359-J - Apagar, destruir, alterar ou por qualquer outra forma inutilizar senha ou outro meio de acesso a computador, programa de computador ou dados, de forma indevida ou não autorizada.

Pena – detenção de um a dois anos e multa.

Uso indevido de dados ou instrução de computador

Art.359-L- Obter, usar, manter ou fornecer a terceiros, de forma indevida ou não autorizada, dado ou instrução de computador.

Pena – detenção de um a dois anos e multa.

Destruição de dados ou programas de computador

Art.359-M- Destruir, apagar, modificar ou de qualquer forma inutilizar, no todo ou em parte, dado, programa de computador ou conteúdo de comunicação eletrônica, de forma indevida ou não autorizada.

Pena: reclusão de um a três anos e multa.

Produção clandestina de programa de computador com fins nocivos.

Art.359-N- Produzir clandestinamente programa de computador ou outro meio capaz de destruir, apagar, inutilizar ou modificar, no todo ou em parte, conteúdo de informática, impossibilitando ou dificultando sua utilização em computador ou em rede de computadores.

Pena – reclusão de dois a quatro anos e multa.

Parágrafo único. Na mesma pena incorre quem distribui ou comercializa o produto.

Uso de programa clandestino de computador para fins nocivos.

Art.359-O- Usar, inserindo ou fazendo inserir, programa de computador ou outro meio produzido clandestinamente, capaz de destruir, apagar, inutilizar ou modificar, no todo ou em parte, conteúdo de informática, impossibilitando ou dificultando sua utilização em computador ou em rede de computadores.

Pena – reclusão de três a seis anos e multa.

Veiculação imprópria de pornografia.

Art.359-P- Oferecer serviço ou informação de caráter pornográfico em rede de computadores, sem exibir previamente e de forma visível e destacada, aviso sobre sua natureza, indicando o seu conteúdo e inadequação para crianças e adolescentes.

Pena – detenção de um a dois anos e multa.

Violação de informações secretas armazenadas em computador.

Art.359-Q- Violar ou fornecer segredos de indústria, comércio ou de informações pessoais armazenadas em computador, rede de computadores, meio

eletrônico de natureza magnética, óptica ou similar de forma indevida ou não autorizada.

Pena – reclusão de um a três anos e multa.

Parágrafo Único. Nas mesmas penas incorre quem, nas mesmas condições, fornece a terceiros segredos de indústrias, comércio ou de informações pessoais armazenadas em computador, rede de computador, meio eletrônico de natureza magnética, óptica ou similar.

CAPÍTULO II
DAS DISPOSIÇÕES GERAIS

Aumento de Pena

Art.359-R- As penas previstas neste título serão aumentadas de um sexto até a metade, caso os crimes sejam cometidos:

I – em detrimento de entidade de direito público ou de instituto de economia popular, assistência social ou beneficência;

II - com considerável prejuízo para a vítima;

III - com intuito de vantagem para si ou para outrem;

IV – com abuso de confiança;

V – com emprego de grave ameaça ou violência à pessoa.

Parágrafo único – Sendo o réu reincidente nos crimes deste título, a pena será aplicada em dobro.

Art.2º. Esta lei entra em vigor no prazo de noventa dias decorridos da sua publicação.

Sala da Comissão, 21 de maio de 2002.

Senador JUVÊNCIO DA FONSECA
Relator

COMISSÃO DE EDUCAÇÃO

ASSINAM O PARECER AO PLS N.º 76/00 (TRAMITANDO EM CONJUNTO COM O PLS Nº 137/00) NA REUNIÃO DE 21.05.02 OS SENHORES SENADORES:

PRESIDENTE:	RICARDO SANTOS
RELATOR:	JUVÊNCIO DA FONSECA

PMDB	
AMIR LANDO	1-MAURO MIRANDA
CASILDO MALDANER	2-PEDRO SIMON
GERSON CAMATA	3-(VAGO)
GILVAM BORGES	4- SÉRGIO MACHADO
MARLUCE PINTO	5-ALBERTO SILVA
NABOR JÚNIOR	6-MAGUITO VILELA
JOSÉ SARNEY	7-JUVÊNCIO DA FONSECA
VALMIR AMARAL	8-(VAGO)
NEY SUASSUNA	9-(VAGO)

PFL	
GERALDO ALTHOFF	1-LINDBERG CURY
MOREIRA MENDES	2-BERNARDO CABRAL
WALDECK ORNELAS	3-FRANCELINO PEREIRA
LEOMAR QUINTANILHA	4-JONAS PINHEIRO
JOSÉ JORGE	5-ROMEU TUMA
MARIA DO CARMO ALVES	6-PAULO SOUTO
ARLINDO PORTO - PTB	7-ANTONIO CARLOS JÚNIOR

BLOCO (PSDB/PPB)	
FREITAS NETO	1- EDUARDO SIQUEIRA CAMPOS
ARTUR DA TÁVOLA	2-LÚDIO COELHO
RICARDO SANTOS	3- CHICO SARTORI
TEOTÔNIO VILELA FILHO	4-LÚCIO ALCANTARA
BENÍCIO SAMPAIO - PPB	5-ROMERO JUCÁ
REGINALDO DUARTE	6-LUIZ OTÁVIO - PPB

BLOCO DE OPOSIÇÃO (PT-PDT-PPS)	
EDUARDO SUPLICY-PT	1-LAURO CAMPOS - PDT
EMÍLIA FERNANDES-PT	2-GERALDO CÂNDIDO - PT
MARINA SILVA-PT	3-SEBASTIÃO ROCHA - PDT
ÁLVARO DIAS-PDT	4-TIÃO VIANA - PT

PSB	
PAULO HARTUNG	1-ROBERTO SATURNINO - PT

PARECERES SOBRE O PROJETO DE DA CÂMARA Nº 89, DE 2003; E PRJETOS DE LEI DO SENADO Nº 76 E 137, DE 2000, NOS TERMOS DO REQUERIMENTO Nº 857, DE 2005.

PARECER Nº 583, DE 2008
(Da Comissão de Educação, Cultura e Esporte)

RELATOR: Senador **EDUARDO AZEREDO**

I – RELATÓRIO

Chegam a esta Comissão, para parecer, o Projeto de Lei da Câmara (PLC) nº 89, de 2003 (nº 84, de 1999, na origem), e os Projetos de Lei do Senado (PLS) nº 137, de 2000, e nº 76, de 2000, todos referentes a crimes na área de informática. Tramitam em conjunto, em atendimento ao Requerimento nº 847, de 2005, do Senador Renan Calheiros. Em decorrência do Requerimento nº 848, de 2005, foi extinta a urgência na tramitação do PLC nº 89, de 2005, que havia sido declarada em decorrência da aprovação do Requerimento nº 599, de 2005, de autoria da Senadora Ideli Salvatti. Os projetos de lei do Senado perdem o caráter terminativo nas comissões.

O PLS nº 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 delitos cometidos com o uso de computadores, e lhes atribui as respectivas penas, sem entretanto alterar o 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 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 Decreto-Lei n° 2.848, de 7 de dezembro de 1941 (Código Penal), 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 PLC 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* ao tipo penal de atentado contra a segurança de serviço de utilidade pública (art. 265) e ao 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).

Tendo estado à disposição dos senhores Senadores, o PLC n° 89, de 2003 não recebeu emendas.

II – ANÁLISE

Muitas são as proposições legislativas já produzidas e debatidas no Congresso Nacional a respeito do tema da criminalidade nas áreas da informática, das telecomunicações e da Internet, a rede mundial de computadores. A evolução das tecnologias relacionadas à produção, ao processamento, ao armazenamento e à difusão da informação tem ocorrido com muita velocidade, gerando lacunas no ordenamento jurídico vigente.

A existência dessas lacunas tem motivado a proliferação de casos de fraudes e de danos ao patrimônio e danos morais de agentes públicos e privados. Estima-se que bilhões de reais já foram desviados de contas bancárias de pessoas físicas ou jurídicas em decorrência da atuação indevida de especialistas da área. Além disso, a violação de bases de dados mantidas em meio eletrônico tem provocado danos de grande monta pelo roubo de informações pessoais.

Não bastasse isso, há evidências de ligação entre o cibercrime e o financiamento do terrorismo internacional, e o crescimento do tráfico de seres humanos e de drogas. E 2004 foi apontado como o ano em que os crimes cibernéticos passaram a gerar lucros superiores aos do tráfico de drogas. De acordo com pesquisa realizada pela firma de consultoria americana *Computer Economics*, em 2004 as perdas totais chegam a 18 bilhões de dólares, com uma taxa de crescimento anual próxima de 35%.

A sociedade clama por medidas eficazes no combate ao crime cibernético. Não é mais possível que divergências hermenêuticas acerca da possível aplicabilidade das nossas normas jurídicas a esse tipo de conduta continuem a impedir a punição de condutas extremamente nocivas ao País.

A imprensa nacional destaca recentemente que alguns internautas já começam a fazer denúncias contra usuários pedófilos ou terroristas do sítio *Orkut*, denunciando-os ao provedor. O *Orkut*, um serviço da multinacional americana *Google*, imediatamente retira aqueles usuários do sistema mas não consegue detectar e impedir a sua reinclusão, face á liberalidade, inerente à rede mundial de computadores. Estabelece-se assim o círculo da denúncia e da punição responsável. Esse círculo, entretanto, tem como resposta novo círculo vicioso com o reinício dos delitos por novos usuários não identificados, tudo isto sem que se perceba um fim próximo.

O teor do PLS nº 137, de 2000, reflete preocupação idêntica àquela que conduziu o legislador na formulação dos dois outros projetos que acompanha, qual seja: a de disciplinar as condutas perniciosas que utilizem ou danifiquem sistemas de computador. Não obstante, é de abrangência e precisão mais restrita que aqueles, que o englobam integralmente.

O projeto limita-se a estabelecer que os crimes contra a pessoa, o patrimônio, a propriedade imaterial e intelectual, os costumes, bem como contra a criança e o adolescente, cometidos com a utilização de meios de tecnologia de informação e telecomunicações, terão suas penas triplicadas. Ou seja, a pena seria agravada em razão do meio utilizado pelo agente para perpetrar o crime.

A alteração legislativa proposta pelo PLS nº 137, de 2000, não é conveniente por duas razões.

Em primeiro lugar, tornaria superlativo o desvalor do meio utilizado pelo agente, que prevaleceria tanto sobre o desvalor do resultado quanto sobre o desvalor da intenção (genericamente considerada) – aquele, inspirador da teoria clássica da ação; este, da teoria finalista da ação, ambas adotadas de forma alternada pelo Código Penal a partir da reforma da sua Parte Geral, empreendida pela Lei nº 7.209, de 11 de julho de 1984. A segunda razão, que decorre da anterior, é a desproporcionalidade na aplicação das penas, haja vista que um delito menos grave poderia ser apenado mais severamente do que outro mais reprovável, apenas por ter sido cometido por meio da Internet.

O PLC nº 89, de 2003, pretende inserir a Seção V no Capítulo VI do Título I do Código Penal, onde seriam definidos os crimes contra a inviolabilidade dos sistemas informatizados. São nove as condutas delituosas por meio de acesso a sistema eletrônico de que trata o PLC:

- o acesso indevido a meio eletrônico;
- a manipulação indevida de informação eletrônica;
- o dano eletrônico;
- a pornografia infantil;
- o atentado contra a segurança de serviço de utilidade pública;
- a interrupção ou perturbação de serviço telegráfico e telefônico;
- a falsificação de cartão de crédito;
- a falsificação de telefone celular;
- a divulgação de informações pessoais ou de empresas.

Vejamos cada um desses tipos.

a) Arts. 154-A, 154-B e 154-C do CP, ou seja, o acesso indevido, a manipulação indevida de informação e a definição de meio eletrônico e sistema informatizado.

A redação pode ser aperfeiçoada para registrar que o meio eletrônico ou sistema informatizado é protegido contra as hipóteses em que o agente consegue o acesso mediante a violação desse sistema de proteção. Já a pena, que seria aplicada ao *hacker*, nome dado ao usuário que tenta violar ou viola o sistema de proteção, deveria ser mais severa.

Ademais, embora os três artigos possam ser reunidos em um só, preferimos manter a redação dada pelo PLC n° 89 de 2003, que define com maior clareza os delitos que se pretende tipificar. Entretanto propomos a alteração da pena original de detenção de 3 (três) meses a 1 (um) ano, e multa para detenção, de 1 (um) a 4 (quatro) anos, e multa, mantendo os mesmos parágrafos.

Ainda, quando este PLC n° 89 de 2003 estava sendo relatado nesta Comissão, o atento Senador Hélio Costa fez algumas sugestões de emendas que os membros da Comissão entenderam necessárias, mas que deveriam fazer parte de um novo Projeto de Lei a fim de que aquele projeto em discussão, uma vez aprovado, pudesse ir à sanção presidencial. Estando ele apensado ao PLS n° 76 de 2000 entendemos que é hora de acatar aqui algumas sugestões.

A primeira sugestão aqui acatada trata da definição e tipificação da Fraude Eletrônica, conhecida pelos profissionais de Tecnologia de Informação e Comunicação (TIC) como *phishing* ou *port fishing*, incluindo-a no Código Penal como segue:

"Fraude Eletrônica

Art. 154 - D. Difundir, por qualquer meio, sistema informatizado com o propósito de induzir alguém a fornecer, espontaneamente e por qualquer meio, dados ou informações que facilitem ou permitam o acesso indevido ou sem autorização, a dispositivo de comunicação ou a sistema informatizado:

Pena – reclusão de dois a quatro anos e multa.

Parágrafo único. 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, ou se o sistema informatizado fraudador tiver potencial de propagação ou alastramento."

Aqui acolhemos contribuição valiosa, de advogado especialista e com vasta experiência na defesa contra os crimes de informática, de que deveríamos evitar o nome "fraude", em seu título, para não haver confusão com a "fraude material" ou com o "furto mediante fraude". Nossa proposta é que o crime seja nominado "difusão maliciosa de código" ou "disseminação de armadilha eletrônica".

Se mantivéssemos a nomenclatura "fraude eletrônica", olvidando a confusão de natureza dos tipos, estaríamos engendrando, na verdade, uma hipótese aberta de "tentativa de fraude", pois a conduta do agente difusor, a partir de um eventual resultado, pode ser qualquer uma. A partir do fornecimento espontâneo de dados, o agente pode praticar fraude, dano, furto, chantagem ou qualquer outro crime, inclusive fora da esfera digital (mundo atômico).

Nossa proposta, finalmente, é no sentido de que a redação do caput seja a seguinte, com sua inclusão no Título VIII (Dos crimes Contra a Incolumidade Pública), Capítulo II (Dos Crimes Contra a Segurança Dos Meios de Comunicação e Transporte e Outros Serviços Públicos):

"Difusão Maliciosa de Código

Art. 266 -A. Difundir, por qualquer meio, sistema informatizado com o propósito de induzir alguém a fornecer, espontaneamente e por qualquer meio, dados ou informações que facilitem ou permitam o acesso indevido ou sem autorização, a dispositivo de comunicação ou a sistema informatizado, ou a obtenção de qualquer vantagem ilícita:

Pena – reclusão de um a dois anos.

Parágrafo único - A pena é aumentada de sexta parte, se o agente se vale de anonimato, de nome suposto ou da utilização de identidade de terceiros para a prática de acesso."

Outra sugestão do Senador refere-se à inclusão de alteração ao art. 46 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940, Código Penal, mediante a inclusão a ele do § 5º dando a opção ao juiz a aplicação de pena alternativa, sugestão não acatada por entendermos que as penas alternativas já estão bem definidas no Código Penal. Ademais, a aplicação desta espécie de pena alternativa aumentará exponencialmente os riscos e as vulnerabilidades dos sistemas de informática das instituições públicas, que ficarão ainda mais expostas aos ataques de *hackers* e organizações cibernéticas criminosas, tendo em vista a possibilidade de instalação de *backdoors* e outros dispositivos fraudulentos nos *softwares* manipulados durante o cumprimento da pena.

Finalmente o Senador sugeriu a mudança do termo "meio eletrônico" por "dispositivo de comunicação" no art. 154-C, à qual acatamos e no substitutivo promovemos sua atualização e complementação:

"Dispositivo de Comunicação e Sistema Informatizado

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

I – dispositivo de comunicação: o computador, o processador de dados, o disquete, o CD-ROM ou qualquer outro meio capaz de armazenar ou transmitir dados de maneira magnética, ótica, ou eletronicamente.

II – sistema informatizado: a rede de computadores, a base de dados, o programa de computador ou qualquer outro sistema capaz de armazenar ou transmitir dados eletronicamente."

b) Arts. 163, §§ 2ºe 3º

A equiparação feita pelo § 2º (equiparação à coisa do dado, informação ou a base de dados; a senha ou qualquer meio de identificação) é pertinente, mas poderia estar posicionada no Capítulo VIII do Título II (Disposições Gerais), pois dessa forma a regra seria válida para todos os tipos de crimes contra o patrimônio.

Por contribuição valiosa de vários advogados especialistas em crimes de informática, quanto à conduta do § 3º, entendemos que a pena deva ser mais severa, tendo em conta a potencialidade do dano material que se pode causar, por isso sugerimos a criação de um tipo autônomo com pena mais agravada do que a

prevista no *caput* e parágrafo único do art. 163 e mais ainda se praticada no anonimato. Em vista disso, sugerimos a seguinte redação:

"Dano por Difusão de Vírus Eletrônico

Art. 163-A. Criar, inserir ou difundir vírus em dispositivo de comunicação ou sistema informatizado, com a finalidade de destruí-lo, inutilizá-lo ou dificultar-lhe o funcionamento.

Pena: detenção, de 1 (um) a 3 (três) anos, e multa.

Parágrafo único - A pena é aumentada de sexta parte, se o agente se vale de anonimato,de nome suposto ou da utilização de identidade de terceiros para a prática de acesso. "

c) Art. 167 do CP

Por sua vez, a alteração proposta para o art. 167 do CP não é conveniente, pois proceder-se mediante queixa, quando o dado ou informação não tiver potencial de propagação ou alastramento, é um tratamento diferenciado para uma conduta por sí só inaceitável e que justamente por isso ganha tipo penal autônomo no art. 163-A.

d) Art. 218-A do CP (Pornografia Infantil)

O delito descrito nesse dispositivo já está previsto, de modo mais abrangente, nos arts. 240 e 241 do Estatuto da Criança e do Adolescente (ECA).

e) Arts. 265 e 266 do CP, respectivamente "atentado contra a segurança de serviço de utilidade pública" e "interrupção ou perturbação de serviço telegráfico ou telefônico":

As alterações propostas para esses dispositivos são convenientes.

f) Arts. 298 e 298-A do CP

A redação que se propõe para o art. 298 é conveniente (falsificação de cartão de crédito); quanto ao art. 298-A procedemos a pequenas modificações de

forma a melhorar sua clareza e compreensão, (falsificação de telefone celular ou meio de acesso a sistema eletrônico).

g) Art. 2º, § 2º, da Lei nº 9.296, de 1996

A alteração prevista no art. 2º da Lei nº 9.296, 24 de julho de 1996, é conveniente conforme o art. 15 do Substitutivo.

Não há que se falar em inconstitucionalidade da medida proposta, pois a reserva legal expressa e qualificada prevista no inciso XII do art. 5º da Constituição Federal estabeleceu apenas dois requisitos a serem observados pelo legislador ordinário no momento da regulamentação da restrição ao direito fundamental à privacidade das comunicações, quais sejam: existência de autorização judicial prévia à interceptação e 'para fins de investigação criminal ou instrução processual penal'.

O constituinte não estabeleceu o requisito de os 'crimes serem apenados com pena de reclusão'. Esta foi uma decisão do legislador ordinário, da Lei nº 9.296, de 1996, decisão que pode ser alterada a qualquer momento sem que isto signifique qualquer afronta à Lei Maior.

Há que se frisar, ainda, que referida alteração será importante para apuração de crimes punidos com detenção praticados com o uso de sistemas informatizados, tais como:

- calúnia (aplicação do art. 138 à conduta de falar falsamente em *chat* ou comunidade *online* que alguém cometeu crime),
- difamação (aplicação do art. 139 à conduta de difamar alguém através de boato eletrônico ou *hoax*),
- injúria (aplicação do art. 140 à conduta de enviar *e-mail* com ofensas pessoais ao destinatário),
- violação de direito autoral (aplicação do art. 184 à conduta de copiar conteúdo de página da Internet sem citar a fonte),
- falsa identidade (aplicação do art. 307 à conduta de enviar *spam* com remetente falso),
- exercício arbitrário das próprias razões (aplicação do art. 345 à conduta de atacar emissário de *spam* ou vírus para evitar novos danos).

Todos esses delitos são praticados por meio dos sistemas informatizados, mas seriam punidos, conforme a proposta aqui endossada, com pena de detenção, o que impede a interceptação para fins de instrução criminal, dificultando sua comprovação pelos ofendidos e pelo Ministério Público.

Essa medida, ademais, viabilizará a possibilidade de manter a apenação de crimes informáticos com pena de detenção, afastando a necessidade de se estipularem penas de reclusão para esses delitos, ferindo o princípio da proporcionalidade da pena. Se, para viabilizar a apuração e a investigação criminal, estabelecêssemos pena de reclusão para esses crimes, ao invés de viabilizar a quebra legal do sigilo para crimes apenados com detenção, estaríamos provocando severa e injustificada distorção do sistema penal.

h) Art. 10 do PLC nº 89, de 2003

O dispositivo é necessário, com as inclusões propostas no substitutivo, análogas aos artigos incluídos no Código Penal, para tipificar os crimes no Código Penal Militar, usando ferramentas de tecnologia da informação e comunicações.

Por fim, o art. 11 do projeto mostra-se adequado, enquanto o art. 12 não é conveniente, sendo preferível manter o sistema de crimes estabelecido nos arts. 240 e 241 do ECA. A Lei nº 10.764, de 12 de novembro de 2003, alterou o art. 241 do Estatuto da Criança e do Adolescente (Lei nº 8.069, de 13 de julho de 1990), para tipificar e punir de forma mais severa a pornografia infantil.

O PLS nº 76, de 2000, revestido de norma autônoma, afigura-se o projeto mais abrangente entre os que estão sendo aqui analisados. Os crimes informáticos estão divididos, no projeto, em crimes 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 opção sexual e contra a segurança nacional.

Realmente a visão ampla que se tem dos crimes de informática é o grande mérito deste projeto inovador proposto pelo eminente Senador Renan Calheiros. Seus dispositivos mostram a gravidade crescente dos delitos praticados com instrumentos informatizados, cujas punições ainda não contam com o necessário suporte legal. Isto vem trazendo enorme insegurança a toda a sociedade

pois crimes são praticados no anonimato da internet sem que haja a mínima possibilidade de defesa para o usuário.

Entretanto, a descrição de algumas das condutas deixa dúvidas em relação aos elementos dos respectivos delitos, o que pode prejudicar sua compreensão.

Vale lembrar que a Lei Complementar nº 95 de 1998 determina que havendo legislação em vigor deve-se preferir a sua alteração à criação de nova norma e desta forma o substitutivo proposto promove alterações ao Decreto-Lei nº 2.848, de 7 de dezembro de 1940, o Código Penal.

Comentamos, a seguir, sobre as disposições do PLS nº 76, de 2000.

a) Art. 1º, § 1º – crimes contra a inviolabilidade de dados e sua comunicação

Os incisos I, IV e V são espécies de crime de dano, descrito no art. 163 do CP; além disso, o inciso V deveria tipificar não a mera programação de instruções, mas a sua efetiva utilização, pois o nosso direito, via de regra, não pune os atos meramente preparatórios. Pode-se, alternativamente, prever, no art. 163 do CP, a equiparação dos dados informatizados à coisa, como o fez o PLC nº 89, de 2003, ou fazê-lo ao final do Título II do CP.

O inciso II pode ser tido como furto (art. 155 do CP), se houver subtração da coisa, ou como apropriação indébita (art. 168 do CP), se o agente tinha a posse ou a detenção da coisa. Quanto ao inciso III, melhor seria punir o uso indevido dos dados em razão da finalidade do agente: se atenta contra a intimidade da pessoa, contra o patrimônio, contra a fé pública, etc. Entretanto, há que se ter em conta que a maioria desses crimes já existe, e que a informática é apenas um meio para realização da conduta delituosa. A equiparação à coisa que se pode fazer ao final do Título II do CP resolveria o problema.

Além disso, as penas propostas são muito brandas em face da gravidade das condutas equiparadas que acima citamos.

b) Art. 1°, § 2°

Os incisos I e II são espécies de furto, crime definido no art. 155 do CP, cuja pena é bem mais severa do que a proposta no PLS n° 76, de 2000.

c) Art. 1°, § 3°

O inciso I está incluso no crime de injúria, descrito no art. 140 do CP; a conduta do inciso II, por sua vez, poderia ser inserida no Código Penal, mediante acréscimo do art. 154 D. Cabe observar que, se a informação for lesiva à honra, sua divulgação importará em um dos crimes tipificados no Capítulo V do Código Penal (calúnia, difamação ou injúria). Para desestimular o anonimato permitido pela internet, normalmente o caminho usado pelos autores dos crimes aqui tipificados, incluímos o artigo 154-F criando a obrigatoriedade de cadastramento identificador, além de estabelecermos, nos crimes em que tal conduta é especialmente perversa (Art. 154-A, § 3°, 154-D, parágrafo único e 266-A, parágrafo único), causas de aumento de pena a serem aplicadas pelo juiz, no momento de fixação da pena.

Todos os atos e fatos que se materializam através destes meios chegam, fácil e rapidamente, ao conhecimento de milhões de pessoas, causando um considerável prejuízo aos bens jurídicos tutelados. Em vista disso o potencial lesivo da conduta que ofende a honra da pessoa é incomensuravelmente maior quando o agente o faz por meio eletrônico como acontece nas redes de computadores. Isso já é bastante para justificar uma resposta penal mais severa, para que o agente sinta-se seriamente desestimulado a cometer o delito contra a honra por esse meio. É necessário, portanto, maior força penal coercitiva para evitá-los e assim fizemos incluir o art. 141-A conforme o art. 8° do substitutivo, estabelecendo causa especial de aumento de pena, com acréscimo de dois terços quando o meio utilizado é um dispositivo de comunicação ou sistema informatizado.

Novamente, em relação ao crime de ameaça, conduta que chega a ser banal no sítio do Orkut, por exemplo, a coibição do anonimato permitido pela internet, normalmente o caminho usado pelo agente da ameaça, entendemos suficiente a inclusão do artigo 154-F e dos parágrafos incluídos nos artigos 154-A, 154-D e 266-A.

d) Art. 1°, § 4°

O inciso I, a depender do resultado da conduta, será crime de lesão corporal ou homicídio, ambos já tipificados no Código Penal (arts. 129 e 121, respectivamente). O inciso II traz a incriminação de ato meramente preparatório. Além disso, os artefatos explosivos têm ampla utilização na indústria, não sendo conveniente definir como crime o trabalho intelectual de elaboração de um sistema informatizado de detonação.

e) Art. 1°, § 5°

As condutas descritas nos incisos I e II configuram crime contra a ordem tributária, definidos de forma mais abrangente e adequada nos arts. 1° e 2° da Lei n° 8.137, de 27 de dezembro de 1990.

f) Art. 1°, § 6°

O inciso I já está definido no art. 218 do CP (corrupção de menores). Os incisos II e III estão inclusos no art. 234 do CP (escrito ou objeto obsceno). Novamente, com o anonimato coibido pelo artigo 154-F e pelos parágrafos incluídos nos artigos 154-A, 154-D e 266-A do substitutivo, os autores destes crimes estarão desestimulados a cometê-los.

g) Art. 1°, § 7°

Os crimes definidos nesse parágrafo já estão contemplados na Lei n° 7.170, de 14 de dezembro de 1983 (Lei de Segurança Nacional), especificamente nos seus arts. 13, 15 e 23.

Recentemente em Audiência Pública sobre o PLS n° 279 de 2003, do qual também sou relator, de autoria do nobre Senador Delcídio Amaral e que propõe a criação de um cadastro de titulares de correio eletrônico na internet, ficou evidente que, para fins de investigação, é necessário estabelecer um prazo legal de armazenamento dos dados de conexões e comunicações realizadas pelos equipamentos componentes da internet, o que será feito pelos seus provedores de acesso. Os serviços de telefonia e transmissão de dados mantêm por cinco anos os dados de conexões e chamadas realizadas por seus clientes para fins judiciais, mas na internet brasileira inexiste procedimento análogo.

Registre-se que naquela audiência foram ouvidos representantes do Comitê Gestor da Internet no Brasil (CGIBr) do Ministério da Ciência e Tecnologia; da Fundação de Amparo à Pesquisa de São Paulo (FAPESP) que representa no Brasil o ICANN (*Internet Corporation for Assigning Names and Numbers)*, gestora do registro de nomes e números IP (*Internet Protocol),* ou seja, os endereços na internet; da– Associação Brasileira dos Provedores de Internet (ABRANET); do Instituto de Criminalística em Informática da Polícia Federal, do Ministério da Justiça (PF); da Agência Nacional de Telecomunicações (ANATEL).

Há apenas uma recomendação do Comitê Gestor da Internet Brasil (CGIBr) aos provedores nacionais: que mantenham, por no mínimo três anos, os dados de conexões e comunicações realizadas por seus equipamentos – a saber, identificação dos endereços de IP (protocolo de internet) do remetente e do destinatário da mensagem, bem como a data e horário de início e término da conexão, sem registrar o conteúdo da mensagem, preservando assim o sigilo da comunicação. É clara a necessidade de se transformar tal recomendação em imposição legal, razão por que apresentamos a inclusão no Código Penal do art.154-E conforme o art. 2° do substitutivo.

Além disso, também para fins de investigação, na mesma Audiência Pública, registrou-se a necessidade de estabelecer a obrigatoriedade de identificação positiva do usuário que acesse a Internet, ou qualquer rede de computadores, perante seu provedor ou junto a quem lhe torne disponível o acesso a dispositivo de comunicação ou sistema informatizado, muito embora todos tenham reconhecido as dificuldades técnicas, econômicas e culturais que a regra possa oferecer. Incluem-se aqui os *cyber-cafe* ou *hot zones*.

Vêm à memória os episódios danosos que ocorreram no início da operação com os celulares pré-pagos, o que obrigou o seu cadastramento obrigatório pelas operadoras, contra todos os argumentos então apresentados, ou seja, a sociedade brasileira mostrou o seu bom senso e mudou seu comportamento.

Desde já, alertamos que tal identificação e cadastramento necessitam serem necessariamente presenciais, com cópias de documentos originais, mas admite-se a alternativa de se utilizarem os certificados digitais, cuja emissão já é presencial conforme definido em Lei.

Outras formas alternativas de identificação e cadastramento podem ser usadas a exemplo do que os bancos, operadoras de telefonia, operadores de *call-center* e o comércio eletrônico em geral já vêm fazendo, usando cadastros disponíveis mediante convênios de cooperação ou simples colaboração.

Dados como nome de acesso (*login* ou *username*), nome completo, filiação, endereço completo, data de nascimento, números de telefone e senha criteriosa (número de caracteres, mistura de letras e números etc) devem ser requeridos no momento do cadastramento de um novo usuário. Este, ao solicitar um acesso posterior, usará seu nome de acesso e sua senha e outros procedimentos de validação e conferência automáticas realizados pelo sistema do provedor de acesso, procedimentos que têm o nome de "autenticação do usuário".

Conforme já citado em parágrafo anterior, a identificação e conseqüente cadastramento já acontecem com os serviços de telefonia, transmissão de dados e rádio-transmissão, onde cada operador já é obrigado por regulamento a manter um cadastro de proprietários de telefones fixos, móveis ou de aparelhos transmissores e receptores de rádio - cadastro usado exclusivamente para fins de investigação ou judiciais. Novamente, procedimento obrigatório análogo não existe na internet brasileira.

Novas tecnologias de transmissão, como a conexão sem fio, conhecida como *wireless* ou *Wi-Fi,* estão cada vez mais disponíveis. Como são padronizadas internacionalmente, tendem a se tornar extremamente baratas e a serem disseminadas largamente por todas as cidades, distritos ou aglomerações urbanas ou rurais, libertando o usuário de internet do local físico a que hoje está obrigado. Com o advento próximo da televisão digital tal disseminação será ainda mais efetiva.

Ainda, em qualquer outro serviço privado que se utilize da internet, seja instituição financeira, operadoras de cartões de crédito, empresas de comércio ou indústria, ou nas redes internas das instituições públicas e privadas, a autenticação do usuário mediante senha acompanhada, ou não, de outros requisitos de identificação, como certificado digital, tabela de códigos alfanuméricos e assim por diante, são requeridos para que o usuário acesse os serviços ou as informações.

Em outro caso, em decisão recente, o Tribunal Superior do Trabalho (TST) deu ganho de causa a um banco contra um funcionário que divulgava informações incorretas sobre as aplicações em um fundo de investimentos. O referido agente fora denunciado por uma cliente que tivera prejuízos com as informações e, em razão disso, foi demitido por justa causa, já que usou equipamento do banco, em horário de trabalho funcional, distribuindo informes não-verdadeiros na internet.

Assim, não é demais lembrar, principalmente para esses casos de difamação e injúria ou de prejuízos pessoais, o que dispõe a Carta Magna no seu art. 5º inciso IV que diz "é livre a manifestação do pensamento, sendo vedado o anonimato", o que por si só já justificaria a identificação, o cadastramento e a respectiva autenticação do usuário pelo provedor de acesso à internet brasileira.

Para tanto, transformamos a identificação, o cadastro e respectiva autenticação do usuário em imposição legal, conforme o caput do Art. 15 do substitutivo e incluindo no Código Penal o artigo 154-F e os parágrafos incluídos nos artigos. 154-A, 154-D e 266-A, conforme o art. 2º do substitutivo.

A fim de preservar a intimidade dos usuários, o cadastro somente poderá ser fornecido a terceiros mediante expressa autorização judicial ou em casos que a Lei determinar, conforme o § 2º do art. 14 do substitutivo.

Mas reconhecendo a existência de ferramentas de segurança mais potentes, previmos, conforme o § 3º do art. 14 do substitutivo, a troca opcional, pelo provedor, da identificação e do cadastro do usuário, pelo certificado digital. Este requer, de maneira presencial quando da sua emissão, todas as informações cadastrais, inclusive a constituição tecnicamente adequada de senha.

A regra é condizente com a Medida Provisória número 2.200-2, de 24 de agosto de 2001, mantida em vigor conforme a Emenda Constitucional número 32, de 12 de setembro de 2001. Como toda tecnologia inovadora o certificado digital inicialmente se restringiu às trocas interbancárias, a Transferência Eletrônica Disponível (TED), instituída pelo Sistema de Pagamentos Brasileiro (SPB), implantado em 2002 pelo Banco Central do Brasil. Estatísticas recentes mostram a ocorrência de quase 100 milhões de transações e mais de R$ 5 trilhões de reais transferidos com toda segurança em tempo real.

É público o fato de que o custo de cada certificado digital e seu suporte físico, (cartão de plástico, CD-ROM, ou outro dispositivo de comunicação), tende a cair em proporção geométrica, à medida que se dissemine o seu uso, uma característica conhecida das inovações tecnológicas.

Ao dispor sobre o uso do certificado digital como opcional, a presente norma permite a sua própria evolução, aguardando que a sociedade se adapte à nova realidade transformada a cada dia pela tecnologia, sem obrigar o usuário ou os provedores a novos custos ou a novos hábitos e comportamentos.

Por fim, mantendo a necessária segurança e respeitando os pressupostos de uma rede de computadores, naturalmente ágil, compatível, interoperável, colaborativa e cooperativa, previmos, conforme o § 4º do art. 14 do substitutivo, a substituição opcional do cadastro de identificação, a critério daquele que torna disponível o acesso, por cadastro que poderá ser obtido mediante instrumento público de convênio de cooperação ou colaboração com aqueles que já o tenham constituído na forma prevista no substitutivo.

III – VOTO

Diante do exposto, e considerando a pertinência e importância da solução proposta, somos pela aprovação do Projeto de Lei do Senado nº 76, de 2000, incorporando parcialmente o Projeto de Lei da Câmara nº 89, de 2003 (nº 84, de 1999, na Câmara dos Deputados) e o Projeto de Lei do Senado nº 137, de 2000, na forma do substitutivo que apresentamos.

EMENDA Nº 2 – CE (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) e o Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), para tipificar condutas realizadas mediante uso de rede de computadores ou internet, ou que sejam praticadas contra sistemas informatizados e similares, e dá outras providências.

O CONGRESSO NACIONAL decreta:

Art. 1° O Capítulo IV do Título II da Parte Especial do Decreto-Lei n° 2.848, de 7 de dezembro de 1940 (Código Penal) fica acrescido do art. 163-A, assim redigido:

"Dano por Difusão de Vírus Eletrônico

Art. 163-A. Criar, inserir ou difundir vírus em dispositivo de comunicação ou sistema informatizado, com a finalidade de destruí-lo, inutilizá-lo ou dificultar-lhe o funcionamento.

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

Parágrafo único - A pena é aumentada de sexta parte, se o agente se vale de anonimato, de nome suposto ou da utilização de identidade de terceiros para a prática de acesso. "(NR)

Art. 2° O Título I da Parte Especial do Código Penal fica acrescido do Capítulo VII-A, assim redigido:

"Capítulo VII-A

DA VIOLAÇÃO DE DISPOSITIVO DE COMUNICAÇÃO OU SISTEMA INFORMATIZADO

Acesso indevido a dispositivo de comunicação

Art. 154-A. Acessar indevidamente, ou sem autorização, dispositivo de comunicação ou sistema informatizado:

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

§ 1° Nas mesmas penas incorre quem fornece a terceiro meio indevido ou não autorizado de acesso a dispositivo de comunicação ou sistema informatizado.

§ 2° 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.

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

Manipulação indevida de informação eletrônica

Art. 154-B. Manter consigo, transportar ou fornecer indevidamente ou sem autorização, dado ou informação obtida em dispositivo de comunicação ou sistema informatizado:

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

Parágrafo único - 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, identificação de usuário e autenticação de usuário

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

I – dispositivo de comunicação: o computador, o computador de mão, o telefone celular, o processador de dados, os meios de armazenamento de dados digitais, ou qualquer outro meio capaz de processar, armazenar ou transmitir dados utilizando-se de tecnologias magnéticas, óticas ou qualquer outra tecnologia digital.

II – sistema informatizado: a rede de computadores, 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, armazenar ou transmitir dados eletronicamente.

III – identificação de usuário: os dados de nome de acesso, senha criteriosa, nome completo, filiação, endereço completo, data de nascimento, numero da carteira de identidade ou equivalente legal, que sejam requeridos no momento do cadastramento de um novo usuário de dispositivo de comunicação ou sistema informatizado.

IV – autenticação de usuário: procedimentos de validação e conferência da identificação do usuário, quando este tem acesso ao dispositivo de comunicação ou sistema informatizado, realizados por quem os torna disponíveis ao usuário.

Divulgação de informações depositadas em banco de dados

Art. 154-D. Divulgar, ou tornar disponíveis, para finalidade distinta daquela que motivou a estruturação do banco de dados, informações privadas referentes, direta ou indiretamente, a dados econômicos de pessoas físicas ou jurídicas, ou a dados de pessoas físicas 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 por decisão da autoridade competente, ou mediante expressa anuência da pessoa a que se referem, ou de seu representante legal.

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

Parágrafo único: A pena é aumentada de sexta parte, se o agente se vale de anonimato, de nome suposto ou da utilização de identidade de terceiros para a prática de divulgação.

Dados de conexões e comunicações realizadas

Art. 154-E. Deixar de manter, aquele que torna disponível o acesso a rede de computadores, os dados de conexões e comunicações realizadas por seus equipamentos, aptas à identificação do usuário, endereços eletrônicos de origem e destino no transporte dos registros de dados e informações, data e horário de início e término da conexão, incluindo protocolo de internet ou mecanismo de identificação equivalente, pelo prazo de cinco anos.

Pena – detenção, de dois a seis meses, e multa.

Permitir acesso por usuário não identificado e não autenticado

Art. 154-F. Permitir, aquele que torna disponível o acesso a rede de computadores, a usuário, sem a devida identificação e autenticação, qualquer tipo de acesso ou uso pela rede de computadores.

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

Parágrafo único. Na mesma pena incorre, o responsável por provedor de acesso a rede de computadores, que deixa de exigir, como condição de acesso à rede, a necessária, identificação e regular cadastramento do usuário.

Art. 3º O Código Penal passa a vigorar acrescido do seguinte art. 183-A:

Art. 183-A. Equiparam-se à coisa o 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.

Art. 4º 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 ou telefônico"

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

..... (NR)"

Art. 5º O Capitulo II do Título VIII do Código Penal passa a vigorar acrescido do seguinte artigo:

"Difusão Maliciosa de Código

Art. 266-A. Difundir, por qualquer meio, programa, conjunto de instruções ou sistema informatizado com o propósito de induzir alguém a fornecer, espontaneamente e por qualquer meio, dados ou informações que facilitem ou permitam o acesso indevido ou sem autorização, a dispositivo de comunicação ou a sistema informatizado, ou a obtenção de qualquer vantagem ilícita:

Pena – detenção de um a dois anos.

Parágrafo único - A pena é aumentada de sexta parte, se o agente se vale de anonimato, de nome suposto ou da utilização de identidade de terceiros para a prática de acesso.(NR)"

Art. 6º 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 portátil de armazenamento e processamento de informações

Parágrafo único. Equipara-se a documento particular o cartão de crédito ou débito ou qualquer dispositivo eletrônico portátil de armazenamento ou processamento de informações. (NR)"

Art. 7º O Código Penal passa a vigorar acrescido do seguinte art. 298-A:

"Falsificação de telefone celular ou meio de acesso a sistema eletrônico

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

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

Art. 8º O Código Penal passa a vigorar 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 dispositivo de comunicação ou sistema informatizado.

Art. 9º 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 Vírus Eletrônico

Art. 262-A. Criar, inserir ou difundir vírus em dispositivo de comunicação ou sistema informatizado, com a finalidade de destruí-lo, inutilizá-lo ou dificultar-lhe o funcionamento.

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

Parágrafo único - A pena é aumentada de sexta parte, se o agente se vale de anonimato, de nome suposto ou da utilização de identidade de terceiros para a prática de acesso. "(NR)

Art. 10 O Título VII da Parte Especial do Livro I do Código Penal Militar, Decreto-Lei, nº 1.001, de 21 de outubro de 1969, fica acrescido do Capítulo VII-A, assim redigido:

"Capítulo VII-A

DA VIOLAÇÃO DE DISPOSITIVO DE COMUNICAÇÃO OU SISTEMA INFORMATIZADO

Acesso indevido a dispositivo de comunicação

Art. 339-A. Acessar indevidamente, ou sem autorização, dispositivo de comunicação ou sistema informatizado:

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

§ 1º Nas mesmas penas incorre quem fornece a terceiro meio indevido ou não autorizado de acesso a dispositivo de comunicação ou sistema informatizado.

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

Manipulação indevida de informação eletrônica

Art. 339-B. Manter consigo, transportar ou fornecer indevidamente ou sem autorização, dado ou informação obtida em dispositivo de comunicação ou sistema informatizado:

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

Dispositivo de comunicação, sistema informatizado, identificação de usuário e autenticação de usuário

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

I – dispositivo de comunicação: o computador, o computador de mão, o telefone celular, o processador de dados, os meios de armazenamento de dados digitais, ou qualquer outro meio capaz de processar, armazenar ou

transmitir dados utilizando-se de tecnologias magnéticas, óticas ou qualquer outra tecnologia digital.

II – sistema informatizado: a rede de computadores, 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, armazenar ou transmitir dados eletronicamente.

III – identificação de usuário: os dados de nome de acesso, senha criteriosa, nome completo, filiação, endereço completo, data de nascimento, numero da carteira de identidade ou equivalente legal, que sejam requeridos no momento do cadastramento de um novo usuário de dispositivo de comunicação ou sistema informatizado.

IV – autenticação de usuário: procedimentos de validação e conferência da identificação do usuário, quando este tem acesso ao dispositivo de comunicação ou sistema informatizado, realizados por quem os torna disponíveis ao usuário.

Divulgação de informações depositadas em banco de dados

Art. 339-D. Divulgar, ou tornar disponíveis, para finalidade distinta daquela que motivou a estruturação do banco de dados, informações privadas referentes, direta ou indiretamente, a dados econômicos de pessoas físicas ou jurídicas, ou a dados de pessoas físicas 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 por decisão da autoridade competente, ou mediante expressa anuência da pessoa a que se referem, ou de seu representante legal.

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

Parágrafo único: A pena é aumentada de sexta parte, se o agente se vale de anonimato, de nome suposto ou da utilização de identidade de terceiros para a prática de divulgação.

Dados de conexões e comunicações realizadas

Art. 339-E. Deixar de manter, aquele que torna disponível o acesso a rede de computadores, os dados de conexões e comunicações realizadas por seus equipamentos, aptas à identificação do usuário, endereços eletrônicos de origem e destino no transporte dos registros de dados e informações, data e horário de início e término da conexão, incluindo protocolo de internet ou mecanismo de identificação equivalente, pelo prazo de cinco anos.

Pena – detenção, de dois a seis meses, e multa.

Permitir acesso por usuário não identificado e não autenticado

Art. 339-F. Permitir, aquele que torna disponível o acesso a rede de computadores, a usuário, sem a devida identificação e autenticação, qualquer tipo de acesso ou uso pela rede de computadores.

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

Parágrafo único. Na mesma pena incorre, o responsável por provedor de acesso a rede de computadores, que deixa de exigir, como condição de acesso à rede, a necessária, identificação e regular cadastramento do usuário.(NR)"

Art. 11 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 Maliciosa de Código

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

Pena – detenção de um a dois anos.

Parágrafo único - A pena é aumentada de sexta parte, se o agente se vale de anonimato, de nome suposto ou da utilização de identidade de terceiros para a prática de acesso.(NR)"

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

"Capítulo VIII-A

DISPOSIÇÕES GERAIS

Art. 267-A. Equiparam-se à coisa o 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 (NR)"

Art. 13 Todo aquele que desejar acessar uma rede de computadores, local, regional, nacional ou mundial, deverá identificar-se e cadastrar-se naquele que torne disponível este acesso.

Parágrafo único. Os atuais usuários terão prazo de cento e vinte dias após a entrada em vigor desta Lei para providenciarem ou revisarem sua identificação e cadastro junto a quem, de sua preferência, torne disponível o acesso aqui definido.

Art. 14 Todo aquele que torna disponível o acesso a uma rede de computadores somente admitirá como usuário pessoa ou dispositivo de comunicação ou sistema informatizado que for autenticado conforme validação positiva dos dados cadastrais previamente fornecidos pelo contratante de serviços. A contratação dar-se-á exclusivamente por meio formal, vedado o ajuste meramente consensual.

§1° O cadastro mantido por aquele que torna disponível o acesso a uma rede de computadores conterá obrigatoriamente as seguintes informações prestadas por meio presencial e com apresentação de documentação original: nome de acesso; senha de acesso ou mecanismo similar; nome completo; endereço completo com logradouro, número, complemento, código de endereçamento postal, cidade e estado da federação; número de registro junto aos serviços ou institutos de identificação das Secretarias de Segurança Pública Estaduais ou conselhos de registro profissional; número de inscrição no Cadastro de Pessoas Físicas (CPF), mantido pelo Ministério da Fazenda ou o Número de Identificação do Trabalhador (NIT), mantido pelo Ministério da Previdência Social.

§ 2° O cadastro somente poderá ser fornecido a terceiros mediante expressa autorização da autoridade competente ou em casos que a Lei venha a determinar.

§ 3° A senha e o cadastro de identificação, a critério daquele que torna disponível o acesso, poderão ser substituídos por certificado digital emitido dentro das normas da Infra-estrutura de Chaves Públicas Brasileira (ICP–Brasil), conforme determina a MP 2.200-2 de 24 de agosto de 2001.

§ 4° O cadastro de identificação, a critério daquele que torna disponível o acesso, poderá ser obtido mediante instrumento público de convênio

de cooperação ou colaboração com aqueles que já o tenham constituído na forma deste artigo.

§ 5º Para assegurar a identidade e a privacidade do usuário a senha de acesso poderá ser armazenada criptografada por algoritmo não reversível.

Art. 15. 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:

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

Art. 16 Esta Lei entra em vigor sessenta dias após a data de sua publicação.

Sala da Comissão, 20 de maio de 2006.

, Presidente Eventual

Senador Juvêncio da Fonseca,

, Relator

COMISSÃO DE EDUCAÇÃO

ASSINAM O PARECER AOS PLS Nº 076/00 E PLS Nº 137/00 E AO PLC Nº 089/03 NA REUNIÃO DE 20/20/06 OS SENHORES SENADORES:

PRESIDENTE EVENTUAL:	(Sen. Juvêncio da Fonseca

BLOCO DA MINORIA (PFL E PSDB)

DEMÓSTENES TORRES	1- ROSEANA SARNEY
JORGE BORNHAUSEN	2- JONAS PINHEIRO
JOSÉ JORGE	3- CÉSAR BORGES
MARIA DO CARMO ALVES	4- CRISTOVAM BUARQUE
EDISON LOBÃO	5- MARCO MACIEL
MARCELO CRIVELLA	6- ROMEU TUMA
MARCOS GUERRA	7- EDUARDO AZEREDO RELATOR
JUVÊNCIO DA FONSECA	8- SÉRGIO GUERRA
LEONEL PAVAN	9- LÚCIA VÂNIA
(VAGO)	10- JOÃO BATISTA MOTTA

PMDB

WELLINGTON SALGADO DE OLIVEIRA	1- AMIR LANDO
GILVAM BORGES	2- GARIBALDI ALVES FILHO
VALDIR RAUPP	3- (VAGO)
ÍRIS DE ARAÚJO	4- GERALDO MESQUITA
SÉRGIO CABRAL	5- MÃO SANTA
JOSÉ MARANHÃO	6- LUIZ OTÁVIO
NEY SUASSUNA	7- ROMERO JUCÁ
GILBERTO MESTRINHO	8- (VAGO)

BLOCO DE APOIO AO GOVERNO (PT, PSB E PL)

AELTON FREITAS	1- SIBÁ MACHADO
PAULO PAIM	2- ALOÍZIO MERCADANTE
FÁTIMA CLEIDE	3- FERNANDO BEZERRA
FLÁVIO ARNS	4- ANTONIO JOÃO
IDELI SALVATTI	5- ANTÔNIO CARLOS VALADARES
ROBERTO SATURNINO	6- MAGNO MALTA
MOZARILDO CAVALCANTI	7- PATRÍCIA SABOYA GOMES
SÉRGIO ZAMBIASI	8- JOÃO RIBEIRO

PDT

AUGUSTO BOTELHO	1- (VAGO)

PARECER Nº 584, DE 2008

(Da Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática)

RELATOR: Senador **EDUARDO AZEREDO**

I – RELATÓRIO

Vem a esta Comissão, para exame, o Projeto de Lei da Câmara (PLC) nº 89, de 2003 (nº 84, de 1999, na origem), e os Projetos de Lei do Senado (PLS) nº 137, de 2000, e nº 76, de 2000, todos referentes a crimes na área de informática. Tramitam em conjunto em atendimento ao Requerimento nº 847, de 2005, do Senador Renan Calheiros. Em decorrência do Requerimento nº 848, de 2005, foi extinta a urgência na tramitação do PLC nº 89, de 2003, que havia sido declarada em decorrência da aprovação do Requerimento nº 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 nº 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 n° 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 § 1° e acrescentar o § 2° 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 § 4° do art. 155 do Código Penal e acrescentarmos o inciso V do § 6° 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.

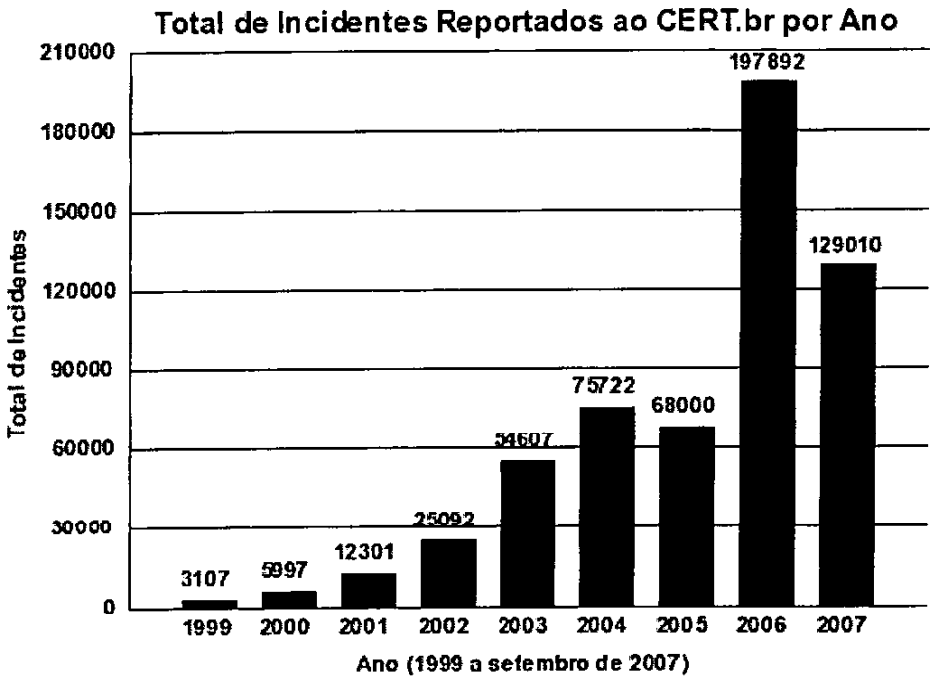
O tema é atual e merece a devida atenção do Congresso Nacional. Segundo recentes dados divulgados pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (www.cert.br), os códigos maliciosos, classificados como *worm*, representam 40%, ou 51 mil, de todos os incidentes reportados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

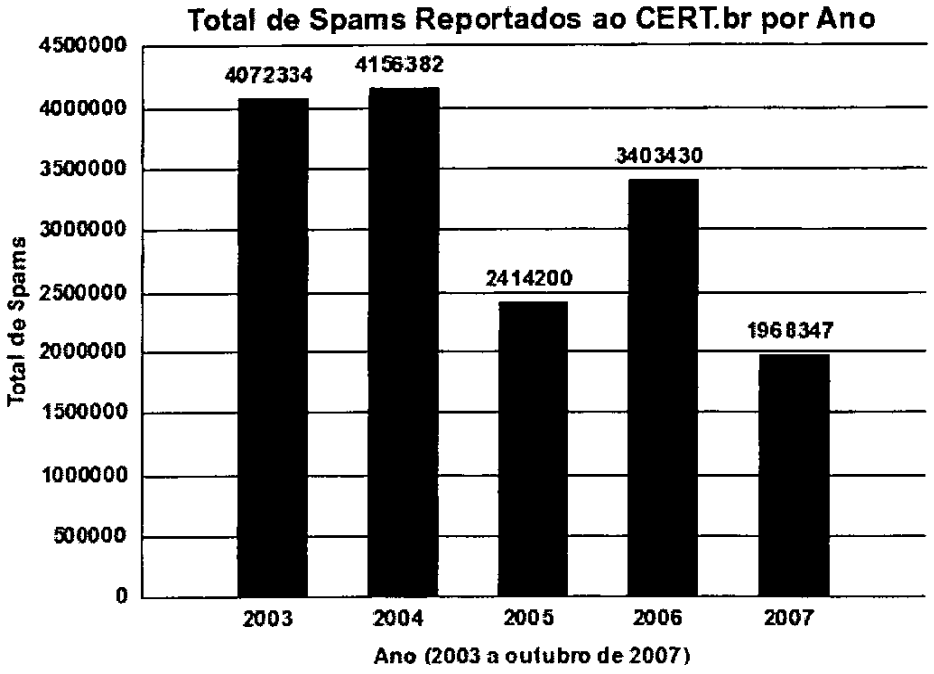
Os números, frise-se bem, podem ser muito maiores, dado que o CERT.br considera apenas as informações reportadas espontaneamente pelos usuários e administradores de redes. Ao todo, o CERT.br recebeu, no ano passado, 197 mil comunicações de incidentes relacionados à internet, alta de 191% em relação a 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 nº 89, de 2003 (nº 84, de 1999, na Câmara dos Deputados), e dos Projetos de Lei do Senado nº 76 e nº 137, ambos de 2000, na forma do novo Substitutivo que ora oferecemos a esta Comissão de Ciência e Tecnologia.

EMENDA Nº 3 - CCT
(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.

§ 1° 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.

§ 2° 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.

§ 3° 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.

§ 1° 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.

§ 2° 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.

§ 3° 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.

§ 1° 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.

§ 2° 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. 4° O § 4° do art. 155 do Decreto-Lei n° 2.848, de 7 de dezembro de 1940 (Código Penal), passa a vigorar acrescido do seguinte inciso V:

"**Art. 155.** .....

.....

§ 4° .....

.....

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. 5° O Capítulo IV do Título II da Parte Especial do Decreto-Lei n° 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

§ 1° 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

§ 2° 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.

§ 3° 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. 6° 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.

§ 1° 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. 7° 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.** .....

.....

§ 2° 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.

§ 1° 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.

§ 2° 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.

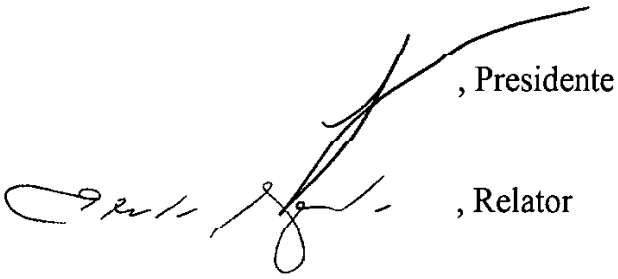
§ 3° O responsável citado no *caput* deste artigo que não cumprir o disposto no § 2°, independentemente do ressarcimento por perdas e danos ao lesado, estará sujeito ao pagamento de multa variável de R$ 2.000,00 (dois mil reais) a R$ 100.000,00 (cem mil reais) a cada verificação ou solicitação, aplicada 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.

§ 4° 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, 12 de dezembro de 2007.



, Presidente

, Relator

COMISSÃO DE CIÊNCIA, TECNOLOGIA, INOVAÇÃO, COMUNICAÇÃO E INFORMÁTICA

ASSINAM O PARECER AO PLC Nº 89/03 (TRAMITANDO EM CONJUNTO COM OS PLS 76/00 E 137/00) NA REUNIÃO DE 12/12/07 OS SENHORES SENADORES:

PRESIDENTE:	(Senador Wellington Salgado de Oliveira)
Bloco de Apoio ao Governo (PT, PR, PSB, PC do B, PRB e PP)	
MARCELO CRIVELLA	1. EXPEDITO JÚNIOR
AUGUSTO BOTELHO	2. FLÁVIO ARNS
RENATO CASAGRANDE	3. JOÃO RIBEIRO
SÉRGIO ZAMBIASI	4. FRANCISCO DORNELLES
IDELI SALVATTI	5. FÁTIMA CLEIDE
PMDB	
VALDIR RAUPP	1. ROMERO JUCÁ
WELLINGTON SALGADO DE OLIVEIRA	2. GARIBALDI ALVES FILHO
GILVAM BORGES	3. MÃO SANTA
VALTER PEREIRA	4. LEOMAR QUINTANILHA
BLOCO DA MINORIA (DEM E PSDB)	
DEMÓSTENES TORRES	1. ELISEU RESENDE
ROMEU TUMA	2. HERÁCLITO FORTES
MARIA DO CARMO ALVES	3. MARCO MACIEL
ANTONIO CARLOS JÚNIOR	4. ROSALBA CIARLINI
JOAO TENORIO	5. FLEXA RIBEIRO
EDUARDO AZEREDO RELATOR	6. MARCONI PERILLO
CÍCERO LUCENA	7. PAPALÉO PAES
PDT	
CRISTOVAM BUARQUE	1- VAGO

PARECER Nº 585, DE 2008
(Da Comissão de Assuntos Econômicos)

RELATOR: Senador **ALOIZIO MERCADANTE**

I – RELATÓRIO

Vem a esta Comissão, para exame, o Projeto de Lei da Câmara (PLC) nº 89, de 2003 (nº 84, de 1999, na origem), e os Projetos de Lei do Senado (PLS) nº 137, de 2000, e nº 76, de 2000, todos referentes a crimes na área de informática. Tramitam em conjunto em atendimento ao Requerimento nº 847, de 2005, do Senador Renan Calheiros. Em decorrência do Requerimento nº 848, de 2005, foi extinta a urgência na tramitação do PLC nº 89, de 2003, que havia sido declarada em decorrência da aprovação do Requerimento nº 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 nº 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 nº 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. Além das alterações feitas em artigos do CP, o projeto visa 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).

Em 2004 e 2005, o Senador Eduardo Azeredo relatou com muita propriedade essas proposições perante a Comissão de Educação (CE). Após amplos debates, em 2006 foi aprovado o parecer final na forma do Substitutivo ao PLS n° 76, de 2000 – por ser mais abrangente e mais antigo –, com proveito parcial dos demais.

Durante o longo processo de debate sobre a matéria, dentro e fora do Senado Federal, o Substitutivo foi aperfeiçoado para ser apresentado à Comissão de Constituição e Justiça (CCJ).

Foram apresentadas 4 emendas no âmbito da CCJ, e uma delas retirada logo em seguida. As emendas foram incorporadas ao Substitutivo proposto.

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

Em dezembro de 2007, o parecer do Senador Eduardo Azeredo foi aprovado pela CCT, na forma do Substitutivo apresentado.

Até o momento 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.

Materialmente, não vislumbramos inconstitucionalidades ou vícios de juridicidade nos projetos de lei sob exame. No mérito, propomos alterações para o aperfeiçoamento do Substitutivo aprovado na CCT, em comum acordo com o Senador Eduardo Azeredo, após várias consultas feitas a especialistas na matéria.

Concordamos com as premissas apresentadas pelo Senador Eduardo Azeredo, em seus pareceres anteriores, de que o assunto merece e necessita regulamentação no direito brasileiro, bem como reconhecemos a tendência internacional de tutela e fiscalização do meio cibernético. Além disso, reconhecemos a necessidade de harmonizar a nossa futura lei de crimes cibernéticos com a *Convenção sobre o Cibercrime* da Europa. A Convenção recomenda procedimentos processuais penais, a guarda criteriosa das informações trafegadas nos sistemas informatizados e sua liberação para as autoridades. A compatibilidade das previsões legais produz efeitos em questões de extradição, de assistência judiciária mútua entre os Estados e de cooperação internacional de uma forma geral. A harmonia com as tendências internacionais é importante para otimizar a repressão dos crimes de informática, notadamente transnacionais.

Analisando o Substitutivo e os projetos apensados, concluímos que a matéria, complexa e abrangente, tratando de crimes contra a pessoa, contra o patrimônio e contra serviços públicos, requeria novos aperfeiçoamentos, sem se alterar, contudo, o núcleo substantivo do texto. Esses aperfeiçoamentos, fruto de consenso, são apresentados na forma de emendas ao Substitutivo aprovado pela CCT.

Alguns crimes que, no Substitutivo, estavam localizados topograficamente no Título dos "Crimes contra a Pessoa" do Código Penal, foram deslocados para o Título dos "Crimes contra a Incolumidade Pública", por melhor traduzir o bem jurídico que se quer tutelar. O nome do novo Capítulo passa a ser "Dos Crimes Contra a Segurança dos Sistemas Informatizados". É o caso dos novos artigos 285-A, 285-B e 285-C.

Optamos por adotar a estratégia de não trazer, no próprio Código Penal ou Código Penal Militar (CPM), o rol de conceitos dos elementos típicos "dispositivo de comunicação", "sistema informatizado", "código malicioso", entre outros constantes do Substitutivo (arts. 154-C no CP e 339-C, no CPM). Sugerimos que o rol constitua um artigo autônomo da lei. Julgamos tratar-se de melhor estratégia para a orientação normativa das diversas leis que o projeto altera.

Sugerimos a supressão do art. 141-A, que prevê causa de aumento de pena para os crimes contra a honra quando praticados por meios informáticos. Julgamos tratar-se de desnecessário *bis in idem*, em face do que já dispõe o inciso III do art. 141 do CP.

Para esclarecer a distinção de valor atribuída às condutas constantes dos arts. 154-A e 154-B (novos 285-A e 285-B, conforme emendas), as redações dos *caput* foram levemente alteradas e as estruturas dos tipos simplificadas. Parágrafos repetidos foram reunidos em dispositivo único (art. 285-C). A proporcionalidade das penas foi adaptada aos outros crimes presentes na nova localização proposta.

O art. 154-D (novo art. 154-A) foi mantido no Título original, dado o bem jurídico tutelado, e a sua redação simplificada, para a melhor identificação do desvalor atribuído à conduta.

Propomos a supressão da equiparação do dado e do dispositivo informático à "coisa", para efeitos de crimes contra o patrimônio (arts. 183-A e 155, § 4º, V). Essa equiparação poderia acarretar desdobramentos sistêmicos imprevisíveis na lei penal, perdendo-se os parâmetros de tangibilidade e de intangibilidade de bens que o sistema penal resguarda. Preferimos a estratégia de prever, em artigo autônomo da nova lei, que são considerados bens protegidos o dado, o dispositivo de comunicação, a rede de computadores e o sistema informatizado, o que limita e especifica o alcance dos efeitos de tal previsão (novo art. 18, conforme emenda).

O tipo penal sobre a difusão de código malicioso (art. 163-A) também foi simplificado, para a melhor identificação do desvalor da ação. O mesmo foi feito na redação do art. 298-A. Em relação ao "estelionato eletrônico" (art. 171-A), propomos o seu deslocamento topográfico para o rol do § 2° do mesmo art. 171, com a simplificação de sua redação.

Alterações equivalentes foram propostas para os dispositivos que alteram o Código Penal Militar.

Outrossim, sugerimos a simplificação da alteração proposta para o art. 20 da Lei n° 7.716, de 1989, a supressão da alteração sugerida para a Lei n° 8.078, de 1990 (parágrafo único do art. 9°), pelo fato de a previsão já constar do *caput* do mesmo artigo, e aperfeiçoamos a alteração proposta no Estatuto da Criança e do Adolescente (art. 241), para punir também a conduta de manter consigo imagens pornográficas que envolvam crianças e adolescentes.

Por fim, sugerimos a supressão dos arts. 16 e 17 do parecer da CCT. O art. 16 prevê exceção à regra determinada pelo art. 2° da Lei 9296/96, que exclui a possibilidade de interceptação de comunicação para os crimes apenados com detenção. Já a alteração do art. 313 do Código de Processo Penal acrescenta novo inciso V, prevendo a possibilidade de prisão preventiva para os crimes "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", enquanto o inciso I do mesmo art. 313 já prevê essa possibilidade para os crimes punidos com reclusão. Ambos perdem o sentido, uma vez que todas as penas previstas nas emendas ora apresentadas são de reclusão.

Como se pode observar nas 23 emendas propostas a seguir, não se toca no núcleo material do Substitutivo aprovado pela CCT. Julgamos tratarem-se de sugestões que aperfeiçoam e simplificam o projeto, sem perder de vista a eficácia, o rigor e a harmonia com a tendência normativa internacional.

III – VOTO

Diante do exposto, 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 nº 137, ambos de 2000, na forma do Substitutivo aprovado pela CCT com as seguintes subemendas:

SUBEMENDA Nº 1 – CAE À EMENDA Nº 3 -CCT (SUBSTITUTIVO)

Dê-se à ementa do Substitutivo aprovado pela CCT 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, e a Lei nº 8.069, de 13 de julho de 1990, e a Lei nº 10.446, de 8 de maio de 2002, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra dispositivos de comunicação ou sistemas informatizados e similares, e dá outras providências."

SUBEMENDA Nº 2 – CAE À EMENDA Nº 3 CCT (SUBSTITUTIVO)

Dê-se ao art. 1º do Substitutivo aprovado pela CCT 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, e a Lei nº 8.069, de 13 de julho de 1990, e a Lei nº 10.446, de 8 de maio de 2002, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra dispositivos de comunicação ou sistemas informatizados e similares, e dá outras providências."

SUBEMENDA Nº 3 – CAE À EMENDA Nº 3 -CCT (SUBSTITUTIVO)

Dê-se ao art. 2º do Substitutivo aprovado pela CCT a seguinte redação:

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

Capítulo IV

DOS CRIMES CONTRA A SEGURANÇA DOS SISTEMAS INFORMATIZADOS

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

Art. 285-A. Acessar rede de computadores, dispositivo de comunicação ou sistema informatizado, sem autorização do legítimo titular, quando exigida:

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

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

Obtenção, transferência ou fornecimento não autorizado de dado ou informação

Art.. 285-B. Obter ou transferir dado ou informação disponível em rede de computadores, dispositivo de comunicação ou sistema informatizado, sem autorização ou em desconformidade à autorização, do legítimo titular, quando exigida:

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

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

Ação Penal

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

SUBEMENDA Nº 4 – CAE À EMENDA Nº 3 -CCT (SUBSTITUTIVO)

Dê-se ao art. 3º do Substitutivo aprovado pela CCT a seguinte redação:

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

Divulgação ou utilização indevida de informações e dados pessoais

154-A. Divulgar, utilizar, comercializar ou disponibilizar dados e informações pessoais contidas em sistema informatizado com finalidade distinta da que motivou seu registro, salvo nos casos previstos em lei ou mediante expressa anuência da pessoa a que se referem, ou de seu representante legal.

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

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

.....(NR)"

SUBEMENDA N' 5 – CAE À EMENDA Nº 3 -CCT (SUBSTITUTIVO)

Dê ao art. 4º do Substitutivo aprovado pela CCT, a seguinte redação:

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

Dano

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

.....(NR)"

SUBEMENDA Nº 6 – CAE À EMENDA Nº 3 -CCT (SUBSTITUTIVO)

Dê-se ao art. 5º do Substitutivo aprovado pela CCT a seguinte redação:

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

Inserção ou difusão de código malicioso

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

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

Inserção ou difusão de código malicioso seguido de dano

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

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

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

SUBEMENDA Nº 7 – CAE À EMENDA Nº 3 -CCT (SUBSTITUTIVO)

Dê-se ao art. 6º do Substitutivo aprovado pela CCT a seguinte redação:

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

Art. 171 .....

§ 2º Nas mesmas penas incorre quem:

.....

Estelionato Eletrônico

VII – difunde, por qualquer meio, código malicioso com intuito de facilitar ou permitir acesso indevido à rede de computadores, dispositivo de comunicação ou sistema informatizado:

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

..... (NR)"

SUBEMENDA Nº 8 – CAE À EMENDA Nº 3 -CCT (SUBSTITUTIVO)

Dê-se ao art. 7º do Substitutivo aprovado pela CCT a seguinte redação:

"**Art. 7º** Os arts. 265 e 266 do Código Penal passam a vigorar com as seguintes redações:

Atentado contra a segurança de serviço de utilidade pública

Art. 265. Atentar contra a segurança ou o funcionamento de serviço de água, luz, força, calor, informação ou telecomunicação, ou qualquer outro de utilidade pública:

..... (NR)

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)"

SUBEMENDA Nº 9 – CAE À EMENDA Nº 3 -CCT (SUBSTITUTIVO)

Dê-se ao art. 8º ao Substitutivo aprovado pela CCT a seguinte redação:

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

Falsificação de dado eletrônico ou documento público

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

.....(NR)"

SUBEMENDA Nº 10 – CAE À EMENDA Nº 3 -CCT (SUBSTITUTIVO)

Dê-se o art. 9º do Substitutivo aprovado pela CCT a seguinte redação:

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

Falsificação de dado eletrônico ou documento particular

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

.....(NR)"

SUBEMENDA Nº 11 – CAE À EMENDA Nº 3 -CCT (SUBSTITUTIVO)

Dê-se ao art. 10 do Substitutivo aprovado pela CCT a seguinte redação:

"**Art. 10.** O Capítulo VII do Título V da Parte Especial do Livro I do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), fica acrescido do art. 262-A, assim redigido:

Inserção ou difusão de código malicioso

Art. 262-A. Inserir ou difundir código malicioso em dispositivo de comunicação, rede de computadores, ou sistema informatizado:

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

Inserção ou difusão código malicioso seguido de dano

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

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

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

SUBEMENDA Nº 12 – CAE À EMENDA Nº 3 -CCT (SUBSTITUTIVO)

Dê-se ao art. 11 do Substitutivo aprovado pela CCT a seguinte redação:

"**Art. 11.** O Título VII da Parte Especial do Livro I do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), fica acrescido do Capítulo VII-A, assim redigido:

Capítulo VII-A

DOS CRIMES CONTRA A SEGURANÇA DOS SISTEMAS INFORMATIZADOS

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

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

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

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

Obtenção, transferência ou fornecimento não autorizado de dado ou informação

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

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

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

SUBEMENDA Nº 13 – CAE À EMENDA Nº 3 -CCT (SUBSTITUTIVO)

Dê-se ao art. 12 do Substitutivo aprovado pela CCT a seguinte redação:

"**Art. 12.** O Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), fica acrescido do art. 339-C, assim redigido:

Divulgação ou utilização indevida de informações e dados pessoais

Art. 339-C Divulgar, utilizar, comercializar ou disponibilizar dados e informações pessoais contidas em sistema informatizado com finalidade distinta da que motivou seu registro, salvo nos casos previstos em lei ou mediante expressa anuência da pessoa a que se referem, ou de seu representante legal.

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

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

SUBEMENDA Nº 14 – CAE À EMENDA Nº 3 -CCT (SUBSTITUTIVO)

Dê-se ao art. 13 do Substitutivo aprovado pela CCT a seguinte redação:

"**Art. 13.** 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 - Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada da sexta parte."

SUBEMENDA Nº 15 – CAE À EMENDA Nº 3 -CCT (SUBSTITUTIVO)

Dê-se ao art. 14 do Substitutivo aprovado pela CCT a seguinte redação:

"**Art. 14.** Para os efeitos penais considera-se, dentre outros:

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

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

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

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

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

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

SUBEMENDA Nº 16 – CAE À EMENDA Nº 3 -CCT (SUBSTITUTIVO)

Dê-se ao art. 15 do Substitutivo aprovado pela CCT a seguinte redação:

"**Art. 15.** Para efeitos penais consideram-se também como bens protegidos o dado, o dispositivo de comunicação, a rede de computadores, o sistema informatizado."

SUBEMENDA Nº 17 – CAE À EMENDA Nº 3 -CCT (SUBSTITUTIVO)

Dê-se ao art. 16 do Substitutivo aprovado pela CCT a seguinte redação:

> **"Art. 16.** Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado."

SUBEMENDA Nº 18 – CAE À EMENDA Nº 3 -CCT (SUBSTITUTIVO)

Dê-se ao art. 17 do Substitutivo aprovado pela CCT a seguinte redação:

> "**Art. 17.** O inciso II do § 3º do art. 20 da Lei nº 7.716, de 5 de janeiro de 1989, passa a vigorar com a seguinte redação:
>
> **Art. 20** .....
>
> .....
>
> **§ 3º**.....
>
> **II** – a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas, ou da publicação por qualquer meio.
>
> ..... (NR)"

SUBEMENDA Nº 19 – CAE À EMENDA Nº 3 -CCT (SUBSTITUTIVO)

Dê-se ao art. 18 do Substitutivo aprovado pela CCT a seguinte redação:

> "**Art. 18.** 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, receptar, fornecer, divulgar, publicar ou armazenar consigo, por qualquer meio de comunicação, inclusive rede mundial de computadores ou Internet, fotografias, imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente:
>
> ..... (NR)"

SUBEMENDA Nº 20 – CAE À EMENDA Nº 3 -CCT (SUBSTITUTIVO)

Dê-se ao art. 19 do Substitutivo aprovado pela CCT a seguinte redação:

"**Art. 19.** 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 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, e fornecê-los exclusivamente à autoridade investigatória mediante prévia requisição judicial;

II – preservar imediatamente, após requisição judicial, no curso de investigação, os dados de que cuida o inciso I deste artigo e outras informações requisitadas por aquela investigação, respondendo civil e penalmente pela sua absoluta confidencialidade e inviolabilidade;

III – informar, de maneira sigilosa, à autoridade 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.

§ 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.

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

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

SUBEMENDA Nº 21 – CAE À EMENDA Nº 3 -CCT (SUBSTITUTIVO)

Dê-se ao art. 20 do Substitutivo aprovado pela CCT a seguinte redação:

"**Art. 20.** O art. 1° da Lei n° 10.446, de 8 de maio de 2002 passa a vigorar com a seguinte redação:

Art. 1° .....

.....

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

.....(NR)"

SUBEMENDA Nº 22 – CAE À EMENDA Nº 3 -CCT (SUBSTITUTIVO)

Dê-se ao art. 21 do Substitutivo aprovado pela CCT a seguinte redação:

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

SUBEMENDA Nº 23 – CAE À EMENDA Nº 3 -CCT (SUBSTITUTIVO)

Suprimam-se os arts. 22, 23, 24 e 25 do Substitutivo aprovado pela CCT.

Sala da Comissão, em 10 de junho de 2008.

, Presidente

, Relator

COMISSÃO DE ASSUNTOS ECONÔMICOS
PROJETO DE LEI DA CÂMARA Nº 89, DE 2003, QUE TRAMITA EM CONJUNTO COM OS PROJETOS DE LEI DO SENADO Nºs 76 E 137, DE 2000
NÃO TERMINATIVOS

ASSINARAM O PARECER NA REUNIÃO DE 10 / 06/ 08, OS SENHORES(AS) SENADORES(AS):
PRESIDENTE: Senador ELISEU RESENDE, Vice-Presidente
RELATOR(A):

Bloco de Apoio ao Governo (PT, PR, PSB, PCdoB, PRB e PP)	
EDUARDO SUPLICY (PT)	1-FLÁVIO ARNS (PT)
FRANCISCO DORNELLES (PP)	2-PAULO PAIM (PT)
DELCÍDIO AMARAL (PT)	3-IDELI SALVATTI (PT)
ALOIZIO MERCADANTE (PT)	4-VAGO
RENATO CASAGRANDE (PSB)	5-MARCELO CRIVELLA (PRB)
EXPEDITO JÚNIOR (PR)	6-INÁCIO ARRUDA (PCdoB)
SERYS SLHESSARENKO (PT)	7-PATRÍCIA SABOYA GOMES (PDT)
	8-ANTÔNIO CARLOS VALADARES (PSB)
	9-CÉSAR BORGES (PR)
Maioria (PMDB)	
ROMERO JUCÁ	1-VALTER PEREIRA
VALDIR RAUPP	2-ROSEANA SARNEY
PEDRO SIMON	3-WELLINGTON SALGADO
MÃO SANTA	4-LEOMAR QUINTANILHA
GEOVANI BORGES	5-EDISON LOBÃO FILHO
NEUTO DE CONTO	6-PAULO DUQUE
GERSON CAMATA	7-JARBAS VASCONCELOS
Bloco Parlamentar da Minoria (DEM e PSDB)	
DELMIR SANTANA (DEM)	1-GILBERTO GOELLNER (DEM)
HERÁCLITO FORTES (DEM)	2-ANTONIO CARLOS JÚNIOR (DEM)
ELISEU RESENDE (DEM)	3-DEMÓSTENES TORRES (DEM)
JAYME CAMPOS (DEM)	4-ROSALBA CIARLINI (DEM)
KÁTIA ABREU (DEM)	5-MARCO MACIEL (DEM)
RAIMUNDO COLOMBO (DEM)	6-ROMEU TUMA (PTB)
CÍCERO LUCENA (PSDB)	7-ARTHUR VIRGÍLIO (PSDB)
FLEXA RIBEIRO (PSDB)	8-EDUARDO AZEREDO (PSDB)
SÉRGIO GUERRA (PSDB)	9-MARCONI PERILLO (PSDB)
TASSO JEREISSATI (PSDB)	10-JOÃO TENÓRIO (PSDB)
PTB	
JOÃO VICENTE CLAUDINO	1-
GIM ARGELLO	2-
PDT	
OSMAR DIAS	1-JEFFERSON PRAIA

PARECER Nº 586, DE 2008

(Da Comissão de Constituição, Justiça e Cidadania)

RELATOR: Senador **EDUARDO AZEREDO**

I – RELATÓRIO

Vem a esta Comissão, para exame, o Projeto de Lei da Câmara (PLC) nº 89, de 2003 (nº 84, de 1999, na origem), e os Projetos de Lei do Senado (PLS) nº 137, de 2000, e nº 76, de 2000, todos referentes a crimes na área de informática. Tramitam em conjunto em atendimento ao Requerimento nº 847, de 2005, do Senador Renan Calheiros. Em decorrência do Requerimento nº 848, de 2005, foi extinta a urgência na tramitação do PLC nº 89, de 2003, que havia sido declarada em decorrência da aprovação do Requerimento nº 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 nº 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 nº 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. Além das alterações feitas em artigos do CP, o projeto visa 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).

Em 2004 e 2005, o PLC 89 de 2003 foi objeto de discussão perante a Comissão de Educação (CE). Após amplos debates, em 2005 foi aprovado o parecer final na forma do Substitutivo ao PLC 89 de 2003.

Durante o longo processo de debate sobre a matéria, dentro e fora do Senado Federal, o Substitutivo foi aperfeiçoado para ser apresentado à Comissão de Constituição e Justiça (CCJ), ao final de 2006, tendo sido apensados a ele o PLS n° 137 de 2000 e o PLS n° 76, de 2000, e este por ser mais abrangente e mais antigo no Senado Federal, passou a ser o projeto com prioridade na tramitação.

Foram apresentadas 4 subemendas no âmbito da CCJ, uma delas retirada logo em seguida, e foram acatadas pelo Relator.

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

Em dezembro de 2007, o parecer do Relator, Senador Eduardo Azeredo, foi aprovado pela CCT, aprovando parcialmente os três projetos, na forma do Substitutivo apresentado, incorporando as subemendas oferecidas no âmbito da CCJ.

Os três projetos seguiram então para a Comissão de Assuntos Econômicos – CAE - e em junho de 2008, o parecer do Relator, Senador Aloízio Mercadante, foi aprovado pela CAE, aproveitando o Substitutivo aprovado pela CCT, com a apresentação de 23 subemendas, de mérito e de redação, aperfeiçoando com qualidade técnica, concisão de redação, juridicidade e constitucionalidade, resultado de notável esforço de articulação parlamentar.

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.

Materialmente, não vislumbramos inconstitucionalidades ou vícios de juridicidade nos projetos de lei sob exame.

No mérito, ainda propomos pequenas alterações no Decreto-Lei 1.001 - Código Penal Militar, ajustando-as ao aperfeiçoamento do Substitutivo aprovado na CCT, com as Subemendas aprovadas pela CAE, de autoria do Senador Aloizio Mercadante, após várias consultas feitas a especialistas na matéria.

Reiteramos, conforme os pareceres anteriores, de que o assunto merece e necessita regulamentação no direito brasileiro, bem como reconhecemos a tendência internacional de tutela e fiscalização do meio cibernético. Além disso, reconhecemos a necessidade de harmonizar a nossa futura lei de crimes cibernéticos com a *Convenção sobre o Cibercrime* do Conselho da Europa. A Convenção recomenda procedimentos processuais penais, a guarda criteriosa das informações trafegadas nos sistemas informatizados e sua liberação para as autoridades. A compatibilidade das previsões legais produz efeitos em questões de extradição, de assistência judiciária mútua entre os Estados e de cooperação internacional de uma forma

geral. A harmonia com as tendências internacionais é importante para otimizar a repressão dos crimes de informática, notadamente transnacionais.

Analisando o Substitutivo, os projetos apensados e as Subemendas aprovadas pela CAE, concluímos que a matéria, complexa e abrangente, tratando de crimes contra a pessoa, contra o patrimônio e contra serviços públicos, requeria novos aperfeiçoamentos, sem se alterar, contudo, o núcleo substantivo do texto.

Na análise das Subemendas CAE, alguns crimes que, no Substitutivo, estavam localizados topologicamente no Título dos "Crimes contra a Pessoa" do Código Penal, foram deslocados para o Título dos "Crimes contra a Incolumidade Pública", por melhor traduzir o bem jurídico que se quer tutelar. O nome do novo Capítulo passou a ser "Dos Crimes Contra a Segurança dos Sistemas Informatizados". É o caso dos novos artigos 285-A, 285-B e 285-C.

Continuando, o rol de conceitos dos elementos típicos "rede de computadores", "dispositivo de comunicação", "sistema informatizado", "código malicioso", "dados informáticos" e "dados de tráfego" (arts. 154-C no CP e 339-C, no CPM) foram deslocados do Código Penal e do Código Penal Militar como artigo autônomo da Lei que se pretende aprovar, deixando clara a *"mens legis"* ou o *"espírito da lei"*, na medida em que estão definidos *"para os efeitos penais"*, entendendo tratar-se de melhor estratégia para a orientação normativa das diversas leis que o projeto altera.

Foi suprimido o art. 141-A, que prevê causa de aumento de pena para os crimes contra a honra quando praticados por meios informáticos. Julgamos tratar-se de desnecessário *bis in idem*, em face do que já dispõe o inciso III do art. 141 do CP.

Para esclarecer a distinção de valor atribuída às condutas constantes dos arts. 154-A e 154-B (novos 285-A e 285-B, conforme subemendas), as redações dos *caput* foram levemente alteradas e as estruturas dos tipos simplificadas. Parágrafos repetidos foram reunidos em dispositivo único (art. 285-C). A proporcionalidade das penas foi adaptada aos outros crimes presentes na nova localização proposta.

O art. 154-D (novo art. 154-A) foi mantido no Título original, dado o bem jurídico tutelado, e a sua redação simplificada, para a melhor identificação do desvalor atribuído à conduta.

Foi suprimida a equiparação do dado e do dispositivo informático à "coisa", para efeitos de crimes contra o patrimônio (arts. 183-A e 155, § 4º, V). Essa equiparação poderia acarretar desdobramentos sistêmicos imprevisíveis na lei penal, perdendo-se os parâmetros de tangibilidade e de intangibilidade de bens que o sistema penal resguarda. Novamente foi escolhida a estratégia de prever, em artigo autônomo da nova lei, que são considerados bens protegidos, "*para efeitos penais*", o dado, o dispositivo de comunicação, a rede de computadores e o sistema informatizado, o que limita e especifica o alcance dos efeitos de tal previsão.

O tipo penal sobre a difusão de código malicioso (art. 163-A) também foi simplificado, para a melhor identificação do desvalor da ação. O mesmo foi feito na redação do art. 298-A. Em relação ao "estelionato eletrônico" (art. 171-A), foi deslocado para o rol do § 2º do mesmo art. 171, como novo inciso e assim com redação simplificada e concisa.

E concluiu-se pela necessidade de novo tipo penal sobre a destruição de dados eletrônicos alheios, mediante a alteração do *caput* do art. 163, que tipifica o crime de dano.

Com o mesmo pensamento foram alterados o *caput* dos arts. 297 e 298, que definem os tipos de falsificação de documento público e particular, respectivamente, e que passam a abranger a falsificação de "dados eletrônicos" em ambos os tipos, substituindo os dispositivos do PLC 89 de 2003 sobre a falsificação de cartão de crédito e da falsificação de telefone celular, dando neutralidade tecnológica à norma.

Alterações equivalentes foram propostas por oficiais superiores das três forças, sob coordenação do Ministério da Defesa, para os dispositivos que alteram o Código Penal Militar, relocando o art. 281-A para o art. 251. como inciso definidor do Estelionato Eletrônico, "*em prejuízo da administração militar*" acompanhando a alteração realizada no Código Penal.

No art. 339-D, renumerado para 339-C, divulgação não autorizada de dados pessoais, foi incluída a expressão "*sob administração militar*" qualificando o sistema informatizao.

Nos demais artigos foi incluída a expressão "*desde que o fato atente contra a administração militar*", a exemplo de outros artigos do CPM.

Foi incluída a expressão "*ou dado eletrônico*" nos *caput* do art. 259, "Dano simples", art. 262, "Dano em material ou aparelhamento de guerra" e art. 311 "Falsificação de Documento", acompanhando a alteração do arts. 163, 297 e 298 do Código Penal.

A assessoria parlamentar militar apresentou um novo tipo, específico, que trata da Traição ou Favor ao Inimigo, sugerindo a alteração do art. 356 do Código Penal Militar, nele incluindo a referência ao dado eletrônico nos incisos II e III. Assim visa a dar proteção ao dado eletrônico em caso de guerra, para criminalizar a sua entrega ao inimigo ou a sua perda, destruição, inutilização, deterioração ou exposição a perigo de perda, destruição, inutilização ou deterioração em favorecimento ou tentativa de favorecimento ao inimigo. Assim, estará se protegendo o dado eletrônico em caso de guerra declarada.

Foi simplificada a proposta para o art. 20 da Lei nº 7.716, de 1989 e suprimida a alteração sugerida para a Lei nº 8.078, de 1990 (parágrafo único do art. 9º), pelo fato de a previsão já constar do *caput* do mesmo artigo.

A alteração proposta no Estatuto da Criança e do Adolescente (art. 241), recebeu nova emenda para a definição de novas condutas de "receptar" e de "armazenar consigo" imagens pornográficas que envolvam crianças e adolescentes.

Foi suprimido o art. 16 do Substitutivo da CCT, que prevê exceção à regra determinada pelo art. 2º da Lei 9296/96, que exclui a possibilidade de interceptação de comunicação para os crimes apenados com detenção, uma vez que os novos tipos são apenados com reclusão e estão cobertos pela legislação em vigor.

Pela mesma razão acima também foi suprimido o art. 17 do Substitutivo da CCT que prevê a alteração do art. 313 do Código de Processo Penal acrescentando novo inciso V, prevendo a possibilidade de prisão preventiva para os crimes "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", enquanto o inciso I do mesmo art. 313 já prevê essa possibilidade para os crimes punidos com reclusão.

Finalmente, a análise das 23 subemendas propostas a seguir permitem a conclusão de que não se toca no núcleo material do Substitutivo aprovado pela CCT.

São aperfeiçoamentos que simplificam o projeto, sem perder de vista a juridicidade, a constitucionalidade, a eficácia, o rigor e a harmonia com a tendência normativa internacional.

III – VOTO

Diante do exposto, 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 n° 76 e n° 137, ambos de 2000, na forma do Substitutivo aprovado pela CCT, com as Subemendas CAE e com as adequações propostas neste Parecer ao Código penal Militar, consolidadas no seguinte Substitutivo:

EMENDA Nº 4 – CCT/CCJ
(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 7.716, de 5 de janeiro de 1989, e a Lei nº 8.069, de 13 de julho de 1990, e a Lei nº 10.446, de 8 de maio de 2002, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra dispositivos de comunicação ou sistemas informatizados e similares, e dá outras providências."

O CONGRESSO NACIONAL decreta:

Art.1º Esta Lei altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), o Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), a Lei nº 7.716, de 5 de janeiro de 1989, e a Lei nº 8.069, de 13 de julho de 1990, e a Lei nº 10.446, de 8 de maio de

2002, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra dispositivos de comunicação ou sistemas informatizados e similares, e dá outras providências.

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

"Capítulo IV

DOS CRIMES CONTRA A SEGURANÇA DOS SISTEMAS INFORMATIZADOS

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

Art. 285-A. Acessar rede de computadores, dispositivo de comunicação ou sistema informatizado, sem autorização do legítimo titular, quando exigida:

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

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

Obtenção, transferência ou fornecimento não autorizado de dado ou informação

Art. 285-B. Obter ou transferir dado ou informação disponível em rede de computadores, dispositivo de comunicação ou sistema informatizado, sem autorização ou em desconformidade à autorização, do legítimo titular, quando exigida:

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

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

Ação Penal

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

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

"Divulgação ou utilização indevida de informações e dados pessoais

154-A. Divulgar, utilizar, comercializar ou disponibilizar dados e informações pessoais contidas em sistema informatizado com finalidade distinta da que motivou seu registro, salvo nos casos previstos em lei ou mediante expressa anuência da pessoa a que se referem, ou de seu representante legal.

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

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

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

"Dano

Art. 163. Destruir, inutilizar ou deteriorar coisa alheia ou dado eletrônico alheio:
....."(NR)

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

"Inserção ou difusão de código malicioso

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

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

Inserção ou difusão de código malicioso seguido de dano

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

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

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

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

"Art. 171 .....

§ 2º Nas mesmas penas incorre quem:

.....

Estelionato Eletrônico

VII – difunde, por qualquer meio, código malicioso com intuito de facilitar ou permitir acesso indevido à rede de computadores, dispositivo de comunicação ou sistema informatizado:

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

Art. 7º Os arts. 265 e 266 do Código Penal passam a vigorar com as seguintes redações:

"Atentado contra a segurança de serviço de utilidade pública

Art. 265. Atentar contra a segurança ou o funcionamento de serviço de água, luz, força, calor, informação ou telecomunicação, ou qualquer outro de utilidade pública:

..... "(NR)

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

"Falsificação de dado eletrônico ou documento público

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

....."(NR)

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

"Falsificação de dado eletrônico ou documento particular

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

....."(NR)

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

"Art. 251. .....

§ 1º - Nas mesmas penas incorre quem:

.....

Estelionato Eletrônico

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

.....

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

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

"Dano Simples

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

.....

.....

"Dano em material ou aparelhamento de guerra ou dado eletrônico

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

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

"Inserção ou difusão de código malicioso

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

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

Inserção ou difusão código malicioso seguido de dano

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

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

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

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

"Capítulo VII-A

DOS CRIMES CONTRA A SEGURANÇA DOS SISTEMAS INFORMATIZADOS

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

Art. 339-A. Acessar rede de computadores, dispositivo de comunicação ou sistema informatizado, sem autorização do legítimo titular, quando exigida e desde que o fato atente contra a administração militar:

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

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

Obtenção, transferência ou fornecimento não autorizado de dado ou informação

Art. 339-B. Obter ou transferir dado ou informação disponível em rede de computadores, dispositivo de comunicação ou sistema informatizado, sem autorização ou em desconformidade à autorização, do legítimo titular, quando exigida, desde que o fato atente contra a administração militar:

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

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

"Divulgação ou utilização indevida de informações e dados pessoais

Art. 339-C Divulgar, utilizar, comercializar ou disponibilizar dados e informações pessoais contidas em sistema informatizado sob administração militar com finalidade distinta da que motivou seu registro, salvo nos casos previstos em lei ou mediante expressa anuência da pessoa a que se referem, ou de seu representante legal.

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

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

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

"Falsificação de documento

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

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

"CAPÍTULO I

DA TRAIÇÃO

Favor ao inimigo

Art. 356. .....:

.....

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

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

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

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

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

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

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

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

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

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

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

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

"Art. 20 .....

.....

§ 3º.....

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

..... "(NR)

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

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

..... "(NR)

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

"Art. 1º .....

.....

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

....."(NR)

Art. 22. 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 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, e fornecê-los exclusivamente à autoridade investigatória mediante prévia requisição judicial;

II – preservar imediatamente, após requisição judicial, no curso de investigação, os dados de que cuida o inciso I deste artigo e outras informações requisitadas

por aquela investigação, respondendo civil e penalmente pela sua absoluta confidencialidade e inviolabilidade;

III – informar, de maneira sigilosa, à autoridade 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.

§ 1° 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.

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

§ 3° 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. 23. Esta Lei entrará em vigor cento e vinte dias após a data de sua publicação.

Sala da Comissão, 18 de junho de 2008. 2008.

, Presidente

, Relator

COMISSÃO DE CONSTITUIÇÃO, JUSTIÇA E CIDADANIA

PROPOSIÇÃO: PLC Nº 89 DE 2003
(Tramita em conjunto com os PLS's nºs 76 e 137, de 2000).
ASSINAM O PARECER NA REUNIÃO DE 18/06/2008, OS SENHORES(AS) SENADORES(AS):

PRESIDENTE:	
RELATOR:	Sen. Eduardo Azeredo
BLOCO DE APOIO AO GOVERNO (PT, PR, PSB, PCdoB, PRB e PP)[2]	
SERYS SLHESSARENKO	1.JOÃO RIBEIRO
MARINA SILVA	2.INÁCIO ARRUDA
EDUARDO SUPLICY	3.CÉSAR BORGES
ALOIZIO MERCADANTE	4.MARCELO CRIVELLA
IDELI SALVATTI	5.MAGNO MALTA
ANTONIO CARLOS VALADARES	6.JOSÉ NERY (PSOL)[3]
PMDB	
JARBAS VASCONCELOS	1.ROSEANA SARNEY
PEDRO SIMON	2.WELLINGTON SALGADO DE OLIVEIRA
ROMERO JUCÁ	3.LEOMAR QUINTANILHA
ALMEIDA LIMA	4.VALDIR RAUPP
VALTER PEREIRA	5.JOSÉ MARANHÃO
GEOVANI BORGES[6]	6.NEUTO DE CONTO
BLOCO DA MINORIA (DEM e PSDB)	
ADELMIR SANTANA	1.ELISEU RESENDE
MARCO MACIEL[1] (PRESIDENTE)	2.JAYME CAMPOS
DEMÓSTENES TORRES	3.JOSÉ AGRIPINO
KÁTIA ABREU	4.ALVARO DIAS[4]
ANTONIO CARLOS JÚNIOR	5.VIRGINIO DE CARVALHO
ARTHUR VIRGÍLIO	6.FLEXA RIBEIRO
EDUARDO AZEREDO (RELATOR)	7.JOÃO TENÓRIO
LÚCIA VÂNIA	8.MARCONI PERILLO
TASSO JEREISSATI	9.MÁRIO COUTO
PTB[5]	
EPITÁCIO CAFETEIRA	1.MOZARILDO CAVALCANTI
PDT	
OSMAR DIAS	1.CRISTOVAM BUARQUE

Atualizada em: 04/06/2008

[1] Eleito Presidente da Comissão em 08/08/2007;
[2] O PTB deixou de integrar o Bloco de Apoio ao Governo, a partir de 22/11/2007 (DSF de 28/11/07);
[3] Vaga cedida pelo Bloco de Apoio ao Governo;
[4] Vaga cedida pelo Democratas;
[5] Nos termos da decisão do Presidente do Senado, publicada no DSF de 14.02.2008;
[6] Em 17/04/2008, o Senador Geovani Borges é designado titular em vaga antes ocupada pelo Senador Gilvam Borges, que se encontra licenciado, nos termos do art. 43, I, do Regimento Interno, no período de 17.04.2008 a 24.08.2008 (Of. 112/08-GLPMDB).

LEGISLAÇÃO CITADA ANEXADA PELA SECRETARIA-GERAL DA MESA

CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL DE 1988

.....

Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

.....

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

.....

XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal; (Vide Lei nº 9.296, de 1996)

.....

Art. 22. Compete privativamente à União legislar sobre:

I - direito civil, comercial, penal, processual, eleitoral, agrário, marítimo, aeronáutico, espacial e do trabalho;

.....

EMENDA CONSTITUCIONAL Nº 32, DE 11 DE SETEMBRO DE 2001

Altera dispositivos dos arts. 48, 57, 61, 62, 64, 66, 84, 88 e 246 da Constituição Federal, e dá outras providências.

.....

DECRETO-LEI Nº 2.848, DE 7 DE DEZEMBRO DE 1940.

Código Penal.

.....

SEÇÃO II
DAS PENAS RESTRITIVAS DE DIREITOS

.....

Art. 46. A prestação de serviços à comunidade ou a entidades públicas é aplicável às condenações superiores a seis meses de privação da liberdade. (Redação dada pela Lei nº 9.714, de 1998)

§ 1º A prestação de serviços à comunidade ou a entidades públicas consiste na atribuição de tarefas gratuitas ao condenado. (Incluído pela Lei nº 9.714, de 1998)

§ 2º A prestação de serviço à comunidade dar-se-á em entidades assistenciais, hospitais, escolas, orfanatos e outros estabelecimentos congêneres, em programas comunitários ou estatais. (Incluído pela Lei nº 9.714, de 1998)

§ 3º As tarefas a que se refere o § 1º serão atribuídas conforme as aptidões do condenado, devendo ser cumpridas à razão de uma hora de tarefa por dia de condenação, fixadas de modo a não prejudicar a jornada normal de trabalho. (Incluído pela Lei nº 9.714, de 1998)

§ 4º Se a pena substituída for superior a um ano, é facultado ao condenado cumprir a pena substitutiva em menor tempo (art. 55), nunca inferior à metade da pena privativa de liberdade fixada. (Incluído pela Lei nº 9.714, de 1998)

Interdição temporária de direitos (Redação dada pela Lei nº 7.209, de 11.7.1984)

.....

PARTE ESPECIAL

TÍTULO I
DOS CRIMES CONTRA A PESSOA
CAPÍTULO I
DOS CRIMES CONTRA A VIDA

Homicídio simples

Art 121. Matar alguem:

Pena - reclusão, de seis a vinte anos.

Caso de diminuição de pena

§ 1º Se o agente comete o crime impelido por motivo de relevante valor social ou moral, ou sob o domínio de violenta emoção, logo em seguida a injusta provocação da vítima, ou juiz pode reduzir a pena de um sexto a um terço.

Homicídio qualificado

§ 2º Se o homicídio é cometido:

I - mediante paga ou promessa de recompensa, ou por outro motivo torpe;

II - por motivo futil;

III - com emprego de veneno, fogo, explosivo, asfixia, tortura ou outro meio insidioso ou cruel, ou de que possa resultar perigo comum;

IV - à traição, de emboscada, ou mediante dissimulação ou outro recurso que dificulte ou torne impossivel a defesa do ofendido;

V - para assegurar a execução, a ocultação, a impunidade ou vantagem de outro crime:

Pena - reclusão, de doze a trinta anos.

Homicídio culposo

§ 3º Se o homicídio é culposo: (Vide Lei nº 4.611, de 1965)

Pena - detenção, de um a três anos.

Aumento de pena

§ 4º No homicídio culposo, a pena é aumentada de 1/3 (um terço), se o crime resulta de inobservância de regra técnica de profissão, arte ou ofício, ou se o agente deixa de prestar imediato socorro à vítima, não procura diminuir as conseqüências do seu ato, ou foge para evitar prisão em flagrante. Sendo doloso o homicídio, a pena é aumentada de 1/3 (um terço) se o crime é praticado contra pessoa menor de 14 (quatorze) ou maior de 60 (sessenta) anos. (Redação dada pela Lei nº 10.741, de 2003)

§ 5º - Na hipótese de homicídio culposo, o juiz poderá deixar de aplicar a pena, se as conseqüências da infração atingirem o próprio agente de forma tão grave que a sanção penal se torne desnecessária. (Incluído pela Lei nº 6.416, de 24.5.1977)

Induzimento, instigação ou auxílio a suicídio

.....

CAPÍTULO II
DAS LESÕES CORPORAIS

Lesão corporal

Art. 129. Ofender a integridade corporal ou a saúde de outrem:

Pena - detenção, de três meses a um ano.

Lesão corporal de natureza grave

§ 1º Se resulta:

I - Incapacidade para as ocupações habituais, por mais de trinta dias;

II - perigo de vida;

III - debilidade permanente de membro, sentido ou função;

IV - aceleração de parto:

Pena - reclusão, de um a cinco anos.

§ 2º Se resulta:

I - Incapacidade permanente para o trabalho;

II - enfermidade incuravel;

III perda ou inutilização do membro, sentido ou função;

IV - deformidade permanente;

V - aborto:

Pena - reclusão, de dois a oito anos.

Lesão corporal seguida de morte

§ 3º Se resulta morte e as circunstâncias evidenciam que o agente não quís o resultado, nem assumiu o risco de produzí-lo:

Pena - reclusão, de quatro a doze anos.

Diminuição de pena

§ 4º Se o agente comete o crime impelido por motivo de relevante valor social ou moral ou sob o domínio de violenta emoção, logo em seguida a injusta provocação da vítima, o juiz pode reduzir a pena de um sexto a um terço.

Substituição da pena

§ 5º O juiz, não sendo graves as lesões, pode ainda substituir a pena de detenção pela de multa, de duzentos mil réis a dois contos de réis:

I - se ocorre qualquer das hipóteses do parágrafo anterior;

II - se as lesões são recíprocas.

Lesão corporal culposa

§ 6° Se a lesão é culposa: (Vide Lei nº 4.611, de 1965)

Pena - detenção, de dois meses a um ano.

Aumento de pena

§ 7° - Aumenta-se a pena de um terço, se ocorrer qualquer das hipóteses do art. 121, § 4°. (Redação dada pela Lei nº 8.069, de 1990)

§ 8° - Aplica-se à lesão culposa o disposto no § 5° do art. 121.(Redação dada pela Lei nº 8.069, de 1990)

Violência Doméstica (Incluído pela Lei nº 10.886, de 2004)

§ 9º Se a lesão for praticada contra ascendente, descendente, irmão, cônjuge ou companheiro, ou com quem conviva ou tenha convivido, ou, ainda, prevalecendo-se o agente das relações domésticas, de coabitação ou de hospitalidade: (Redação dada pela Lei nº 11.340, de 2006)

Pena - detenção, de 3 (três) meses a 3 (três) anos. (Redação dada pela Lei nº 11.340, de 2006)

§ 10. Nos casos previstos nos §§ 1º a 3º deste artigo, se as circunstâncias são as indicadas no § 9º deste artigo, aumenta-se a pena em 1/3 (um terço). (Incluído pela Lei nº 10.886, de 2004)

§ 11. Na hipótese do § 9º deste artigo, a pena será aumentada de um terço se o crime for cometido contra pessoa portadora de deficiência. (Incluído pela Lei nº 11.340, de 2006)

.....

CAPÍTULO V
DOS CRIMES CONTRA A HONRA

Calúnia

Art. 138 - Caluniar alguém, imputando-lhe falsamente fato definido como crime:

Pena - detenção, de seis meses a dois anos, e multa.

§ 1° - Na mesma pena incorre quem, sabendo falsa a imputação, a propala ou divulga.

§ 2° - É punível a calúnia contra os mortos.

Exceção da verdade

§ 3° - Admite-se a prova da verdade, salvo:

I - se, constituindo o fato imputado crime de ação privada, o ofendido não foi condenado por sentença irrecorrível;

II - se o fato é imputado a qualquer das pessoas indicadas no nº I do art. 141;

III - se do crime imputado, embora de ação pública, o ofendido foi absolvido por sentença irrecorrível.

Difamação

Art. 139 - Difamar alguém, imputando-lhe fato ofensivo à sua reputação:

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

Exceção da verdade

Parágrafo único - A exceção da verdade somente se admite se o ofendido é funcionário público e a ofensa é relativa ao exercício de suas funções.

Injúria

Art. 140 - Injuriar alguém, ofendendo-lhe a dignidade ou o decoro:

Pena - detenção, de um a seis meses, ou multa.

§ 1º - O juiz pode deixar de aplicar a pena:

I - quando o ofendido, de forma reprovável, provocou diretamente a injúria;

II - no caso de retorsão imediata, que consista em outra injúria.

§ 2º - Se a injúria consiste em violência ou vias de fato, que, por sua natureza ou pelo meio empregado, se considerem aviltantes:

Pena - detenção, de três meses a um ano, e multa, além da pena correspondente à violência.

§ 3º Se a injúria consiste na utilização de elementos referentes a raça, cor, etnia, religião, origem ou a condição de pessoa idosa ou portadora de deficiência: (Redação dada pela Lei nº 10.741, de 2003)

Pena - reclusão de um a três anos e multa. (Incluído pela Lei nº 9.459, de 1997)

Disposições comuns

Art. 141 - As penas cominadas neste Capítulo aumentam-se de um terço, se qualquer dos crimes é cometido:

I - contra o Presidente da República, ou contra chefe de governo estrangeiro;

II - contra funcionário público, em razão de suas funções;

III - na presença de várias pessoas, ou por meio que facilite a divulgação da calúnia, da difamação ou da injúria.

IV – contra pessoa maior de 60 (sessenta) anos ou portadora de deficiência, exceto no caso de injúria. (Incluído pela Lei nº 10.741, de 2003)

Parágrafo único - Se o crime é cometido mediante paga ou promessa de recompensa, aplica-se a pena em dobro.

.....

SEÇÃO IV
DOS CRIMES CONTRA A INVIOLABILIDADE DOS SEGREDOS

.....

Violação do segredo profissional

Art. 154 - Revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem:

Pena - detenção, de três meses a um ano, ou multa.

Parágrafo único - Somente se procede mediante representação.

TÍTULO II
DOS CRIMES CONTRA O PATRIMÔNIO
CAPÍTULO I
DO FURTO

Furto

Art. 155 - Subtrair, para si ou para outrem, coisa alheia móvel:

Pena - reclusão, de um a quatro anos, e multa.

§ 1º - A pena aumenta-se de um terço, se o crime é praticado durante o repouso noturno.

§ 2º - Se o criminoso é primário, e é de pequeno valor a coisa furtada, o juiz pode substituir a pena de reclusão pela de detenção, diminuí-la de um a dois terços, ou aplicar somente a pena de multa.

§ 3º - Equipara-se à coisa móvel a energia elétrica ou qualquer outra que tenha valor econômico.

Furto qualificado

§ 4º - A pena é de reclusão de dois a oito anos, e multa, se o crime é cometido:

I - com destruição ou rompimento de obstáculo à subtração da coisa;

II - com abuso de confiança, ou mediante fraude, escalada ou destreza;

III - com emprego de chave falsa;

IV - mediante concurso de duas ou mais pessoas.

§ 5º - A pena é de reclusão de três a oito anos, se a subtração for de veículo automotor que venha a ser transportado para outro Estado ou para o exterior. (Incluído pela Lei nº 9.426, de 1996)

.....

CAPÍTULO IV
DO DANO

Dano

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

Pena - detenção, de um a seis meses, ou multa.

Dano qualificado

Parágrafo único - Se o crime é cometido:

I - com violência à pessoa ou grave ameaça;

II - com emprego de substância inflamável ou explosiva, se o fato não constitui crime mais grave

III - contra o patrimônio da União, Estado, Município, empresa concessionária de serviços públicos ou sociedade de economia mista; (Redação dada pela Lei nº 5.346, de 3.11.1967)

IV - por motivo egoístico ou com prejuízo considerável para a vítima:

Pena - detenção, de seis meses a três anos, e multa, além da pena correspondente à violência.

.....

CAPÍTULO V
DA APROPRIAÇÃO INDÉBITA

Apropriação indébita

Art. 168 - Apropriar-se de coisa alheia móvel, de que tem a posse ou a detenção:

Pena - reclusão, de um a quatro anos, e multa.

Aumento de pena

§ 1º - A pena é aumentada de um terço, quando o agente recebeu a coisa:

I - em depósito necessário;

II - na qualidade de tutor, curador, síndico, liquidatário, inventariante, testamenteiro ou depositário judicial:

III - em razão de ofício, emprego ou profissão.

Apropriação indébita previdenciária (Incluído pela Lei nº 9.983, de 2000)

Art. 168-A. Deixar de repassar à previdência social as contribuições recolhidas dos contribuintes, no prazo e forma legal ou convencional: (Incluído pela Lei nº 9.983, de 2000)

Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa. (Incluído pela Lei nº 9.983, de 2000)

§ 1º Nas mesmas penas incorre quem deixar de: (Incluído pela Lei nº 9.983, de 2000)

I – recolher, no prazo legal, contribuição ou outra importância destinada à previdência social que tenha sido descontada de pagamento efetuado a segurados, a terceiros ou arrecadada do público; (Incluído pela Lei nº 9.983, de 2000)

II – recolher contribuições devidas à previdência social que tenham integrado despesas contábeis ou custos relativos à venda de produtos ou à prestação de serviços; (Incluído pela Lei nº 9.983, de 2000)

III - pagar benefício devido a segurado, quando as respectivas cotas ou valores já tiverem sido reembolsados à empresa pela previdência social. (Incluído pela Lei nº 9.983, de 2000)

§ 2º É extinta a punibilidade se o agente, espontaneamente, declara, confessa e efetua o pagamento das contribuições, importâncias ou valores e presta as informações devidas à previdência social, na forma definida em lei ou regulamento, antes do início da ação fiscal. (Incluído pela Lei nº 9.983, de 2000)

§ 3º É facultado ao juiz deixar de aplicar a pena ou aplicar somente a de multa se o agente for primário e de bons antecedentes, desde que: (Incluído pela Lei nº 9.983, de 2000)

I – tenha promovido, após o início da ação fiscal e antes de oferecida a denúncia, o pagamento da contribuição social previdenciária, inclusive acessórios; ou (Incluído pela Lei nº 9.983, de 2000)

II – o valor das contribuições devidas, inclusive acessórios, seja igual ou inferior àquele estabelecido pela previdência social, administrativamente, como sendo o mínimo para o ajuizamento de suas execuções fiscais. (Incluído pela Lei nº 9.983, de 2000)

.....

CAPÍTULO VI
DO ESTELIONATO E OUTRAS FRAUDES

Estelionato

Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento:

Pena - reclusão, de um a cinco anos, e multa.

§ 1º - Se o criminoso é primário, e é de pequeno valor o prejuízo, o juiz pode aplicar a pena conforme o disposto no art. 155, § 2º.

§ 2º - Nas mesmas penas incorre quem:

Disposição de coisa alheia como própria

I - vende, permuta, dá em pagamento, em locação ou em garantia coisa alheia como própria;

Alienação ou oneração fraudulenta de coisa própria

II - vende, permuta, dá em pagamento ou em garantia coisa própria inalienável, gravada de ônus ou litigiosa, ou imóvel que prometeu vender a terceiro, mediante pagamento em prestações, silenciando sobre qualquer dessas circunstâncias;

Defraudação de penhor

III - defrauda, mediante alienação não consentida pelo credor ou por outro modo, a garantia pignoratícia, quando tem a posse do objeto empenhado;

Fraude na entrega de coisa

IV - defrauda substância, qualidade ou quantidade de coisa que deve entregar a alguém;

Fraude para recebimento de indenização ou valor de seguro

V - destrói, total ou parcialmente, ou oculta coisa própria, ou lesa o próprio corpo ou a saúde, ou agrava as conseqüências da lesão ou doença, com o intuito de haver indenização ou valor de seguro;

Fraude no pagamento por meio de cheque

VI - emite cheque, sem suficiente provisão de fundos em poder do sacado, ou lhe frustra o pagamento.

§ 3º - A pena aumenta-se de um terço, se o crime é cometido em detrimento de entidade de direito público ou de instituto de economia popular, assistência social ou beneficência.

.....

CAPÍTULO VIII
DISPOSIÇOES GERAIS

.....

Art. 183 - Não se aplica o disposto nos dois artigos anteriores:

I - se o crime é de roubo ou de extorsão, ou, em geral, quando haja emprego de grave ameaça ou violência à pessoa;

II - ao estranho que participa do crime.

III – se o crime é praticado contra pessoa com idade igual ou superior a 60 (sessenta) anos. (Incluído pela Lei nº 10.741, de 2003)

TÍTULO III
DOS CRIMES CONTRA A PROPRIEDADE IMATERIAL
CAPÍTULO I
DOS CRIMES CONTRA A PROPRIEDADE INTELECTUAL

Violação de direito autoral

Art. 184. Violar direitos de autor e os que lhe são conexos: (Redação dada pela Lei nº 10.695, de 1º.7.2003)

Pena – detenção, de 3 (três) meses a 1 (um) ano, ou multa. (Redação dada pela Lei nº 10.695, de 1º.7.2003)

§ 1º Se a violação consistir em reprodução total ou parcial, com intuito de lucro direto ou indireto, por qualquer meio ou processo, de obra intelectual, interpretação, execução ou fonograma, sem autorização expressa do autor, do artista intérprete ou executante, do produtor, conforme o caso, ou de quem os represente: (Redação dada pela Lei nº 10.695, de 1º.7.2003)

Pena – reclusão, de 2 (dois) a 4 (quatro) anos, e multa. (Redação dada pela Lei nº 10.695, de 1º.7.2003)

§ 2º Na mesma pena do § 1º incorre quem, com o intuito de lucro direto ou indireto, distribui, vende, expõe à venda, aluga, introduz no País, adquire, oculta, tem em depósito, original ou cópia de obra intelectual ou fonograma reproduzido com violação do direito de autor, do direito de artista intérprete ou executante ou do direito do produtor de fonograma, ou, ainda, aluga original ou cópia de obra intelectual ou fonograma, sem a expressa autorização dos titulares dos direitos ou de quem os represente (Redação dada pela Lei nº 10.695, de 1º.7.2003)

§ 3º Se a violação consistir no oferecimento ao público, mediante cabo, fibra ótica, satélite, ondas ou qualquer outro sistema que permita ao usuário realizar a seleção da obra ou produção para recebê-la em um tempo e lugar previamente determinados por quem formula a demanda, com intuito de lucro, direto ou indireto, sem autorização expressa, conforme o caso, do autor, do artista intérprete ou executante, do produtor de fonograma, ou de quem os represente: (Redação dada pela Lei nº 10.695, de 1º.7.2003)

Pena – reclusão, de 2 (dois) a 4 (quatro) anos, e multa. (Incluído pela Lei nº 10.695, de 1º.7.2003)

§ 4º O disposto nos §§ 1º, 2º e 3º não se aplica quando se tratar de exceção ou limitação ao direito de autor ou os que lhe são conexos, em conformidade com o previsto na Lei nº 9.610, de 19 de fevereiro de 1998, nem a cópia de obra intelectual ou fonograma, em um só exemplar, para uso privado do copista, sem intuito de lucro direto ou indireto. (Incluído pela Lei nº 10.695, de 1º.7.2003)

.....

CAPÍTULO VI
DO ULTRAJE PÚBLICO AO PUDOR

.....

Art. 234 - Fazer, importar, exportar, adquirir ou ter sob sua guarda, para fim de comércio, de distribuição ou de exposição pública, escrito, desenho, pintura, estampa ou qualquer objeto obsceno:

Pena - detenção, de seis meses a dois anos, ou multa.

Parágrafo único - Incorre na mesma pena quem:

I - vende, distribui ou expõe à venda ou ao público qualquer dos objetos referidos neste artigo;

II - realiza, em lugar público ou acessível ao público, representação teatral, ou exibição cinematográfica de caráter obsceno, ou qualquer outro espetáculo, que tenha o mesmo caráter;

III - realiza, em lugar público ou acessível ao público, ou pelo rádio, audição ou recitação de caráter obsceno.

.....

CAPÍTULO II
DOS CRIMES CONTRA A
SEGURANÇA DOS MEIOS DE COMUNICAÇÃO
E TRANSPORTE E OUTROS SERVIÇOS PÚBLICOS

.....

Art. 265 - Atentar contra a segurança ou o funcionamento de serviço de água, luz, força ou calor, ou qualquer outro de utilidade pública:

Pena - reclusão, de um a cinco anos, e multa.

Parágrafo único - Aumentar-se-á a pena de 1/3 (um terço) até a metade, se o dano ocorrer em virtude de subtração de material essencial ao funcionamento dos serviços. (Incluído pela Lei nº 5.346, de 3.11.1967)

Interrupção ou perturbação de serviço telegráfico ou telefônico

Art. 266 - Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento:

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

Parágrafo único - Aplicam-se as penas em dobro, se o crime é cometido por ocasião de calamidade pública.

CAPÍTULO III
DOS CRIMES CONTRA A SAÚDE PÚBLICA

.....

Forma qualificada

Art. 285 - Aplica-se o disposto no art. 258 aos crimes previstos neste Capítulo, salvo quanto ao definido no art. 267.

.....

CAPÍTULO II
DA FALSIDADE DE TÍTULOS E OUTROS PAPÉIS PÚBLICOS

.....

Falsificação de documento público

Art. 297 - Falsificar, no todo ou em parte, documento público, ou alterar documento público verdadeiro:

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

§ 1º - Se o agente é funcionário público, e comete o crime prevalecendo-se do cargo, aumenta-se a pena de sexta parte.

§ 2º - Para os efeitos penais, equiparam-se a documento público o emanado de entidade paraestatal, o título ao portador ou transmissível por endosso, as ações de sociedade comercial, os livros mercantis e o testamento particular.

§ 3º Nas mesmas penas incorre quem insere ou faz inserir: (Incluído pela Lei nº 9.983, de 2000)

I – na folha de pagamento ou em documento de informações que seja destinado a fazer prova perante a previdência social, pessoa que não possua a qualidade de segurado obrigatório;(Incluído pela Lei nº 9.983, de 2000)

II – na Carteira de Trabalho e Previdência Social do empregado ou em documento que deva produzir efeito perante a previdência social, declaração falsa ou diversa da que deveria ter sido escrita; (Incluído pela Lei nº 9.983, de 2000)

III – em documento contábil ou em qualquer outro documento relacionado com as obrigações da empresa perante a previdência social, declaração falsa ou diversa da que deveria ter constado. (Incluído pela Lei nº 9.983, de 2000)

§ 4º Nas mesmas penas incorre quem omite, nos documentos mencionados no § 3º, nome do segurado e seus dados pessoais, a remuneração, a vigência do contrato de trabalho ou de prestação de serviços.(Incluído pela Lei nº 9.983, de 2000)

Falsificação de documento particular

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

Pena - reclusão, de um a cinco anos, e multa.

.....

DECRETO-LEI Nº 3.689, DE 3 DE OUTUBRO DE 1941.

Código de Processo Penal.

.....

Art. 313. Em qualquer das circunstâncias, previstas no artigo anterior, será admitida a decretação da prisão preventiva nos crimes dolosos: (Redação dada pela Lei nº 6.416, de 24.5.1977)

I - punidos com reclusão; (Redação dada pela Lei nº 6.416, de 24.5.1977)

II - punidos com detenção, quando se apurar que o indiciado é vadio ou, havendo dúvida sobre a sua identidade, não fornecer ou não indicar elementos para esclarecê-la; (Redação dada pela Lei nº 6.416, de 24.5.1977)

III - se o réu tiver sido condenado por outro crime doloso, em sentença transitada em julgado, ressalvado o disposto no parágrafo único do art. 46 do Código Penal. (Redação dada pela Lei nº 6.416, de 24.5.1977)

IV - se o crime envolver violência doméstica e familiar contra a mulher, nos termos da lei específica, para garantir a execução das medidas protetivas de urgência. (Incluído pela Lei nº 11.340, de 2006)

.....

DECRETO-LEI Nº 1.001, DE 21 DE OUTUBRO DE 1969.

Código Penal Militar

.....

TÍTULO V
DOS CRIMES CONTRA O PATRIMÔNIO
CAPÍTULO I
DO FURTO

Furto simples

Art. 240. Subtrair, para si ou para outrem, coisa alheia móvel:

Pena - reclusão, até seis anos.

Furto atenuado

§ 1º Se o agente é primário e é de pequeno valor a coisa furtada, o juiz pode substituir a pena de reclusão pela de detenção, diminuí-la de um a dois terços, ou considerar a infração como disciplinar. Entende-se pequeno o valor que não exceda a um décimo da quantia mensal do mais alto salário mínimo do país.

§ 2º A atenuação do parágrafo anterior é igualmente aplicável no caso em que o criminoso, sendo primário, restitui a coisa ao seu dono ou repara o dano causado, antes de instaurada a ação penal.

Energia de valor econômico

§ 3º Equipara-se à coisa móvel a energia elétrica ou qualquer outra que tenha valor econômico.

Furto qualificado

4º Se o furto é praticado durante a noite:

Pena reclusão, de dois a oito anos.

§ 5º Se a coisa furtada pertence à Fazenda Nacional:

Pena - reclusão, de dois a seis anos.

6º Se o furto é praticado:

I - com destruição ou rompimento de obstáculo à subtração da coisa;

II - com abuso de confiança ou mediante fraude, escalada ou destreza;

III - com emprêgo de chave falsa;

IV - mediante concurso de duas ou mais pessoas:

Pena - reclusão, de três a dez anos.

7º Aos casos previstos nos §§ 4º e 5º são aplicáveis as atenuações a que se referem os §§ 1º e 2º. Aos previstos no § 6º é aplicável a atenuação referida no § 2º.

.....

CAPÍTULO IV
DO ESTELIONATO E OUTRAS FRAUDES

Estelionato

Art. 251. Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em êrro, mediante artifício, ardil ou qualquer outro meio fraudulento:

Pena - reclusão, de dois a sete anos.

§ 1º Nas mesmas penas incorre quem:

Disposição de coisa alheia como própria

I - vende, permuta, dá em pagamento, em locação ou em garantia, coisa alheia como própria;

Alienação ou oneração fraudulenta de coisa própria

II - vende, permuta, dá em pagamento ou em garantia coisa própria inalienável, gravada de ônus ou litigiosa, ou imóvel que prometeu vender a terceiro, mediante pagamento em prestações, silenciando sôbre qualquer dessas circunstâncias:

Defraudação de penhor

III - defrauda, mediante alienação não consentida pelo credor ou por outro modo, a garantia pignoratícia, quando tem a posse do objeto empenhado;

Fraude na entrega de coisa

IV - defrauda substância, qualidade ou quantidade de coisa que entrega a adquirente;

Fraude no pagamento de cheque

V - defrauda de qualquer modo o pagamento de cheque que emitiu a favor de alguém.

2º Os crimes previstos nos ns. I a V do parágrafo anterior são considerados militares sòmente nos casos do art. 9º, nº II, letras *a* e *e* .

Agravação de pena

3º A pena é agravada, se o crime é cometido em detrimento da administração militar.

.....

CAPÍTULO VII
DO DANO

Dano simples

Art. 259. Destruir, inutilizar, deteriorar ou fazer desaparecer coisa alheia:

Pena - detenção, até seis meses.

Parágrafo único. Se se trata de bem público:

Pena - detenção, de seis meses a três anos.

Dano atenuado

.....

Dano em material ou aparelhamento de guerra

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

Pena - reclusão, até seis anos.

.....

CAPÍTULO VIII
DA USURA

Usura pecuniária

Art. 267. Obter ou estipular, para si ou para outrem, no contrato de mútuo de dinheiro, abusando da premente necessidade, inexperiência ou leviandade do mutuário, juro que excede a taxa fixada em lei, regulamento ou ato oficial:

Pena - detenção, de seis meses a dois anos.

Casos assimilados

§ 1º Na mesma pena incorre quem, em repartição ou local sob administração militar, recebe vencimento ou provento de outrem, ou permite que êstes sejam recebidos, auferindo ou permitindo que outrem aufira provcito cujo valor excede a taxa de três por cento

.....

TÍTULO VI
DOS CRIMES CONTRA A INCOLUMIDADE PÚBLICA
CAPÍTULO I
DOS CRIMES DE PERIGO COMUM

.....

Art. 281. Causar, na direção de veículo motorizado, sob administração militar, ainda que sem culpa, acidente de trânsito, de que resulte dano pessoal, e, em seguida, afastar-se do local, sem prestar socorro à vítima que dêle necessite:

Pena - detenção, de seis meses a um ano, sem prejuízo das cominadas nos arts. 206 e 210.

Isenção de prisão em flagrante

Parágrafo único. Se o agente se abstém de fugir e, na medida que as circunstâncias o permitam, presta ou providencia para que seja prestado socorro à vítima, fica isento de prisão em flagrante.

.....

CAPÍTULO V
DA FALSIDADE

Falsificação de documento

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

Pena - sendo documento público, reclusão, de dois a seis anos; sendo documento particular, reclusão, até cinco anos.

Agravação da pena

§ 1º A pena é agravada se o agente é oficial ou exerce função em repartição militar.

Documento por equiparação

§ 2º Equipara-se a documento, para os efeitos penais, o disco fonográfico ou a fita ou fio de aparelho eletromagnético a que se incorpore declaração destinada à prova de fato jurìdicamente relevante.

.....

CAPÍTULO VII
DOS CRIMES PRATICADOS POR PARTICULAR CONTRA A ADMINISTRAÇÃO MILITAR

.....

Art. 339. Impedir, perturbar ou fraudar em prejuízo da Fazenda Nacional, concorrência, hasta pública ou tomada de preços ou outro qualquer processo administrativo para aquisição ou venda de coisas ou mercadorias de uso das fôrças armadas, seja elevando arbitràriamente os preços, auferindo lucro excedente a um quinto do valor da transação, seja alterando substância, qualidade ou quantidade da coisa ou mercadoria fornecida, seja impedindo a livre concorrência de outros fornecedores, ou por qualquer modo tornando mais onerosa a transação:

Pena - detenção, de um a três anos.

§ 1º Na mesma pena incorre o intermediário na transação.

§ 2º É aumentada a pena de um terço, se o crime ocorre em período de grave crise econômica.

.....

LIVRO II
DOS CRIMES MILITARES EM TEMPO
DE GUERRA
TÍTULO I
DO FAVORECIMENTO AO INIMIGO
CAPÍTULO I
DA TRAIÇÃO

.....

Favor ao inimigo

Art. 356. Favorecer ou tentar o nacional favorecer o inimigo, prejudicar ou tentar prejudicar o bom êxito das operações militares, comprometer ou tentar comprometer a eficiência militar:

I - empreendendo ou deixando de empreender ação militar;

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

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

IV - sacrificando ou expondo a perigo de sacrifício fôrça militar;

V - abandonando posição ou deixando de cumprir missão ou ordem:

Pena - morte, grau máximo; reclusão, de vinte anos, grau mínimo.

.....

LEI COMPLEMENTAR Nº 95, DE 26 DE FEVEREIRO DE 1998

Mensagem de veto

Vide Decreto nº 2.954, de 29.01.1999

Dispõe sobre a elaboração, a redação, a alteração e a consolidação das leis, conforme determina o parágrafo único do art. 59 da Constituição Federal, e estabelece normas para a consolidação dos atos normativos que menciona.

.....

Art. 7º O primeiro artigo do texto indicará o objeto da lei e o respectivo âmbito de aplicação, observados os seguintes princípios:

I - excetuadas as codificações, cada lei tratará de um único objeto;

II - *a lei não conterá matéria estranha a seu objeto ou a este não vinculada por afinidade*, pertinência ou conexão;

III - o âmbito de aplicação da lei será estabelecido de forma tão específica quanto o possibilite o conhecimento técnico ou científico da área respectiva;

IV - o mesmo assunto não poderá ser disciplinado por mais de uma lei, exceto quando a subseqüente se destine a complementar lei considerada básica, vinculando-se a esta por remissão expressa.

.....

LEI Nº 5.250, DE 9 DE FEVEREIRO DE 1967.

Regula a liberdade de manifestação do pensamento e de informação.

.....

LEI Nº 7.170, DE 14 DE DEZEMBRO DE 1983.

Define os crimes contra a segurança nacional, a ordem política e social, estabelece seu processo e julgamento e dá outras providências.

.....

Art. 13 - Comunicar, entregar ou permitir a comunicação ou a entrega, a governo ou grupo

estrangeiro, ou a organização ou grupo de existência ilegal, de dados, documentos ou cópias de documentos, planos, códigos, cifras ou assuntos que, no interesse do Estado brasileiro, são classificados como sigilosos.

Pena: reclusão, de 3 a 15 anos.

Parágrafo único - Incorre na mesma pena quem:

I - com o objetivo de realizar os atos previstos neste artigo, mantém serviço de espionagem ou dele participa;

II - com o mesmo objetivo, realiza atividade aerofotográfica ou de sensoreamento remoto, em qualquer parte do território nacional;

III - oculta ou presta auxílio a espião, sabendo-o tal, para subtraí-lo à ação da autoridade pública;

IV - obtém ou revela, para fim de espionagem, desenhos, projetos, fotografias, notícias ou informações a respeito de técnicas, de tecnologias, de componentes, de equipamentos, de instalações ou de sistemas de processamento automatizado de dados, em uso ou em desenvolvimento no País, que, reputados essenciais para a sua defesa, segurança ou economia, devem permanecer em segredo.

.....

Art. 15 - Praticar sabotagem contra instalações militares, meios de comunicações, meios e vias de transporte, estaleiros, portos, aeroportos, fábricas, usinas, barragem, depósitos e outras instalações congêneres.

Pena: reclusão, de 3 a 10 anos.

§ 1° - Se do fato resulta:

a) lesão corporal grave, a pena aumenta-se até a metade;

b) dano, destruição ou neutralização de meios de defesa ou de segurança; paralisação, total ou parcial, de atividade ou serviços públicos reputados essenciais para a defesa, a segurança ou a economia do País, a pena aumenta-se até o dobro;

c) morte, a pena aumenta-se até o triplo.

§ 2º - Punem-se os atos preparatórios de sabotagem com a pena deste artigo reduzida de dois terços, se o fato não constitui crime mais grave.

.....

Art. 23 - Incitar:

I - à subversão da ordem política ou social;

II - à animosidade entre as Forças Armadas ou entre estas e as classes sociais ou as instituições

civis;

III - à luta com violência entre as classes sociais;

IV à prática de qualquer dos crimes previstos nesta Lei.

Pena: reclusão, de 1 a 4 anos.

LEI Nº 7.209, DE 11 DE JULHO DE 1984.

Altera dispositivos do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, e dá outras providências.

.....

LEI Nº 7.716, DE 5 DE JANEIRO DE 1989.

Mensagem de veto

Define os crimes resultantes de preconceito de raça ou de cor.

.....

Art. 20. Praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional. *(Redação dada pela Lei nº 9.459, de 15/05/97)*

Pena: reclusão de um a três anos e multa.

§ 1º Fabricar, comercializar, distribuir ou veicular símbolos, emblemas, ornamentos, distintivos ou propaganda que utilizem a cruz suástica ou gamada, para fins de divulgação do nazismo. *(Redação dada pela Lei nº 9.459, de 15/05/97)*

Pena: reclusão de dois a cinco anos e multa.

§ 2º Se qualquer dos crimes previstos no caput é cometido por intermédio dos meios de comunicação social ou publicação de qualquer natureza: *(Redação dada pela Lei nº 9.459, de 15/05/97)*

Pena: reclusão de dois a cinco anos e multa.

§ 3º No caso do parágrafo anterior, o juiz poderá determinar, ouvido o Ministério Público ou a pedido deste, ainda antes do inquérito policial, sob pena de desobediência: *(Redação dada pela Lei nº 9.459, de 15/05/97)*

I - o recolhimento imediato ou a busca e apreensão dos exemplares do material respectivo;

II - a cessação das respectivas transmissões radiofônicas ou televisivas.

§ 4º Na hipótese do § 2º, constitui efeito da condenação, após o trânsito em julgado da decisão, a destruição do material apreendido. *(Parágrafo incluído pela Lei nº 9.459, de 15/05/97)*

.....

LEI Nº 8.069, DE 13 DE JULHO DE 1990.

Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências.

.....

Art. 240. Produzir ou dirigir representação teatral, televisiva, cinematográfica, atividade fotográfica ou de qualquer outro meio visual, utilizando-se de criança ou adolescente em cena pornográfica, de sexo explícito ou vexatória: (Redação dada pela Lei nº 10.764, de 12.11.2003)

Pena - reclusão, de 2 (dois) a 6 (seis) anos, e multa.

§ 1º Incorre na mesma pena quem, nas condições referidas neste artigo, contracena com criança ou adolescente. (Renumerado do parágrafo único, pela Lei nº 10.764, de 12.11.2003)

§ 2º A pena é de reclusão de 3 (três) a 8 (oito) anos: (Incluído pela Lei nº 10.764, de 12.11.2003)

I - se o agente comete o crime no exercício de cargo ou função;

II - se o agente comete o crime com o fim de obter para si ou para outrem vantagem patrimonial.

Art. 241. Apresentar, produzir, vender, fornecer, divulgar ou publicar, 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: (Redação dada pela Lei nº 10.764, de 12.11.2003)

Pena - reclusão de 2 (dois) a 6 (seis) anos, e multa.

§ 1º Incorre na mesma pena quem: (Incluído pela Lei nº 10.764, de 12.11.2003)

I - agencia, autoriza, facilita ou, de qualquer modo, intermedeia a participação de criança ou adolescente em produção referida neste artigo;

II - assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens produzidas na forma do **caput** deste artigo;

III - assegura, por qualquer meio, o acesso, na rede mundial de computadores ou internet, das fotografias, cenas ou imagens produzidas na forma do **caput** deste artigo.

§ 2º A pena é de reclusão de 3 (três) a 8 (oito) anos: (Incluído pela Lei nº 10.764, de 12.11.2003)

I - se o agente comete o crime prevalecendo-se do exercício de cargo ou função;

II - se o agente comete o crime com o fim de obter para si ou para outrem vantagem patrimonial.

.....

LEI Nº 8.078, DE 11 DE SETEMBRO DE 1990.

Regulamentação

Dispõe sobre a proteção do consumidor e dá outras providências.

.....

CAPÍTULO IV
Da Qualidade de Produtos e Serviços, da Prevenção e da Reparação dos Danos
SEÇÃO I
Da Proteção à Saúde e Segurança

.....

Art. 9º O fornecedor de produtos e serviços potencialmente nocivos ou perigosos à saúde ou segurança deverá informar, de maneira ostensiva e adequada, a respeito da sua nocividade ou periculosidade, sem prejuízo da adoção de outras medidas cabíveis em cada caso concreto.

.....

LEI Nº 8.137, DE 27 DE DEZEMBRO DE 1990.

Vide Lei 9.249, de 1995

Mensagem de veto

Define crimes contra a ordem tributária, econômica e contra as relações de consumo, e dá outras providências.

CAPÍTULO I
Dos Crimes Contra a Ordem Tributária
Seção I
Dos crimes praticados por particulares

Art. 1º Constitui crime contra a ordem tributária suprimir ou reduzir tributo, ou contribuição social e qualquer acessório, mediante as seguintes condutas: (Vide Lei nº 9.964, de 10.4.2000)

I - omitir informação, ou prestar declaração falsa às autoridades fazendárias;

II - fraudar a fiscalização tributária, inserindo elementos inexatos, ou omitindo operação de qualquer natureza, em documento ou livro exigido pela lei fiscal;

III - falsificar ou alterar nota fiscal, fatura, duplicata, nota de venda, ou qualquer outro documento relativo à operação tributável;

IV - elaborar, distribuir, fornecer, emitir ou utilizar documento que saiba ou deva saber falso ou inexato;

V - negar ou deixar de fornecer, quando obrigatório, nota fiscal ou documento equivalente, relativa a venda de mercadoria ou prestação de serviço, efetivamente realizada, ou fornecê-la em desacordo com a legislação.

Pena - reclusão de 2 (dois) a 5 (cinco) anos, e multa.

Parágrafo único. A falta de atendimento da exigência da autoridade, no prazo de 10 (dez) dias, que poderá ser convertido em horas em razão da maior ou menor complexidade da matéria ou da dificuldade quanto ao atendimento da exigência, caracteriza a infração prevista no inciso V.

Art. 2° Constitui crime da mesma natureza: (Vide Lei nº 9.964, de 10.4.2000)

I - fazer declaração falsa ou omitir declaração sobre rendas, bens ou fatos, ou empregar outra fraude, para eximir-se, total ou parcialmente, de pagamento de tributo;

II - deixar de recolher, no prazo legal, valor de tributo ou de contribuição social, descontado ou cobrado, na qualidade de sujeito passivo de obrigação e que deveria recolher aos cofres públicos;

III - exigir, pagar ou receber, para si ou para o contribuinte beneficiário, qualquer percentagem sobre a parcela dedutível ou deduzida de imposto ou de contribuição como incentivo fiscal;

IV - deixar de aplicar, ou aplicar em desacordo com o estatuído, incentivo fiscal ou parcelas de imposto liberadas por órgão ou entidade de desenvolvimento;

V - utilizar ou divulgar programa de processamento de dados que permita ao sujeito passivo da obrigação tributária possuir informação contábil diversa daquela que é, por lei, fornecida à Fazenda Pública.

Pena - detenção, de 6 (seis) meses a 2 (dois) anos, e multa.

.....

LEI Nº 9.296, DE 24 DE JULHO DE 1996.

art. 5°, inciso XII da Constituição Federal

Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal.

.....

Art. 2° Não será admitida a interceptação de comunicações telefônicas quando ocorrer qualquer das seguintes hipóteses:

I - não houver indícios razoáveis da autoria ou participação em infração penal;

II - a prova puder ser feita por outros meios disponíveis;

III - o fato investigado constituir infração penal punida, no máximo, com pena de detenção.

Parágrafo único. Em qualquer hipótese deve ser descrita com clareza a situação objeto da investigação, inclusive com a indicação e qualificação dos investigados, salvo impossibilidade manifesta, devidamente justificada.

.....

DOCUMENTO ANEXADO PELA SECRETARIA-GERAL DA MESA, NOS TERMOS DO ART. 250, PARÁGRAFO ÚNICO DO REGIMENTO INTERNO.

COMISSÃO DE CONSTITUIÇÃO, JUSTIÇA E CIDADANIA - CCJ
COMISSÃO DE CIÊNCIA E TECNOLOGIA, INOVAÇÃO, COMUNICAÇÃO E INFORMÁTICA - CCT

21ª REUNIÃO EXTRAORDINÁRIA DA COMISSÃO DE CONSTITUIÇÃO, JUSTIÇA E CIDADANIA EM CONJUNTO COM A 19ª REUNIÃO EXTRAORDINÁRIA DE COMISSÃO DE CIÊNCIA E TECNOLOGIA, INOVAÇÃO, COMUNICAÇÃO E INFORMÁTICA DA 1ª SESSÃO LEGISLATIVA ORDINÁRIA DA 53ª LEGISLATURA. REALIZADA NO DIA 04 DE JULHO DE 2007, ÀS 12 HORAS E 05 MINUTOS.

SR. PRESIDENTE SENADOR VALTER PEREIRA (PMDB-MS): Havendo número regimental, e sob a proteção de Deus declaro aberta a 21ª Reunião da Comissão de Constituição e Justiça e Cidadania em conjunto com a 19ª Reunião de Comissão de Ciência e Tecnologia, Inovação, Comunicação e Informática da 1ª Sessão Legislativa Ordinária da 53ª Legislatura.

Os Srs. Senadores que aprovam queiram permanecer como se encontram.

A presente reunião destina-se a Audiência Pública para instruir o PLC 89/2003, o PLS nº 76/2000 e o PLS nº. 137/2000 que tramita em conjunto e dispõe sobre crimes na área de informática. Requerimento da Mesa. Requerimento à Mesa subscrito pelo Senador Crivella. Requeiro nos termos do art. 3º do Regimento Interno seja considerado como missão política de interesse Parlamentar a minha ausência nas Sessões do dia 3, 4 e 5 de julho quando estarei cumprindo agenda previamente marcada no Estado do Rio de Janeiro. Por essa razão não está presente o Senador Marcelo Crivella.

Requerimento da Senadora Serys Slhessarenko para acrescentar ao rol elencado anteriormente os Srs. Tiago Tavares Nunes de Oliveira, Presidente da ONG SaferNet, e Sérgio Amadeu, ex-Presidente do Instituto Nacional de Tecnologia de Informação ITI, além do Sr. Ronaldo Lemos, coordenador do Centro de Tecnologia da Sociedade da Fundação Getúlio Vargas.

Então, nós já temos aqui os outros convidados que estavam pré-agendados e eu consulto ao Plenário--

SENADORA SERYS SLHESSARENKO (PT-MT): Questão de ordem, Sr. Presidente.

SR. PRESIDENTE SENADOR VALTER PEREIRA (PMDB-MS): Pela ordem.

SENADORA SERYS SLHESSARENKO (PT-MT): Eu gostaria de dar uma explicação, pela ordem, Sr. Presidente, nós fizemos esses requerimentos, nós estamos vendo aí que já tem cinco membros participantes da Audiência Pública, e como estava previsto seis, uma pessoa faltou, eu pediria que... Para realmente contemplar um pouco o meu Requerimento que eu já tinha feito esse Requerimento há bastante tempo e ele não foi votado, e que se convidasse pelo menos uma das pessoas que compõem, que estão nessa lista desse Requerimento, que é o Sr. Tiago que está presente aqui que poderia participar. Eu acho que aí contemplaria pelo menos um pouco o nosso Requerimento, uma pessoa faltou que viesse se complementar--

SR. PRESIDENTE SENADOR VALTER PEREIRA (PMDB-MS): De minha parte não vejo óbice. Consulto ao Plenário se enxerga algum obstáculo.

SENADOR EDUARDO AZEREDO (PSDB-MG): Da minha parte também não vejo nenhum obstáculo. Apenas nós vamos ter problema de tempo aqui talvez pelo número elevado de participantes.

SENADORA SERYS SLHESSARENKO (PT-MT): Mas já estavam previstos seis participantes.

SR. PRESIDENTE SENADOR VALTER PEREIRA (PMDB-MS): Já é um número alto, excessivo. Eu acho que é só disciplinar a questão do tempo. Nós poderíamos fazer uma exposição máxima de 10 minutos por cada um, mostrando só os pontos nevrálgicos, e agora eu gostaria de... Eu ia convidar o Senador Wellington, que é Presidente da Comissão de Ciência e Tecnologia, mas ele já está convidado e já assumiu o seu posto na co-presidência desta Audiência Pública. E vamos então iniciar os nossos trabalhos.

Bom, aqui sobre a Mesa a justificativa da Drª. Ela. Drª. Sheila. Aliás... Quem subscreve é a Drª. Sheila. De ordem em resposta ao Ofício 65/2007 encaminha o anexo em estudo sobre o projeto de lei da Câmara nº. 89/2003 para subsidiar os trabalhos dessa Comissão visto a impossibilidade do comparecimento da Procuradora Federal dos Direitos do cidadão Ela Volkmer de Castilho por motivo de férias. Está aqui o material disponível para todos os Srs. Senadores.

SENADORA SERYS SLHESSARENKO (PT-MT): Pela ordem, Senador. Acho que para começar, teria já que foi aprovada a participação de uma das pessoas que ele também compusesse a Mesa.

SR. PRESIDENTE SENADOR VALTER PEREIRA (PMDB-MS): V.Exª indique qual dos...

SENADORA SERYS SLHESSARENKO (PT-MT): Tiago Tavares, por favor.

SR. PRESIDENTE SENADOR VALTER PEREIRA (PMDB-MS): Nós vamos passar a palavra ao primeiro convidado, Dr. Fernando Neto

Botelho, Juiz de Direito, membro da Comissão de Tecnologia e Informação do Tribunal de Justiça de Minas Gerais. S.Exª terá 10 minutos para abordar os tópicos mais importantes da matéria que está em questão.

SENADOR WELLINGTON SALGADO DE OLIVEIRA (PMDB-MG): Sr. Presidente, só pela ordem antes dos nosso primeiro convidado.

SR. PRESIDENTE SENADOR VALTER PEREIRA (PMDB-MS): Com a palavra, pela ordem.

SENADOR WELLINGTON SALGADO DE OLIVEIRA (PMDB-MG): Sr. Presidente, eu estou achando que nós aqui estamos muito apertados aqui. Eu queria, se V.Exª autorizasse, se eu pudesse sentar de frente para V.Exª para acompanhar dali, para que pudéssemos trabalhar melhor. Eu estou sentindo que está um pouco apertado aqui.

SR. PRESIDENTE SENADOR VALTER PEREIRA (PMDB-MS): Mas V.Exª não está apertado aqui. Aliás V.Exª é um dos Senadores que... É um dos Senadores menos apertados aqui de todo o colegiado. [risos] Então é um dos menos apertados Senador.

SENADOR WELLINGTON SALGADO DE OLIVEIRA (PMDB-MG): Só para dar mais espaço, para trabalharmos melhor. Mas se V.Exª autorizar.

SR. PRESIDENTE SENADOR VALTER PEREIRA (PMDB-MS): Está indeferido o requerimento de V.Exª. Bom, com a palavra então o nosso primeiro convidado, Dr. Fernando Neto Botelho.

SR. FERNANDO NETO BOTELHO: Exmº. Sr. Senador Presidente da Comissão de Constituição e Justiça do Senado Federal, Exmº. Sr. Senador Presidente da Comissão de Ciência e Tecnologia do Senado Federal, Srªs. e Srs. Senadores que integram a presente Audiência Pública, senhoras e senhores.

Primeiramente gostaríamos de agradecer a honrosa oportunidade que nos concede o convite para a participação nessa histórica Audiência Pública. Sr. Presidente, eu havia preparado, em razão da amplitude da matéria uma abordagem dividida em três tópicos que seriam a uma análise dos dados que compõem a atual realidade cibernética brasileira. Segundo tópico, a opção, de criminalização dos ilícitos cibernéticos Estado Brasileiro, e o terceiro e último tópico, finalmente, uma breve análise dos dispositivos sugeridos pelo substitutivo em discussão. Todavia, dada a limitação do tempo, e sem dúvida nenhuma pela importância da matéria nós devemos nos ater a ele, eu não terei condições visivelmente de abordar toda a extensão que pretendia dentro desse tempo.

SR. PRESIDENTE SENADOR VALTER PEREIRA (PMDB-MS): Quantos minutos V.Exª julga que é necessário?

SR. FERNANDO NETO BOTELHO: Talvez uns 20 minutos no mínimo eu tentaria fazer alguma coisa mais ampla... No mínimo. Não sei se seria cabível com os outros que vão abordar.

SR. PRESIDENTE SENADOR VALTER PEREIRA (PMDB-MS): Vamos fazer o seguinte, nós vamos ser tão inflexíveis. A matéria é relevante. Vai ter grande repercussão no futuro, de sorte que nós ponderamos sobre o tempo de 10 minutos, mas não vamos ser tão inflexíveis assim. V.Exª terá o tempo necessário para fazer a sua exposição.

SR. FERNANDO NETO BOTELHO: Eu agradeço a Presidência, a compreensão e vou fazê-lo da forma mais objetiva possível. Passo a abordar, portanto, então o primeiro tópico que nós chamamos os dados que compõe a atual realidade cibernética brasileira. Pedimos permissão antes de entrarmos propriamente nesses três temas para uma breve citação. Trata-se de um trabalho que elaboramos e estamos juntando, Sr. Presidente, juntamente com esse parecer técnico e documentos anexos também de ordem técnica esse trabalho que se denomina crimes e cibercrimes. Nele fazemos uma abordagem inicial para a fixação de um princípio que nos parece extremamente importante na apreciação da matéria por esta Comissão e que envolve todos os três projetos. E é ela: "O crime cibernético tal como crime físico comum tem raízes antigas, humanas. Seu traço antropológico não está fora do que marca o mito do mal. A maldade humana e seu fundamento básico é o seu ponto psico comum com o crime físico. Diferenciar no tratamento o criminoso do crime comum físico do delinqüente cibernético é errar profundamente a análise sociológica do crime. É medir equivocadamente sua causação antropológica. Pior, equivale diferenciar por mera sofisticação dos meios usados na execução do mal o tratamento do psiquismo delitivo dispensando ao melhor preparado em meios repercussão criminal menos rigorosa. A cibernética altera tão só o meio, o instrumento de execução do crime. Não a sua conformação negativa, como fato que atenta contra importantes interesses comunitários". E aí fechamos aspas.

Quanto ao primeiro tópico, os dados que compõem a atual realidade cibernética brasileira. Países como os Estados Unidos estimam hoje a rentabilidade atual dos chamados crimes cibernéticos em cifras estratosféricas. Em 2004, para citar apenas um exemplo, a Conselheira do Tesouro americano Valerie MacNiven, tornou público uma afirmação que com a prática de fraudes, espionagem corporativa, manipulação de ações, pedofilia, extorsão virtual, pirataria dentre outros ilícitos eletrônicos o faturamento dos chamados crimes cibernéticos havia chegado à impressionante soma de 105 bilhões de dólares. Comparativamente no Brasil no período entre 2004 e 2005, apenas as fraudes bancárias e financeiras por meio eletrônico saltaram de 5% em 2004 para 40% em 2005, do total dos incidentes eletrônicos registrados

no País naquele período. O dado é do CRT.BR, Centro de Estudos, Resposta e Tratamento de Incidência e Segurança no Brasil. WWW.CERT.BR. Informe que as tentativas de fraudes pela rede mundial cresceram naquele ano de 2005, 579%. As armadilhas eletrônicas, a pescaria eletrônica de incautos, o *fishing scam*, uma expressão inglesa, uma expressão de origem da linha inglesa, por exemplo, [ininteligível] as piadas de má intenção voltadas para obtenção de vantagem ilícita patrimonial que estamos todos recebendo na atualidade nas caixas postais cunharam uma nova aplicação da engenharia do mal ou a engenharia social, entendida como rol de práticas implementadas por "expert" para engodo, engano, indução a erro de pessoas e corporações não habilitadas à lida técnica com recursos sofisticados de tecnologia da informação.

O que surgiu como ataque e defesa de caráter puramente tecnológico, *hackers* que sofisticalizando o abandono dos rigores técnicos de seu ofício profissional, tornaram-se *crackers* e avançaram sobre sistemas e redes eletrônicos não adequadamente estruturados passou a velha e milenar característica humana que é o abuso do homem pelo homem. A chamada engenharia social não passa de uma vergonhosa disputa no meio eletrônico da superioridade cultural técnica dos maus "experts" sobre a limitada capacidade popular de conhecimento técnico dos recursos das redes. Onde há o desconhecimento técnico navega livre o abuso, o ímpeto cruel da exploração, da indução a erro e com ele o desejo do proveito fácil como ocorrem com as senhas secretas obtidas hoje por e-mails falsos, falsos anúncios de cancelamentos de títulos eleitorais, convites para entrada em sites de premiação, simulação de *web sites* para coleta de logs secretos, enfim, um arsenal de fraudes e simulações que passaram a ter na sofisticação do meio e no desconhecimento humano um novo ar de atuação.

Estamos juntando a essa abordagem, Srs. Senadores, três publicações, todas recentes, de 2006 uma e de abril/maio de 2007 as duas outras, especializadas em segurança da informação eletrônica no Brasil. Foram todas editadas pela conceituada empresa MODULO - TECHNOLOGY FOR RISK MANAGEMENT que hoje inicia processo de exame dos recursos tecnológicos eletrônicos do Tribunal de Justiça de Minas Gerais, para prestação de serviços de mapeamento e planejamento de segurança da informação eletrônica interna e externa, e que vem prestando serviço também a outros importantes órgãos públicos da União e dos Estados.

V.Exªs. poderão ver nesses volumosos que estamos encaminhando dados impressionantes do crescimento da demanda por serviços eletrônicos no Brasil e com eles por segurança mínima contra fraudes e crimes cibernéticos já implantados. São eles: O Serviço de Declaração do Imposto de Renda pela internet que acaba de

complementar 10 anos foi usado agora em 2007 por 99% dos contribuintes declarantes. Isto é, das 23 milhões, 270 mil declarações recebidas pela Secretaria da Receita Federal, 22 milhões e 900 mil foram enviadas pela internet, numa amostra do volume quase absoluto da adoção da população contribuinte a sistemas eletrônicos convencionais, página 3 do volume 12 da revista *Risk Management Review*.

Por outro lado, ou em paralelo com esta crescente adesão voluntária popular ao meio eletrônico público e privado registrou o País número expressivo de incidente de insegurança na internet no mesmo ano do exercício fiscal agora recentemente declarado. 197 mil ocorrências em 2006 ou um crescimento de 191% em relação aos 68 mil ocorrências registradas em 2005. Desses números, apenas a prática do *fishing scam*, a pescaria eletrônica de incautos pela internet usualmente por e-mails não autorizados, uma característica da tal engenharia social respondeu por 21% destas ocorrências. O *fishing scam* para obtenção de senhas bancárias e de números de cartões de crédito cresceu em 2006 53%. Outro dado da página 14 da mesma revista. As empresas de grande porte estão investindo crescentes somas de seus orçamentos na tentativa de proteção a clientes, consumidores e a seus próprios ativos. E aqui citamos um caso de fraudo específica, eu vou saltar para que não haja comprometimento maior do tempo. A maior empresa brasileira de distribuição de petróleo e derivados anuncia na página 34 dessa revista que possuindo uma força de trabalho por mais de 5 mil pessoas espalhadas por todo o Brasil teve que fazer significativos investimentos em segurança interna da informação eletrônica. As empresas de cartão de crédito informam um salto nas dimensões do mercado com uso dessa sistemática, transações eletrônicas, cartões de crédito, uma somatória total de 4 bilhões de reais de 2006, saltou para 4,9 bilhões de reais em 2007. As compras de softwares, segundo o *Gartner Group*, somaram... Houve um aumento nas compras de software para a defesa corporativa de 10,7% em 2007.

E assim, Srs. Senadores, vários outros dados de defesa tecnológica tentada contra a atuação humana em redes corporativas e privadas. Uma pesquisa feita com 600 profissionais pela MODULO nas áreas de segurança e tecnologia da informação, de organizações privadas, públicas, de economia mista do País no segmento de governos financeiro, informática, indústria, prestação de serviço, telecomunicações, comércio, educação, energia elétrica, saúde e mineração apurou 15% dos ataques se devem a ataques eletrônicos por vírus. Ataques eletrônicos por *spam*, 10%, fraudes eletrônicas 8%, vazamentos de informações sensíveis, 7%, acesso remoto indevido 6%, divulgação de roubo de senhas eletrônicas 5% e invasão de sistemas internos 4%. Furto de informações proprietárias, 2%. Sabotagem eletrônica 2%. Pirataria 2% e espionagem 1%.

Outras particularidades da vida eletrônica brasileira têm chamado atenção de organismos internacionais. Um exemplo é o das comunidades relacionadas do ORKUT. Muito conhecido. Programa gerado e concebido como sistema relacional via internet destinado conceitualmente à formação de grupos científicos, acadêmicos, relacionais, familiares, afetivos, etc, criado a mais ou menos três anos nos Estados Unidos por uma empresa norte-americana Google Inc. tem como sua maior comunidade mundial a de jovens brasileiros que compõem hoje mais de 50% do universo das comunidades ORKUT de todo o globo. Pois o ORKUT tem provocado ao lado de seu incomensurável efeito benéfico relacional, atentados brasileiros dos mais variados como páginas de ataque à honra de personalidades públicas, de corporações privadas, de formação eletrônica de comunidades voltadas para o crime financeiro, comercialização internacional e nacional de entorpecentes, e mais recentemente organização de ataques físicos e cibernéticos coletivos. Fatos que começam agora a chegar às barras dos tribunais sob intensa discussão de tipicidade penal.

Em suma, Srs. Senadores, podemos resumir esses dados em objetivas conclusões. Primeiro, o nível do envolvimento crescente da população, das pessoas naturais e das corporações com sistemas eletrônicos em geral, com as redes corporativas internas, externas, internet, telefonia móvel, fixa, atinge na atualidade um volume majoritário do interesse brasileiro. Cem milhões de telefones celulares, 50 milhões de telefones fixos, 20 milhões aproximadamente de usuários de Internet. Os serviços públicos eletrônicos brasileiros dos poderes Executivo, Legislativo e Judiciário, cresceram e crescerão significativamente de agora em diante, de modo a exigirem cautelas e cuidados especiais por parte do Estado Brasileiro quanto à segurança da informação relativamente aos dados sensíveis, custodiados no âmbito de cada porte. Srs. Senadores, neste exato momento nós estamos sob coordenação do Conselho Nacional de Justiça implantando aquele que será o maior paradigma do serviço judiciário brasileiro que é o processo eletrônico totalmente sem papel, com base na Lei 11.419/2006, que institui o processo sem papel. No meu Estado, Minas Gerais, há três milhões e quinhentos mil processos em papel atualmente em tramitação e a partir de agosto estaremos implantando pilotos de processos completamente sem papel, o que significa um encargo imenso com os cuidados da segurança da informação, razão pela qual uma empresa como a MODULO está neste momento começando um trabalho de mapeamento dos backups, dos logs, de toda a nossa infra-estrutura de tecnologia sem a qual nós não podemos permitir que os dados sensíveis da população, dados esses hoje *sub judice*, sob discussão judicial sejam disponibilizados livremente nas redes e eventualmente absolvidos por um cuidado não adequado para aquele nível. Nos Estados Unidos um Sistema Pacer, Pacer que é o nome do sistema norte-americano, ele

pode ser procurado no Google por qualquer interessado que controla todo o procedimento de 25 milhões de processos sem papel da Justiça Federal norte-americana, possui um aplicativo rigoroso, inclusive com repercussão criminal para aquele que eventualmente obtenha dado indevidamente de processo judicial na Justiça Federal norte-americana. De modo que o Poder Judiciário, e aqui eu falo como membro especificamente do judiciário mineiro e ali controlando, coordenando o trabalho do processo eletrônico, tem um cuidado especial com a questão relacionada com a segurança da informação e com a necessidade de termos instrumento de responsabilização das pessoas a respeito dos dados sensíveis que vão ser gerados nesse processo. Os ataques e condutas lesivas contrárias a uma mínima visão de razoabilidade social denotam crescente tendência delitiva por parte de usuários de sistemas eletrônicos de comunicação. Estes fatos arriscam interesses da majoritária parcela de usuários formada por inocentes, gerando uma desigualdade prática que tem cunhado expressões as mais inaceitáveis para o convívio harmônico como da engenharia social. As ações criminosas eletrônicas, por razões de sofisticação, massificação e alto poder ofensivo humano rompem o poder de defesa gerado por emprego de meros softwares ou medidas paliativas de proteção. A ação produtiva do injusto eletrônico reclama uma contra ação estatal minimamente preventiva que contenha a necessidade de emprego de grandes somas de recursos financeiros, o custo operacional de um projeto estratégico para o Poder Judiciário de Minas Gerais apenas com segurança da informação compromete o interesse público porque sobrecarregará o nosso orçamento para essa finalidade.

Finalmente, o grau de interesses lesados ou sujeito a risco de lesão potencial já sobe ao porte dos interesses tuteláveis do Estado através de emprego de medidas penais, especificamente de criminalização dessas condutas. Passamos assim a tratar do segundo ponto brevemente.

Senhores, o moderno Direito Penal e estudos de criminologia que foram editados no mundo moderno especialmente na Europa após a fase do Iluminismo repugnam aquela idéia primitiva que vigorou até a idade média da Lei de Talião, do uso da pena, do Direito Penal como meio de retribuição pelo mal causado. A criminalização não pode derivar de um ímpeto estatal retributivo. A decisão do Estado de tornar determinada conduta crime deve ser a última providência. Tomada diante de indicadores éticos, sociais mínimos que a justifiquem, com foco no resguardo das garantias fundamentais sobre as quais estruturado o próprio Estado. Preserva-se com isso a idéia de mínima intervenção do Estado sancionador na vida comunitária que é própria do Estado de Direito. Este o princípio da intervenção mínima que se alia da fragmentariedade, no gerenciamento de uma visão moderna no Direito Penal que deve habitar um Estado social de direito. Ambos indicando a necessidade de seleção de condutas que sejam efetivamente

exorbitantes da razoabilidade do convívio para que se sujeitam a criminalização. Uma vez decidida a adoção da via penal como solução para uma dada tendência social, deve-se respeitar ainda o derradeiro princípio gerenciador do moderno Direito Penal que é da proporcionalidade entre a criminalização, a pena e o fim buscado. O fim buscado pela pena, pela sanção penal não pode ser outro que não o estrito intuito de educação. A pena deve educar. A criminalização deve educar. Limitativamente a tendência social contra a prática de crime. Chama-se a esta finalidade de princípio da prevenção geral limitadora da pena, por ela, pela pena, se educa socialmente. Se educa o grupo. O povo como um todo, disseminando-se uma lição prévia, teórica, formalizada no texto do crime instituído de que o crime e principalmente o valor jurídico social que ele resguarda e representa constituirá um atentado à harmonia social como uma resposta educativa pelo Estado. Tudo isso, no entanto, não afastou dos Estados, e é preciso enfatizar isso, o poder. Aliás, um poder dever de intensa valia social coletiva de delimitação das condutas que mesmo por exceção, mesmo como última raço(F) reclamem solução criminalizante. O Estado não se demitiu pela visão moderna de Direito Penal de sua precípua missão institucional que é de realizar o bem comum. A Constituição e as leis não suprimiram do Estado o poder de criminalizar condutas sociais e infracionais de grande relevo para o resguardo do interesse comunitário. Ao contrário, em respeito ao próprio Estado de Direito, é muitas vezes através de adequada delimitação criminal da conduta típica que se resguardará o conjunto dos cidadãos de sabem. A analogia não pode suprir em matéria penal a lacuna na dá lei penal antiga. Isso significa que diante da ausência de uma lei expressa sobre determinada conduta nova não se pode impor criminalização em juízo e conseqüentemente a pena. É o princípio da reserva legal. É nula a pena e o crime sem prévia lei que os defina. Sem lei expressa que regule novas atividades criminosas, nem se conseguirá com a analogia do suprimento incriminação de condutas graves nem se assegurará ao inocente delas segurança de livramento acusações que busquem interpretações extensivas da norma antiga. Isso é que nos parece ocorrer com o crime eletrônico cibernético brasileiro. Tamanha as alternativas já empregadas coletivamente na atual perpetração [soa a campainha] do injusto coletivo, que ele reclama neste momento típica e definida criminalização com a qual seja este novo fato social extremado de outros tipos penais antigos. Lembro aqui que o Código Penal Brasileiro para que o exemplo se limite a essa Lei Geral do País, Lei Geral Penal, data de mais de 60 anos e não contempla meios de interpretação extensiva. Será extremamente arriscado entregar ao Poder Judiciário a interpretação extensiva destes tipos penais convencionais na tentativa de adequação desses crimes aos fatos cibernéticos atuais tamanha complexidade da estrutura eletrônica brasileira. O atual Código Penal não possui estruturação de crimes para essa finalidade, que possam abranger as imensas inovadoras hipóteses

do cibercrime, o *krekking(F)*, o *fishing scam,* os atos *de gray hat, black hat*, de pichamento digital, a espionagem eletrônica, as difusões de códigos eletrônicos maliciosos danosos e não danosos ou a fraude eletrônica. A proporção desses novos crimes como se demonstrou saiu há muito da esfera de ocorrências para as quais se pudesse cogitar de marcos ou sanções puramente regulatórios, civis, reparatórios, éticos ou administrativos. Sem uma firme decisão do Estado Brasileiro. Já neste momento em que é intenso o crescimento da planta de prestadores de usuários dos variados sistemas eletrônicos no sentido de submeter a baliza seguras, garantidoras de um ambiente minimamente saudável, atividade eletrônica cibernética deixar-se-á a realidade densa, criminal e eletrônica já posta em prática a própria sorte. Somente a coercitividade estatal, o poder de império do Estado que habilita a imposição da sanção penal típica e pré-definida poderá educar, prevenir na generalidade com um piso de efetividade o conjunto da população usuária de sistemas eletrônicos. A população majoritariamente, a população de bem. Educação prévia que se direcionará à extensa juventude "orkutiana" brasileira. A imensa maioria dos atuais usuários de redes internas e externas. A fatia crescente dos internautas e prestadores dos serviços brasileiros de internet. A centena de milhões de usuários à telefonia móvel celular, e aos milhões de correntistas do sistema financeiro, consumidores dos serviços de saúde, dos serviços públicos estatais, como os da Justiça dentre outros, a respeitarem regras mínimas do convivo eletrônico. Não nos parece adequado aguardar marcos regulatórios para instituição civil de regras, coisa, aliás, que nunca exigida na incriminação de condutas eletrônicas no Brasil para que o Estado atenda sob a ótica do Direito Penal a presente necessidade.

Em termos de política criminal, Sr. Senadores, em respeito à história do tratamento penal das telecomunicações brasileiras, reparem V.Exªs. que a exatos 10 anos, em 1997, a própria Lei Geral de Telecomunicações que é a Lei 9.472 foi votada aqui nessa Casa, em seu art. 183 lançou-se a criminalização direta de específicas condutas sem o aguardo de qualquer marco regulatório civil, ético ou administrativo prévio. E o fez diante da também direta constatação do legislador da alta potencialidade ofensiva do ilícito de telecomunicações já se falou no passado quando não vivíamos inclusive o Estado de direito que era a questão de Estado a segurança das telecomunicações. Coisa inclusive que o legislador de 62 quando editou o antigo Código de Telecomunicações que é a Lei 4.117 também implementou com amplitude a Lei Geral das Telecomunicações resolveu referendar em seu art. 215. Aliás, é bom frisar, os crimes definidos pela Lei Geral de Telecomunicações penalizam com pena privativa da liberdade de dois a quatro anos aumentada da metade, se houver dano a terceiro, o desenvolvimento clandestino de atividades de telecomunicação. Não houve surpresa ou questionamento sobre isso na época da tramitação

congressual da Lei Geral de Telecomunicações e a questão atual quando passado uma década do fenômeno da desestatização do sistema Telebrás, se apresenta muito mais grave a nosso juízo, mais extensa, pois ao invés de termos no Brasil meros circuitos de telecomunicações, há serviços densos, extensos de comunicação eletrônica por dados e voz trafegando por redes corporativas públicas e privadas de grande relevância. E aí transcrevemos o art. 183.

Com base nessas premissas, finalmente, falamos então sobre o os dispositivos sugeridos pelo substitutivo em discussão. O primeiro ponto deste tópico ou aquele que nos preocupa nesse momento é o que se relaciona com a linguagem normativa que está proposta no substitutivo do eminente Senador Eduardo Azeredo. Na medida em que decidida a criminalização, a linguagem que define o tipo penal se mostra de grande relevância. Sobretudo no Brasil, em que a interpretação da norma penal deve observar um rigoroso limite de legalidade que comanda o princípio de que a dúvida prestigiará sempre a inocência. Famoso adágio latino *in dubio pro reu*. Entretanto, paralelamente a este aspecto deve-se salientar que a tendência moderna mundial de regramento dos tipos tecnológicos caminha para um antagônico sentido, que é o da delimitação aberta dos elementos ou das circunstâncias elementares que os caracterizam, foi essa inclusive a política adotada pelo legislador na edição da Lei Geral de Telecomunicações, pois em razão da inovação tecnológica o ciclo de inovação é muito maior na tecnologia da inovação, não se pode perder a essência da definição legal frente as evolutivas alterações estruturais que o tempo permite. Em matéria penal então a questão se avoluma, pois na medida em que se pode inovar o meio com maior velocidade, corre-se o risco no fechamento gramatical de hipóteses normativas de se transformar a norma incriminadora em instrumento inócuo de aplicação por rápida desatualização. Como conciliar no bojo da antiga Lei Penal Brasileira do Código Penal e dentro do escopo constitucional de observância da legalidade estrita, a correta definição que será sempre gramatical com os recursos quase infinitos na nossa língua portuguesa, dos novos crimes informáticos? Dosagem da linguagem, sua adequação teleológica, os valores ontológicos das expressões contidas nessa definição, e isso me parece uma missão da atividade empregável a posteriori desse momento de formação da lei, e não a priori, pois está ligado ao trabalho interpretativo jurisdicional. É o Judiciário que fará essa interpretação ao final. Portanto, a matéria passa a ser jurisdicional e jurisprudencial, e uma certa inspiração me parece dosada por medidas externas ao âmbito nacional. Precisamos ver o que ocorre fora. E nos parece que o maior exemplo desse do que está ocorrendo fora do País sobre cibercrimes é exatamente a convenção européia dos cibercrimes. Conquanto esteja sobre alguns pontos em discussão na Europa, ela foi subscrita por mais de 40 países,

e ela sintetiza, digamos, um Estado da arte que poderá ser adotado na missão disciplinar criminalmente--

[troca de presidência]

SR. PRESIDENTE SENADOR WELLINGTON SALGADO DE OLIVEIRA (PMDB-MG): Um minutinho para V.Exª tomar uma água. V.Exª. [risos] Eu gostaria de saber se mais cinco minutos seria possível para que pudesse terminar sua explanação. Só para nós colocarmos ordem na Casa, porque tem muitos explanadores. Senão não teríamos tempo para todos. Só por essa razão. Cinco minutos seria possível? Para que V.Exª pudesse fazer um resumo do restante?

SR. FERNANDO NETO BOTELHO: Sim, claro. Encerro nesse momento.

SENADOR WELLINGTON SALGADO DE OLIVEIRA (PMDB-MG): Não, não, não.

SR. FERNANDO NETO BOTELHO: Com cinco minutos eu encerro.

SENADOR WELLINGTON SALGADO DE OLIVEIRA (PMDB-MG): Ok. Cinco minutos. Por favor, marque mais cinco minutos para o Sr. Fernando Neto Botelho. Pode continuar, por favor.

SR. FERNANDO NETO BOTELHO: Neste ponto parece-nos que o substitutivo apresentado aos três projetos em análise atende a este propósito. E passo aí então a uma análise tópica artigo por artigo do substitutivo. Mas, em razão da questão relacionada com o tempo eu entrego à Comissão este parecer e me mantenho claro à disposição dos eminentes Senadores para indagação tópica a respeito destes dispositivos.

E passo finalmente à conclusão. Disso se tem além da adequação da criminalização o seguinte. Afora as propostas de instituição do crime de furto qualificado que está no projeto, e de crime preterdoloso de dano, todos os demais tipos penais criados pelo substitutivo ou transportados para o substitutivo contém penalidades, penas privativas da liberdade que se sujeitam ora à conversão direta à indenização e penas restritivas de direito. É preciso ver que em matéria penal o legislador delimita o mínimo e o máximo. Mas há uma repercussão dentro da estrutura penal brasileira quanto a essa delimitação. O Código Penal Brasileiro e a Lei 9.099 que é a lei dos juizados especiais estabeleceram alguns benefícios para essa delimitação penal.

Então, esses tipos penais definidos no substitutivo, fora o furto qualificado e fora o crime preterdoloso têm limites máximos e mínimos de pena que permitem a conversão em penas restritivas de direito,

portanto, sem privação da liberdade, em indenização e em multa direta. Portanto, não podemos nos impactar desde logo com os limites máximos e mínimos da pena porque eles servirão para o atendimento daquele princípio da educação geral da prevenção geral contra a prática do ilícito. Mas necessariamente não levará o infrator ao recolhimento e a privação da liberdade. Aliás, na maior parte das vezes sendo ele primário sem antecedentes criminais ele será mantido em liberdade com penas convertidas em restritivas de direito, multa ou indenização. Não se proclama, portanto, exacerbação penalizadora pelo que se vê preservação de proporcionalidade na resposta penal cominada a cada infração nova proposta.

Por todo esse exposto, somos de opinião de que o substitutivo apresentado aos três Projetos de Lei recomenda sua aprovação como está, pela adequação com a gravidade dos fatos tratados e pelo respeito que promove a finalidade preventiva geral dos ilícitos proclamados. Sendo que a penalização proposta evidencia submissão a princípios e balizas aceitáveis de proporcionalidade e razoabilidade. Sugerimos a aprovação do substitutivo no âmbito desta Comissão. Muito obrigado, Sr. Presidente. Entrego a V.Exª o trabalho com os anexos.

[troca de presidência]

SR. PRESIDENTE SENADOR VALTER PEREIRA (PMDB-MS): Vou valer-me desse trabalho para distribuir depois a todos os componentes da Comissão. Sobre a Mesa justificativa da Senadora Lúcia Vânia, que informa que não pôde estar presente aqui hoje em razão de missão política que cumpre em seu Estado.

O próximo expositor é o Dr. Marcelo Bechara de Souza Hobaika, Consultor Jurídico representante do Ministério das Comunicações, no Comitê Gestor na Internet no Brasil, e a ele faremos o mesmo apelo que fizemos ao Dr. Fernando, no sentido de usar criteriosamente o tempo, o mais racional possível, a fim de que todos possam expor suas opiniões sobre a matéria que está em discussão.

SR. MARCELO BECHARA DE SOUZA HOBAIKA: Pois não, Excelência. Exmº. Senador Valter Pereira, Presidente da Comissão de Constituição e Justiça do Senado, Exmº. Senador Wellington Salgado, Presidente da Comissão de Ciência e Tecnologia, grande amigo, Exmº. Senador Eduardo Azeredo, Relator da matéria, companheiros de Mesa, vou tentar ser breve, o mais breve possível.

Bom, antes de mais nada, é preciso que nós identifiquemos o seguinte. Nós estamos falando de um projeto que trata de matéria penal. Toda vez que nós estamos falando de uma questão de matéria

penal, nós estamos inserindo dentro do contexto do ordenamento jurídico novos crimes. Ou chamados tipos penais. Conseqüentemente nós estamos então atribuindo a determinadas condutas a chamada prática criminosa e a sanção a ela cabível. É o que dispõe a Constituição da República que não há crime sem lei anterior que o defina e nem pena sem prévia combinação legal. Aliás, princípio conhecido de todos. Para ter a efetiva constituição da prática delituosa, no direito brasileiro, há que ter dois elementos importantes que é a autoria e a materialidade do crime.

Bom, tentando conceituar essa questão do direito no âmbito do delito informático, nós temos uma grande dificuldade, haja vista o processo da TIC, ou Tecnologia da Informação e da Comunicação, muitos conceitos isolados na área de informática, telecomunicações, telemática, passam então a se fundir e por isso criam algumas dificuldades no âmbito da conceituação dos dispositivos penais, haja vista que já que nós estamos falando de crime, crime tem que ter clareza. Crime tem que ser preciso. Tem que ser claro. Não dá para fazer um crime em que o magistrado ele possa fazer aplicação como analogia. Como bem falou o Exmº. Juiz Fernando Botelho Neto, grande conhecedor da matéria, o *in dubio* é o *pro reu*, ou seja, sempre beneficiar ao réu.

Bom, então tentando encontrar um pouco esse conceito, ao exceder, atribuir aos delitos informáticos qualquer comportamento ilegal a ético, ou não autorizado envolvendo processamento automático de dados ou transmissão de dados. Existem, Srs. Senadores, dois tipos basicamente de delitos informáticos. Os chamados crimes impuros e os crimes puros. O que é o crime impuro? O crime impuro é aquele que utiliza o sistema informático apenas como meio. Ou seja, muitos crimes que já existem dentro do nosso ordenamento jurídico desde o código de 1940, são crimes informáticos impuros. Por exemplo, o caso dos crimes contra a honra, calúnia injúria e difamação. Eu posso fazer isso através da carta, eu posso fazer isso verbalmente, mas também posso fazer isso através da internet, aliás, é um crime que acontece bastante, a questão da difamação e da injúria através da rede de computadores internet. Portanto, usa o meio informático, o sistema informatizado, o processamento eletrônico como meio. É o chamado crime impuro. Já o chamado crime puro, é aquele que visa atingir o sistema informático. Lembramos que no Direito Penal nós trabalhamos com bens jurídicos a serem tutelados. Como a vida, o patrimônio, a honra, o trabalho... Nesse caso do crime informático puro, o próprio bem jurídico a ser tutelado seria o sistema informático. Alguns agentes conhecidos como *hackers, freackerse* e *crackers*, muitas vezes a gente chama todo mundo de *hacker*, não necessariamente o *hacker* é um agente delituoso. Muitas vezes ele apenas está fazendo um protesto ou está tentando verificar alguma segurança no sistema. Mas os *freackers* que são um termo já utilizado no âmbito das telecomunicações, hoje as

telecomunicações estão completamente interligadas ao processo tecnológico de informação, os *crackers* que são realmente agentes que causam muitos danos e os *lammers* aqueles que têm poucos conhecimentos, mas acabam também cometendo também algumas práticas criminosas.

Uma coisa que é importante nós entendermos é o seguinte, a administração pública brasileira já se adiantou na proteção a determinados crimes informáticos. Nós já encontramos no âmbito do ordenamento jurídico pátrio alguns crimes que poderiam ser considerados crimes informáticos. Através da Lei 9.983/2000 que foi inspirada no Projeto de Lei do então Deputado Luiz Piauhylino que deu origem ao PLC 89/2003 que foi aprovado na Câmara e que veio para o Senado e que hoje nós estamos debatendo boa parte desse projeto. Então eu troço aqui alguns... Não vou me ater a todos, mas alguns crimes informáticos que já são efetivamente crimes que já podem ser aplicados suas penas. Lembrando que a vítima, no caso, é a administração pública. E o agente o funcionário público. É claro que aquele que não é funcionário público, mas comete o crime, valendo-se dessa situação pode ser equiparado a funcionário público para fins das penas. Porque nós sabemos que nos casos de crimes contra a administração pública as penas elas são um pouco mais majoradas. Por exemplo, crimes de divulgar sem justa causa conteúdo de documento particular ou correspondência. Inserir ou facilitar o funcionário, autorizada inserção de dados falsos com fim de obter vantagem indevida para si ou para outrem. Modificar ou alterar sistemas de informações, programa de informática. Esses dispositivos já estão no Código Penal Brasileiro. Já estão no Código Penal Brasileiro. É o caso do 313 B. Bom, revelar fato de que tem ciência em razão de cargo. Veja que é sempre a situação da administração pública. Comete também o crime quem permite ou facilita o acesso de pessoas não autorizadas a sistemas de informação de banco de dados da administração pública. Então nós estamos vivendo uma situação no País hoje em que a administração pública ela já é protegida em razão de algumas práticas criminosas no âmbito da informática e que a maior parte dos cidadãos não está efetivamente protegido.

Temos que lembrar também que haja vista que o processo eleitoral brasileiro é um processo eletrônico, então os crimes eleitorais também são crimes eletrônicos. É o caso, por exemplo, de crime eleitoral de obter ou tentar obter o acesso a sistema de tratamento automático de dados, tentar desenvolver ou introduzir comando ou instrução capaz de destruir, apagar ou eliminar, alterar, gravar ou transmitir dados de instrução de programa, ou provocar qualquer outro resultado diverso do esperado sistema de tratamento automático do serviço eleitoral, enfim, vários crimes no âmbito do sistema informático.

Tem também nos crimes contra a ordem tributária desde o início da década de 90, utilizar ou divulgar programa de processamento de dados, que permita o sujeito passivo, agora estamos falando de um âmbito tributário, possui informação contábil diverso daquela que é por lei fornecida à Fazenda Pública.

Finalmente, o crime de interceptação de 1996, que é interceptação ou grampo de comunicações telefônicas, de informática ou telemática, e aqui é a única vez que eu encontrei na norma brasileira a expressão telemática utilizada, expressão essa criada na década de 80 por [ininteligível], França, que foi o primeiro conceito que foi criado no âmbito do processo de convergência tecnológica e o legislador absorveu esse princípio dentro da norma de 96.

Algumas normas no âmbito do direito comparado, já foi citado aqui pelo Fernando a questão da conversão de Budapeste, do cibercrime, que existe em alguns países que são signatários, lembrando que o fato de um País ser signatário da convenção de Budapeste não significa absorção de todos os seus conteúdos, evidentemente cada País tem a sua liberdade e soberania para fazer adaptação dentro do seu ordenamento, a diretiva européia de 2006, e vários e vários países inclusive a Nigéria tem um crime de ciber terrorismo, a Austrália, a Venezuela que tem um projeto muito interessante já alguns anos o Chile, Portugal, Espanha, e vários outros países eu trouxe apenas aqui alguns em caráter meramente exemplificativos.

Bom, eu vou tentar aqui ser muito rápido na abordagem do substitutivo do eminente Senador Eduardo Azeredo, mas eu gostaria de fazer uma lembrança em relação ao Projeto de Lei que veio da Câmara dos Deputados, para que a gente pudesse fazer uma comparação daquilo que evoluiu em relação ao que foi aprovado na Casa aqui ao lado em relação ao que está sendo discutido no âmbito dessa Comissão.

Bom, aqui estão alguns dispositivos, eu não vou passar todos, mas eu gostaria de colocar, por exemplo, no art. 154 A, em que tem acessar indevidamente, nós reconhecemos que houve uma melhora muito grande que acessar indevidamente era um termo do ponto de vista jurídico complicado no âmbito penal e que acessar sem autorização seria muito mais adequado, contudo, veja que a pena ela aumentou sobremaneira o que era uma detenção de três meses a um ano e multa passou para reclusão de dois a quatro anos e multa. Eu acho com... E essa é a minha opinião, que é uma pena realmente muito gravosa para a prática desse crime.

Bom, em relação a por exemplo a defesa digital eu não vou mencioná-la porque já foi... Ela inclusive foi objeto de Emenda supressiva do Senador Flexa Ribeiro, eu fiz algum comentário que depois eu passo para frente.

Bom, vou tentar mesmo sem o computador consigo fazer algumas colocações. Na prática, nós observamos que esse projeto ele está melhor, e eu acho que o Senador Eduardo Azeredo teve essa grandeza, em relação àquele que foi discutido e que gerou polêmica, isso é notório e sabido no final do ano passado. Houve alguma melhora. Contudo, o projeto merece e deve ser melhorado em vários aspectos. Um dos aspectos que me deixa muito preocupado é em relação aos aumentos substantivos de algumas penas que eu não acho que essa tendência do Direito Penal moderno. Ainda mais no âmbito desse tipo de crime. Eu acho que alguns crimes realmente como o caso da pornografia infantil que em que pese estivesse no PLC 89 já foi resolvido, e o Tiago Tavares tem muito mais autoridade para falar disso do que eu, numa lei de 2003. Então acho que é uma questão que já está resolvida, mas que também merece alguns ajustes e o Tiago vai falar sobre isso. Agora, alguns dispositivos do ponto de vista conceitual como a lei coloca para os fins dessa lei é sistema informatizado ou sistema de comunicação, os conceitos estão confusos. Os conceitos ainda não são claros. Os conceitos eles acabam tendo uma vinculação. E eu acho, Senador Azeredo, que a grande dificuldade e realmente é muito difícil em relação justamente sou grande especialista na área de tecnologia, de conseguir delimitar no aspecto criminal conceitos que tem um dinamismo muito maior do que a norma penal consegue alcançar. Nós estamos retardatários no âmbito do processo em correr atrás da tecnologia. E nós temos que reconhecer isso. Portanto, mas nós não podemos, ao mesmo tempo, no âmbito do Direito Penal, permitir expressões do tipo similares, análogas. Isso não cabe dentro do Direito Penal. Porque não é permitido nesse caso ao magistrado, e com todo respeito ao Fernando Botelho eu falo isso, esse tipo de interpretação. Porque nós estamos lidando com a liberdade do ser humano. E isso tem que ficar claro aqui. Quando nós estamos falando de matéria penal nós estamos falando de restringir a liberdade do ser humano.

Então, nós temos que ter muita responsabilidade. E eu acho que é a grandeza dessa Audiência Pública a felicidade dela se realizar justamente de a gente ter a oportunidade de debater com a sociedade essas questões.

Uma coisa também que me deixa muito preocupado em relação ao art. 21. Eu acho que o art. 21 não deveria estar nessa lei. O art. 21 trata de matéria não penal civil. Do ponto de vista do processo legislativo isso não tem nenhum problema. Não é essa questão que eu estou enfrentando. O que eu enfrento é que eu acho que não houve debate com a sociedade de forma plena para tratar de responsabilidade civil de provedores de acesso à internet. Até porque o Código Civil Brasileiro já traz no seu ordenamento a questão da responsabilidade objetiva. Eu acho que nós já temos elementos dentro do Direito Civil, o que é diferente do Direito Penal que você precisa precisar a norma, elementos suficientes para responsabilizar aquele que cause

efetivamente algum dano. Então eu não entendo e não vejo a necessidade neste momento do art. 21. Eu acho que se o art. 21 não tivesse sido inserido no projeto, talvez o projeto já tivesse sido aprovado. Porque o projeto é importante, o projeto é urgente. E eu não sou daqueles que critica o projeto para que o projeto não aconteça. Eu gostaria muito que ele saísse esse ano. Mas nós não podemos ao mesmo tempo permitir que o projeto saia com alguns tipos de incoerências e inconsistências, inclusive conceituais como ele se encontra. Existem tipos penais, infelizmente o power point saiu, que são oito linhas de conceituação de tipo penal. Criar, divulgar, modificar, inserir, facilitar, quer dizer, são uma série de dispositivos que vão durante a questão do ponto de vista do caso concreto gerar algum tipo de confusão. Basta por exemplo você ver o art. 121 matar alguém. Simples. Aplicação. Matar alguém. O conceito tem que ser objetivo. O Direito Penal exige isso. Isso é um princípio que nós não podemos fugir. Os textos estão muito extensos. E isso tende a gerar confusão. Quem milita no direito sabe muito bem do que estou falando. E é tudo que um bom Advogado precisa para arrumar brechas. Brechas para que as penas não sejam aplicadas. E não adianta, não é essa a realidade que nós queremos nesse projeto. Nós queremos, sim, que esse projeto saia, queremos que esse projeto saia o mais rápido possível, e queremos que ele seja exeqüível, que ele seja aplicado. Nós não podemos correr o risco de deixar que infelizmente no Brasil, Senador Valter Pereira, encontramos algumas leis que pegam e leis que não pegam. Infelizmente essa é a realidade. E nós não podemos correr o risco dessa lei não pegar. Acho que nós não podemos correr esse risco.

Existem alguns dispositivos que são muito interessantes, em relação, por exemplo, à questão do dano. Agora, existem alguns conceitos que podem gerar algum tipo de constrição, de repressão ao uso comum da internet. Como é o caso, por exemplo, difundir código malicioso. Essa questão de difundir código malicioso, qualquer um de nós pode acontecer isso. Veja bem, a partir do momento que eu recebo um *orm*(F) ou um vírus que se multiplica dentro do meu sistema sem que eu perceba e ele comece a ser multiplicado e vá sendo então replicado a vários usuários, eu poderia estar insculpido dentro da prática desse crime. O que eu acho que é extremamente temerário. Então nós temos que ter mais clareza em relação a quem? Àquele que cria, desenvolve, àquele vírus malicioso e que tem efetivamente a intenção ou o dolo de causar o dano. E não simplesmente aquele que foi uma vítima e que por conta disso acabou também sendo difusor desse vírus. Porque nós sabemos que na tecnologia da informação isso é plenamente possível e acontece diariamente. O caso de *orms*(F), inclusive isso já tem acontecido em programas de mensagens, como o caso, por exemplo, do Messenger, o MSN.

Alguns outros aspectos que eu acho que merecem atenção, são em relação à questão do... Já falei alguns aspectos em relação à

questão conceitual, a questão de coisa. A questão de coisa no âmbito do processo criminal informático. Eu até como defensor do direito informático, eu sempre fico brigando para dizer que o bem intangível, aquele que a gente não consegue carregar, ele tem valor. Nesse caso, eu acho temerário. O direito brasileiro no que trata da questão de coisa, está atrelado à questão do bem corpóreo. Eu acho que a coisa informática que poderia estar sendo prejudicada poderia ser em relação a informação das pessoas a privacidade. E eu acho que isso a Constituição já traz proteção. Eu acho que nós temos na própria norma vários outros dispositivos que poderiam ser aplicados.

Então, eu entendo que essa questão da coisa deveria ser extraída do projeto. Eu estou tentando ver se eu lembro de algumas questões aqui, mas eu acho que eu consegui falar amplamente. Nós vamos ter vários debatedores, grandes especialistas que vão conseguir tratar com muito mais precisão e autoridade do que eu sobre o tema. O que eu gostaria de deixar claro a todos é o seguinte. Quando nós estamos fazendo uma lei, e eu vou ter a ousadia aqui de falar para legisladores em relação a isso [risos], mas eu entendo que a elaboração de uma norma ela visa atender a uma resposta que a sociedade precisa. Quando nós estamos falando de Direito Penal, existe uma questão chamada paz social. O Direito Penal visa a paz social.

Então, o que nós temos que fazer é realmente ter uma norma que seja clara, precisa, objetiva, eficiente, que condene e puna o agente. E único e exclusivamente o agente. Aquele que vai fazer do uso da internet, aquele que vai se aproveitar do uso da internet para obter algum proveito ou prejudicar outrem. Nós não podemos correr jamais o risco de ter numa norma penal, sobretudo, que condutas do uso normal da internet ou condutas que possam ser equiparadas ao uso normal da internet em última análise possam ser consideradas crimes, porque aí nós não vamos estar atendendo ao objetivo da paz social muito antes pelo contrário. Nós vamos estar correndo o risco, sim, de estar dando, de querendo tocar para matar o macaco tocar fogo na floresta. E aí nós vamos prejudicar a própria rede. Nós temos uma internet, senhoras e senhores, que eu costumo dizer, a internet brasileira é uma internet de primeiro mundo. Pena que ela é para poucos. Pena que ela é para muito poucos. Infelizmente. Eu espero que esse projeto ele proteja essa internet desses poucos para que mais possam ser acrescidos e a gente tenha realmente um ordenamento jurídico mesmo no âmbito cibernético que isso possa ser bem protegido. Porque eu não quero correr o risco de ter uma norma que prejudique esse crescimento. Principalmente porque nós temos que levar em consideração, os provedores de acesso à internet foram massacrados nesse País nos últimos anos, são pequenas empresas que funcionam muitas vezes em pequenos Municípios. E que atendem àquela determinada localidade com muita dificuldade. Esses provedores eles têm que ser homenageados. Têm que ser prestigiados. E não correr o risco de ter ainda mais oneradas as

suas atividades porque eu entendo que isso significaria morte dos provedores e dos pequenos provedores de acesso à internet para o País que são pequenas empresas nas localidades.

Bom, eu espero ter sido claro [soa a campainha] nas minhas colocações, e acho que cumpri meu tempo, Senador, e agradeço imensamente a oportunidade.

E queria fazer aqui uma observação especial ao Senador Eduardo Azeredo pela coragem. V.Exª teve a coragem de colocar em pauta um assunto de grande relevância para o País. Eu tenho certeza que depois de superado todos os debates e essa lei for realmente aprovada da forma como tem que ser aprovada, a história vai fazer uma referência ao senhor por ter enfrentado o tema. Muito obrigado a todos.

SR. PRESIDENTE SENADOR VALTER PEREIRA (PMDB-MS): Bom, eu quero crer que o... Todos aqui entenderam que o Dr. Bechara não está fazendo apologia do crime contra o macaco e nem contra a floresta. [risos] Então, o próximo expositor será o Dr. Demi Getschko.

SR. DEMI GETSCHKO: Bom dia a todos. Eu agradeço o convite de estar participando dessa Mesa tão importante e interessante. Eu estou muito honrado com isso. E contrastando com os dois que me antecedem, que fizeram uma abordagem extremamente jurídica e adequada do projeto, eu vou tentar dar uma visão um pouco mais conceitual do ponto de vista de alguém que trabalha na área da internet, e que de alguma forma faz apologia da internet como um novo cenário que vai ser extremamente importante para todos nós.

Então a primeira coisa que eu queria fazer, é tentar fazer uma abordagem do ponto de vista geral, uma abordagem da floresta, e não das árvores, sem os macacos ou com os macacos, e tentar mostrar que alguns conceitos precisam ser tomados com devida cautela.

É claro que o projeto trata de redes de computador, mas também é claro que a internet hoje é a Rede, com maiúsculo, que causa essa discussão que nós estamos travando hoje. Nós não estaríamos discutindo isso se tivéssemos com as redes proprietárias que havia nos anos 60 e 80 e cada empresa cuidava dela e tudo mais. Então a rede internet é um ser diferente do que nós conhecíamos nos anos 80, 70, e ela tem algumas características que são muito interessantes e difíceis de mapear, e difíceis às vezes de entender ou de lidar com elas. Ela é uma rede mundial, ela trabalha com a colaboração de inúmeros atores, quer dizer, ela funciona porque todos colaboram em mantê-la no ar, esse todo são dezenas de milhares, centenas de milhares mantenedores de pequenas redes que fazem a gestão de pequenos segmentos da rede, de grandes segmentos da rede, de redes de países, redes de *backbone*, em suma, de pedaços de rede que falam entre si e que se mantém coordenados. Essa coordenação é muito leve, mas é

fundamental para que a rede funcione como algo uniforme e para todos.

Então o primeiro comentário que eu faria é em cima de algumas impostas que foram comentadas aqui, que são verdadeiras, mas a tese que eu derivo delas não é a mesma que foi derivada aqui. Então vou dar um exemplo, sem dúvida nós temos um problema muito grande de *fishing*, temos um problema muito grande de *spam*, temos um problema muito grande de fraudes e de vírus. Mas essa é uma rede mundial, se nós tivéssemos em um País perfeito, se nós tivéssemos zero em geração de *spam*, zero geração de vírus, zero geração de *fishing* dentro do País, isso reduziria o total para 95% do que é hoje, e não 100%. Então a nossa participação nisso é pequena. E nós não podemos solucionar esse problema simplesmente agindo em cima da comunidade brasileira. Quer dizer, se todos brasileiros a partir de amanhã gerarem zero *spam*, nós vamos receber 90% do *spam* que nós recebemos hoje, porque essa é a participação brasileira no total desse tipo de ilícito.

Então a primeira coisa que eu quero dizer é que os números que foram apontados são verdadeiros, mas a solução dos números não está em nossas mãos. Quer dizer, nós não temos como melhorar esse cenário do 100 para o zero atuando localmente. A rede é uma rede mundial e ela precisa de atuação mundial.

O segundo ponto que eu queria tornar claro e colocar em discussão e que me deixa um pouco desconfortável em relação ao projeto é que eu acho que a rede tem alguns atributos que são extremamente interessantes para o desenvolvimento social.

Então, tivemos uma pesquisa que o comitê gestor apoiou que o IBGE fez, e deu uns resultados muito estranhos que a gente precisa, digamos, dedicar um certo tempo de meditação para poder entender. Por exemplo, dos Estados brasileiros, o Estado que apontou a rede com maior porcentagem como uso educativo, é o Amazonas. Por que o Amazônia usa rede para se educar e os demais Estados essa porcentagem é menor? Porque provavelmente o primeiro acesso de um usuário à rede, a primeira vez que alguém entra na rede ele busca lá a informação. Ele não busca ação. Ele não quer fazer um blog ou escrever ou tomar uma atitude. Ele procura ver as notícias do dia, o que tem acontecido.

Então, precisamos tomar muito cuidado em proteger o aspecto visitante da rede. Eu acho que a rede, primeiro, não é nossa, então nós não podemos dizer quem pode ou não acessar a rede porque a rede não nos pertence, é a mesma coisa dizer quem acessa o ar que é usado para transmitir a minha voz chega até vocês pelo ar. Mas o ar não é controlado. O que eu fala é responsabilidade minha. Mas o ar em si não. Então a rede é o meio pelo qual a informação flui de um lado outro. O pessoal que usa a rede para se informar é o pessoal que vai à banca de

jornal para ler uma revista, que vai a uma biblioteca, que vai aonde for. Esse pessoal não pode ser tratado como o pessoal que é ativo na rede. O pessoal que é ativo na rede é o pessoal que pode gerar uma transação, que pode causar um dano, que pode propagar uma calúnia, coisa assim. O primeiro ponto que eu diria é esse.

O segundo ponto é o seguinte, muito bem, foi dito que o Brasil é um participante importante de ORKUT e outras comunidades. E com isso descobriram um monte de ilícitos, vários ilícitos e delitos que são praticados ali. Eu vejo de uma forma positiva. Por que é que eu vejo de uma forma positiva? Porque a expressão digital permitiu-nos rastrear delitos que provavelmente não foram criados porque a rede existe. Mas foram expressos pela rede e, portanto, permitiram que fôssemos atrás deles.

Então, em vez de ver eles como ponto negativo, veja quantas comunidades que fazem apologia à droga foram encontradas no ORKUT. Não. Isso é uma forma de se ir atrás desses delitos e eventualmente coibi-los de alguma forma. Se não houvesse essa abertura via exposição aberta das intenções do indivíduo, nós estaríamos num cenário muito mais difícil.

E aí eu vou dar um segundo ponto que acho importante. Nós temos, por exemplo, um fator na rede que eu chamo aqui de fator evanescente que é o seguinte. A rede é mundial. O pessoal usa a rede aqui enquanto ela for confortável. Quando deixar de ser confortável eles usam em outro lugar. Vou tentar exemplificar pelo registro brasileiro. Os domínios do Brasil costumam terminar em ponto BR. 90% dos domínios do Brasil terminam em ponto BR. 10% não termina em ponto BR. O pessoal que tem domínio termina em ponto BR ele dá os seus dados para registrar o domínio. Então nós temos o CNPJ dele, o CPF quando é pessoa física, temos endereço, temos telefone, temos e-mail de contato. Ele dá isso ali voluntariamente porque ele quer esse ponto BR. Ele acha importante essa marca distintiva. Se nós obrigarmos ele a dar muito mais dados do que a gente obriga hoje ou exigir que ele apresente credenciais que de fato provam que ele não tem antecedentes ou raio que for, [ininteligível] provocássemos uma diminuição da informação que nós temos via ponto BR que o pessoal vai se registrar em domínios que não são ponto BR. Isso não vai gerar uma melhor qualidade da nossa informação. Ao contrário, vai gerar uma menor relevância do que nós temos de informação sobre a internet brasileira. Então se nós queremos ter informação sobre a internet brasileira, este é um caminho de duas mãos. Nós temos que ser adequados e equilibrados no que pedimos para contarmos com a contribuição dos internautas. Nós não temos como forçar eles a usarem o BR. Eles podem usar o que eles quiserem.

Então, a internet ela é evanescente. Nós espremos num lugar eles vão para outro lugar. Então existe uma utopia que se nós fizermos

um controle completo de quem entra ou deixa de entrar nós teremos um melhor controle... Não. Perderemos informação que nós temos hoje. Porque vários incomodados vários inocentes que se sentirão digamos abusados no tipo de exigência que fazemos a eles, procurarão uma saída mais simples, uma solução mais... Menos onerosa a eles em todos os aspectos. Onerosa financeiramente, onerosa socialmente, onerosa em termos de privacidade, onerosa em termos gerais. Então essa é uma consideração que nós temos que ter sempre em mente. Nós não estamos legislando sobre as estradas do Brasil, sobre o limite de velocidade das estradas do Brasil. Nós estamos legislando sobre algo que escapa do braço brasileiro no seu contexto geral. Um exemplo na prática. Nós tivemos aí uma decisão judicial proibindo um vídeo de uma conhecida artista brasileira prevaricando na praia. A decisão judicial cortou o acesso ao site onde esse conteúdo estava exibido.

Bom, com isso o que se fez? Primeiro, se eliminou o acesso a população de uma porção de conteúdos que eram totalmente diferentes àquele e que a população queria acessar. Segundo, os que realmente queriam ver o vídeo continuavam vendo. Porque existem "n" formas técnicas de driblar isso aí. Então não é verdade que essa vedação foi efetiva do ponto de vista legal.

Então, sem entrar no mérito da decisão que acho que é perfeitamente razoável que se condene ou não, se tome a decisão sobre isso, disse que a medida não teve a eficiência que se esperava dela porque se imaginou que poderia simplesmente bloqueando determinando canal internacional se impediu acesso a um determinado vídeo quando se pode apoiar em outros caminhos. Quem quiser ver aquilo ia conseguir continuar vendo. Essa é a característica da rede que às vezes esquecemos que está aí.

Aí tem trechos que falam mais ou menos isso, dizendo que a rede não tem fronteiras, a legislação dificilmente aplicável localmente, e às vezes até o próprio crime pode ser questionável. Quer dizer, em alguns lugares, por exemplo, o consumo de álcool é crime e outros lugares não é. Existe uma rede que faz apologia a bebidas alcoólicas pode ser considerada criminosa em alguns países do mundo e em outros não. Poligamia pode ser considerada crime em alguns lugares e em outros lugares não. E como é que você identifica onde isso está sendo praticado é uma coisa complicada que eu não tenho competência para discutir, mas certamente meus antecessores aqui na Mesa já o fizeram com grande propriedade. O que eu faria é esse comentário do Gilmore, que é um comentário técnico dizendo que isso exatamente que eu comentei sobre o caso do vídeo, uma censura na rede, a rede trata como se fosse um defeito técnico e contorna aquilo. Quando você tenta vedar o caminho a arquitetura da rede é tal que ela tenta procurar um caminho alternativo. Ela simplesmente considera aquilo, caiu um link,

tem um defeito na rede, vamos dar a volta. Essa é a postura que a tecnologia em geral adota nesse caso.

Bom, essa contribuição, digamos, bastante humilde perante exemplificando a minha falta de competência para dar contribuição na área, mas acho que realmente poucos delitos são novos e que existem na verdade novas formas de praticar velhos delitos. Eu reforço a característica de colaboração que a internet tem e que nós deveríamos sempre aplicar esses princípios. Eu acho que a internet tem riscos, apresenta riscos para crianças, apresenta riscos para pessoas que usam transações, e a gente acha que existe tecnologia que tenta consertar isso. E nós estamos vendo isso todo dia. O próprio registro brasileiro agora criou um domínio específico para Bancos chamado B ponto BR que vai ter um negócio chamado DNSSEC, que é um DNS seguro, que vai impedir que o nome seja fraudado na hora de resolver nome para número. Existem várias formas de tentar melhorar a confiabilidade das transações utilizando a tecnologia. Eu não excluo a necessidade de legislação. Acho que é muito bem vindo, são muito bem vindos projetos que conceituem e que punam novos delitos que são os delitos da rede. Acho que existe um grande espaço para isso nessa parte de código malicioso, e de coisas que são específicas da rede. Só que o meu alerta aí seria que não ligássemos isso com tecnologia porque tecnologia muda muito rapidamente e sem dúvida pode levar a lei a se tornar obsoleta e inadequada em pouco tempo. Então no caso específico do projeto o comentário é de que devemos ter em mente essas características e tentar então eliminar trechos da coisa que podem ser um problema.

Só para fazer de novo um comentário em relação aos números, os números de *fishing*, de *scam*, são números de denúncia. Não quer dizer que tudo aquilo tenha virado de fato ocorrência. Até o número de denúncias crescer, pode indicar que mais usuários estão identificando os ataques. E não que mais usuários estão sendo vítimas de ataques. É diferente. Quer dizer, o número de denúncia mais gente começa a ficar aculturada em relação o que a rede está causando e começa a notar que alguns e-mails do tipo você recebeu um cartão de boas festas, nem sempre é exatamente que o assunto da mensagem diz.

Eu termino com três frases de um pessoal bom da área, dizendo que sem tirar a importância de termos uma legislação específica em relação a isso, nós devemos tentar desenvolver uma solução que envolva tecnologia ética e legislação.

Então, certamente aqui o assunto é legislação, mas eu trago à Mesa essa característica de que a legislação em si sozinha não conseguiria resolver esse problema. A rede como eu falei já tem uma gestão que é uma solução política, essa é a frase do Mitch Karpor que é o cara que fez 1 2 3, o Lost(F) 1, 2 e 3 dizendo que a arquitetura é política, e termina com uma frase do Jon Postel que realmente é um dos

pais da rede e que faleceu nove anos atrás dizendo que nós devemos ser liberais no que aceitamos e conservadores no que fazemos.

Então a minha mensagem no caso do projeto é o seguinte, nós temos um novo universo não claramente identificado florescendo, o Brasil está muito bem nesse cenário, é muito bem visto internacionalmente, tem se expandido maravilhosamente nisso, o exemplo do Imposto de Renda, por exemplo, é um exemplo claríssimo. Quer dizer, os brasileiros têm usado a rede para tudo. O setor bancário brasileiro é extremamente evoluído melhor que a maioria países desenvolvidos, e tem tecnologia para fazer frente a essas coisas. Muitos conceitos que nós temos hoje mudarão por causa da rede, conceito intelectual pode mudar, modelo de economia, vejam, por exemplo, telefonia, telecomunicações em cima da rede. Isso tudo está mudando rapidamente. Então nós temos que ser grandiosos, temos que pensar grande quando tentarmos legislar nessa área para não sufocar, digamos, o florescimento da rede através de mecanismos que podem ser obstrutivos.

Para citar dois ou três pontos específicos do projeto que eu acho perigosos, por exemplo, o projeto que fala de código malicioso ou de código que se insere no micro, precisaria levar em conta códigos que são inseridos sem o conhecimento do usuário. Se levarmos isso ao pé da letra boa parte das aplicações de transação mesmo bancárias já ofendem esse princípio ao introduzir no seu micro interfaces específicas para se garantir. Então já estão ilegais eventualmente perante essa lei O usuário que é infectado por um vírus é potencialmente criminosos por estar difundindo algo que não é intenção dele. Certamente não é essa a intenção da lei. Eu tenho certeza que não é essa o objeto. Mas eu diria sou favorável a uma discussão mais ampla nesse contexto internet, tentando olhar a floresta num ponto grande para que detalhes que possam ser melhorados sejam melhorados. Porque uma vez promulgado de uma certa forma um texto, ele pode ser usado de uma forma destorcida que fugiu à intenção nobre dos que o propuseram e com a qual nós estamos totalmente de acordo. Então, são esses meus comentários, e agradeço o tempo aí. Obrigado.

SR. PRESIDENTE SENADOR VALTER PEREIRA (PMDB-MS): A Mesa agradece o expositor. Só diverge dê dele num ponto. Que o Dr. Demi Getschko é uma das maiores autoridades de internet que nós temos no mercado e ele se postou com tanta humildade. A sua contribuição foi substancial para aclarar todos aqueles que vão avaliar esse projeto que foi... Que está em discussão.

Mas o próximo expositor é o Dr. Paulo Quintiliano. Com a palavra o Dr. Paulo Quintiliano que é perito criminal do Instituto Nacional de Criminalística do Departamento de Polícia Federal.

SR. PAULO QUINTILIANO DA SILVA: Bom, boa tarde a todos. Primeiramente eu gostaria de agradecer aos Srs. Senadores, e demais pessoas presentes essa é a oportunidade de participar nesse momento.

Bom, então eu vou procurar ser breve, atender dentro dos 10 minutos.

Bom, então gostaria inicialmente de fazer uma retrospectiva com relação à questão dos crimes cibernéticos. A minha exposição será mais voltada para o aspecto da necessidade que nós da polícia, a Polícia Federal temos em termos da investigação da perícia nos casos de crimes cibernéticos.

Bom, então no início o que surgiram, os primeiros crimes cibernéticos, os criminosos eles eram muito... Eles eram mais românticos, praticavam os seus ilícitos mais com a finalidade de mostrar para os outros que eles eram os melhores, que conseguiam burlar as maiores seguranças e conseguir invadir os *sites* mais seguros e provar para os outros grupos que eram os melhores. Mas, hoje o criminoso do espaço cibernético atua exatamente com o objetivo de obtenção de vantagem financeira ilícita. Nas várias operações que temos feito isso fica bem claro que esses criminosos querem realmente obter vantagem financeira ilícita por meio da internet. E para tanto, eles utilizam vários tipos de golpes.

Bom, eu estive em 2004 numa conferência em Santiago do Chile, onde a representante do BANCO MUNDIAL naquela época afirmou que os golpes praticados por meio do espaço cibernético já movimentava mais dinheiro do que o tráfico de drogas. Naquela época. E seguramente isso vem aumentando. Ou seja, é cada vez mais e mais, se praticam crimes por meio do espaço cibernético. As tradicionais quadrilhas, por exemplo, assaltantes a Bancos e outras, eles estão migrando as suas atividade para os seus espaços cibernéticos. Eles fazem o quê? Estão coptando os jovens que entendem muito de informática ou entendem alguma coisa de informática para comporem a quadrilha e fazerem essa parte mais técnica dos golpes. E inclusive nesses casos, nessas quadrilhas que atuam golpes financeiros, a gente percebe claramente isso. E por que é que isso acontece? Porque na verdade, o crime cometido por meio da internet, é muito mais, vamos dizer, muito mais seguro. O criminoso não vai precisar trocar tiro, de enfrentar a polícia de forma trocar tiro armado, não. Eles vão apenas fazer uso de um teclado, de um mouse, do computador e da rede e vão conseguir muito mais sucesso em suas ações criminosas. Vão obter a vantagem financeira com muito mais facilidade e muito maior volume, muito mais rapidamente, sem grandes riscos.

Bom, com relação à lei, ao Projeto de Lei, desde 96 nós esperamos ansiosos para ter uma lei que trate especificamente dos crimes cibernéticos. O primeiro Projeto de Lei todos sabemos é do Deputado Cássio Cunha Lima e desde então a gente acompanha de

longe ou às vezes mais de perto a evolução desse trabalho legislativo. E realmente estamos ansiosos para que tenhamos essa lei aprovada. Em vários outros países já existem leis específicas que tratam desse assunto. Temos uma rede de contato 24/7 com vários países e a gente sempre tem oportunidade de trabalhar de fazer cooperação policial direta com eles para facilitar o trabalho de investigação de criminosos cibernéticos, especialmente quando dois ou mais países estão envolvidos na situação.

A República Dominicana participa dessa rede também e eles já nos avisaram que mandaram até cópia e foi aprovada uma lei específica tratando desse assunto.

Bom, o fato é que a cada dia que passa novos golpes surgem, novas tecnologias cada vez mais avançadas e sofisticadas surgem. E que são naturalmente utilizadas para o bem, para o conforto das pessoas. Mas também estão sendo utilizadas largamente para o crime por meio do espaço cibernético. E isso realmente é preocupante e há realmente a necessidade de uma ação governamental para o enfrentamento desse tipo de ação criminosa. E agora já temos a questão do *mobile bank* que é considerada a terceira onda da automação bancária que certamente já está sendo atacada fortemente pelos criminosos do espaço cibernético. E que possivelmente com grande possibilidade esses criminosos terão muito sucesso nesse tipo de ataque visto que nas duas primeiras ondas eles também tiveram. A primeira onda foi aquela dos ATMs, aquelas máquinas onde você não precisaria mais entrar nas agências, pode fazer os saques. Então naquelas ATMs o golpe mais utilizado é que eles plantam um chips conhecido como "chupa-cabra", e que todas as pessoas que vão fazer acesso àquelas máquinas tem as suas informações de senha, número de conta e tudo gravado naquele chip. A pessoa então pega aquele chip e clona os cartões e enfim personifica todas as pessoas e movimentam a conta, tiram, fazem saque, transferem dinheiro das contas e tudo mais.

A segunda que é o *homebank* também foi e está sendo fortemente atacado com muito sucesso. Os criminosos movimentam milhões e milhões de reais, quadrilhas estão espalhadas em todo o País e fazem ataques diuturnamente de forma eficaz.

Então, o crime cibernético infelizmente ele está tendo muito sucesso. Os criminosos estão movimentando quantidades cada vez maiores e maiores de volume financeiro.

SENADOR EDUARDO SUPLICY (PT-SP): Permite, Sr. Presidente, se o Paulo Quintiliano puder quantificar um pouco essa informação e precisar... Se o senhor puder dizer um exemplo típico do crime cibernético. O senhor está dizendo hoje que eles estão movimentando milhões e milhões. Se puder dar um exemplo

quantificável para que tenhamos idéia da gravidade. Na sua própria exposição, por favor.

SR. PAULO QUINTILIANO DA SILVA: Perfeito. Então eu disse inicialmente que o BANCO MUNDIAL já em 2004 afirmou que o crime cibernético já movimentava àquela época mais recurso financeiro de forma ilícita e criminosa do que o tráfico de drogas. De forma exemplificativa, nós tivemos uma operação, Cavalo de Tróia dois, salvo engano, mas acho que é isso mesmo, em que foi estimado que os criminosos subtraíram cerca de 200 milhões de reais. Se não me engano esse é o número. Já tem algum tempo. E em pouco tempo. Não sei se foi em um ano e meio, um ano e alguma coisa assim. No Brasil.

Então, é um volume muito grande que eles estão movimentando. Bom, então são crimes que fazem uso de tecnologia, e nesse sentido é importante que as pessoas, os peritos e demais policiais envolvidos no trabalho de investigação, perícia e combate a esses tipos de crime eles estejam sempre atualizados. A tecnologia evolui muito rapidamente, a questão de treinamentos, de equipamentos, tecnologias, aquisição, é uma necessidade grande que nós temos. Então estamos a todo momento buscando novos conhecimentos para fazer, para enfrentar os criminosos.

Bom, então os pontos frágeis que... Os principais pontos frágeis que existem na rede, vamos assim dizer, que dificultam o trabalho do combate, do enfrentamento a esses tipos de crimes basicamente são aqueles pontos sem registro. Inicialmente conhecidos como *airpoint ports*, ou seja, pontos de aeroportos, porque inicialmente não sei quantos anos, talvez uns seis anos começaram nos aeroportos eles instalaram aquelas máquinas onde você colocava uma moeda, uma cédula e tinha acesso completo à internet sem nenhum registro, ou seja, de forma completamente anônima. Ninguém tinha registro de quem fez uso da internet naquele local. E os criminosos sabendo disso vão a esses pontos para praticar as atividades criminosas em que dificulta e muito o trabalho da investigação. Como também os conhecidos como cibercafés, que são locais públicos de acesso à internet, e que muitos deles não têm registro ainda. Sei muito bem que já no Estado de São Paulo e em Mato Grosso já existem leis que obrigam os provedores a fazerem registros dos seus usuários. Eles têm que apresentar documentação, nome, etc, para que possam fazer uso da internet.

Eu estive na Itália, lá, e fiz uso de cibercafés de vários deles e em todos os locais eles exigem a documentação, eles escaneiam a sua identidade, passaporte, o que quer que seja e tem o registro da hora que você iniciou e terminou o seu uso em cada uma das máquinas relacionado ao IP. Então dessa forma em caso de um crime ter ocorrido naquele local, é muito fácil você identificar o autor após o trabalho de investigação. Agora, não havendo essa identificação, realmente dificulta

o trabalho da polícia. Outro aspecto de fragilidade é a questão das redes sem fio. Redes wireless. Já foi feito trabalhos de verificação inclusive na cidade de São Paulo onde foi a equipe com carro e verificar, foram rastrear as redes e um percentual muito grande dessas redes não tinha nenhuma proteção. Ou seja, o criminoso ele pode fazer uso dessas redes, rastrear uma rede dessa, fazer uso da rede e cometer todo tipo de crime que ele quiser e quando tiver a notícia, e a polícia for fazer a investigação, vamos chegar no IP daquela casa, ou do escritório onde tem a rede. Mas a pessoa não está sabendo, ninguém sabe. Quem fez foi o criminoso nas proximidades, acessou a rede e praticou todo tipo de ação criminosas que queria. Então esses são aspectos frágeis que têm que ser trabalhados para que facilite e possibilite o trabalho da polícia de investigação, e determinação de autoria dos crimes.

Bom, então ainda agora com relação à lei, realmente nós que trabalhamos nessa área de perícias, de investigação de crimes cibernéticos, realmente sentimos muito a necessidade de uma lei que preencha essas lacunas, que entendo que esse Projeto de Lei está preenchendo. Pois existem muitos fatos que hoje são atípicos, que na verdade a gente não pode fazer nada. Como, por exemplo, a própria... O próprio acesso sem autorização a sistemas de informações, porque hoje essa ação, essa conduta hoje atípica, o que ocorre é que quando a pessoa, o internauta ganha acesso sem autorização a um sistema de informação, normalmente ele não se contenta com isso. Ele vai querer ir além, vai querer destruir alguma coisa, querer pichar ou atacar a honra de alguém e aí sim ele vai ser enquadrado. Mas a conduta de ele simplesmente ganhar o acesso hoje a gente não pode fazer nada. E a gente tem inclusive por meio da rede 24/7 temos recebido solicitações de cooperação policial internacional de alguns países, principalmente os Estados Unidos, onde internautas brasileiros cometem esse tipo de ação ilícita, mas que a gente não pode fazer nada que não é crime. Outro fato é a difusão de códigos maliciosos, obtenção de dados forma indevida, a divulgação de informações obtidas em banco de dados de forma indevida.

Então, entendemos que é muito importante a aprovação dessa lei e isso seguramente vai nos ajudar muito no nosso trabalho. Pois vamos ter uma ferramenta útil e necessária para o desenvolvimento de nosso trabalho.

Bom, então era essa a nossa colocação, e muito obrigado pela oportunidade.

SR. PRESIDENTE SENADOR VALTER PEREIRA (PMDB-MS): Agradecemos a contribuição do Dr. Paulo Quintiliano, e o próximo é o Dr. Eduardo Fumes Parajo, Presidente da Associação Brasileira dos Provedores de Acesso, Serviços e Informações da Rede Internet, ABRANET.

SR. EDUARDO FUMES PARAJO: Obrigado, Presidente. Gostaria de agradecer o convite e agradecer também aos Senadores presentes.

Bom, queria aqui colocar um pouco a ABRANET no contexto. A ABRANET é uma entidade que nasceu em 1996, com o início da internet comercial no Brasil. A internet começou um pouquinho antes, em 95 já tinha alguns provedores atuando. Hoje a associação representa mais de 300 entidades, provedores, empresas, instituições de ensino, profissionais da região do Brasil, e tem como principal objetivo aí estar desenvolvendo a internet no Brasil auxiliar os associados, questão operacional, legal, representatividade junto a autoridades governamentais e tudo mais. Uma atuação hoje junto ao comitê gestor no Brasil, que é, vamos dizer assim, o principal órgão que está ligado à internet, além de outras instituições que também nós temos relacionamento.

Queria dizer que a internet no Brasil vai muito bem. Hoje, de acordo com o IBOPE/Net Ratings, em abril de 2007 nós somos mais de 33 milhões de usuários de internet. Isso quer dizer que a evolução aí em poucos anos, três anos, já dobramos a quantidade de usuários conectados à internet. Hoje nós somos líderes já. O Brasil é líder hoje em tempo de acesso à internet. Superando Estados Unidos, França, Espanha, países de primeiro mundo hoje o Brasil já é líder. Fonte IBOPE/Net Ratings também. Em média 21 horas conectados mensalmente.

Bom, no e-business não precisa nem dizer, né. O comércio eletrônico na rede é uma coisa, felizmente apesar de todo o processo e tudo mais, está um espetáculo. Só no primeiro quadrimestre desse ano já se fala em 2.1 bilhões pela rede. Então estima-se que no final do ano temos mais de 10 bilhões de e-commerce, B2C, B2B, tudo que a gente puder imaginar. Isso dá um panorama geral de como está indo a internet no Brasil.

Bom, é importante ressaltar que na primeira fase da internet nós estávamos focados aí na classe A e B. 96. 97. Aonde a classe A e B detendo mais poder econômico tinha condição de estar comprando computador e acessando a internet. Havia problemas regulatórios, ágil para aquisição de linha de telefone, custo dos computadores, três reais um dólar, dificuldade de aquisição de PCs, de softwares, e aí a conclusão o seguinte: além de todos esses problemas nós tínhamos uma questão de analfabetismo digital. Pouquíssimas pessoas, pouquíssimos usuários tinham conhecimento de como utilizar a internet. Isso complexidade de software, de conexão, as linhas telefônicas eram ruins, tinha uma série de problemas. A ABRANET, a primeira Associação Nacional Brasileira que vem defendendo os provedores, tem um quadro diretivo hoje bastante atuante, tecnologia, mercadológico, educacional, jurídico e marketing. Hoje nós estamos com um canal aberto mantendo sempre uma comunicação com todas as outras entidades de classe,

associativas, federativas, com finalidades convergentes. Mas o mais importante aqui, a ABRANET também ela não está só defendendo a questão dos provedores. Acho que nós temos que observar bem o usuário de internet brasileiro. Então hoje eu colocaria aqui para vocês o seguinte, estamos defendendo os usuários de internet no Brasil, pois acreditamos que sem esses plenamente satisfeitos, nenhuma de nossas empresas que representamos terão seus objetivos sociais e econômicos realizados e o Brasil não se desenvolverão nessa área. Não adianta ter nossos provedores, nossas empresas, os fins econômicos e nós não termos usuários.

Outro dado importante, o Brasil hoje é um dos países que tem o maior custo para conectar internet. Fiz um comparativo aqui só a grosso modo, chegamos em média a ser 10 vezes mais caro que países desenvolvidos a questão do nosso principal insumo que é acesso ao *backbone*.

Então, para vocês verem a dificuldade que hoje os provedores de acesso à internet têm nessa questão. 10 vezes mais caro no mínimo. No acesso usuário final, um outro dado importante, nós somos um dos mais baratos do mundo. Se você for comparar em relação a Estados Unidos, Europa, o Brasil em média 20, 30% no mínimo mais barato. Temos até internet gratuita. Então você imagina, custos 10 vezes maiores e menor mensalidade acesso internet no mundo. É um milagre o nós fazemos efetivamente.

Bom, falando do Projeto de Lei do Senador Azeredo, eu gostaria de colocar alguns pontos importantíssimos, já que o... Desculpa, esqueci seu nome. Quintiliano. Colocou bem a questão financeira disso aí. Acho que vai muito além. Acho que nós temos alguns aspectos dentro do Projeto de Lei que não estão sendo observados os custos que representarão para a internet no Brasil. Não estou falando só de provedor de acesso, estou falando de toda a sociedade, Governo, empresa, provedor. Todo mundo vai ter um custo muito grande na implementação disso. Por quê? No art. 21 fala que nós teremos que guardar as informações de conexões realizadas para a indenização do usuário. Isso não fica claro que a obrigação é só dos provedores. Se vocês prestarem atenção, todos os responsáveis pelo provimento de acesso à rede de computadores terão por obrigação guardar por três anos todas as informações de conexão realizada. No nosso entendimento na sua casa hoje você ter um banda larga e tem mais de um computador, dois computadores, isso já é uma rede de computadores.

Então, quer dizer, você pode ter um problema aí de estar afetando não só o mercado de provimento de acesso, porém todo o setor, todo mundo que utiliza a internet. Aí eu vou fazer algumas continhas aqui, o custo para o setor hoje, estou falando só de provedores aqui, fizemos alguns cálculos estimativo que cada usuário

em média, só estou falando log de acesso, quer dizer, o usuário entra na internet e sai. Só esse log. Essa informação. Fizermos um levantamento junto a nossos associados, e mais ou menos isso utiliza 20 megabytes de informação por ano. Um custo de armazenamento de mais ou menos 40 centavos por usuário/ano, então nós temos uma conta de 13 milhões e duzentos mil reais mais ou menos só para armazenar logs. Dinheiro que poderia estar sendo investido pelos provedores na ampliação do seu acesso, no atendimento ou coisa desse tipo. Com relação a outro parâmetro importante que nós gostaríamos de deixar claro é que os provedores já têm atuado em conjunto com o Ministério Público Federal, inclusive, e no Estado de São Paulo, e nós estamos criando uma forma de ter um consenso dos provedores na área para que se mantenha no mínimo tez três anos de log de acesso. Então quando eu mostrei aqui os 13 milhões, os provedores estão dispostos a colocar esse investimento para manter essa informação disponível. Todo mundo está indo na linha de ter um parâmetro para manter os logs de acesso por três anos de guarda, para que isso seja possível ser verificado a partir da conexão no acesso.

Questão da identificação do usuário, no art. 21, conforme a gente pôde verificar, uma das opções que a gente verificaria seria a questão da certificação digital. Tecnicamente falando essa seria uma das hipóteses que nós teríamos condições de ter uma rastreabilidade do usuário, saber que o próprio usuário é aquele lá. Mas infelizmente a nosso ver isso é totalmente inviável. Se pensarmos hoje em 33 milhões de usuários, um a custo estimado mais ou menos de 130 reais por um certificado digital, nós consultamos o site do SERASA para ter uma base, nós estamos falando de uma conta de quatro bilhões e duzentos milhões, muito aquém de qualquer outro valor que possa ser...

SENADOR EDUARDO AZEREDO (PSDB-MG): Presidente, pela ordem. Você podia me dizer onde está escrito isso no art. 21? Não existe aquela informação ali que a solução técnica sugerida pelo Senador Azeredo não consta aqui no 21.

SR. EDUARDO FUMES PARAJO: Nós demos uma lida no parece que foi encaminhado pra nós e dentro da resenha didática--

SENADOR EDUARDO AZEREDO (PSDB-MG): Então não consta do art. 21.

SR. EDUARDO FUMES PARAJO: Não, não. Eu estou falando que uma das soluções técnicas.

SENADOR EDUARDO AZEREDO (PSDB-MG): Então não está.

SR. EDUARDO FUMES PARAJO: Não está.

SENADOR EDUARDO AZEREDO (PSDB-MG): Então, vamos colocar com clareza que isso não está no art. 21.

SR. EDUARDO FUMES PARAJO: Isso. Ok, além disso, Senador, aproveitando, desculpe a... Nós recebemos a semana passada um documento que seria a resenha para nós estarmos discutindo hoje. Infelizmente hoje na hora que nós chegamos aqui no Senado nós recebemos um outro documento. Que nós não tivemos tempo de dar uma analisada com mais detalhe.

SENADOR EDUARDO AZEREDO (PSDB-MG): Me desculpe, Presidente, também não bate com a verdade. O que ele recebeu e que não tinha é apenas a Emenda do Senador Flexa Ribeiro que tira a questão da defesa digital. Apenas essa alteração.

SR. EDUARDO FUMES PARAJO: Bom, mas nós não tínhamos recebido. Bom, continuando aqui eu queria colocar para vocês o seguinte, tecnicamente falando. Será que a certificação digital vai resolver o nosso problema? Será que o usuário ter o seu e-CPF ou a sua impressão digital aí efetivamente vai resolver? Fizemos uma outra consulta aproveitando essa consulta. No próprio site do SERASA ele deixa claro no certificado que existe sim risco de identificação do usuário. Além disso, ele coloca um limite para o certificado.

Então, quer dizer, eu compro um certificado digital achando que eu vou estar protegido, no entanto efetivamente pode ser que eu não esteja de acordo com o próprio site. Pode ter um erro na identificação do usuário. E aí ele limita o valor que ele pagaria num eventual problema desse, em 40 mil reais. Numa conta de quatro bilhões e duzentos milhões. Conclusão, obrigar a certificação do usuário para atender o Projeto de Lei é promover a exclusão digital. Ou seja, poderão arcar com esses custos e mesmo assim não terão 100% de garantia. Tem os dados da fonte do site do SERASA para acesso. O art. 163 A que fala a respeito dos códigos dos maliciosos, nossa preocupação é o seguinte, Senador, estamos agora falando da inclusão digital, da classe C, D e E que não tem acesso a recursos, não tem acesso a computador, felizmente o Governo colocou o programa do computador para todos, isso está facilitando. No entanto, os softwares necessários ou coisas necessárias necessitam de maior investimento. E esse usuário não vai ter. Então como é que nós vamos incluir essa classe D e E que não têm recursos.

Então, por exemplo, se nós falarmos a respeito do Projeto de Lei, quer dizer, o usuário que tiver o seu computador, recebeu um vírus como foi citado aqui o caso sem ter conhecimento e propagar esse vírus na internet está previsto que ele vai ter uma pena de três a cinco anos de prisão. Quer dizer, sem o conhecimento. No entanto, se ele comete um crime intencionalmente, a pena é menor. De um a três anos.

Então, existem pontos importantes que nós precisamos efetivamente estar olhando--

SENADOR EDUARDO AZEREDO (PSDB-MG): Não é assim. O Juiz de Direito está aqui presente depois poderá esclarecer melhor. Não é assim. Existe diferença entre crime culposo e crime doloso.

SR. PRESIDENTE SENADOR VALTER PEREIRA (PMDB-MS): Eu solicitaria ao Senador Azeredo que aguardasse a hora dos debates anotasse os questionamentos...

SENADOR EDUARDO AZEREDO (PSDB-MG): Eu estou anotando. É só porque no momento as pessoas que estão assistindo possam exatamente saber que algumas questões não estão... Não sei se ele está lendo ainda talvez o início do projeto, porque tem coisas que estão totalmente superadas. Não existe a palavra certificado digital aqui. Então não tem porque mostrar curso de certificado digital quando o art. 21 não fala em certificado digital. São questões que acho importante serem colocadas que nós estamos discutindo o projeto, a necessidade do projeto, da implantação do projeto. Nós tivemos a presença, a colaboração do antigo Presidente da ABRANET, o Antônio Tavares, ele concordou com esses três anos aí, agora não sei se... Não está de acordo, está de acordo, ao mesmo tempo que fala que é caro guardar três anos, ele diz que guarda três anos em São Paulo. Se pode guardar em São Paulo, pode guardar para o Brasil todo.

SR. EDUARDO FUMES PARAJO: Desculpe, Presidente, posso? Nós concordamos em guardar três anos de log de acesso, Senador. Acesso. A entrada do sujeito na internet, usuário e saída. Agora, nós temos que olhar--

SENADOR EDUARDO AZEREDO (PSDB-MG): Mas o projeto é só isso.

SR. EDUARDO FUMES PARAJO: Olhar mais profundamente pra ver se é só isso mesmo que abrange. Francamente eu não sou Advogado e não vou poder responder isso para o senhor.

SENADOR EDUARDO AZEREDO (PSDB-MG): Também não sou Advogado. Mas o que está só isso e pode ser guardado em CD-ROM. Não é para guardar online, não. Então não precisa daquele custo todo não porque vai ser guardado em CD-ROM. Vai guardar fora.

SR. EDUARDO FUMES PARAJO: Ok. Bom, mas voltando ao ponto que eu estava colocando, se nós formos pensar na classe D e E, na inclusão digital no Brasil, e essas pessoas necessitarem de ter serviços de anti-vírus, anti-spyware, justamente para combater essas pragas virtuais, um e-mail que venha ou vírus, então quer dizer, nós levantamos um custo aproximado de 65 reais por ano para uma licença de software anti-vírus, se nós pensarmos que o potencial hoje de usuários obviamente é menor a quantidade de computadores, quer dizer, um usuário utiliza um computador do outro, coisas desse tipo, mesmo assim nós temos uma conta de 528 milhões de reais em

investimento de softwares para estar prevenido para o anti-vírus ou combate, ou *fishing*, ou que seja.

Queria colocar também uma outra coisa a respeito da questão da denúncia de condutas delituosas. É um tema até que eu já abordei aqui. Eu acho o seguinte, nós já tivemos um trabalho e temos um trabalho constante na questão da evolução da internet no Brasil. Nosso objetivo é colocar mais gente na rede. Esse é o nosso principal objetivo. O nosso foco é esse. É dar um bom atendimento para o nosso cliente, se possível ajudar, nós temos pequenos provedores hoje espalhados por todo o Brasil. E esses provedores chegam ao ponto de treinar o usuário de como ele acessa a internet.

Então a minha conotação aqui é o seguinte, se nós já fazemos esse trabalho e temos isso como objetivo principal, eu não vejo como nosso papel exercer um papel de polícia, já disse isso em várias entrevistas, para ter ficar canalizando denúncias e repassar isso para a autoridade competente. A polícia já existe. Está aí o nosso amigo da Polícia Federal. O objeto dele é investigar. Correr atrás. Se alguém se sente atingido ou se teve alguma fraude, essa pessoa é que vai ter que denunciar. Não o provedor. Nós hoje fazemos um trabalho junto ao Ministério Público de São Paulo com relação a crimes que isso é crime contra a humanidade. Pedofilia e racismo. Nesses dois itens hoje nós somos atuantes sim, nós pegamos a informação assim que nós recebemos a denúncia, nós temos a condição nesse sentido de fazer uma análise se aquilo existe ou não. Porque é fácil. Se alguém denunciar para o provedor: Olha, tem uma página de pedofilia no seu site, eu tenho condição de ir lá e olhar. A análise para nós fica muito mais simples. Agora se o cara ligar pra gente e ligar tem alguém roubando minha conta. Como que eu vou entrar na conta do sujeito para olhar se está sendo roubado ou não para daí passar isso para autoridade competente? Então, nosso ponto é esse. Nós queremos, sim, ajudamos todas as solicitações que são emitidas pelo Judiciário, pela polícia, os provedores fazem a rastreabilidade, passam as informações para a polícia, já existe até um acordo de alguns casos do Judiciário que não precisa a polícia fazer a indagação, nós já começamos a monitorar aguardando a questão da ordem judicial para estar cumprindo. Então efetivamente acho que isso aqui não é um ônus que nos compete. Nós já temos o nosso foco, nós temos o nosso objetivo e o nosso objetivo é se Deus quiser colocar 100% da população brasileira na internet.

Por último, eu gostaria de colocar aqui, e isso voltando na questão dos valores, o custo que nós possivelmente podemos ter por essa questão. Então nós temos lá 13 milhões e duzentos mil para armazenar, os provedores estão se movimentando nesse sentido para estar cumprindo essa determinação, isso é importante deixar claro. Nós queremos colaborar, sim, com a justiça, queremos sim que os criminosos sejam punidos. Não achamos que a internet... A internet

tem que ser livre. Mas não impune. Então tem que ficar claro. E por isso que nós vamos fazer esse investimento anual pra estar guardando os logs. Se formos basear uma questão tecnológica para monitorar nosso usuário, saber que ele é ele mesmo, e já diz no site do SERASA que não dá para ter certeza se ele é ele mesmo, a própria certificadora deixa claro isso no site. Aí nós precisaríamos investir 4 bilhões e 290 milhões por ano para ter essa certificação. Quem vai pagar essa conta? A sociedade? Esse custo vai ser repassado para alguém.

Bom, continuando na linha de anti-vírus, anti-spyware mais 500 milhões. Obrigação de encaminhamento de denúncia nós teremos que montar uma central dentro do provedor para captar essas denúncias. Quer dizer, nós sairíamos completamente do nosso foco hoje de atender bem o cliente, de fidelizar o cliente, de ensinar o cliente a acessar a internet para ficar captando denúncias.

Resumo, senhores. Nós estamos falando de quase cinco bilhões de reais por ano. Aí nós estamos discutindo a questão tanto da inclusão digital. Como que nós vamos gastar cinco bilhões para fazer essa questão [soa a campainha] se nós temos que efetivamente estar monitorando ou olhando, ou guardando essa informação? Então acho o seguinte, acho que infelizmente vou corroborar aqui com os colegas da Mesa, nosso objetivo é melhorar, Senador, não é só criticar. A idéia nossa é ajudá-lo para que a gente efetivamente tenha uma lei que possa ser exeqüível. Esse é o nosso objetivo.

Eu queria terminar com dois pontos importantes. Não adianta, isso que o Dr. Demi colocou muito bem, não adianta nós fecharmos a torneira do Brasil, pessoal. Senhores, nós vamos botar a lei aqui, o bandido vai para Argentina, vai para o Chile, vai para Venezuela. Vai para onde ele quiser. Ele vai continuar cometendo crime. Se as quadrilhas estiverem bem organizadas da forma que o nosso amigo aqui da Polícia Federal disse, elas vão se organizar em qualquer outro País. E vão fazer as fraudes bancárias. Não tem jeito. A não ser o quê? Nós vamos desconectar o Brasil da internet? É isso? Nós vamos tirar o Brasil do mapa da internet, vamos redesenhar toda a infra-estrutura, fazer tudo isso? Então, não adianta efetivamente só colocar uma lei. Nós temos que pensar muito bem porque a ramificação disso é muito grande. Eu vou dar um exemplo prático. Ele pode ir para um paraíso fiscal que não tem lei nenhuma, montar a quadrilha dele lá, continuar roubando senhas, e estar efetivamente aplicando os golpes. Se você for analisar hoje alguns sites que nós temos vistos, alguns processos, os sites que capturam as informações do cliente bancário, estão fora do Brasil. Então, o que a lei vai resolver disso? É um ponto importante.

E eu gostaria de terminar aqui colocando uma frase aqui que eu li do Vint Surf(F) que é um dos pioneiros da internet, vou seguir as colocações do Demi, e que eu acho que a gente tem que pensar muito na questão da inclusão digital. Se nós pensamos em incluir classes D e

E na internet, que acho que é o futuro, é o que o nosso País precisa pra estar globalizado, para estar competitivo, para estar educado, a internet pode ser efetivamente o meio? Então a frase do nosso amigo Vint Surf(F) é o seguinte, a exclusão da internet caça os direitos dos usuários de participarem da maior revolução da história da informação. E é o que estamos vivendo. A internet trouxe essa revolução. Hoje eu vejo quantos dos nossos provedores, micro provedores, às vezes com um funcionário, o proprietário e um funcionário, é o proprietário e a esposa dele que trabalha. O trabalho que eles fazem localmente em comunidades que não são assistidas.

Então, temos que pensar muito bem. A nossa idéia é que esse debate evolua e que a sociedade possa estar contribuindo. Porque como eu disse, não são só os provedores que vão ser afetados, o Brasil vai ser afetado. Obrigado.

SENADOR EDUARDO AZEREDO (PSDB-MG): Presidente, antes só de passar para o próximo, só para ficar bem claro para o Senador Suplicy também, é que na verdade naqueles cálculos colocados ali, dos quatro milhões e setecentos, quatro milhões e trezentos são de certificação digital. Não existe, eu gostaria que o Dr. Eduardo Parajo depois mostrasse, mas ele mesmo já concordou. Não existe a palavra certificação digital no Projeto de Lei.

Então, aqueles números todos caem por terra. O custo na verdade é menos de 1% do que está listado ali, já que o custo com *spyware*, isso é um custo normal. E com relação à denúncia, eu quero só lembrar o que está inscrito aqui. Informar de maneira sigilosa autoridade policial competente denúncia da qual tenha tomado conhecimento, e que contém indícios de conduta delituosa na rede de computadores sob sua responsabilidade. Então não tem nenhum papel de policial para o provedor nada não. É só se ele receber uma denúncia, ele faça como fazem em São Paulo no caso de racismo, no caso de pedofilia. Que ele também informe. Não vejo aí também nenhuma mudança de função do provedor, de maneira que eu queria só esclarecer porque senão fica o quadro ali e aquele quadro não bate com a realidade. O quadro não é correto.

SR. PRESIDENTE SENADOR VALTER PEREIRA (PMDB-MS): Vai ter o debate. Vamos ouvir o outro expositor e depois o senhor participa do debate. O Senador Azeredo com certeza ele não quer perder o *timing*. Certamente receoso de que possa haver cobrança de tantos operadores no Brasil então ele já está preocupado com isso, com as cobranças.

Mas o último expositor vai ser o Tiago Tavares, que está aqui. Enquanto ele se arma lá nós agradecemos aqui a contribuição do Sr. Eduardo, Presidente da Associação dos Provedores de Acesso, ABRANET.

SR. TIAGO TAVARES NUNES DE OLIVEIRA: Sr. Presidente, Srs. Senadores, Senador Eduardo Suplicy, Senador Eduardo Azeredo, senhoras e senhores. Para nós da SaferNet é uma honra muito grande comparecer a esta Audiência Pública. Queríamos deixar registrado o nosso profundo agradecimento à Senadora Serys Slhessarenko por ter tido a iniciativa de apresentar um Requerimento aditando a lista de convidados desta Sessão.

Rapidamente eu gostaria de registrar que a SaferNet é uma Organização Não-Governamental sem fins lucrativos ou econômicos, fundada por um grupo que reúne professores e pesquisadores das áreas de ciência da computação e de direito. Portanto, nós somos vinculados à Universidade Federal da Bahia e Universidade Católica em Salvador. E atuamos com a missão de defender e promover os Direitos Humanos na internet. E somos os idealizadores de um projeto chamado Central Nacional de Denúncias e Crimes Cibernéticos que recebe denúncias anônimas de crimes e violações contra os direitos humanos praticados por meio da internet. Essa central de denúncias é operada em parceria com o Ministério Público Federal, que tem acesso integral e irrestrito ao nosso banco de dados, e é o receptor das notícias crime que nós produzimos e que nós encaminhamos.

Para a minha intervenção, eu gostaria de iniciar por três premissas que considero necessárias. A primeira não é minha. Mas sim do sociólogo Émile Durkheim, quando diz que onde há sociedade, há crime. Então não é surpreendente que exista crime na internet. Ou que a internet seja utilizada como meio para a prática de crimes. Por quê? Porque é rede. Ela muito antes de ser uma rede de computadores, ela é uma rede de pessoas. Uma rede de pessoas interconectadas entre si através de laptop, através de computadores de mesa, através de celulares. Ou seja, a internet ela é na sua essência um espaço de socialização. E em todo o espaço de socialização existe conflito. Conflito de ordem econômica, conflito de ordem social, conflitos de gênero, conflitos étnicos e etc. E esses conflitos quando exacerbados muitas vezes descambam para o crime. Então, não é, portanto, surpreendente que exista crime na internet, uma vez que a rede é um espaço de socialização.

A segunda premissa que considero necessária é de que a internet é e pelo menos o nosso desejo é de que ela continue sendo, um espaço neutro e livre. O que eu quero dizer com isso? Eu quero chamar atenção dos senhores para o fato de que a internet ela é o que é e ela chegou onde chegou porque não existe controle prévio de conteúdo na rede. Ou seja, a todo usuário da internet, é dado o direito de publicar o que quiser sem pedir autorização prévia a ninguém. Logo, nós não temos na internet um controle editorial prévio de conteúdo, assim como nós temos nas redações de jornais, assim como nós temos nas redações de revistas, etc. Para você publicar um artigo ou matéria no jornal, o editor

do jornal tem que aprovar aquele artigo. Uma matéria em um meio de publicação na imprensa tradicional, aquele conteúdo tem que ser aprovado previamente antes de ser veiculado. Na internet não existe isso. Qualquer um que esteja conectado à rede pode exercer o seu livre direito de liberdade de expressão e opinião diretamente sem precisar pedir autorização a ninguém. Evidente que o efeito e a conseqüência lógica disso é de que esse direito pleno ao livre exercício de liberdade de expressão ele serve para o bem e para o mal. A esmagadora maioria dos usuários usa essa característica, se valem dessa característica de neutralidade e liberdade da rede para publicar conteúdos saudáveis, conteúdos lícitos, conteúdos que agregam informação e conhecimento à humanidade. A maior enciclopédia já construída pela humanidade é uma enciclopédia livre. E se chama Wikipédia, e é produzida de forma colaborativa por milhões de pessoas espalhadas no mundo. Esse sistema operacional que estou usando aqui, e esse software com o qual estou fazendo minha apresentação, ele é produzido de forma colaborativa por uma comunidade de desenvolvedores espalhada no mundo que hoje já chega à marca de um milhão e meio de desenvolvedores de softwares de projetos cadastrados. Ou seja, estou usando aqui o sistema operacional GNU/Linux e o pacote de escritórios OpenOffice. Que é uma opção tecnológica inclusive adotada pelo Governo brasileiro.

Terceiro e última premissa que considero necessária, é de que a vida humana ela é mais importante que o patrimônio. É uma premissa óbvia, e que dispensa explicações. Mas que eu quero deixar registrado. O problema. Crimes transacionais. Como enfrentá-los a partir de legislações e jurisdições nacionais? O Dr. Paulo Quintiliano explicou de forma muito didática e precisa como se dar o *modus operandi* do crime cibernético. É muito comum você ter um criminoso em um País A praticando um crime contra um cidadão ou uma instituição localizada em um País B, usando a infra-estrutura tecnológica situadas geograficamente num País C. Isso cria uma primeira dificuldade. Que é a de definir a legislação aplicável, e obter os meios e as provas necessárias para comprovar a materialidade do crime e os indícios de autoria. Foi citado aqui a questão do uso dos provedores e acessos e conteúdo fora do País para... Como meios preferenciais para a prática de crimes. Na SaferNet nós recebemos no ano passado 356 mil, 213 denúncias de crimes e violações contra os direitos humanos praticadas por meio da internet. Dessas, 95% refere-se a perfis de comunidades criminosas no serviço ORKUT, que também foi citado aqui. O serviço ORKUT é um serviço de propriedade do grupo econômico Google que mantém uma filial no Brasil e que mantém a sua infra-estrutura tecnológica localizada geograficamente nos Estados Unidos, mais especificamente no Estado de Dealer(F) na Califórnia. E sob esse argumento durante muito tempo a empresa Google Brasil se recusou a fornecer os dados necessários à identificação de pedófilos, neonazistas,

racistas, que usam o serviço ORKUT para praticar crimes no Brasil, contra brasileiros, e, portanto, sob responsabilidade, sob competência submetidos, portanto, à legislação brasileira e à autoridade policial brasileira. Esse é um problema. O mundo tem se questionado como resolver isso. Esse é um modelo dos chamados Internet Hotlines ou canais nacionais de denúncias. Nós somos o ponto de presença no Brasil de uma rede que reine hoje 26 países em torno do combate à pornografia infantil e aos crimes de ódio. Esses canais de denúncias eles cooperam entre si e também cooperam com as autoridades. No nosso caso aqui temos uma estreita colaboração com o Ministério Público Federal, mediante termos formais de cooperação assinados, e também com o Departamento de Polícia Federal. A nossa função em hipótese nenhuma é a de substituir, fazer investigações ou substituir o trabalho policial ou substituir, se vestir de poder de polícia. Pelo contrário. A nossa função é fornecer à autoridade policial e fornecer ao Ministério Público a matéria prima que essas autoridade precisam para poder desempenharem bem o seu trabalho. E essa matéria-prima é informação.

Então, nós redigimos notícias crimes e relatórios técnicos e encaminhamos esses relatórios para as autoridades. Eu trago aqui para os senhores um exemplo de um Relatório datado de 21 de fevereiro de 2006 que foi encaminhado para o Departamento de Polícia Federal e que retrata um fenômeno que se tornou infelizmente muito comum no Brasil, que é a vingança privada na internet. Ou seja, o exercício arbitrário das próprias razões, o crime de justiça com as próprias mãos. Usuários da rede que se investem desse poder de polícia começam a exercer funções que não cabem a um cidadão. Pessoas que começam a pichar páginas, começam a desenvolver scripts, começam a desenvolver ferramentas com o objetivo de capturar logins e senhas, com o objetivo de alterar dados armazenados em computadores, em servidores, com o objetivo de recolher informações de dados pessoais, e com isso perpetrar as suas ações que consideram legítimas, mas que são ações ilegais. Aqui esse relatório está consubstanciado em casos concretos, esse relatório alerta as autoridades para o fato de que na época existiam mais de 50 mil pessoas diretamente envolvidas nessas práticas chamadas de vingança privada na internet e aqui um estudo de caso que mostra como as conseqüências da atuação desses indivíduos. A destruição das provas e esse caso aqui é um caso que envolvia a pornografia infantil, eles atacaram o álbum de fotografias e com isso comprometeram as provas. As provas que foram obtidas e foram mencionadas acima são provas ilegais, porque elas foram obtidas ao arrepio da lei, elas foram obtidas sem autorização judicial, o suposto IP desse criminoso que foi publicado no ORKUT também é uma prova que pode ser facilmente invalidada em juízo e os próprios criminosos resolveram criar um site para poder receber informações de páginas e

criar um índice público para que eles pudessem agir por sua própria conta e resolver digamos aqueles delitos, punir aqueles crimes.

Então nós estamos diante de uma situação em que um indivíduo, um técnico, normalmente, um técnico em informática, ele ao se defrontar ao caso de pornografia infantil, que é o caso aqui, ele aplica a lei, interpreta a lei, julga, e aplica, executa a pena. Sem a participação do Estado. E eu estou citando isso, senhores, porque uma das medidas previstas no projeto substitutivo em análise era o tal da chamada defesa digital. O conceito de defesa digital que nada mais faz de que institucionalizar a possibilidade de que um agente técnico ou--

SENADOR EDUARDO AZEREDO (PSDB-MG): E claro que foi acatada a Emenda a esse e não está mais em discussão.

SR. TIAGO TAVARES NUNES DE OLIVEIRA: Concordo e agradeço, Senador. Eu ia fazer menção--

SENADOR EDUARDO AZEREDO (PSDB-MG): Perfeito, então não está mais em discussão.

SR. TIAGO TAVARES NUNES DE OLIVEIRA: Perfeito. Eu ia fazer menção a essa Emenda supressiva do Senador Flexa Ribeiro acatada por V.Exª que retirou do projeto esse dispositivo. Mas o fato, senhores, é que isso chegou a ser proposto. Chegou a ser proposto e caso não houvesse uma reação forte, contundente da sociedade como um todo, e eu me incluo no rol de críticos desse ponto específico e fiz esse posicionamento público e contundente por meio da imprensa, isso teria sido aprovado.

Então, eu gostaria de deixar, Senador, Presidente, esse relatório e pediria que fosse juntado aos autos dessa audiência para que ficasse como contribuição para que os outros Senadores possam avaliar propostas que acabam sendo incluídas no debate e que podem trazer conseqüências extremamente preocupantes.

Eu queria me adiantar e também solicitar que fosse anexado aos autos dessa audiência um relatório produzido pelo NCMEC que fala exatamente sobre harmonização legislativa a nível global. O NCMEC é um órgão dos Estados Unidos, esse Relatório foi produzido com a colaboração de mais de 45 países, com agências inclusive com a participação da Interpol e de várias representações diplomáticas ao redor do mundo e ele apresenta os principais pontos que devem ser considerados em relação à criminalização e a repressão do crime de pornografia infantil na internet. Ele faz o mapeamento por País e ele inclusive fala sobre a questão da obrigatoriedade dos provedores dessas obrigações incluindo aí a preservação de logs. Vemos que segundo esse Relatório que é de 2006, o Brasil não preenche três dos principais requisitos que é: Primeiro, a definição legal do que venha ser pornografia infantil. Dois. A criminalização da posse intencional. O Dr. Paulo Quintiliano está aqui e sabe da dificuldade da Polícia Federal em

prender pedófilos que mantém em seus computadores vídeos e fotografias envolvendo cenas de abuso sexual de crianças. Em que pese a lei ter sido alterada em 2003, o Brasil esqueceu de criminalizar a posse de pornografia infantil. A posse intencional. Então digamos que eu tivesse nesse computador um milhão de fotografias, isso não é crime. Já é crime na maior parte do mundo. Mas no Brasil ainda não é. E a Polícia Federal só pode na maioria das vezes cumprir mandados de busca e apreensão. Com o objetivo de uma vez recolhido o material, comprovar por laudo pericial se houve ou não distribuição daquele conteúdo. Se houve, houve o crime. Se não houve, não está configurado o crime.

Logo, aqueles computadores, aquele material apreendido terá que ser devolvido. Sem que aquele criminoso seja punido. E também a questão da atuação dos provedores e aqui é uma postura proativa dos provedores em encaminhar às autoridades a denúncias de pornografia infantil. Isso já existe em várias partes do mundo, nos Estados Unidos é o exemplo mais significativo desse aspecto, e aqui no Brasil também não existe. Em que pese existir o acordo celebrado com o Ministério Público Federal em São Paulo. Mas ainda não é lei e só vale para o Estado de São Paulo.

Então eu gostaria de caminhar para a minha conclusão, me referindo a um caso. O caso que eu pretendo focar é exatamente a questão da pornografia infantil, e aqui eu faço menção ao art. 227 da nossa Constituição Federal que diz que é dever da família, da sociedade e do Estado assegurar à criança e o adolescente com absoluta prioridade o direito à vida, à saúde, à alimentação, à educação, ao lazer, à profissionalização, cultura, dignidade, respeito, liberdade, convivência familiar e comunitária. Além de colocá-los a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão.

Esse aqui, senhores, é um site internacional, eu borrei as páginas porque essas imagens são absolutamente impublicáveis, ainda que numa reunião técnica. Porque elas envolvem crianças de seis meses, um ano, dois anos de idade sendo estupradas. Bebês que têm, são abusados sexualmente tem suas fotos. O registro desse abuso publicado na internet. Esse site foi denunciado na SaferNet, nós fizemos um rastreamento e identificamos que ele estava hospedado na República Tcheca. E vejam os senhores. Depois do tour macabro que expunha essas fotos, o site continha esse conteúdo, levava ao final para esse conteúdo. Eu peço desculpas por estar em inglês, mas vou fazer uma tradução simultânea. "Nós somos os reais provedores de pornografia infantil. Nós vendemos materiais como esse no passado para alguns sites amigos. Nós realmente tentamos promover a pornografia infantil para que mais e mais pessoas tomem conhecimento e a tornem mais popular. Mas o que você viu é uma pequena parte do

que realmente nós temos. Todos os meses nós gastamos, alguma, vez com mais freqüência entre mil e dois mil dólares para atualizar o nosso banco de dados. Esse tipo de negócio é muito caro. Mas nós temos dez anos de experiência com essas coisas. A nossa última atualização foi em janeiro de 2005. Foi a mais chocante atualização de pornografia infantil dos últimos tempos. Foi uma experiência realmente *hardcore*(F), impactante. O segredo na nossa longa existência é de que nós dominamos o processo nós mesmos. [soa a campainha] Sem intermediários. Desde a produção das fotos e vídeos até a busca por novos modelos, etc. Nosso site contém mais de 125 mil imagens de qualidade, mais de 5.700 vídeos de qualidade. Todos exclusivos - Atentem para o item seis - Nosso site é ilegal em todos os países. E por isso nós temos problemas de vez em quando. De vez em quando nosso site fica inacessível. Mas nós rapidamente efetivamente resolvemos o problema que costuma não exceder 24 horas. Muito importante. De nossa parte, tudo é absolutamente seguro. Nós não gravamos suas informações nem as forneceremos a ninguém. Nosso negócio *our business* depende da honestidade. Todas as fotos e vídeos na área de membros podem ser salvas diretamente no seu computador para posterior deleite. Nós somos as únicas pessoas sérias nesse negócio, nós somos os melhores, e se realmente você quer pornografia infantil, venha realizar os seus sonhos conosco. Atualmente nós temos mais de dez gigabytes de pornografia infantil e estamos crescendo". E aqui, senhores, a próxima tela que exige que o sujeito para ter acesso aos 125 mil fotos e 5.700 vídeos de crianças sendo abusada sexualmente paguem por meio de seu cartão de crédito um acesso exclusivo que custa 89 dólares e 99 centavos. O acesso a isso é feito mediante pagamento. Por meio de cartão de crédito.

Então, eu queria dizer que nós, no Brasil, temos que dar um passo adiante. Que já foi dado, por exemplo, nos Estados Unidos. Estabelecer mecanismos de cooperação não apenas com provedores, mas com todos os agentes e todos os atores que participam de alguma maneira ou que estão envolvidos ainda que por evidentemente não concordar com isso, desse processo, desse fenômeno criminoso. A operação marc(F) de 2003, que foi a maior operação no mundo de repressão a pornografia infantil e prendeu 1.700 pessoas e identificou 26 mil e quinhentos usuários na internet em 166 países. Identificou no meio desses 26 mil pessoas, 235 brasileiros que estavam comprando e vendendo pornografia infantil na internet utilizando-se de cartão de crédito e que por alguma razão não sei até onde nos consta não houve punição, não houve um avanço em relação à identificação desses 235 brasileiros e a posterior punição e condenação.

Então eu queria para encerrar sugerir que paralelamente à discussão sobre a responsabilidade dos provedores de acesso de conteúdo, que deve existir, nós defendemos a preservação dos logs por parte dos provedores de acesso, por parte dos provedores de conteúdo,

concordamos com esse dispositivo do projeto do Senador que prevê a retenção desses logs por três anos, é uma das matérias-primas para a investigação policial, nós concordamos com isso, mas consideramos que é insuficiente. Principalmente para reprimir o crime de pornografia infantil. A maior fonte de informação, a principal matéria-prima hoje para prender, identificar e prender essas quadrilhas é através do mapeamento do fluxo do dinheiro das pessoas que compram e vendem pornografia infantil na internet. E para isso é absolutamente necessário que haja uma colaboração dos agentes financeiros que fazem a intermediação desses pagamentos e que têm condição de estar colaborando com as autoridades na identificação desses criminosos. Eu fico por aqui e agradeço imensamente a atenção. Muito obrigado.

SR. PRESIDENTE SENADOR VALTER PEREIRA (PMDB-MS): Nós é que agradecemos a contribuição importante dada pelo Dr. Tiago Tavares, Presidente da SaferNet.

E agora vamos passar para a segunda parte, que é a parte dos debates. Encerrada a exposição, e o primeiro inscrito obviamente é o autor, Senador Azeredo.

SENADOR EDUARDO AZEREDO (PSDB-MG): Sr. Presidente, eu quero primeiro agradecer a presença de todos os expositores, acho que sem dúvida alguma é importante o que puderam trazer para nós continuarmos a discussão desse projeto. Nós já tínhamos tido uma Audiência Pública na Comissão de Educação antes dela ser aprovada lá, desse projeto ser aprovado lá, depois sofreu realmente uma série de alterações e depois tivemos outra discussão na Câmara dos Deputados. Vários debates em que eu pude participar. De maneira que eu considero que realmente essa discussão tem sido bem feita em todo o País e evidentemente chega o momento que nós temos que votar. Como bem colocou o Dr. Paulo Quintiliano, desde 96 nós estamos discutindo um projeto como esse.

Quer dizer, quando às vezes eu demonstro uma certa ansiedade é porque eu quero que o Brasil tenha uma legislação em consonância com que tem no resto do mundo. Eu participei recentemente a convite no conselho da Europa e eu pude ver que os países mais desenvolvidos todos eles estão, Dr. Paulo também estava lá, todos eles estão com as legislações sendo atualizadas em relação aos crimes cibernéticos. Então a minha pressa é nesse sentido. Eu evidentemente que estou pronto sempre a aceitar todas as sugestões ou as críticas que vierem. Já fizemos e aceitamos várias críticas. Eu acredito que, por exemplo, essa questão do nome real é um tema polêmico, e a semana passada a Alemanha estava começando a discutir isso lá. Tá bom. Deixa que a Alemanha discuta lá. Podemos discutir num outro projeto aqui. Eu pessoalmente continuo achando que o anonimato só interessa aos maus internautas e não aos bons internautas. Recentemente o jornal O Estado de São Paulo colocou que nos seus blogs agora exige o nome

real para poder alguém colocar o nome no blog. Então se tem que ser o nome real para usar um blog, o que dizer para usuário os computadores como um todo, o exemplo da Itália, é claro, no caso dos cibercafés.

Eu tenho algumas dúvidas aqui, no caso aqui dos provedores eu acho que eu já coloquei. Desculpe até de interromper o Dr. Parajo, mas é porque era no momento para mostrar que aqueles números não batem com a realidade porque nós não estamos falando em certificação digital. Quando estávamos discutindo a questão do nome real, realmente ali naquele momento nós estávamos colocando a questão de que uma das formas que os provedores poderiam autenticar o nome era exatamente através de certificação digital e isso evidentemente com o uso intensivo os custos cairiam, não seria mais aqueles custos ali, aqueles custos são custos de hoje e na verdade nós estávamos apenas colocando que a defesa do nome real ela poderia ser feita dessa forma.

Então, nessa questão. Então não tenho dúvida, acho que o custo nesse caso ele é muito pequeno em relação à segurança que trará para os brasileiros em geral utilizarem o sistema de tecnologia da informação.

Quero lembrar que nós não estamos falando apenas de rede de internet, o Demi colocou bem isso, mas é a rede mais importante, mas nós temos também nesse projeto a própria questão da clonagem de cartão de crédito, da clonagem de celular, são 11 tipos de crime que estão sendo descritos em seis códigos, em seis instrumentos penais que estamos fazendo essa alteração. E aí eu quero colocar essa questão realmente da criança e do adolescente, não sei se o Tiago sabe, eu fui Vice-Presidente da CPI aqui que analisou essa questão da pornografia infantil junto com a Senadora Patrícia Saboya e aquela CPI ela deu origem a vários projetos de lei, um deles trata exatamente dessa questão de que as operadoras de cartão de crédito elas possam informar devidamente quando tiver, o fluxo financeiro como um todo esse projeto alguns já foram aprovados aqui no Senado. Eles estão na Câmara agora. A nossa legislação da criança e do adolescente ela está atualizada em relação aos crimes cometidos na pornografia infantil, apenas a questão da posse já foi aprovada agora como adendo na Câmara. Vai chegar ao Senado e eu já conversei com a Senadora Patrícia para que a gente possa ter maior rapidez na questão da posse. Realmente apenas a posse é que não estava no Estatuto da Criança e do Adolescente. Então, sendo aprovado lá ele será incluído aqui.

A questão da legítima defesa digital, só fazendo um esclarecimento, ela foi colocada como um detalhamento da legítima defesa que existe no Código Penal. Quer dizer, eu também não sou Advogado, mas eu tenho me assessorado exatamente de consultores do Senado e nesse caso específico da defesa digital o que estava se detalhando que aquela pessoa poderia argumentar junto ao Juiz que ele agiu em legítima defesa digital. Não estava dizendo que ele podia fazer

o que quisesse, não. Em nenhum momento teve isso escrito. Agora, exatamente eu acatei a Emenda do Senador Flexa porque deixaremos que isso fique na legítima defesa geral do Código Penal. O Dr. Fernando é que pode explicar se isso atenderá bem. Era um detalhamento, esse detalhamento está sendo mal entendido, tiramos esse detalhamento. Mas em nenhum momento foi defendido a questão de que nós tivéssemos justiceiros, estava se buscando a proteção àqueles que tivessem que usar instrumentos de contra-ataque que eles então pudesse provar perante o Juiz. Mas eles estariam sempre praticando um crime o Juiz que ia dizer que não. Isso que seria a questão. Assim que funciona a legítima defesa como um todo. A legítima defesa se o sujeito dá um tiro, para todos os efeitos ele cometeu um crime. Agora, se ele mostrar que deu o tiro e foi em legítima defesa, o Juiz é que vai julgar isso. Então não está dizendo que ele pode dar tiro a qualquer momento.

Mas eu pediria talvez ao Dr. Fernando que pudesse essa questão do conceito de coisa que foi colocado pelo Marcelo Bechara, quer dizer, qual a importância de termos realmente essa questão do conceito de coisa que o dado está sendo equiparado a coisa. E pediria no primeiro momento essa informação para que pudesse clarear um pouco mais, e ainda... Acho que seria no primeiro momento apenas esse esclarecimento com relação ao conceito de coisa.

SR. PRESIDENTE SENADOR VALTER PEREIRA (PMDB-MS): Terminou? Algum questionamento?

SR. FERNANDO NETO BOTELHO: Senador, eu entendi na lógica, porque um critério de interpretação que nós fazemos absolutamente necessário, seja na estrutura só dessa lei seja na estrutura dela já no contexto do Código Penal é um interpretação sistêmica. Não tem como fazer uma interpretação de um dispositivo desse isoladamente e atendê-lo por si. Quer dizer, a lei tem uma capa organizacional, vocabular, mas ela vai ser interpretada naquilo que ela tem de espírito. A gente chama até da investigação da *mens legis*, da *mens legislatoris*, quer dizer, aquilo que passou no cenário do processo legislativo e qual é o foco buscado pela lei. Então ela tem aqui na interpretação sistêmica, quer dizer, fazendo uma conexão dos dispositivos eu entendi que a definição de coisa que está na lei está ligada à definição que ela também faz dos crimes contra o patrimônio. Inclusive do inédito crime de furto qualificado. Ela insere uma qualificadora do furto que é tradicionalmente, nós conhecemos o furto da história humana que é a apropriação de coisa alheia móvel e a retirada da coisa da esfera de posse do legítimo titular, ela então faz um esclarecimento que equipara-se à coisa porque ela define lá que vai ser furto qualificado o uso de sistemas eletrônicos para a apropriação de vantagem econômica equipara-se a coisa exatamente o sistema. Foi assim que fiz a leitura do dispositivo. Ou seja, conectado com o esclarecimento que cabe ao legislador para a informação da

interpretação de que a coisa está vinculada efetivamente aos dispositivos penais que tratam dela especificamente aos crimes contra o patrimônio.

SENADOR EDUARDO AZEREDO (PSDB-MG): Obrigado. Eu queria só colocar que intenção de qualquer lei ela tem que fazer uma descrição mais ampla, então as questões ligadas ao detalhamento, acho que foi bem colocado também que depois a jurisprudência é que vai criando a estrutura em várias alternativas. Nós não temos como ter uma lei que entre em detalhe de tudo. O senhor colocou também que essa jurisprudência que vai colaborar a partir do início de vigência da lei.

SR. FERNANDO NETO BOTELHO: Aliás, é de extrema importância pegando um gancho no que o senhor fala a respeito do que o Dr. Marcelo Bechara adiantou das ações que estão ditas ali repetitivas, criar e inserir, difundir, é uma tendência da legislação brasileira, às vezes, ser casuística na intenção vocabular de botar as ações todas e depois ela se delimitarem na jurisprudência, na interpretação dos tribunais de uma forma maior ou menor. Faz parte da cultura, acho que da cultura até latina nós sermos vocabulários. O americano usa uma expressão *Word*(F). Nós falamos muito da ação e deixamos pouco para que ela seja interpretada. Isso não tem funcionado muito. Na interpretação hoje, no moderno critério de interpretação das normas jurídicas, das normas constitucionais, nós estamos sendo educados, a estrutura judiciária brasileira está sendo educada hoje a interpretar a norma com a mais próxima finalidade dela do momento, do local, da realidade social, da realidade econômica.

Então, a repetição, Dr. Marcelo Bechara, que é um conhecedor da estrutura jurídica sabe disso, a repetição do verbo criar, inserir difundir delimita o que se chama na estrutura de direito norte-americano o *standart*, o padrão, dentro do qual nós vamos fazer a interpretação. Agora, os senhores não tenham dúvidas. Nós veremos esses dispositivos: criar, inserir, difundir código malicioso, verbos da ação, substantivos e adjetivos. Malícia. São valores ontologicamente extensos, não é Senador? Serão interpretados dentro da cultura do Tribunal, da cultura do julgamento, do caso específico e essa jurisprudência será profusa a respeito desse assunto. O que nós precisamos, o senhor me permite, e aí faço coro com que o Paulo disse, que trabalha na investigação preparatória da ação judicial que nós precisamos é do instrumento, da matéria-prima delimitadora desse arcabouço dentro do qual nós possamos interpretar. Porque nós não podemos fugir na certeza de que temos que cumprir e interpretar a lei. Agora, a forma como ela vai ser interpretada será seguramente extensa nesse sentido.

SR. PRESIDENTE SENADOR VALTER PEREIRA (PMDB-MS): Muito bem. Antes de passar a palavra ao próximo orador, aliás, orador

não, próximo questionador aqui que vai ser a Senadora Serys Slhessarenko, eu gostaria de prestar um esclarecimento técnico para que não paire nenhuma dúvida.

Essa matéria que nós estamos discutindo começa com um PL da Câmara, um Projeto de Lei da Câmara de autoria do então Deputado Luiz Piauhylino. É o projeto nº. 89 que vem de 2003. Segue com outro projeto de autoria do Senador Renan Calheiros, que é o Projeto de Lei do Senado nº. 76/2000. E o terceiro projeto é de autoria do Senador Leomar Quintanilha que é também do Senado, de nº. 137. E a relatoria é única, comandada pelo Senador Eduardo Azeredo.

Então o próximo inscrito é a Senadora Serys.

SENADORA SERYS SLHESSARENKO (PT-MT): Obrigada. Eu peço em primeiro lugar, Sr. Presidente, Srs. Senadores, senhores participantes dessa Audiência Pública tão relevante, pedir desculpas ao Senador Eduardo Azeredo, especialmente, como Relator, eu tive que me ausentar por outro compromisso aqui no Senado e só consegui chegar agora. Só participei do início e dos finalmente.

Em primeiro lugar dizer da importância desse projeto nós não temos dúvida do tanto que o Senador Eduardo Azeredo tem trabalhado, batalhado literalmente em prol de levar essa questão ao melhor termo. Que não é só a questão de a gente aprovar um projeto. É aprová-lo realmente com qualidade que venha atender os interesses, necessidades, aspirações da sociedade como um todo e não de alguns.

Um dos problemas, e aí eu peço desculpas por não ter assistido as exposições, só assisti do primeiro, Dr. Fernando, e eu sei que eu vou falar aqui vai ser repetitivo, por isso vou ser breve. O problema, por exemplo, que eu acho que está muito bem contemplado, Senador Eduardo Azeredo, que é a questão da clonagem dos cartões e cartões de crédito, celulares, etc, eu mesma já fui vítima inúmeras vezes. Eu já sou sem dinheiro ainda esgotaram toda a minha conta da CAIXA ECONÔMICA de um dia para o outro. Uma coisa incrível. Que eu só podia transferir mil reais por dia, acho que é isso e pode sacar mil por dia também. E na época os que fizeram, que esgotaram a minha conta esgotaram em três dias, tirando dois mil por dia, transferindo não sei quantos mil. Uma coisa que não dá para você entender. Se não pode, como é que o titular não pode, alguém lá pôde. Então eu acho que isso aí é uma questão que me parece que está bem amarrada já no projeto dentre tantas outras. Acho que é de extrema relevância.

Uma questão que eu já... O meu Assessor me informou que já foi bastante bem tratada aqui essa questão da pornografia infantil. Extremamente preocupante porque a criançada está toda aí na internet. As minhas netas e os meus netos tudo desse tamanhinho assim e todo mundo... eu não entendo nada, mas eles entendem tudo. Quer dizer, é extremamente complicado, como que isso passa e principalmente a

proliferação da pornografia infantil para os adultos fazerem uso desse tipo de coisa. Eu fui informada que acho que foi o Dr. Tiago que já leu um negócio que me estarreceu. É pago com o cartão de crédito. Isso aqui é uma outra amarração que tem que acontecer. Eu não sei se está bem amarrado, Senador Eduardo... Os dois são Eduardo. Eu chamo um Eduardo e os dois olham... [risos] Senador Eduardo Azeredo, essa questão do cartão de crédito. Deve ter uma forma, uma fórmula de também se evitar que isso possa ser feito através de cartão de crédito. Porque aqui, pelo menos esses documentos que eu recebi são cartões de crédito usando para pagar pornografia infantil. Eu não sei como isso já está amarrado, se é possível também dar uma trabalhada nessa questão.

Segundo, o winrop(F) organização que reúne canais de denúncias de 26 Países, existem 3.500 portais comerciais destinados a compra e venda de fotografias e vídeo de crianças e adolescentes sendo abusadas. Não sei se esses dados já foram colocados aqui. Esses dados realmente me assustaram, Senador. 3.500 portais comerciais destinados à venda de fotografias e vídeos de crianças e adolescentes sendo abusados. Quando eu participei da Comissão que o senhor já falou aqui, da CPI da Criança e Adolescente, o senhor deve, claro, nós vimos, barbaridades que a Polícia Federal tinha apreendido de pornografia em termo de crianças. Coisas que não dá pra gente pensar que dá um estado de ira tamanho. Eu acho que seria importante para combater a pornografia infantil seria interessante que se acompanhasse a Convenção de Budapeste, no que diz respeito à posse intencional e a responsabilização criminal dos agentes que fazem essa intermediação de compra e venda da pornografia infantil na internet. Eu diria que se a gente puder também fazer esse reforço, Senador, o senhor que vem fazendo esse esforço que eu já disse aqui, hercúleo, gigantesco, digno de louvor e que a gente tá dando o maior apoio. Às vezes o senhor pode achar que a gente tá perturbando um pouco, questionando e perguntando, mas é sempre tentando valorizar mais e mais o seu trabalho que realmente está tentando aprofundar e amarrar cada vez mais estes crimes, contra os crimes.

Combate à exploração sexual das crianças e adolescentes deve ser mais e mais rigoroso. Precisamos atacar em todas as suas frentes. Eu acredito que somente a penalização radical dos provedores não é suficiente. Nós precisamos ir além. Tem que ter mais intermediação, vamos dizer assim, nessa questão do risco de fazer com que se criminalize para ver qualquer coisa nesse sentido. E facilitar que a gente consiga realmente identificar. Que o grande problema é conseguir identificar os criminosos. Então que se consiga ainda nesse projeto, Senador, fazer com que essa coisa fique mais contundente em termos de identificação dos criminosos e radicalizar mesmo com a pornografia infantil. Essa aí é radicalizar. E radicalizar significa inclusive fazer com que não se possa mais, não possam aqueles que fazem isso adquirir,

fazer a compra através de cartão de crédito como nós temos aqui documentado através de cópias e xerox de que isso é verdadeiro, que isso está acontecendo. Eu acho que é por aí. Existem mecanismos, que mecanismos existem que se possa policiar mais ainda essa questão e realmente descobrir quem são os criminosos e puni-los severamente. Que mecanismos a mais pode se acrescentar? [interrupção no áudio].

SR. PRESIDENTE SENADOR VALTER PEREIRA (PMDB-MS): Pode responder.

SR. FERNANDO NETO BOTELHO: Senadora, a senhora me permite, pegando aqui um gancho a respeito da pergunta com que o Dr. Tiago disse a respeito exatamente desses crimes transnacionais. A senhora talvez não estivesse, mas o que a senhora apresentou foi mostrado pelo Dr. Tiago na tela. Basta ver para trazer esse espírito de rebeldia, de revolta. Nós queremos investigar onde está isso e tirar isso no ar. A verdade é o seguinte, nós não podemos imaginar, se não criamos um sofisma, quer dizer, nós não temos um direito transnacional, fora do País e não temos um nacional. É exatamente a conexão dos dois. Nós temos que buscar o direito transnacional, a Convenção de Cibercrimes da Europa hoje prevê hoje, aliás, é um ponto polêmico, ele será objeto sempre de discussão. Prevê a possibilidade de países solicitarem investigação policial nos outros. Mesmo não estando ali o criminoso. Agora, é necessário que o País detenha uma estrutura mínima legal interna. E aí vem a conexão. Porque senão eu vou criar o sofisma de que eu não tenho convenção externa porque não tem direito interno. Não tem direito interno porque não tem convenção externa. Se nós fizermos as duas coisas nós armamos internamente com o respaldo da convenção e se firmarmos a convenção nós criamos então a possibilidade da investigação transnacional. Esse é um ponto extremamente importante.

O outro é que a Emenda Constitucional 45, a famosa Reforma do Judiciário adicionou um parágrafo, se não me engano o terceiro ou quinto ao Art. 5° da Constituição Federal que estabelece expressamente hoje, isso é recente, que se nós firmarmos tratados ou convenções internacionais que tratem de direitos humanos ele tem força de Emenda Constitucional. Então nós podemos absorver uma estrutura forte, grande já, firmada na Europa, por exemplo, com força de aplicação constitucional tendo norma infra-constitucional aqui que pode ser exatamente essa que está sendo objeto da discussão.

SR. TIAGO TAVARES NUNES DE OLIVEIRA: Complementando, eu gostaria de chamar atenção também para a previsão contida na Convenção de Cibercrime, na Convenção de Budapeste em relação ao tema pornografia infantil. É sabido que o projeto substitutivo do Senador Eduardo Azeredo se baseia na Convenção de Cibercrime para poder criar os novos tipos penais, as novas condutas delituosas. Mas é fato que a legislação brasileira necessita de ajustes em relação à

criminalização da posse intencional da pornografia infantil e também daquele que adquire pornografia infantil e daquele que intermedeia a compra e venda. Então isso está previsto na Convenção de Budapeste. Mas não está contemplado no projeto. Como o projeto ainda está aberto à fase de recebimento de Emenda, etc, eu faria um apelo para que alguns dos Srs. Senadores, ou mesmo o próprio Senador Eduardo Azeredo, Relator do projeto, acrescentasse um dispositivo no projeto com o objetivo de harmonizar a legislação brasileira com a Convenção de Cibercrime no que se refere à pornografia infantil. E também levasse em consideração os resultados de uma pesquisa que nós fizemos em 2005 e que eu também peço ao Sr. Presidente que seja anexada aos autos dessa audiência uma pesquisa exatamente com esse objetivo de mapear os Projetos de Lei em tramitação na Câmara e no Senado, nós fizemos esse levantamento, chegamos àquele resultado, e ao final, no Relatório final da pesquisa nós fizemos uma proposição em relação aquilo que foi identificado como lacuna legislativa e aquilo que deveria ser contemplado ou pelo menos considerado nos Projetos de Lei em tramitação no Congresso.

Essa é uma questão urgente. Nós precisamos olhar com muita seriedade para esse problema sem esquecer do fato de que o fenômeno ele é transnacional, os números, as estatísticas comprovam que menos de 1% do conteúdo de pornografia infantil está hospedado em provedores brasileiros, menos de 1%, e que 99% está hospedado no exterior.

Então, de pouco adianta você ter logs de provedores brasileiros de conteúdo, porque eles não têm uma grande quantidade de páginas hospedadas no Brasil de pornografia infantil. A maioria dessas páginas está hospedada no exterior. Evidente que os acessos estão sendo feitos no Brasil. Então é fundamental que você tenha logs desses provedores de acesso, em que pese isso não ser também uma solução definitiva. Porque o sujeito ele pode discar para um provedor de acesso em um outro País, se conectar à rede através desse provedor de acesso em outro País e com isso o registro dessa conexão vai estar em outro País. Mas o fato é que se nós tivermos instrumentos que permitam que a polícia possa ter acesso às informações dos brasileiros que compram pornografia infantil na internet, e essa informação só quem tem são os agentes financeiros que fazem a intermediação da compra e venda, se a polícia estiver essa informação, certamente as investigações, a identificação da autoria ela fica muito favorecida e as prisões e as operações policiais certamente vão aumentar consideravelmente. Então eu gostaria de fazer uma sugestão. De que já que existe a previsão de que os provedores informem à polícia os casos envolvendo pornografia infantil, logo nada mais razoável do que estender essa obrigação para os agentes financeiros que ao tomarem conhecimento de que um cliente está comprando ou vendendo pornografia infantil na internet ele

também informe a polícia a identidade desse sujeito sob pena de responder civilmente, pagar uma multa, etc.

SENADOR EDUARDO AZEREDO (PSDB-MG): Presidente, perfeito. Acho que o Tiago coloca uma preocupação que é de todo brasileiro, que é essa questão da pornografia. O que eu quero insistir é que na verdade o projeto ele não é um estatuto contra o crime cibernético. Ele é na verdade uma série de alterações nos instrumentos legais já existentes.

Então, o Estatuto da Criança e do Adolescente já está harmonizado com a Convenção de Budapeste. Com exceção de um único ponto que é da posse, ele já fala em compra, já fala em divulgação, já fala em intermediação... Isso tudo já fala no Estatuto da Criança e do Adolescente. Então se nós fossemos alterar agora eu terei que fazer uma alteração no Estatuto da Criança e do Adolescente. Eu não ia fazer uma alteração no projeto. É uma alteração no estatuto. E como estatuto precisa apenas desse acréscimo da posse e a informação é de que a Câmara já fez isso num projeto. Então talvez seja mais rápido o que a Câmara está fazendo, alteração no mesmo... Eu ia fazer a mesma coisa. O que a Câmara já fez no estatuto é que eu proporia aqui também. Acrescentar no estatuto--

SR. PRESIDENTE SENADOR VALTER PEREIRA (PMDB-MS): De qualquer forma é bom observar, fazer o acompanhamento.

SENADOR EDUARDO AZEREDO (PSDB-MG): Sim, perfeitamente, é claro.

SR. PRESIDENTE SENADOR VALTER PEREIRA (PMDB-MS): Que se houver alguma lacuna podemos preencher.

SENADOR EDUARDO AZEREDO (PSDB-MG): Evidente que sim.

SR. PRESIDENTE SENADOR VALTER PEREIRA (PMDB-MS): Senador Eduardo Suplicy.

SENADOR EDUARDO SUPLICY (PT-SP): Sr. Presidente, Senador Valter Pereira, senhores convidados, quero cumprimentar a todos pelos depoimentos. Não pude assistir a todos porque eu estava na Comissão que estava tratando dos biocombustíveis e ouvindo hoje pela manhã os diversos depoimentos sobre a situação do trabalhador na agricultura da cana-de-açúcar, e quero cumprimentar também o Senador Eduardo Azeredo por este projeto que envolve uma complexidade grande e assunto que nem todos nós Senadores conhecemos tão bem.

Então, a contribuição que os senhores estão nos dando é de extrema valia. Eu sou daqueles que não sou um cibernético, um especialista na internet. Claro, uso e cada vez mais, quisera ter podido aprender desde a minha infância, mas foi algo que eu comecei a utilizar mais quando me tornei Senador, a partir de 91 e pouco a pouco mais e

mais comecei a... No ano 91 foi o primeiro ano em que batalhamos aqui e por um período longo, cerca de 100 dias para que o Governo do então Presidente Collor, depois de ter suspendido, Voltasse a prover o acesso aos Senadores ao Sistema de Administração financeiro da União. Mas é incomparável a utilização que nós hoje fazemos, a interação que temos. Ainda ontem à noite um dos principais jornais televisivos, o jornal da Globo, fez uma matéria sobre o número de e-mails que inúmeros Senadores estamos recebendo a respeito dos problemas aqui do Conselho de Ética. É algo que há cinco, seis anos atrás não tínhamos. Hoje cada um de nós Senadores recebemos centenas, às vezes mais de mil mensagens de e-mail do Brasil inteiro. Por cada um de nossos atos, de nossas palavras, de nossos votos aqui.

ORADOR NÃO IDENTIFICADO: [pronunciamento fora do microfone]

SENADOR EDUARDO SUPLICY (PT-SP): E alguns muito bravos. Mas outros muito estimuladores de nosso trabalho. Então, portanto, muitos dos fatos sobre os quais os senhores nos deram conhecimento hoje eu sinceramente não conhecia. Eu até quero também perguntar, Sr. Presidente, e nós vamos ter outras audiências porque se trata de uma questão de muita complexidade, estamos todos aprendendo a partir desta iniciativas e de toda essa complexidade de projetos, o Senador Eduardo Azeredo apresentou um substituto, uma primeira pergunta que quero fazer aqui é se antes de uma regulação jurídica, senão seria próprio termos e indispensável a construção de um marco regulatório destinado a regular os conteúdos, serviços e produtos independentemente de tecnologias. Uma outra pergunta acredito que essa--

SR. PRESIDENTE SENADOR VALTER PEREIRA (PMDB-MS): V.Exª específica bem a quem está dirigindo.

SENADOR EDUARDO SUPLICY (PT-SP): A primeira pergunta será para quem melhor se achar pronto para responder. A segunda pergunta ao Juiz Dr. Fernando Neto Botelho, como o senhor vê a aplicabilidade dos textos legal se aprovado tal na forma do substitutivo do Senador Eduardo Azeredo. Ao perito do Departamento da Polícia Federal, Paulo Quintiliano da Silva, se o monitoramento e obtenção de dados, que possam indicar cometimento de crime não se trata da atuação exclusiva do poder de polícia conferido às polícias federal, civil e militar. Eu gostaria ainda, no que diz respeito a algumas das informações que nos foram apresentadas, uma relativa à questão da pornografia e do texto que o Sr. Tiago Tavares Nunes de Oliveira nos apresentou daquele caso que tanto nos impressionou, o senhor mencionou que se trata de algo localizado na República Tcheca, e que há dez anos funciona.

Então, se foi possível detectar que está na República Tcheca, imagino que deva ser possível detectar qual a cidade, o Município de

onde se está transmitindo aquilo. Se não há justamente nos acordos internacionais relativos a se tentar coibir o problema da pornografia através da internet, pornografia infantil, ainda mais se não haveria com as autoridades do Governo tcheco, a possibilidade de se detectar isto de uma maneira mais adequada, inclusive com os instrumentos que hoje a polícia investigativa e com os instrumentos que tem normalmente acredito que tem e teria a tecnologia para detectar, e por que é que ainda não se documentou e para coibir aquele procedimento, se se trata de um problema de um melhor entendimento internacional, conforme o Juiz Dr. Fernando há pouco mencionava, ou será que as autoridades do Governo tcheco ali não estão preocupadas com este assunto.

Acredito que tenha sido, o Presidente da ABRANET, Eduardo Fumes Parajo, que nos deu uma informação a respeito do volume de multas. Não foi isso? De quatro bilhões e... De... Dizendo que o projeto se aplicado custaria algo como quatro bilhões e oitocentos... Eu gostaria de estar bem informado. Esta arrecadação que custará tanto, se aplicado o projeto na forma do substitutivo previsto por estes cálculos, então esta seria uma arrecadação na forma de multas que iria para quem? Seria de alguma forma seriam multas que, por exemplo, iriam para a Receita Federal? É uma possibilidade? Seriam multas que seriam para... Eu não entendo tão bem de... Para os proprietários de provedores, seriam multas que seriam arrecadadas pelas instituições financeiras... Eu não sei. Então gostaria de conhecer.

E ao Senador Eduardo Azeredo, então eu gostaria até que diante da resposta houvesse uma reflexão da parte de V.Exª para que possamos compreender inclusive... V.Exª... De compreender a natureza dessa pergunta. Porque obviamente há interesses muito grandes que possivelmente estejam sendo objeto da atenção na hora de apreciarmos e votarmos este projeto. E então é natural que essa pergunta seja levantada do ponto de vista...

Bom, vai haver uma arrecadação assim tão grande, para quem? E se estas instituições, seja o Governo Federal--

SENADOR EDUARDO AZEREDO (PSDB-MG): Só esclarecer. Na verdade, os números que o Dr. Eduardo Parajo colocou seriam de custo para os provedores poderem tomar algumas providências. A questão de multas está previsto aqui é no caso de multas que forem aplicadas... Aí essas multas vão de dois mil a cem mil reais, aí essas multas iriam para o Fundo Nacional de Segurança pública.

SENADOR EDUARDO SUPLICY (PT-SP): Exato. Mas então eu gostaria, se o Consultor Jurídico de Ministério das Comunicações puder complementar, porque obviamente se esse projeto vai envolver um volume de recursos, então é natural que se faça a pergunta em benefício de quem? Ou representará uma receita para tal ou qual instituição, ou tal ou qual organização? Que por seu turno, e aí é uma questão importante, se vai receber um tanto, então será que esta

instituição ou esta organização ou a própria Receita, o Governo, se vão receber tais recursos, então que tipo de serviço prestarão pelo fato de estarem recebendo tais recursos?"

Sr. Presidente, eu como estou aqui aprendendo, o Congresso Nacional, o Senado Federal, cada dia percebo se constitui numa extraordinária universidade para nós. Todos os dias nós aqui estamos aprendendo. Inclusive com os senhores que nos trouxeram tantos conhecimentos hoje. Mas ainda vamos ter que aprender muito mais sobre cibernética, internet. Muito obrigado.

SR. PRESIDENTE SENADOR VALTER PEREIRA (PMDB-MS): V.Exª está se "cibernitizando". Aos poucos vai se "cibernitizando". E aqui todos nós que não nascemos na geração da cibernética, claro que temos essas dificuldades. Mas estão aqui os expositores instados para responder. Pode responder.

SR. MARCELO BECHARA DE SOUZA HOBAIKA: Eu gostaria de responder a primeira pergunta do Senador Suplicy, aliás, como sempre brilhante, uma pergunta extremamente pertinente, Senador. Na verdade, o objeto da demanda que está sendo tratada nessa questão trata de uma matéria penal que envolve condutas e práticas que serão, passarão a ser consideradas como crimes, e que a partir do momento que sejam cometidas elas sejam devidamente penalizadas. O senhor fez uma pergunta muito interessante a respeito de marco legal na questão do conteúdo. Paralelamente a essa discussão, essa Casa vem travando alguns debates, não só aqui, mas também na Câmara dos Deputados, a respeito da questão do conteúdo. Porque o conteúdo ele deixou de ser apenas um elemento, uma informação vinculada a um determinado tipo de tecnologia, ou seja, uma televisão, rádio, e com a internet principalmente começou a circular de forma muito mais potencial e muito mais livre.

Então, a visão que se dá dentro desses projetos que estão sendo tratados é em relação à produção de um conteúdo, conteúdo nacional, em relação a difusão desse conteúdo que é um debate também extremamente importante. Esse debate aqui é especificamente em relação a práticas delituosas na internet que podem ou não envolver questões de conteúdo, inclusive. Quando, por exemplo, você está acessando de forma não autorizada determinado tipo de informação, uma rede, e isso segundo o projeto constituirá crime, você pode estar fazendo isso para atender algum tipo de conteúdo. Então é plenamente possível. Mas acho que são coisas independentes. Acho que a lei que vai tratar da questão de conteúdo, seja ela no âmbito de uma lei de convergência, ela é igualmente importante, tão importante quanto essa que está tratando a questão no âmbito penal. E só para aproveitar já o espaço do último questionamento, pelo que eu pude entender da colocação do representante dos provedores, é claro que se nós estamos falando de um projeto que vai trazer obrigações, essas obrigações

custam alguma coisa. Eu acho que algumas obrigações elas devem ser suportadas. Eu acho que tem investimentos que vão ter que ser feitos e que vão ter que ser suportados. Eu acho plenamente viável investimentos que os provedores têm que fazer e eles mesmos já colocaram isso, em manter os logs de acesso durante três anos para facilitar, inclusive, o trabalho das investigações, isso é razoável. Agora, como bem colocou o Senador Azeredo, o art. 21 do projeto, que é o que eu na minha colocação, na minha manifestação eu entendo que não deve ser tratado nesse momento, é uma opinião pessoal minha, eu acho que deve ser tratado de uma lei em separado, ele traz sim algumas penas pecuniárias e multas que variam no caso de dois mil a cem mil reais, e o senhor perguntou para onde seriam revertidos esses recursos. O § 4º do dispositivo estabelece que o recolhimento dessas multas serão destinadas ao Fundo Nacional de Segurança Pública que seriam colocados. A minha única crítica, não é em relação ao conteúdo desse art. 21, mas de tratar o art. 21 nesse momento que ele trata obrigações de natureza cível, eu acho que a gente teria que focar nesse momento, Senador, na questão criminal, nos tipos penais que precisam ainda de uma redação um pouco mais refinada para que ele seja mais precisos, claro, os objetivos, e possam ser exeqüíveis. Que tudo que a gente quer é que essa lei saia e que ela seja aplicável. Obrigado.

SR. FERNANDO NETO BOTELHO: Presidente, posso responder a pergunta do eminente Senador Eduardo Suplicy, que pela história e pela importância que tem no contexto nacional, não é só no Senado, não necessita de qualquer [ininteligível] aprimoramento cibernético e é extremamente importante que mesmo que num ato como esse absolva o máximo possível do pouco que nós temos para oferecer porque a convicção de V.Exª será sem dúvida histórica e importante para um projeto histórico como esse. Quando o senhor faz a referência--

SR. PRESIDENTE SENADOR VALTER PEREIRA (PMDB-MS): Então V.Exª está absolvendo.

SR. FERNANDO NETO BOTELHO: Estou a...?

SR. PRESIDENTE SENADOR VALTER PEREIRA (PMDB-MS): Absolvendo.

SR. FERNANDO NETO BOTELHO: Plenamente. Pela história, eternamente absolvido. Senador, quando o senhor se refere à questão do marco regulatório administrativo indenizatório, digamos, prévio antes de se chegar a uma atuação pelo Estado Brasileiro de se criminalizar, eu tive a oportunidade, estou até apresentando aqui um modesto trabalho a respeito desse assunto da história do Direito Penal e da forma como ele é interpretado hoje na chamada moderna criminologia, em que os Estados que praticam, efetivamente Estado de Direito, sobretudo Estado Social de Direito, usam a ferramenta, o instrumento Direito Penal, criminalização de fatos da vida social com comedimento, é sempre a última providência para preservar a estrutura

de direitos fundamentais. Mas o Estado não se demitiu. Nem normativamente, nem constitucionalmente, em infra-constitucionalmente da prerrogativa de fazê-lo. E seguramente não fará isso jamais porque o dia que o fizer vai deixar o interesse público abandonado diante de coisas que podem eclodir amanhã com a gravidade muito grande e tenham que ser incriminadas.

Nós mostrávamos aqui dados significativos de várias práticas cibernéticas no meio eletrônico. Não só de internet. Por exemplo, eu fiz referência e falo como Juiz de Direito do Tribunal de Justiça do Estado de Minas Gerais, e como coordenador desse projeto em Minas Gerais nós estamos hoje implantando o processo judicial eletrônico completamente sem papel. A justiça de Minas Gerais tem três milhões e quinhentos mil processos em andamento.

ORADORA NÃO IDENTIFICADA: [pronunciamento fora do microfone]

SR. FERNANDO NETO BOTELHO: Cuja Relatora foi a eminente Senadora, estava inclusive na Sessão do Supremo Tribunal Federal agora quando a Ministra Ellen Gracie fez, pela primeira vez na história, a distribuição do recurso extraordinário eletrônico. Foi graças a esse trabalho que nós estávamos todos os tribunais brasileiros lá, são 91, aguardando que o papel se diminua ou se extinga na justiça. Esses dados da população, Minas Gerais tem três milhões e quinhentos mil processos na Justiça Estadual, o Estado de V.Exª tem 12 milhões de processos. Esses são dados da população. São cláusulas contratuais, são informações bancárias, fiscais, da intimidade das pessoas, Senador, que estão no papel dentro dos escaninhos e sujeito a uma publicidade técnica. Nós vamos pegar tudo isso e vamos elevar uma publicidade inédita que poderá ser acessada pela internet. Sem um conceito de segurança da informação, mas honrado com a população justo, seguro, nos moldes em que o Pacer, P-A-C-E-R, ele significa uma sigla, pode ser procurado pelo Google que vão achar páginas da Secretaria de Justiça norte-americana, faz com o sistema eletrônico norte-americano proibindo acesso, criminalizando condutas de obtenção de dados dos processos judiciais norte-americanos nós não vamos chegar a um resultado satisfatório. Porque não basta digitalizar, Senadora. Nós temos que assegurar a proteção mínima que nós damos hoje a esse dado. Somados ao que ocorre hoje, o *fishing scam*, que é a pescaria eletrônica, os e-mails falsos, a tentativa de fraude que é monumental no Brasil, esses dados a gente está relatando, nós entendemos que há hoje um motivo justificável para considerar esses fatos já num percentual alto do interesse nacional. A demandar a criminalização direta. E não simplesmente tentar resolvê-lo com posturas administrativas, indenizatórias, civis, que não inibirão o ilícito. O que é que nós queremos? É que se pratique. E este é o que o Estado moderno pratica quando criminaliza a chamada prevenção geral do ilícito. Quer

dizer, nós educarmos a população, a população de bem e a minoritária que pratica crime, tem uma tendência delitiva, que se o fizer haverá a resposta também educativa, ressocializante, etc, mas haverá a devida resposta penal e, portanto, nós comecemos a normalizar essa imensa comunidade eletrônica que fora da internet, por exemplo, já atinge cem milhões de usuários de telefonia móvel celular, cujo consumidor inclusive hoje não é o classe A, mas é o classe C e D que o maior número de telefones no Brasil hoje, não sei se sabem, acima de 70%, é o telefone pré-pago. E ele servirá amanhã como moeda de pagamento, por exemplo, de atividades comerciais.

Então, nós estamos entendendo, respondendo agora objetivamente a pergunta de V.Exª, que é hora mais do que hora de que se dê a Justiça brasileira um instrumento delimitador da responsabilidade criminal. E que caiba aos tribunais fazer a devida adequação disso à realidade episódica que surgir efetivamente. Para isso inclusive fazemos uma análise da penalização que está aqui mostrando que fora dois tipos penais que passaram do limite de quatro anos, todos eles que estão propostos no projeto são sujeitos à suspensão condicional do processo, portanto, o processo pode ser suspenso por acordo com o Ministério Público a conversão em pena restritiva de direito ou a aplicação de regime aberto diretamente, portanto, sem a cogitação de pena privativa da liberdade. Porque assusta muito a reclusão, a detenção, é preciso entender que dentro do limite máximo e mínimo ela será individualizado.

Por último, como vejo a aplicação da lei se aprovada. Educando a população, fazendo cumprir o princípio da prevenção geral que é a finalidade da criminalização. Educar a comunidade à abstenção da prática criminosa resguardando os valores éticos e sociais que a norma está protegendo. Quando fala, por exemplo, não disseminar ou incrimina a código malicioso eletrônico do vírus, está dizendo por trás, não difunda código malicioso de vírus. Há algo mais saudável do que isso, num meio eletrônico de um País jovem como esse, que ainda vai praticar internet, por exemplo, ou e-Banking ou processo eletrônico, por exemplo? Nós estamos educando a comunidade. Estamos inibindo o criminoso que já existe hoje que está sendo investigado pela ação da Polícia Federal, da Polícia Civil, das delegacias cibernéticas dos Estados como eu tenho hoje em Minas Gerais, a conter a sua ação pela resposta penal possível que ele terá.

E finalmente, Senador, eu tenho certeza que estaremos educando Juízes, promotores e Advogados. A prática cotidiana do enfrentamento da responsabilidade criminal frente a esse contexto de tecnologia que V.Exª no início da abordagem esclareceu que não conhece profundamente. O senhor esteja certo que não é apenas V.Exª, a nossa comunidade jurídica não conhece. Quantas vezes estamos tendo que fazer ali encontro de colegas para esclarecer o que vem a ser

radiofreqüência, o que é que é ERBs, estação rádio base, o que é que é *bit*. Isso é um ambiente muito comum a toda essa mesa de técnicos, mas muito ainda ausentes do conhecimento dos profissionais. Então não tenha dúvida, nós estaremos habilitando uma densa comunidade jurídica, são mais de 600 mil Advogados, no meu Estado são mil magistrados da Justiça Estadual, inúmeros promotores de justiça a se habilitarem melhor a lidar com essa técnica e julgarem, interpretarem mais justamente o fato em benefício inclusive do inocente.

SR. PRESIDENTE SENADOR VALTER PEREIRA (PMDB-MS): Dr. Demi.

SR. DEMI GETSCHKO: Vou fazer só alguns adendos, em parte algumas intervenções que o Senador Azeredo fez e em parte a esse comentário final. Eu acho que, como eu falei na minha exposição, em hipótese, todos estamos de acordo com os objetivos que se pretende atingir. Eu tenho alguns desconfortos com o projeto e alguns eu já citei, queria pegar três ou quatro que foram comentados agora e voltar a citar.

Acho que nós temos algum problema com o conceito de acesso. Acho que o acesso à rede é uma coisa que tem que ser vista com cuidado. Porque inclusão digital vai envolver acesso em lugares dos mais variados, o acesso à escola em geral não dá para identificar o indivíduo, não há porque identificar o indivíduo normalmente nesses casos, o acesso em pontos livres da rede também tem que ser visto com esse devido cuidado para não sermos excessivamente rigorosos quanto a isso porque isso impedirá a entrada de mais brasileiros na rede. Então o acesso à rede para consulta como tentei especificar na minha apresentação não deveria ser qualificado como devido ou indevido, e eventualmente penalizado com apenamento que é pesado no Projeto de Lei.

Um outro aspecto que envolve dois casos do Projeto de Lei que também deveriam ser reconsiderados, acho que a intenção, por exemplo, de código malicioso, acaba abrangendo também os que fazem a difusão indevida. Só para dar um exemplo parecido, foi dado até o exemplo dos pontos de acesso livre, a impressão que tive do que foi dito foi o seguinte, bom, se alguém deixa a sua rede livre e alguém entra pela rede, aí eu tenho um crime cometido pelo sujeito ter entrado pela rede livre então vou apenar quem deixou a rede livre. Quer dizer, se eu deixei minha carteira em cima da mesa e levaram eu sou co-autor do roubo porque deixei minha carteira na mesa. Quer dizer, eu acho que o fato do acesso ter sido livre não pode apenar quem deu o acesso livre em relação a quem cometeu de fato o delito. Então acho que é importante que seja o agente do problema diretamente qualificado e não simplesmente o fato que ele se aproveitou de uma oportunidade. Se meu carro está destrancado isso não dá direito a ninguém a levá-lo embora. Esses detalhes que eu acho que a lei, o projeto podia ser um

pouco mais específico para tirar esse desconforto que nos traz de alguma forma.

SR. FERNANDO NETO BOTELHO: Presidente, apenas um comentário sobre esse último ponto, porque ele tem muita importância e ele é de ordem jurídica. Eu ouvi aqui várias informações a respeito exatamente dessa questão de deixar aberto. Quer dizer, caiu lá o código malicioso, o zumbi, por exemplo, ele pode entrar na minha máquina, repete dali e eu sou incriminado? Eu nem sei daquilo. Peço apenas atenção dos eminentes Senadores que o texto da lei, o texto do projeto estabelece um tipo doloso. Doloso. Nós chamamos o seguinte, elemento subjetivo do tipo sem o dolo, sem a prova da intenção, não há crime. Porque não há, essa forma não é culposa. Então se entra na minha máquina, o vírus, se ele habita a minha máquina e dali ele faz um zumbi, eu viro um pivô de recebimento envio automático sem saber, ele é atípico ao fato.

SR. PRESIDENTE SENADOR VALTER PEREIRA (PMDB-MS): Bom, ao apagarem as luzes aqui dessa Sessão, eu gostaria de realçar...

SENADOR EDUARDO SUPLICY (PT-SP): [pronunciamento fora do microfone]

SR. PRESIDENTE SENADOR VALTER PEREIRA (PMDB-MS): É que já está sendo realizada a Sessão ordinária. Do Plenário.

SENADOR EDUARDO SUPLICY (PT-SP): Mas só para ele...

SR. PRESIDENTE SENADOR VALTER PEREIRA (PMDB-MS): Rapidinho.

SENADOR EDUARDO SUPLICY (PT-SP): Se vai poder identificar o lugar que estão produzindo aquele site.

SR. TIAGO TAVARES NUNES DE OLIVEIRA: Senador, agradeço a questão, agradeço ao Presidente pela oportunidade.

Bom, nós recebemos a denúncia, no mesmo dia nós encaminhamos essa denúncia para o hotline inglês chamado *Internet Watcher Foundation*, isso aconteceu no dia 25 de março de 2006. Esse é o e-mail que comprova o encaminhamento da denúncia para esse hotline em inglês, e dois dias... 48 horas depois o site foi retirado do ar pelo provedor de acesso.

Então, pelo provedor de conteúdo. Isso devido à atuação do hotline inglês que é nosso parceiro junto à EUROPOL. O problema é que como o próprio site diz aqui na sua apresentação, ele volta pro ar em questão de 24 horas em outro País e muitas vezes envolvendo mais de um País. Nós infelizmente temos lidado com vários casos de que sites de pornografia infantil, as imagens em que pesem ser o mesmo site, as imagens são hospedadas em 10, 15, 20 países diferentes. Por isso essa dificuldade.

SENADOR EDUARDO SUPLICY (PT-SP): Muito obrigado. última.

SR. PRESIDENTE SENADOR VALTER PEREIRA (PMDB-MS): Bom, eu vou interromper porque nós temos que encerrar por força da Sessão Plenária. Mas eu gostaria antes de fazer o encerramento, de dizer o seguinte, há um esforço muito grande do Senado Federal, especialmente da Comissão de Constituição e Justiça para dotar o País de um diploma jurídico compatível com esse momento de grande transformação tecnológica que ocorre no mundo inteiro, e que traz as suas repercussões na área criminal.

Esse trabalho está sendo capitaneado pelo Senador Eduardo Azeredo, com exaustivas discussões, com esforço enorme, e tenho certeza que vai resultar numa produção extraordinária para a operação do direito. Obviamente não vai ser um trabalho perfeito. É um trabalho inovador. Um trabalho que vai resultar em críticas no Plenário e posteriormente na sociedade, e vai exigir muito do Judiciário. Vai exigir um esforço grande para a interpretação do que pensa a sociedade. E aqui pensa, aqui exprime realmente o pensamento da sociedade como nós hoje podemos perceber. Não é só o Senador que está discutindo, são todos aqueles que representam segmentos importantes que operam nessa área de informática.

Portanto, essa vai ser a nossa contribuição. E obviamente isso daí, no futuro, vai ensejar grandes discussões ainda. De qualquer forma nós queremos agradecer a todos aqueles que participaram deste evento. Dr. Fernando, Dr. Marcelo, Dr. Deni, Dr. Paulo, Dr. Eduardo Fumes, Dr. Tiago que foi pescado na última hora pela Senadora Serys, mas que sem dúvida alguma deu uma contribuição também substancial. E agradecemos a todos os Senadores que participaram do debate, inclusive e principalmente o Senador Eduardo Suplicy, que está nesta fase de cibernetização profunda. [risos]

SENADOR EDUARDO SUPLICY (PT-SP): Sr. Presidente, permite. Como todos os participantes fizeram as sugestões, na medida em que puderem encaminhar se tiverem sugestões de Emendas, de aperfeiçoamento por escrito para nós Senadores, para o Relator, para o Presidente, isso poderá ser muito útil.

SR. PRESIDENTE SENADOR VALTER PEREIRA (PMDB-MS): Eu gostaria inclusive de acrescentar ao que o Senador Eduardo Suplicy está ponderando que todos os expositores, aqueles que não deixaram ainda cópia do material oferecido a esta Comissão, que o faça para que nós possamos utilizar esse material como subsídio. Muito obrigado a todos. Está encerrada a Sessão.

Sessão encerrada às 15h30

PFDC

MINISTÉRIO PÚBLICO FEDERAL
PROCURADORIA FEDERAL DOS DIREITOS DO CIDADÃO

OFÍCIO Nº 725 /2007/PFDC/MPF

Brasília, 3 de julho de 2007.

A Sua Excelência o Senhor
Senador VALTER PEREIRA
Vice-Presidente
Comissão de Constituição e Justiça do Senado
NESTA

Assunto: Encaminha documentos.

Senhor Vice-Presidente,

De ordem, em resposta ao Ofício n.º 65/2007-PRESIDÊNCIA/CCJ, encaminho, em anexo, estudo sobre o Projeto de Lei da Câmara N.º 89, de 2003 para subsidiar os trabalhos dessa Comissão, visto a impossibilidade do comparecimento da Procuradora Federal dos Direitos do Cidadão Ela Wiecko Volkmer de Castilho, por motivo de férias.

Respeitosamente,

SHEILA NEVES
Assessora da
Procuradoria Federal dos Direitos do Cidadão

Em novembro de 2006, por ocasião de convite para participar, como expositora, de Seminário na Câmara dos Deputados, *"destinado a debater proposições em tramitação no Congresso Nacional tendentes à regulamentação do combate aos crimes cometidos por meio da internet"*, analisei o Parecer da Comissão de Constituição, Justiça e Cidadania do Senado Federal sobre o Projeto de Lei da Câmara dos Deputados nº 89, de 2003 (PL nº 84/1999, do Deputado Luiz Piauhylino) e Projetos de Lei do Senado nºs 137/2000 e 76/2000. Referido Parecer oferecia um substitutivo a tais projetos, de autoria do Senador Eduardo Azeredo.

Contribuí, em referido Seminário, realizado em 14 de novembro de 2006, com a análise de referido substitutivo, tecendo considerações sob o ponto de vista do Direito Penal.

O substitutivo, agora aprovado na Comissão de Constituição e Justiça do Senado, apresenta ajustes e, assim, em vários pontos, redação diferente da presente no material que analisei, no ano passado. Em suma, encontrei resolvidas, na nova redação do substitutivo, praticamente todas as ressalvas que fiz quanto à adequação das propostas do ponto de vista do Direito Penal.

Há, entretanto, três aspectos que permanecem na redação do substitutivo e que me parecem inadequadas:

a) a manutenção do capítulo referente a "Dos crimes contra rede de computadores, dispositivos de comunicação ou sistema informatizado", no Título I, do Código Penal;

b) a criação de um tipo de dano "por difusão de código malicioso eletrônico ou digital ou similar" que não se classifica, na doutrina penal, como crime de dano;

c) a previsão de aumento de pena para crimes contra a honra, quando praticados por intermédio da rede de computadores, dispositivo de comunicação ou sistema informatizado.

Passo a discorrer sobre cada um desses pontos.

A - Manutenção do capítulo referente a "Dos crimes contra rede de computadores, dispositivos de comunicação ou sistema informatizado", no Título I, do Código Penal

O Código Penal Brasileiro obedece à uma sistemática que divide a Parte Especial do Código – aquela que define os delitos e comina as penas – em Títulos, de acordo com o bem jurídico protegido. Assim, o Título I prevê os crimes contra a pessoa, o Título II, os crimes contra o patrimônio, e assim sucessivamente.

O primeiro título do Código, atuando como a porta de entrada do nosso Código Penal, prevê os crimes contra os bens jurídicos mais importantes a serem protegidos: a vida, a integridade física, a honra e a liberdade das pessoas. Como ensina Cezar Roberto Bitencourt: *"o atual Código Penal inicia a Parte Especial tratando dos crimes contra a pessoa e a encerra com os crimes contra o Estado, colocando o ser humano como o epicentro do ordenamento jurídico, atribuindo à pessoa humana posição destacada na tutela que o Direito Penal pretende exercer."* (BITENCOURT, Cezar Roberto. *Tratado de Direito Penal,* parte especial, v.2, 3ed. São Paulo: Saraiva, 2003, p.1).

Assim, o capítulo **"Dos crimes contra rede de computadores, dispositivos de comunicação ou sistema informatizado"** não tem lugar no Título I, do Código Penal, porque o bem jurídico protegido não são as pessoas, mas a segurança da rede de computadores.

Para preservar a sistematização do Código Penal, sugerimos, para abrigar os crimes sugeridos no capítulo dos crimes contra a rede de computadores, ou a criação de um Título separado, ao final do Código, ou, ainda, um capítulo dentro do Título II (Dos Crimes contra o patrimônio) ou do Título VIII (Dos crimes contra a incolumidade pública), que embora não sejam um abrigo perfeito para o bem-jurídico protegido no novo capítulo sugerido, encontram maior afinidade com a matéria do que o Título I.

B - Criação de um tipo de dano "por difusão de código malicioso eletrônico ou digital ou similar" que não se classifica, na doutrina penal, como crime de dano

O art. 163-A, acrescido pela proposta do substitutivo, contém uma série de impropriedades.

Em primeiro lugar, tipifica a conduta de criar, inserir ou difundir código malicioso, colocando-a no Capítulo IV (Do Dano) e dá ao crime previsto o nome de "Dano por difusão de código malicioso eletrônico ou digital ou similar". Ocorre que não se encontra, na conduta de criar, inserir ou difundir código malicioso, onde está o dano.

O tipo, com a redação proposta, não é crime de dano, mas crime de perigo. Ainda no magistério de Cezar Bitencourt, crime de dano é *"aquele para cuja consumação é necessária a superveniência da lesão efetiva do bem jurídico."* Crime de perigo é *"aquele que se consuma com a simples criação do perigo para o bem jurídico protegido, sem produzir um dano efetivo. Nesses crimes* (de perigo) *o elemento subjetivo é o dolo de perigo, cuja vontade limita-se à criação da situação de perigo, não querendo o dano, nem mesmo eventualmente"* (BITENCOURT, Cezar Roberto. *Tratado de Direito Penal,* parte geral, v.1, 8ed. São Paulo: Saraiva, 2003, p. 148).

Assim, vê-se que a previsão, pura e simples, de criminalizar a conduta de criar, inserir ou difundir código malicioso não pode ser chamada de crime de dano, porque não há, nela, previsão de lesão efetiva, mas apenas a criação da situação de perigo.

Em seguida, o projeto prevê, no parágrafo 1° do art. 163-A, uma qualificadora para a hipótese da conduta prevista no *caput* ser praticada com a 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 e lhe prevê pena de 2 (dois) a 4 (quatro) anos e multa. E, para terminar, prevê a forma mais grave: a do parágrafo 2°, no qual se tem o resultado dano. Para tal conduta, o crime prevê pena de 3 (observe-se que, no projeto, há um equívoco: o número "3" seguido do descritivo "dois") a 5 (cinco) anos.

A impropriedade maior está na redação do parágrafo 2°: "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"** Trata-se, da forma como está previsto, de crime de dano culposo, apenado, no projeto, de forma mais gravosa que o crime de homicídio culposo (detenção de 1 (um) a 3 (três) anos, art. 121, §3°, Código Penal).

Para sanar tais impropriedades, sugere-se, primeiramente, a mudança do nome do crime, retirando o nome "dano". Em seguida, a previsão de dois crimes, no lugar do art. 163-A proposto, que deverão ter lugar não no Capítulo IV, mas no Capítulo "Dos crimes contra rede de computadores, dispositivos de comunicação ou sistema informatizado" já previsto no projeto: a) o crime de criar, inserir ou difundir código malicioso e b) o crime de **inserção** ou **difusão** de código malicioso em dispositivo de comunicação, rede de computadores ou sistema informatizado, **com finalidade de dano**, incluindo-se, nesse tipo, causa de aumento de pena para a hipótese de efetivo dano. Vale dizer que, nesse segundo tipo (alínea b), se deve excluir a conduta de "criar" o código malicioso que, por si só, não gera dano, dependendo, para esse resultado, da inserção ou difusão.

Assim, sugere-se a adoção da seguinte redação:

Art. X. Criar, inserir ou difundir código malicioso em dispositivo de comunicação, rede de computadores, ou sistema informatizado.

Pena – detenção, de 6 (seis) meses a 2 (dois) anos.

Art. Y. "Inserir ou difundir vírus em dispositivo de comunicação, ou rede de computadores ou internet, ou sistema informatizado, com finalidade de destruí-lo, inutilizá-lo, deteriorá-lo, alterá-lo ou dificultar-lhe o funcionamento.

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

§1° 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.

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

§2° 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."

C - Previsão de aumento de pena para crimes contra a honra, quando praticados por intermédio da rede de computadores, dispositivo de comunicação ou sistema informatizado

O substitutivo sugere que seja acrescido ao Código Penal o artigo 141-A, prevendo que as penas previstas no Capítulo V, do Título I (Dos crimes contra a honra) sejam aumentadas de dois terços, *"casos os crimes sejam cometidos por intermédio de rede de computadores, dispositivo de comunicação ou sistema informatizado."*

Adverti, durante minha participação no Seminário em que se discutiu as proposições para crimes de informática, para um conflito possível entre tal causa de aumento de pena e a lei de imprensa. É que, hoje, a quase totalidade dos meios de comunicação reproduzem na internet seus conteúdos escritos e realizam outras atividades em seus sítios, como discussões em *chats* com especialistas, por exemplo. Tais atividades, se ofensivas a honra de alguém, já têm sido enquadradas, na jurisprudência do Superior Tribunal de Justiça, como crime de imprensa.

> "PENAL. INJÚRIA. PUBLICAÇÃO OFENSIVA. SITE DA INTERNET. APLICAÇÃO DA LEI DE IMPRENSA. DECADÊNCIA. EXTINÇÃO DA PUNIBILIDADE.
>
> 1 - Uma entrevista concedida em um chat (sala virtual de bate-papo), disponibilizada de modo "on line", na home page de um jornal virtual, se reveste de publicidade bastante para se subsumir ao art. 12 da Lei n° 5.250/67 e, pois, atrair a incidência do prazo decadencial de três meses (art. 41, § 1°). Precedente da Corte Especial e da Quinta Turma - STJ.
>
> 2 - Extinção da punibilidade decretada.
>
> 3 - Agravo regimental não provido.
>
> (AgRg na APn 442/DF, Rel. Ministro FERNANDO GONÇALVES, CORTE ESPECIAL, julgado em 07.06.2006, DJ 26.06.2006 p. 81).

No julgamento da ação penal acima referida, transcreveu-se ensinamento doutrinário de Demócrito Ramos Reinaldo Filho, in Responsabilidade por Publicações na Internet, editora Forense, 2005, p. 100-104, que demonstra bem como doutrina e jurisprudência, em matéria penal, tem se posicionado no tema dos crimes contra a honra praticados na internet. De se ler, **verbis**:

> "O que se dizer das ofensas, difamações, injúrias e calúnias executadas por meio da Internet? Trata-se de uma mídia inteiramente nova, não, prevista como fenômeno de comunicação e meio de informação e divulgação de notícias quando da edição da Lei n° 5.250, que é de 09 de fevereiro de 1967. O parágrafo único do seu art. 12 limita-se a definir como "meios de informação e divulgação, para os efeitos deste artigo, os jornais e outras publicações periódicas, os serviços de radiodifusão e os serviços noticiosos". Por essa razão, muitos discutem se a ofensa irrogada por meio da Internet deve ser apenada pela Lei de Imprensa ou pelo CP. Para o criminalista Luiz Flávio Gomes, os crimes contra a honra cometidos por meio de redes telemáticas podem ser punidos por um ou outro diploma, indiferentemente. Já o Procurador da Fazenda Nacional Hugo César Hoeschl, que também é especialista em Informática Jurídica pela Univali (SC), lembrando que a Internet não se insere entre os veículos de comunicação elencados no citado dispositivo legal, descrê da possibilidade de tipificação dos crimes de imprensa quando a conduta que se quer apenar é executada por esse meio.
>
> A Corte Especial do STJ, julgando um caso de publicação em site de uma carta contendo denúncias contra uma deputada, recebeu queixa-crime contra o autor da missiva. Durante o julgamento, o Min. Humberto Gomes de Barros levantou dúvidas em relação à aplicação da Lei de Imprensa a crimes praticados por meio da Internet, por não haver norma legal com menção específica a esse meio eletrônico, mas terminou por acompanhar o voto do relator, pelo recebimento da

queixa-crime, depois que o Min. Nilson Naves esclareceu que, mesmo se houvesse qualquer impedimento para a aplicação da Lei de Imprensa, ainda haveria a possibilidade de aplicação do Código Penal para punir quem pratica crimes contra a honra. Em seu voto, o relator, Min. José Delgado, aceitou que as falsas informações noticiadas no site contra a deputada caracterizavam, em tese, crime de calúnia, injúria e difamação, definidos, respectivamente, nos artigos 20, 21 e 22 da Lei de Imprensa. O julgamento foi interrompido com o pedido de vista do Ministro Vicente Leal.

A tendência parece ser a de que o STJ termine por aceitar a aplicabilidade da Lei de Imprensa para regular delitos contra a honra praticados na Internet. Na interpretação do conceito de "meios de informação e divulgação", previsto no parágrafo único do seu art. 12, a jurisprudência sempre lhe emprestou larga extensão, abrangendo desde informativos sindicais (RT 642/321) até jornais clandestinos (RT 541/435). Ademais, a Internet é um veículo de publicação e divulgação de informações que satisfaz o caráter de periodicidade – o artigo em questão define como meios de informação "os jornais e outras publicações periódicas" – que informa esse dispositivo da Lei nº 5.250/67. Em verdade, as características técnicas da rede conferem a uma publicação ou revista eletrônica um caráter bem mais próximo da "permanência", do que propriamente de periodicidade, na medida que as informações nela publicadas podem ficar indefinidamente à disposição do público, que pode acessá-las, reproduzi-las e repassá-las adiante indefinidamente. Também não seria difícil reconhecer a rede global de comunicação informática como canal de "serviços noticiosos", entendidos esses como repositórios que trazem ou contêm notícias. Mesmo no conceito do "serviço de radiodifusão" – também definido pela lei como categoria de "meios de informação" (no art. 12) –, não haveria dificuldade de incluir a Internet. A radiodifusão, como se sabe, envolve a transmissão, por meio de ondas radioclétricas, de

notícias, programas etc., destinada à recepção pública. Compreende a radiodifusão sonora (o rádio) e a radiodifusão de sons e imagens (televisão). Embora hoje a Internet seja acessada predominantemente por linhas e cabos de telefone, alguns serviços a oferecem por ondas radioelétricas. Na verdade, os meios de comunicação estão paulatinamente se fundindo em um único e grande canal, que vai reunir todos os tipos de mídia eletrônica, abrindo os caminhos para uma superhigh way information, por onde transitarão telefone, centenas de ramais de televisão, mensagens eletrônicas (e-mails), sites de notícias e shoppings on-line. Como pressentiu George Gilder, em livro profético, "telefone, televisão e computadores se fundirão rapidamente em uma única e muito inteligente caixa – o telecomputador, conectado em linha com os outros, ao redor do mundo".

Outro argumento ainda pode ser invocado em prol da aplicabilidade da Lei de imprensa à Internet. Não se afastando da lição de Nelson Hungria de que "os crimes de imprensa, chamados tais, não são mais do que crimes comuns praticados por meio da imprensa", o certo é que, embora não constitua "uma família autônoma de infrações penais", os crimes contra a honra praticados através dos veículos de comunicação não estão sujeitos ao CP porque se considera que o meio empregado amplia o dano à vítima. É o meio empregado pelo ofensor para lesar a honra alheia que serve para distinguir os crimes comuns dos crimes de imprensa. A publicidade através da imprensa extravasa os limites restritos da convivência social do indivíduo em seu pequeno círculo de relações, adquirindo maiores dimensões e excedendo em intensidade o dano cometido pelos meios comuns, daí porque as penas do crime capituladas na Lei de Imprensa são mais exacerbadas." Ora, a negativa de aplicação da lei mais rigorosa aos crimes de honra cometidos por meio da Internet levaria à contraditória situação de punir de maneira mais benévola (com as regras do CP) conduta de

maior gravidade (para a vítima), sabendo-se que não há meio de comunicação de maior potencial que a Internet. Não só pelo número de usuários, mas também por suas características técnicas, a rede funciona como o maior instrumento de comunicação já inventado pelo homem. Nada escapa ao seu poder de difusão e propagação. Uma simples mensagem pode ser vista, lida, reproduzida e reenviada para outras pessoas em tempo ínfimo. Uma vez publicada, é mesmo impossível apagar uma mensagem, texto ou arquivo de vídeo, pois ela funciona como uma global copying machine, onde as mensagens de dados vão sendo copiadas em cada um dos pontos intermediários ao longo do trajeto que percorrem na rede. Existe inclusive um autor que lembra que, se alguém quiser que dados ou informações nunca desapareçam, basta disponibilizá-los na Internet. Como meio de comunicação de extenso alcance, não parece lógico punir as ofensas contra a honra praticadas na Internet com penas mais brandas do que aquelas difundidas na mídia impressa ou televisiva. Uma revista eletrônica não deixa de ser revista apenas porque o meio de sua divulgação não é o impresso, mas o digital. O que importa é que ambos são meios de comunicação e, como tal, sujeitos a uma disciplina própria e mais rígida que os "meios comuns" de crimes contra a honra.

Na jurisprudência alienígena, é perceptível uma clara tendência voltada a aplicar aos sites de notícias on-line o mesmo tratamento legal que é dispensado à imprensa tradicional. Na França, um acórdão da Câmara Criminal da Corte de Cassação (Chambre Crimineille de la Cour de Cassation), de 16 de outubro de 2001, decidiu que a Lei de Imprensa francesa, uma lei de 29 de julho de 1881, aplica-se à Internet. A Web, em sendo um meio de comunicação, não derroga o direito comum e, na concepção dos juízes franceses, os crimes contra a honra praticados em ambientes eletrônicos sujeitam-se às disposições das leis existentes. Da jurisprudência norte-americana, pode ser

> trazido à colação o caso BNM v. Narco News, julgado recentemente pela Suprema Corte de Nova Iorque (Supreme Court ofthe State of New York), onde ficou assentado que a Internet é similar a qualquer outro meio de comunicação, equiparando-se ao rádio e à televisão. Nesse julgamento, recebido pela comunidade jurídica como uma groundbreaking decision, dado o seu caráter inovador e a possibilidade de servir como precedente para julgamentos seguintes, a Juíza Paula J. Omansky afirmou categoricamente que os sites noticiosos da Internet devem ser tratados como qualquer outra organização de mídia. "A Internet é similar à televisão e ao rádio na medida em que uma mensagem eletrônica é capaz de alcançar uma larga e diversa audiência quase instantaneamente", sentenciou a Juíza, citando julgado anterior, onde ficara assentado que os princípios da defamation law podiam ser aplicados à Internet.

Como o projeto apenas prevê causa de aumento de pena para os crimes contra a honra do Código Penal, não se tem como afastar o entendimento doutrinário e jurisprudencial que aplica para os crimes contra a honra praticados pela internet a Lei de Imprensa. Até porque a desproporcionalidade da pena a que se chegará pelo art. 141-A, do Código Penal e a aplicável pela Lei de Imprensa será imensa.

Restarão abarcados pela causa de aumento de pena previsto no substitutivo, tão-somente, aqueles casos que não se enquadrarem no art. 12, da Lei de Imprensa, na concepção que lhe têm dado a doutrina e a jurisprudência penal, como aqueles crimes contra a honra praticados por correspondência eletrônica (e-mails) ou grupos de discussão em rede, comuns nos locais de trabalho. E, para tais casos, a desproporcionalidade do aumento de pena ainda é evidente porquanto a situação de amplitude do dano à honra, que é o que se visa proteger, na verdade, com a proposta do substitutivo, já está prevista no art. 141, III, do Código Penal, que prevê aumento de pena de um terço se o crime é cometido *"na presença de várias pessoas, ou por meio que facilite a divulgação da calúnia, da difamação ou da injúria."*

O acréscimo do art. 141-A, ao Código Penal, a meu ver, é desnecessário.

Brasília, 04 de julho de 2.007.

Exmo. Sr.
Senador Presidente da CCJ-Senado Federal,

Exmo. Sr.
Senador Presidente da CCT-Senado Federal,

Senhores e Senhoras Senadores que integram a presente Audiência Pública,

Primeiramente, gostaríamos de agradecer a honrosa oportunidade que nos concede o convite para participação nesta histórica Audiência Pública.

Nela, o Senado da República tratará de um de seus mais importantes projetos – resumido, hoje, no substutitivo que está apresentado aos Projetos de Lei do Próprio Senado (PLS 76 e 137 de 2.000) e da Câmara Federal (PLC 89 de 2.003) sobre crimes ditos

"informáticos" – ou, ilícitos penais eletrônicos-cibernéticos.

Para que nossa abordagem se resuma a uma objetiva e concreta participação, e com ela busquemos contribuir para o enriquecimento da discussão, estamos dividindo nossa participação para resumi-la a três tópicos principais. São eles:

- <u>Primeiro</u> –

OS DADOS QUE COMPÕEM A ATUAL REALIDADE CIBERNÉTICA BRASILEIRA

- <u>Segundo</u> –

A OPÇÃO DE CRIMINALIZAÇÃO DOS ILÍCITOS CIBERNÉTICOS PELO ESTADO BRASILEIRO

- <u>Terceiro</u> –

BREVE ANÁLISE DOS DISPOSITIVOS SUGERIDOS PELO SUBSTITUTIVO EM DISCUSSÃO

Pedimos permissão, antes de entrarmos propriamente nesses tres temas, para uma breve citação. Com ela esclarecemos nossa ligação com o tema – magistrado de carreira, que somos, do Estado de Minas Gerais, responsável, hoje, por projetos de TI-Tecnologia da Informação do Tribunal de Justiça de MG, pela Assessoria Especial de TI à Presidência daquele Tribunal, pela coordenação dos estudos de implantação do processo eletrônico no TRE-MG, e membro de entidades de TI dentre as quais a ABDI-MG (Associação Brasileira de Direito de Informática e Telecomunicações e o CBTMs-Conselho Brasileiro de Telemedicina/SP) – nosso trabalho, além da atividade jurisdicional, tem intensa ligação com a área de TI.

Nossa citação é, assim, extraída do trabalho *"CRIMES E CYBERCRIMES"*, que publicamos recentemente e cujo exemplar anexamos, para análise por esta douta Comissão, como documento do ANEXO II desta abordagem.

Dizíamos, ali, e o repetimos agora:

"....O crime cibernético, tal como o crime físico-comum, tem raízes antigas, humanas; seu traço antropológico não está fora do que marca o "mito do mal". A maldade humana, seu fundamento-básico, é o seu ponto psíquico-comum com o crime físico.
Diferenciar, no tratamento, o criminoso, do crime comum-físico, do delinqüente cibernético é errar profundamente a análise sociológica do crime; é medir equivocadamente sua causação antropológica.
Pior. Equivale diferenciar, por mera sofisticação dos meios usados na execução "do mal", o tratamento do psiquismo delitivo, dispensando, ao melhor preparado (em meios), repercussão criminal menos rigorosa.
A cibernética altera tão só o meio, o instrumento, de execução do crime, não a sua conformação negativa, como fato que atenta contra importantes interesses comunitários. ....."

Com essa filosofia de enfrentamento do tema, passamos a analisar o primeiro ponto proposto.

- Primeiro –

OS DADOS QUE COMPÕEM A ATUAL REALIDADE CIBERNÉTICA BRASILEIRA

Países, como os EUA, estimam, hoje, a rentabilidade atual dos chamados "crimes cibernéticos" em cifras estratosféricas.

Em 2.004, para citar apenas um exemplo, a Conselheira do Tesouro americano, Valeri McNiven, tornou pública uma afirmação de que, com a prática de fraudes, espionagem corporativa, manipulação de ações, pedofilia, extorsão virtual, pirataria, dentre outros ilícitos eletrônicos, o "faturamento" dos chamados crimes cibernéticos havia chegado à impressionante soma de US$ 105 bilhões.

Comparativamente, no Brasil, no período entre 2.004 e 2.005, apenas as fraudes bancárias e financeiras por meio eletrônico saltaram de 5% (2004) para 40% (2005) do total dos incidentes eletrônicos registrados no país naquele período. O dado é do CERT.br ("Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil" – www.cert.br) e informa que as tentativas de fraudes pela rêde mundial cresceram, naquele ano (2.005), 579%.

As armadilhas eletrônicas – a "pescaria" eletrônica de incautos (o "phishing scam", por exemplo, ou, os "hoax" – as piadas de má-intenção voltadas para a obtenção de

vantagem ilícita-patrimonial) – cunharam uma nova "aplicação" da "engenharia do mal", ou, a "engenharia social", entendida como o rol de práticas implementadas por "experts" para engodo, engano, indução a erro, de pessoas e corporações não habilitadas à lida técnica com recursos sofisticados de TI.

O que surgiu como ataque e defesa de caráter puramente tecnológico – "hackers" que, sofisticalizando o abandono dos rigores técnicos de seu ofício profissional, tornaram-se "crackers", e avançaram sobre sistemas e redes eletrônicos não adequadamente estruturados – passou à velha e milenar característica humana, que é o abuso do homem-pelo-homem.

A chamada "engenharia social" não passa de uma vergonhosa disputa, no meio eletrônico, da superioridade cultural-técnica dos maus "experts" sobre a limitada capacidade popular de conhecimento técnico dos recursos das rêdes.

Onde há o desconhecimento técnico, navega, livre, o abuso, o ímpeto cruel da exploração, da indução a erro, com ele o desejo do proveito fácil, como ocorre com as senhas secretas obtidas, hoje, por "e-mails" falsos, falsos anúncios de cancelamentos de títulos eleitorais, convites para entrada em sites de premiação, simulação de websites para coleta de logs secretos, etc., enfim um arsenal de fraudes, simulações, que passaram a ter na sofisticação do meio e no desconhecimento humano-generalizado de suas potencialidades um novo "ar" de atuação.

Estamos juntando a esta abordagem, Senhores Senadores, três publicações, todas recentes – de 2.006, uma, e de abril/maio-2007, as duas outras –especializadas em segurança da informação eletrônica no Brasil. Foram todas editadas pela conceituada empresa "MÓDULO TECHNOLOGY FOR RISK MANAGEMENT", que, hoje, inicia processo de exame dos recursos tecnológicos-eletrônicos do TJMG para prestação de serviços de mapeamento e planejamento de segurança da informação eletrônica interna e

externa, e que vem prestando serviços a outros importantes órgãos públicos da União e dos Estados.

Poderão ver Vvs. Exas., nesses volumes, dados impressionantes do crescimento da demanda por serviços eletrônicos no Brasil – e, com eles, por segurança mínima contra fraudes e crimes cibernéticos já implementados.

São eles:

1 – O Serviço de declaração do IR pela Internet, que acaba de completar 10 anos de existência, foi usado, agora em 2.007, por 99% dos contribuintes-declarantes, isto é, das 23,270 milhões de declarações recebidas pela SRF, 22,900 foram enviadas pela Internet, numa mostra do volume quase absoluto da adesão da população contribuinte a sistemas eletrônicos convencionais (pág. 13 do vol. 12, da rev. "Risk Management Review", em anexo);

2 – Por outro lado, ou, em paralelo com esta crescente adesão voluntária-popular ao meio eletrônico público e privado,

registrou o país número expressivo de incidentes de segurança na internet no mesmo ano do exercício fiscal declarado (197 mil em 2006, ou, um crescimento de 191% em relação aos 68 mil registrados em 2.005). Desses números, apenas a prática do "phishing scam" – a "pescaria eletrônica" de incautos pela Internet, usualmente, por e-mails não-autorizados, uma característica da tal "engenharia social" – respondeu por 21% destas ocorrências. O "phishing scam" para obtenção de senhas bancárias e de números de cartões de crédito cresceu, em 2006, 53% (pág. 14 do vol. 12, da rev. "Risk Management Review", em anexo).

3 – As empresas de grande porte estão investindo crescentes somas de seus orçamentos na tentativa de proteção a clientes, consumidores, e a seus próprios ativos. Cita-se, como exemplo recente, a ocorrência de tentativa de fraude em sistema de pedágio capixaba de grande porte – ocorreram acessos indiretos à base de dados e procedimentos manuais na coleta de informações consolidadas sobre o movimento de

veículos passantes pelo pedágio (portanto, uma atividade supostamente atribuível ao próprio corpo funcional-interno da empresa concessionária, ou indícios de atuação humana conjugada a acessos livres a base eletrônica de dados). Este fato demandou investimentos em reforço de tecnologia da informação, com custos repassáveis aos usuários do próprio sistema público de transporte (caso citado à pág. 32 do vol. 12, da ver. "Risk Management Review").

4 – A maior empresa brasileira de distribuição de petróleo e derivados anuncia, à pág. 34 da mesma revista citada, que, "*....possuindo uma força de trabalho com mais de cinco mil pessoas espalhadas por todo o Brasil...*", teve que fazer significativos investimentos em segurança (interna) da informação eletrônica, pois, acentua, "*...a informação é um dos ativos mais preciosos da companhia, sendo, portanto, fundamental, que todos estejam conscientes da sua preservação...*" (pág. 35).

5. Igualmente, as empresas de cartões de crédito informam um salto nas

dimensões do mercado com uso desta sistemática: transações eletrônicas, com cartões de crédito, passaram, em somatória total, de R$ 4,3 bilhões/2006 para R$ 4,9 bilhões/2007 (pág. 41 da rev.Citada). São informações eletronicamente trocadas pela população usuária dos serviços com prestadores da garantia de pagamento e fornecedores de bens e serviços.

6. Comparativamente a este crescimento, pesquisa do Gartner Group – citada à pág. 22 do vol. 11 da revista "Security Review" (anexa) – sustenta que as compras de softwares "de defesa" corporativa (destinados à segurança da informação eletrônica processada e armazenada) atingirão aumento de 10,7% em 2.007, sendo que, em todo o mundo, a cifra deverá atingir US$ 9,1 bilhões contra US$ 8,2 bilhões em 2.006 e, principalmente, que mais da metade deste mega-investimento, ou o equivalente a 53,8%, será destinada à compra de programas "anti-vírus"., que responderão, sozinhos, por US$ 4,9 bilhões. O "Gartner Group" estima que, em 2.007, em razão da crescente demanda de ataques cibernéticos às

rêdes corporativas, 3 em cada 4 organizações serão atacadas por códigos eletrônicos maliciosos. No Brasil, a venda de programas de computador destinados à proteção eletrônica foi estimada, pelo IDC-International Data Corporation Brasil (http://www.idclatin.com/default2.asp?ctr=bra), em US$ 144 milhões em 2.006, mais que o dobro do volume notado no ano anterior (2.005) (página 22 do vol. 11 da Revista "Security Review", em anexo).

7. Uma das maiores e mais conhecidas empresas de prestação de serviço medico do país – indicada às fls. 45 da revista mencionada – está investindo, apenas no Estado de SP, somas expressivas em segurança da informação, direcionando-as especificamente a sistemas de identificação biométrica para reconhecimento de seus segurados por impressões digitais. Anuncia que o faz porque "*...20% das despesas do atendimento médico no país em 2006 são fraudes*...", chegando à conclusão, por isso, que o investimento em sistemas eletrônicos, e em defesa desses, através de recursos tecnológicos de

segurança da informação que a resguarde contra fraudes humanas-eletrônicas, prestigiará a redução de seus custos operacionais, resultando na busca de melhores tarifas de serviços ao consumo (págs. 45 e 46 do vol. 11 da Revista mencionada – em anexo).

8. O BACEN-Banco Central, em nota publicada à pág. 51 da mesma Revista, anuncia que, até o dia 31.12.2007, todos os bancos brasileiros deverão cumprir a Resolução 3380/BACEN, de 29.06.2006, no sentido de otimizarem seus sistemas eletrônicos para redução de riscos operacionais (reportagem da pág. 51 da Revista mencionada).

9. À pág. 52, o Secretário Geral do CNJ-Conselho Nacional de Justiça, detalha o que será a Justiça brasileira com a completa integração-informatização dos 91 Tribunais brasileiros (a implantação do sistema eletrônico que irá eliminar o papel como matriz física do processo judicial brasileiro, em todas as instâncias, para todas as jurisdições – a questão está prevista na Lei 11.419/2006, e detalhada à

pág. 52/53 da Revista anexa). Sobre este projeto, diria, mega-projeto brasileiro – em nada inferior, talvez até superior, ao porte da transformação do processo eleitoral brasileiro em sistema eletrônico de eleições – *há números significativos*: 42 milhões de processos judiciais, contendo os dados da população brasileira, serão tornados eletrônicos. Suas peças, petições, provas, decisões, pareceres, serão, todos, transformados em "bits" digitais eletrônicos, que se incumbirão, ao invés do papel, da nova estruturação estatal do mecanismo de solução de conflitos do país. Em MG, na Justiça Estadual, há, hoje, 3.500.000 processos judiciais em papel; em SP, são 12.000.000 de processos judiciais na Justiça Estadual. Eles se tornarão eletrônicos. Os Tribunais estão implantando pilotos de experimentação desses processos sem papel. Em SP, foi recentemente inaugurado, na Freguesia do Ó, o primeiro Juizado Especial eletrônico da maior metrópole da AL. Nele, não há papel. Não há papel na Justiça Estadual de Florianópolis – Vara de Família virtual – nem na Vara Federal do JEF de São Gonçalo, no RJ; nem,

tampouco, no Fórum virtual (criminal, cível-de-família) de Manaus, e noutros tantos. Em MG, instalaremos, no Juizado Especial de Telefonia de Belo Horizonte, um dos maiores e mais movimentados do país, em agosto próximo, nosso primeiro experimento estadual de Justiça completamente eletrônica. Isto tem tomado dos Tribunais, particularmente das Diretorias de TI e dos magistrados que ocupam funções de TI, cuidados intensos com a segurança da informação (externa e interna), pois dados sensíveis da população, como os inerentes aos conflitos de família, os criminais, os que dizem respeito à intimidade das pessoas, aos segredos industriais, às cláusulas contratuais "non-disclosure", e tantos outros, não podem ser abertos ao público por sistemas eletrônicos desguarnecidos, ou fornecidos-comercializados desautorizadamente. Investimentos em TI, em mapeamento de pontos de vulnerabilidade eletrônica das rêdes internas e externas dos Tribunais, estão sendo alocados e previstos em "budgets" orçamentários.

10. Ainda assim, há riscos intensos – que precisam ser cuidados. Nos EUA, o sistema PACER, que coordena o programa de processo judicial eletrônico da Secretaria de Justiça norteamericana (mais de 25.000.000 de processos judiciais sem papel, das Côrtes Federais dos EUA), impede acessos a dados de intimidade dos litigantes processuais e responsabiliza, inclusive criminalmente, fraudes na obtenção não-autorizada desses dados. No Brasil, não dispomos de normas legais específicas que autorizem providências incriminadoras ou de criminalização específica, como esta, do acesso indevido a dados eletrônicos-processuais não-autorizados.

11. Não podemos deixar também de mencionar importante trabalho de pesquisa realizado pela empresa MÓDULO TECHNOLOGY FOR RISK MANAGEMENT – com mais de 600 profissionais brasileiros, atuantes nas áreas de Segurança e Tecnologia da Informação de organizações privadas, públicas, e de economia mista do país, nos segmentos de Governo, Financeiro, Informática, Indústria,

Prestação de Serviços, Telecomunicações, Comércio, Educação, Energia Elétrica, Saúde, Mineração, dentre outros. O trabalho – juntado, igualmente, a esta abordagem (entitulado "10ª. Pesquisa Nacional de Segurança da Informação", pág. 6) – mostra, como principais problemas relatados por estas corporações e como causas diretas de perdas financeiras, as seguintes:

a) ataques eletrônicos por vírus (15%);

b) ataques eletrônicos por spam (10%);

c) fraudes eletrônicas (8%);

d) vazamento de informações sensíveis (7%);

e) acesso remoto indevido (6%)

f) divulgação/roubo de senhas eletrônicas (5%);

g) invasão de sistemas internos (4%);

h) furto de informações proprietárias (2%);

i) sabotagem eletrônica (2%);

j) pirataria (2%);

l) espionagem (1%).

12. Estes dados estão refletidos na própria estruturação institucional da inteligência custodiada pelo Estado brasileiro. A ABIN-Agência Brasileira de Inteligência salienta – em reportagem com o Sr. Márcio Buzzanelli, que a dirige com "expertise" de ex-chefe de divisões de crime organizado e terrorismo no Oriente Médio (pág. 8 da Revista "Security Review", vol. 11, anexo) – instituiu o PNPC-Programa Nacional de Proteção ao Conhecimento, desenvolvendo trabalho no CEPESC_Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações, adotando metodologia denominada "risk@Gov" e usando o DSIC-Departamento de Segurança das Informações e Comunicações, criado pelo Presidente Lula especialmente para coordenação das atividades de segurança da

informação do governo federal. Isto, ou este arsenal público destinado à Segurança da Informação, decorre do fato de que, no dizer do referido gestor, "*...o setor público é responsável por uma série de serviços ao cidadão e, em última análise, um ataque à rede de dados de alguma instituição da Administração Pública Federal irá...prejudicar o fornecimento desses serviços, prejudicando o bem-estar do cidadão*...".

13. **Os riscos dos ataques à informação e aos dados sensíveis – corporativos públicos e privados – brasileiros têm crescido a ponto de os Estados internamente se organizarem para a dotação de organismos investigatórios-policiais especializados na coleta de indícios da prática de delitos eletrônicos (como a técnica do rastreamento dos endereçamentos IP). É uma realidade que retrata a que se nota fora do país[1]. Vejam exemplos brasileiros:**

---

[1] Anti-Phishing Working Group
CardCops
Corporate Investigator, The,
Cybercrime - Computer Crime and Intellectual Property Section
Delitos Informáticos (Espanha)
Delitos Informáticos (México)
Digicrime Inc.
The Fake Detective

A - Coordenadoria de Investigações Eletrônicas - MP/RJ
B - Delegacia Virtual - Rio de Janeiro
C - Delegacia de Repressão aos Crimes de Informática - DRCI
Delegacia Eletrônica - São Paulo
D - Delegacia Online - Rio Grande do Sul
E - Ministério Público Federal - Digi-Denúncia
F - Hotline Br - denuncie a pornografia infantil
G - Brasil Telecom - denúncias de fraude
H – Delegacia Especializada em Crimes Informáticos/BH-MG

14 – Outras particularidades da vida eletrônica brasileira têm chamado a atenção de organismos internacionais. Um exemplo é o das comunidades relacionais do "Orkut". Um programa gerado e concebito como

---

FBI
FraudWatch International
Incident Response, Electronic Discovery, and Computer Forensics
Internet Fraud Complaint Center
Internet Identity
Internet Safety - The Police Notebook
Interpol
Newsfactor - Cybercrime & Security
P2P Patrol
Perverted-Justice
Polícia Judiciária - criminalidade informática (Portugal)
US-Cert: Cyber Security Tips
Web Police
ZNet - News - Ecrime, Law & You

-

-

Hacking: (voltar)

-

AdvICE - database of information security
Hackers' Hall of Fame
Hacktivismo
MIT Hack Gallery
Zone-H

-

-

Mecanismos de bloqueio e filtros: (voltar)

-

Cybersitter
Net Nanny
SurfWatch - Internet Filtering Software
SurfControl
http://www.internetlegal.com.br/links/crimes.htm

um sistema relacional via Internet, destinado, conceitualmente, à formação de grupos – científicos, acadêmicos, relacionais familiares, afetivos, etc. – e criado, há três anos, nos EUA, por uma empresa norteamericana ("Google Inc"), tem, como sua maior comunidade mundial, a de jovens brasileiros, que compõe, hoje, mais de cinqüenta por cento do universo das comunidades "Orkut"de todo o globo. Pois o "Orkut" tem provocado, ao lado de seu incomensurável efeito benéfico-relacional, atentados brasileiros os mais variados, como páginas de ataque à honra de personalidades públicas, de corporações privadas, de formação (eletrônica) de comunidades voltadas para o crime financeiro, comercialização internacional e nacional de entorpecentes e, mais recentemente, organização de ataques físicos e cibernéticos coletivos, fatos que começam a chegar às barras dos criminais sob intensa discussão de tipicidade penal. As regras de extraterritorialidade da lei penal-convencional brasileira não têm conseguido inibir este crescente nível de criminalidade eletrônica e um dos

motivos tem sido a alegação do fato de que a estrutura física de armazenamento das páginas Orkut estaria situada em território norteamericano, sem possibilidade de atuação jurisdicional brasileira. O Ministério Público Estadual, de Minas Gerais, acaba, inclusive, de firmar acordo diretamente com a empresa "Google Inc." via do qual a empresa disponibilizará uma página/Internet direta e especialmente para acesso por Promotores de Justiça e Policiais de MG, a fim de que obtenham estes, ali, informações eletrônicas de praticantes de pedofilia eletrônica, promoção eletrônica de venda de armas e entorpecentes (vide http://www.mp.mg.gov.br/extranet/internet.action#o9gDPnwAHrvzTbhBHrxzifMBKXwzY5ICLnwDWvMCHjhkJ9MB0vwDK92qH9glXmdm5idl1Gtk7a).

15. Por último, estatísticas têm demonstrado que os ataques a rêdes corporativas de telecomunicações – intranets, extranets, internets – provêm, em percentuais significativos (acima de 24%), de iniciativas dos próprios empregados-colaboradores internos, bem como a eles tem sido em grande parte atribuída a ação

criminosa de comercialização de senhas, logs computacionais, e até códigos alfa-numéricos de telefonia móvel celular. Quem não se lembra da extensão da "clonagem celular" ? Começou com um singelo ato de cunho tecnológico – o uso de um scanner de radiofreqüência em regiões/antenas em que a emissão do sinal telefônico se fazia no modo analógico. Depois, passou para outro nível, o da fraude humana e não tecnológica, quando então, ao invés de equipamentos, foram subtraídos dados significativos (códigos alfa-numéricos) de bancos de dados das empresas de telefonia para comercialização em praça pública, o que passou a explicar a razão pela qual CDs de baixo custo, com milhares de números de telefones, tornaram-se comercializáveis, ilegalmente, em regiões centrais as mais variadas, como as de São Paulo, Rio de Janeiro, Belo Horizonte, e outras.

Em suma, Senhores Senadores, podemos resumir esses dados em objetivas conclusões. São elas:

A – O nível do envolvimento crescente da população – das pessoas naturais e

das corporações – com os sistemas eletrônicos em geral (rêdes corporativas internas, externas, Internet, telefonia móvel, fixa) atinge, na atualidade, volume majoritário do interesse nacional (cem milhões de telefones celulares, 50 milhões de telefones fixos, 20 milhões de usuários/Internet);

B- Os serviços públicos eletrônicos brasileiros – dos Poderes Executivo, Legislativo, Judiciário – cresceram e crescerão, significativamente, de agora em diante, de modo a exigirem cautelas e cuidados especiais por parte do Estado brasileiro quanto à Segurança da Informação relativamente aos dados sensíveis custodiados no âmbito de cada Poder;

C – Os ataques e condutas lesivas, contrárias a uma mínima visão de razoabilidade social, denotam crescente tendência delitiva por parte de usuários de sistemas eletrônicos de comunicação. Estes fatos arriscam interesses da majoritária parcela de usuários, formada por inocentes, gerando uma desigualdade prática que tem cunhado expressões as mais

inaceitáveis para o convívio harmônico como o da "engenharia social";

D – As ações criminosas eletrônicas, por razões de sofisticação, massificação, e alto poder ofensivo-humano, rompem o poder de defesa gerado por emprego de meros softwares ou medidas paliativas de proteção. A ação produtiva do injusto eletrônico reclama contra-ação estatal minimamente preventiva, que contenha a necessidade de emprego de grandes somas de recursos financeiros, grandes contingentes estratégicos, na defesa de dados sensíveis de interesse público, a portes administráveis;

E – Finalmente, o grau de interesses lesados ou sujeitos a risco de lesão potencial já sobe ao porte dos interesses tuteláveis pelo Estado através do emprego de medidas penais, especificamente de criminalização destas condutas.

Passamos, assim, a tratar do segundo ponto.

- Segundo -

A OPÇÃO DE CRIMINALIZAÇÃO DOS ILÍCITOS CIBERNÉTICOS PELO ESTADO BRASILEIRO

O moderno Direito Penal e os estudos de criminologia editados, no mundo contemporâneo – especialmente na Europa – após a fase do Iluminisno repugnam a primitiva idéia, que vigorou até à Idade Média, "da lei de Talião", do uso da pena, do Direito Penal, como meio de retribuição "pelo mal causado".

A criminalização não pode derivar de ímpeto estatal-retributivo.

A decisão do Estado de tornar determinada conduta crime deve ser a última "ratio", a última providência, tomada diante de indicadores ético-sociais mínimos que a justifiquem, com foco no resguardo das garantias fundamentais sobre as quais estruturado o próprio Estado.

Preserva-se, com isso, a idéia de mínima intervenção do Estado-sancionador na

vida comunitária que é própria do Estado de Direito. Este, o princípio da intervenção mínima, que se alia ao da fragmentariedade, no gerenciamento de uma visão moderna do Direito Penal que deve habitar um Estado Social de Direito, ambos indicando a necessidade de seleção de condutas que sejam efetivamente exorbitantes da razoabilidade do convívio, para que se sujeitem à criminalização.

Uma vez decidida a adoção da via penal como solução para dada tendência social de produção do injusto, deve-se respeitar, ainda, o derradeiro princípio gerenciador do moderno Direito Penal, que é o da proporcionalidade entre a criminalização, a pena e o fim buscado por ela.

O fim buscado pela pena, pela sanção penal, não pode ser outro, por sua vez, que não o estrito intuito de educação. A pena deve educar, a criminalização deve educar, limitativamente, a tendência social quanto à prática do crime (chama-se a esta finalidade de princípio da prevenção geral-limitadora da pena; por ela se educa socialmente, se educa o grupo, o

povo como um todo, disseminando-se uma lição prévia, teórica, formalizada no texto do crime instituído, de que o crime – e, principalmente, o valor jurídico-social que ele resguarda e representa – *constituirá atentado à harmonia* social, com resposta sancionadora-educativa pelo Estado). A pena educará, também, o próprio infrator, na medida em que deve permitir, quando aplicada, sua ressocialização, educando-o para um reingresso social pacífico sem o ímpeto delitivo demonstrado.

Tudo isso, no entanto, não afastou, dos Estados, o poder – aliás, um poder-dever de intensa valia social-coletiva – de delimitação das condutas que, mesmo por exceção, mesmo como última "ratio", reclamem solução criminalizante.

O Estado não se demitiu, pela visão moderna do Direito Penal, de sua precípua missão institucional, que é a de realizar o bem comum.

A Constituição e as leis não suprimiram do Estado o poder de criminalizar condutas sociais-infracionais de grande relevo para o resguardo do interesse comunitário.

Não. Ao contrário, em respeito ao próprio Estado de Direito, é, muitas vezes, através de adequada delimitação criminal da conduta-tipo que se resguardará, ao conjunto dos cidadãos de bem, inocentes, mínima garantia da imunidade aos efeitos do crime. O crime, definido, formalizado, como tal, na lei (em países, como o nosso, que adotam o sistema positivo), é também um veículo, um meio, de realização do próprio Estado de Direito, na medida em que representa a seleção, garantista, da pré-definida conduta-social grave, para submete-la à repercussão sancionatória, ao tempo em que delimita, com ela, todo o campo que deverá ser a ela imune.

Dizendo de outra forma, as incertezas eventuais quanto à incriminação de novas condutas que mantenham limites confusos com os de crimes antigos, pré-definidos, arriscam incriminações (judiciais) injustas.

A analogia – com crimes antigos – não pode suprir, em matéria penal, a lacuna da lei penal antiga. Isto significa que, diante de ausência de lei expressa sobre determinada conduta nova, não se poderá impor a criminalização em juízo e, consequentemente, a pena.

É o princípio da reserva legal e da legalidade estrita em matéria penal – "nullum crimen, nulla poena, sine lege" (é nula a pena e o crime sem prévia lei que os defina) – que impedem que a analogia seja usada para suprimento de lacuna legal em desfavor do acusado.

Assim, sem lei expressa que regule novas atividades criminosas, nem se conseguirá, com analogia de suprimento, incriminação de condutas graves, nem se assegurará, ao inocente delas, segurança de livramento a acusações que busquem intepretações extensivas da norma antiga.

Isto é o que nos parece ocorrer com o crime eletrônico, cibernético, brasileiro.

Tamanhas as alternativas já empregadas, coletivamente, na atual perpetração do injusto eletrônico, que ele reclama, neste momento, típica e definida criminalização, com a qual seja este novo fato social estremado de outros tipos penais antigos (lembrando, aqui, que o Código Penal brasileiro, para que o exemplo se limite à menção da lei geral-penal do país, data de mais de 60 anos e não contempla meios de interpretação extensiva, tampouco analógica, dc fatos eletrônicos que começaram a ser implementados no "Brasil pós-desestatização do Sistema Telebrás").

O atual Código Penal brasileiro não possui estruturação de crimes que possam abranger as imensas e inovadoras hipóteses do cybercrime (o "cracking", o "phishing scam", os atos dc "gray hat", "black hat", o "pichamento digital", a espionagem eletrônica, as difusões de códigos eletrônicos maliciosos danosos e não-danosos, ou a fraude eletrônica).

A proporção episódica desses novos crimes, como se demonstrou, saiu, há muito, da esfera de ocorrências para as quais se pudesse cogitar de marcos ou sanções puramente regulatórios-inibitórios civis, reparatórios, éticos, ou administrativos.

Sem uma firme decisão do Estado brasileiro, já neste momento – de intenso crescimento da planta de prestadores e de usuários dos variados sistemas eletrônicos – no sentido de submeter a balizas seguras, garantidoras de ambiente minimamente saudável, a atividade eletrônica-cibernética, deixar-se-á a realidade densa-criminal eletrônica já posta em prática à própria sorte.

Somente a coercitividade estatal, o poder de império do Estado, que habilita a imposição da "sanctio iuris", da sanção penal típica e pré-definida, ou, a pena, poderá educar, prevenir, na generalidade, com um "piso" de efetividade, o conjunto da população usuária de sistemas eletrônicos, educação prévia que se direcionará à extensa juventude "orkutiana"

brasileira, à imensa maioria dos atuais usuários de rêdes internas e externas, à fatia crescente dos internautas e prestadores dos serviços brasileiros de Internet, à centena de milhões de usuários da telefonia móvel celular, e aos milhões de correntistas do sistema financeiro, consumidores dos serviços de saúde, dos serviços públicos estatais, como os da Justiça, dentre outros, a respeitarem regras mínimas do convívio eletrônico.

Não nos parece adequado aguardar marcos regulatórios, pré-instituição civil de regras – coisa nunca exigida, aliás, na incriminação de condutas eletrônicas no Brasil – para que o Estado atenda, sob a ótica do Direito Penal, à presente necessidade.

Em termos de política criminal, e em respeito à história do tratamento penal das telecomunicações brasileiras, repare-se que, há exatos dez anos, em 1997, a própria LGT- Lei Geral de Telecomunicações (Lei 9.472/97), em seu art. 183, lançou-se à criminalização direta de específicas condutas sem aguardo de qualquer

marco regulatório, civil, ético, ou administrativo, e o fez diante da também direta constatação da alta potencialidade ofensiva do ilícito de telecomunicações, coisa que o legislador de 1.962 – quando editada a Lei 4.117/62 (o antigo Código Brasileito de Telecomunicações[2]) – também

---

2

LEI Nº 4.117, DE 27 DE AGOSTO DE 1962.

CAPÍTULO VII
Das Infrações e Penalidades

Art. 52. A liberdade de radiodifusão não exclui a punição dos que praticarem abusos no seu exercício.

Art. 53. Constitui abuso, no exercício de liberdade da radiodifusão, o emprêgo dêsse meio de comunicação para a prática de crime ou contravenção previstos na legislação em vigor no País, inclusive: (Redação dada pelo Decreto-Lei nº 236, de 1968)

a) incitar a desobediência às leis ou decisões judiciárias; (Redação dada pelo Decreto-Lei nº 236, de 1968)

b) divulgar segredos de Estado ou assuntos que prejudiquem a defesa nacional; (Redação dada pelo Decreto-Lei nº 236, de 1968)

c) ultrajar a honra nacional; (Redação dada pelo Decreto-Lei nº 236, de 1968)

d) fazer propaganda de guerra ou de processos de subversão da ordem política e social; (Redação dada pelo Decreto-Lei nº 236, de 1968)

e) promover campanha discriminatória de classe, côr, raça ou religião; (Redação dada pelo Decreto-Lei nº 236, de 1968)

f) insuflar a rebeldia ou a indisciplina nas fôrças armadas ou nas organizações de segurança pública; (Redação dada pelo Decreto-Lei nº 236, de 1968)

g) comprometer as relações internacionais do País; (Redação dada pelo Decreto-Lei nº 236, de 1968)

h) ofender a moral familiar, pública, ou os bons costumes; (Redação dada pelo Decreto-Lei nº 236, de 1968)

i) caluniar, injuriar ou difamar os Poderes Legislativos, Executivo ou Judiciário ou os respectivos membros; (Redação dada pelo Decreto-Lei nº 236, de 1968)

j) veicular notícias falsas, com perigo para a ordem pública, econômica e social; (Redação dada pelo Decreto-Lei nº 236, de 1968)

l) colaborar na prática de rebeldia desordens ou manifestações proibidas. (Incluído pelo Decreto-Lei nº 236, de 1968)

Parágrafo único. Se a divulgação das notícias falsas houver resultado de êrro de informação e fôr objeto de desmentido imediato, a nenhuma penalidade ficará sujeita a concessionária ou permissionária. (Partes mantidas pelo Congresso Nacional)

.....

Art. 55. É inviolável a telecomunicação nos têrmos desta lei. (Partes mantidas pelo Congresso Nacional)

Art. 56. Pratica crime de violação de telecomunicação quem, transgredindo lei ou regulamento, exiba autógrafo ou qualquer documento do arquivo, divulgue ou comunique, informe ou capte, transmita a outrem ou utilize o conteúdo, resumo, significado, interpretação, indicação ou efeito de qualquer comunicação dirigida a terceiro.

§ 1º Pratica, também, crime de violação de telecomunicações quem ilegalmente receber, divulgar ou utilizar, telecomunicação interceptada.

§ 2º Sòmente os serviços fiscais das estações e postos oficiais poderão interceptar telecomunicação.

I - A recepção de telecomunicação dirigida por quem diretamente ou como cooperação esteja legalmente autorizado;

II - O conhecimento dado:

a) ao destinatário da telecomunicação ou a seu representante legal;

b) aos intervenientes necessários ao curso da telecomunicação;

c) ao comandante ou chefe, sob cujas ordens imediatas estiver servindo;

d) aos fiscais do Govêrno junto aos concessionários ou permissionários;

e) ao juiz competente, mediante requisição ou intimação dêste.

Parágrafo único. Não estão compreendidas nas proibições contidas nesta lei as radiocomunicações destinadas a ser livremente recebidas, as de amadores, as relativas a navios e aeronaves em perigo, ou as transmitidas nos casos de calamidade pública.

Art 57. Não constitui violação de telecomunicação:

I - A recepção de telecomunicação dirigida por quem diretamente ou como cooperação esteja legalmente autorizado;

II - O conhecimento dado:

a) ao destinatário da telecomunicação ou a seu representante legal;

b) aos intervenientes necessários ao curso da telecomunicação;

c) ao comandante ou chefe, sob cujas ordens imediatas estiver servindo;

d) aos fiscais do Govêrno junto aos concessionários ou permissionários;

e) ao juiz competente, mediante requisição ou intimação dêste.

Parágrafo único. Não estão compreendidas nas proibições contidas nesta lei as radiocomunicações destinadas a ser livremente recebidas, as de amadores, as relativas a navios e aeronaves em perigo, ou as transmitidas nos casos de calamidade pública.

Art. 58. Nos crimes de violação da telecomunicação, a que se referem esta Lei e o artigo 151 do Código Penal, caberão, ainda as seguintes penas: (Substituído pelo Decreto-lei nº 236, de 28.2.1967)

I - Para as concessionárias ou permissionárias as previstas no artigos 62 e 63, se culpados por ação ou omissão e independentemente da ação criminal.

II - Para as pessoas físicas:

a) 1 (um) a 2 (dois) anos de detenção ou perda de cargo ou emprego, apurada a responsabilidade em processo regular, iniciado com o afastamento imediato do acusado até decisão final;

b) para autoridade responsável por violação da telecomunicação, as penas previstas na legislação em vigor serão aplicadas em dobro;

c) serão suspensos ou cassados, na proporção da gravidade da infração, os certificados dos operadores profissionais e dos amadores responsáveis pelo crime de violação da telecomunicação.

Art. 59. As penas por infração desta lei são: (Substituído pelo Decreto-lei nº 236, de 28.2.1967)

a) multa, até o valor .....NCR$ 10.000,00; (Incluído pelo Decreto-lei nº 236, de 28.2.1967)

b) suspensão, até trinta (30) dias; (Incluído pelo Decreto-lei nº 236, de 28.2.1967)

c) cassação; (Incluído pelo Decreto-lei nº 236, de 28.2.1967)

d) detenção; (Incluído pelo Decreto-lei nº 236, de 28.2.1967)

§ 1º Nas infrações em que, o juízo do CONTEL, não se justificar a aplicação de pena, o infrator será advertido, considerando-se a advertência como agravante na aplicação de penas por inobservância do mesmo ou de outro preceito desta Lei. (Incluído pelo Decreto-lei nº 236, de 28.2.1967)

§ 2º A pena de multa poderá ser aplicada isolada ou conjuntamente, com outras sanções especiais estatuídas nesta Lei. (Incluído pelo Decreto-lei nº 236, de 28.2.1967)

§ 3º O valor das multas será atualizado de 3 em 3 anos, de acordo com os níveis de correção monetária. (Incluído pelo Decreto-lei nº 236, de 28.2.1967)

Art. 60. A aplicação das penas desta Lei compete: (Substituído pelo Decreto-lei nº 236, de 28.2.1967)

a) ao CONTEL: multa e suspensão, em qualquer caso; cassação, quando se tratar de permissão; (Incluído pelo Decreto-lei nº 236, de 28.2.1967)

b) ao Presidente da República: cassação, mediante representação do CONTEL em parecer fundamentado. (Incluído pelo Decreto-lei nº 236, de 28.2.1967)

Art. 61. A pena será imposta de acordo com a infração cometida, considerados os seguintes fatores: (Substituído pelo Decreto-lei nº 236, de 28.2.1967)

a) gravidade da falta;

b) antecedentes da entidade faltosa;

c) reincidência específica.

implementara com amplitude e a Lei Geral das Telecomunicações, em pleno Estado de Direito democrático, resolveu referendar em seu art. 215[3].

Aliás, os crimes definidos pela LGT penalizam, com pena privativa de liberdade, de dois a quatro anos, aumentada da metade se houver dano a terceiro, o desenvolvimento clandestino de atividades de telecomunicação. Não houve surpresa ou questionamentos na época da tramitação congressual da LGT e a questão atual,

---

Art. 62. A pena de multa poderá ser aplicada por infração de qualquer dispositivo legal ou quando a concessionária ou permissionária não houver cumprido, dentro do prazo estipulado, exigência que tenha sido feita pelo CONTEL. (Substituído pelo Decreto-lei nº 236, de 28.2.1967)

Art. 63. A pena de suspensão poderá ser aplicada nos seguintes casos: (Substituído pelo Decreto-lei nº 236, de 28.2.1967)

a) infração dos artigos 38, alíneas a, b, c, e, g e h; 53, 57, 71 e seus parágrafos;

b) infração à liberdade de manifestação do pensamento e de informação (Lei nº 5.250 de 9 de fevereiro de 1967);

c) quando a concessionária ou permissionária não houver cumprido, dentro do prazo estipulaçao, exigência que lhe tenha sido feita pelo .....CONTEL;

d) quando seja criada situação de perigo de vida;

e) utilização de equipamentos diversos dos aprovados ou instalações fora das especificações técnicas constantes da portaria que as tenha aprovado;

f) execução de serviço para o qual não está autorizado. (Incluído pelo Decreto-lei nº 236, de 28.2.1967)

Parágrafo único. No caso das letras d, e e f deste artigo poderá ser determinada a interrupção do serviço pelo agente fiscalizador. "ad-referedum" do CONTEL.

.....

Art. 70. Constitui crime punível com a pena de detenção de 1 (um) a 2 (dois) anos, aumentada da metade se houver dano a terceiro, a instalação ou utilização de telecomunicações, sem observância do disposto nesta Lei e nos regulamentos. (Substituído pelo Decreto-lei nº 236, de 28.2.1967)

Parágrafo único. Precedendo ao processo penal, para os efeitos referidos neste artigo, será liminarmente procedida a busca e apreensão da estação ou aparelho ilegal.

Art. 72. A autoridade que impedir ou embaraçar a liberdade da radiodifusão ou da televisão fora dos casos autorizados em lei, incidirá no que couber, na sanção do artigo 322 do Código Penal. (Substituído pelo Decreto-lei nº 236, de 28.2.1967)

[3] Art. 215. Ficam revogados:

I - a Lei nº 4.117, de 27 de agosto de 1962, salvo quanto a matéria penal não tratada nesta Lei e quanto aos preceitos relativos à radiodifusão;

quando passada uma década do fenômeno da desestatização do Sistema Telebrás, se apresenta muito mais grave e mais extensa, pois, ao invés de termos, no Brasil, meros circuitos de telecomunicações, há serviços densos, extensos, de comunicação eletrônica (por dados e voz), trafegando por rêdes corporativas, públicas e privadas, de grande relevância.

Confira-se o art. 183 da Lei 9472/97:

" Lei 9472/97:
Capítulo II
Das Sanções Penais
Art. 183. Desenvolver clandestinamente atividades de telecomunicação:
Pena - detenção de dois a quatro anos, aumentada da metade se houver dano a terceiro, e multa de R$ 10.000,00 (dez mil reais).
Parágrafo único. Incorre na mesma pena quem, direta ou indiretamente, concorrer para o crime.
Art. 184. São efeitos da condenação penal transitada em julgado:
I - tornar certa a obrigação de indenizar o dano causado pelo crime;
II - a perda, em favor da Agência, ressalvado o direito do lesado ou de terceiros de boa-fé, dos bens empregados na atividade clandestina, sem prejuízo de sua apreensão cautelar.
Parágrafo único. Considera-se clandestina a atividade desenvolvida sem a competente concessão, permissão ou autorização de serviço, de uso de radiofreqüência e de exploração de satélite.
Art. 185. O crime definido nesta Lei é de ação penal pública, incondicionada, cabendo ao Ministério Público promovê-la."

Nossa posição é, portanto, a de que a criminalização dos ilícitos cibernéticos se impõe, constituindo exigência social de envergadura no momento.

Vamos, com esta premissa, ao derradeiro ponto.

- Terceiro –

BREVE ANÁLISE DOS DISPOSITIVOS SUGERIDOS PELO SUBSTITUTIVO EM DISCUSSÃO

O primeiro grande ponto deste tópico, ou aquele que nos preocupa nesse momento, é o que se relaciona com a linguagem normativa proposta.

Na medida em que decidida a criminalização, a linguagem definidora do tipo penal se mostra de grande relevância, sobretudo no Brasil, em que a interpretação da norma penal deve observar rigoroso limite de legalidade – que comanda o princípio de que a dúvida prestigiará sempre a inocência ("in dubio pro reo").

Entretanto, paralelamente a este aspecto, deve-se salientar que a tendência moderna-mundial, de regramento dos tipos tecnológicos, caminha para antagônico sentido,

que é o da delimitação "aberta" dos elementos, ou, das circunstâncias elementares que os caracterizem, pois, em razão da inovação tecnológica, não se pode perder a essência da definição legal frente às evolutivas alterações estruturais que o tempo permite.

Em matéria penal, então, a questão se avoluma, pois, na medida em que se pode inovar o meio com maior velocidade, corre-se o risco, no enfeixamento gramatical de hipóteses normativas cujo alvo seja a tecnologia da informação, de se transformar a norma incriminadora em instrumento inócuo de aplicação, por rápida desatualização.

Como conciliar, então, no bojo da (antiga) lei penal brasileira, e dentro do escopo constitucional de observância da legalidade estrita, a correta definição, que será sempre gramatical, dos novos crimes informáticos ?

Dosagem da linguagem, sua adequação teleológica ao caráter (universal) das rêdes telecomunicativas – o que constituirá

missão de atividade empregável "a posteriori" e não "a priori" do processo legislativo, pois ligada ao próprio trabalho interpretativo (jurisdicional e jurisprudencial, e não congressual). Além disso, uma certa inspiração dosada por medidas externas ao âmbito nacional – o exemplo maior nos parece ser a Convenção Européia de Cybercrimes, atualmente firmada, na Europa, por mais de 40 países – sintetizam, digamos, o "estado da arte" que poderá ser adotado na missão de disciplinar, criminalmente, o cybercrime.

Neste ponto, parece-nos que o substitutivo apresentado aos três Projetos em análise atende ao propósito.

Vejamos um-a-um os tipos novos por ele editados (nossas notas estão feitas em caixas de texto laterais a cada um):

> " 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, e a Lei nº 8.078, de 11 de setembro de 1990 (Código do Consumidor), 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, e a Lei nº 8.078, de 11 de setembro de 1990 (Código do Consumidor), 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 141-A:

Aumento razoável dos crimes contra a honra, de grde. Incidência no meio eletrônico atual

"**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 A VIOLAÇÃO DE REDE DE COMPUTADORES, DISPOSITIVO DE COMUNICAÇÃO OU SISTEMA INFORMATIZADO

O bem jurídico é a proteção ao sigilo de dados sensíveis. Está bem alocado pois resguarda ao legítimo titular a garantia à guarda de dados sob sigilo. Bem alocado em crimes contra a pessoa. Crime de mera conduta. Se exaure com ela. A conduta é reprimida. É ela que ameaça, que obriga ao grande custo operacional

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.

§ 1° 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.

§ 2° 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.

§ 3° 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.

~~§ 4° Não há crime quando o agente acessa a título de defesa digital, excetuado o desvio de finalidade ou o excesso.~~

Conduta menos grave – o bem jurídico é o de resguardo do sigilo de dados, sendo que, nesta hipótese, não houve o ato de acesso – que é o mais grave, pois acessar é invadir um ambiente eletrônico vedado. Aqui a obtenção não tem a conduta anterior, de acesso. A pena máxima comporta conversão em restritiva de direitos

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.

§ 1° 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.

§ 2° 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.

§ 3° 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.

Relação meramente exemplificativa, não-taxativa. Necessidade mínima de tipo penal que assegure-preveja a hipótese de inovação tecnológica, sem vácuo para a incriminação

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 – defesa digital: manipulação de código malicioso por agente técnico ou profissional habilitado, em proveito próprio ou de seu preponente, e sem risco para terceiros, de forma tecnicamente documentada e com preservação da cadeia de custódia no curso dos procedimentos correlatos, a título de teste de vulnerabilidade, de resposta a ataque, de frustração de invasão ou burla, de proteção do sistema, de interceptação defensiva, de tentativa de identificação do agressor, de exercício de forense computacional e de práticas gerais de segurança da informação;

Bem jurídico ainda é o sigilo de dados sensíveis. Aqui é a divulgação, sem acesso e sem obtenção interna. É o intermediario dos dados, que está hoje intermediando o *negócio do crime* eletrônico e precisa ser contido. A pena é baixa e permite, delito de pequeno potencial ofensivo (pode ser convertida em reparaçção de danos ou restritiva de direitos).

V - 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.

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) "

Forma qualificada do furto – crime mais grave contra o patrimônio. Justifica-se por causa das inúmeras tentativas de obtenção de valores com uso de redes de computadores (fraudes bancárias, etc.). É o tipo mais grave – furto qualificado (2 a 8 anos de reclusão). Regime inicial semi-aberto.

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

O bem jurídico tutelado é a imunidade a vírus de computador, de alta incidência. Pena baixa inclusive, por crimes simples, com possib. de suspensão condicional do processo e imposição de restritiva de direitos (art. 44 da Lei 9099/95)

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.

Dolo específico. "Animus necandi". Forma grave. Não é apenas o pixador digital. Quer destruir com vírus. É o black hat. O pior delinqüente. O crime dá conversão por restritiva de direitos.

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.

Crime preterdoloso. Agravação pela obtenção (involuntária-culposa) do resultado mais grave – o dano do sistema eletrônico. É a única forma de educar socialmente contra a disseminação de vírus, prevendo que sua disseminação danosa, mesmo involuntária, causará pena.A pena pode ser iniciada, se fixada no máximo, em regime semi-aberto, com trabalho extra-muros.

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.

§ 4º Não há crime quando a ação do agente é a título de defesa digital, excetuado o desvio de finalidade ou o excesso."

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

Estelionato digital. Crime contra o patrimônio. O bem jurídico tutelado é o patrimônio do "homus medius", simples, que não está afeito, habilitado à lida com sistemas eletrônicos e está sujeito, por isso, à engenharia social. Pena comporta suspensão condicional do processo, com imposição de restrição de direitos.

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, ou a obtenção de qualquer vantagem ilícita:

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.

~~§ 2º Não há crime quando a difusão ocorrer a título de defesa digital, excetuado o desvio de finalidade ou o excesso.~~"

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

O dispositivo é importante para vincular, dentro da reserva legal-penal, o dado eletrônico ao sentido semântico de coisa

"**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**

O dispositivo nada faz senão acrescentar serviço de informação e de telecomunicação ao escopo de tutela do bem jurídico (a proteção dos meios de comunicação). É uma atualização, no particular, do CP

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. 9° 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.

Equipara o cartão de crédito ou dispositivo eletrônico de captação de dados débito para efeito de falsificação (não há inovação em si; há extensão do crime ao documento eletrônico)

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**

Falsificação de códigos alfanuméricos – sobretudo agora que teremos a portabilidade legal no país – é o meio de se resguardar o bem jurídico representado pelo número alfanumérico e pelos dados de conexão telefônica e de conexão computacional (resguarda e protege contra clonagem e resguarda a prática de VoIP). A pena permite suspensão condicional do processo, com imposição de restrição de direitos.

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 § 6° do art. 240 do Decreto-Lei n° 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 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.

§ 4º Não há crime quando a ação do agente é a título de defesa digital, excetuado o desvio de finalidade ou o excesso."

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

"Capítulo VII-A

DOS CRIMES CONTRA A VIOLAÇÃO DE 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.

§ 3º Não há crime quando o agente acessa a título de defesa digital, excetuado o desvio de finalidade ou o excesso.

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 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.

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

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, 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 – defesa digital: manipulação de código malicioso por agente técnico ou profissional habilitado, em proveito próprio ou de seu preponente, e sem risco para terceiros, de forma tecnicamente documentada e com preservação da cadeia de custódia no curso dos procedimentos correlatos, a título de teste de vulnerabilidade, de resposta a

ataque, de frustração de invasão ou burla, de proteção do sistema, de interceptação defensiva, de tentativa de identificação do agressor, de exercício de forense computacional e de práticas gerais de segurança da informação;

V - 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.

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, ou a obtenção de qualquer vantagem ilícita:

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.

§ 2º Não há crime quando a difusão ocorre a título de defesa digital, excetuado o desvio de finalidade ou o excesso."

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:

O dispositivo permite a interceptação telefônica em crimes apenados com detenção, quando se tratar de telefonia por IP (computadores) – VoIP. Neste caso, mesmo com detenção, poderá haver a interceptação por ordem judicial

"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 IV:

Rigor grande – da prisão preventiva – mas dentro do critério da prevenção geral educativa, no sentido de que, apesar de penas (quase todas) conversíveis em restritiva de direitos e suspensão condicional do processo, o ataque eletrônico pode determinar prisão preventiva.

"Art. 313. .....

IV – *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:

Insere os delitos cibernéticos-eletrônicos na competência de atuação da Polícia Federal, quando tiverem repercussão interesetadual ou internacional, o que logiciza o fato de que o crime eletrônico se desapega de critérios espaciais-convencionais e por isso reclama providências policiais de investigação mais amplas

"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)"

Obrigação não-criminal dos provedores (administrativa), de guarda de dados, que só poderão ser entregues a autoridades públicas e por ordem judicial. O sigilo de comunicações já funciona desta forma, tendo as empresas de telecomunicações igual dever

Art. 21. O responsável por liberar o acesso a uma rede de computadores ou prestar serviços mediante seu uso é obrigado a:

I – manter em ambiente controlado e de segurança os dados de conexões realizadas por seus equipamentos, aptos à identificação do usuário e dos endereços eletrônicos de origem, da data, do horário de início e término e referência GMT, das conexões, pelo prazo de três anos, para prover os elementos probatórios essenciais de identificação da autoria das conexões na rede de computadores;

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 conexões realizadas e os dados de identificação de usuário;

IV – preservar imediatamente, após a solicitação

A norma não inova, pois obriga ao atendimento de um dever, que é o de não ocultar prática criminosa no meio eletrônico. Pois ocultar é praticar crime de favorecimento pessoal ou real (art. 348/349 do CP). Ver art. 22 a seguir

expressa da autoridade judicial, no curso de investigação, os dados de conexões realizadas, os dados de identificação de usuário e o conteúdo das comunicações realizadas daquela investigação, cuidando da sua absoluta confidencialidade e inviolabilidade;

V – informar, de maneira sigilosa, à autoridade policial competente, denúncia da qual tenha tomado conhecimento e que contenha indícios de conduta delituosa na 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 conexões realizadas em rede de computadores, aptos à identificação do usuário, 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.

§ 4° 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. 22. 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 identificação de usuário, quando constatada qualquer conduta criminosa.

Art. 23. Esta Lei entrará em vigor sessenta dias após a data de sua publicação.

Disso se tem, além da adequação da criminalização, o seguinte:

1 – Afora as propostas de instituição do crime de furto qualificado e de crime preterdoloso de dano, todos os demais tipos penais criados pelo Substitutivo contêm penalidades (penas privativas da liberdade) que se sujeitam ora a conversão direta a indenização ou penas restritivas de direito (na forma do art. 61 e 75 da Lei 9.099/95) ora a suspensão condicional do processo (na forma do art. 89 da mesma Lei 9.099/95), ora, ainda, a conversão pura em penas

restritivas de direitos (na forma do art. 33 c/c art. 44 do Código Penal brasileiro);

2 – Não se proclama, portanto, exacerbação penalisadora, pelo que se vê preservação de proporcionalidade na resposta penal cominada a cada infração nova proposta.

CONCLUSÃO

Por todo o exposto, somos de opinião de que o Substitutivo apresentado aos três Projetos de Lei recomenda aprovação, pela adequação com a gravidade dos fatos tratados e pelo respeito que promove à finalidade preventiva-geral dos ilícitos proclamados, sendo que a penalisação proposta evidencia submissão a princípios e balizas aceitáveis de proporcionalidade e razoabilidade.

Opinamos pela aprovação do Substitutivo no âmbito desta Comissão.

Fernando Neto Botelho

RELATÓRIO

RELATOR: Senador **EDUARDO AZEREDO**

I – RELATÓRIO

Chegam a esta Comissão, para parecer, o Projeto de Lei da Câmara (PLC) nº 89, de 2003 (nº 84, de 1999, na origem), e os Projetos de Lei do Senado (PLS) nº 137, de 2000, e nº 76, de 2000, todos referentes a crimes na área de informática. Tramitam em conjunto, em atendimento ao Requerimento nº 847, de 2005, do Senador Renan Calheiros. Em decorrência do Requerimento nº 848, de 2005, foi extinta a urgência na tramitação do PLC nº 89, de 2005, que havia sido declarada em decorrência da aprovação do Requerimento nº 599, de 2005, de autoria da Senadora Ideli Salvatti. Os projetos de lei do Senado perdem o caráter terminativo nas comissões.

O PLS nº 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 delitos cometidos com o uso de computadores, e atribui-lhes as respectivas penas, sem entretanto alterar o 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 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 Decreto-Lei n° 2.848, de 7 de dezembro de 1941 (Código Penal), 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 PLC 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* ao tipo penal de atentado contra a segurança de serviço de utilidade pública (art. 265) e ao 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).

Tendo estado à disposição dos senhores Senadores, o PLC n° 89, de 2003 não recebeu emendas.

II – ANÁLISE

Muitas são as proposições legislativas já produzidas e debatidas no Congresso Nacional a respeito do tema da criminalidade nas áreas da informática, das telecomunicações e da Internet, a rede mundial de computadores. A evolução das tecnologias relacionadas à produção, ao processamento, ao armazenamento e à difusão da informação tem ocorrido com muita velocidade, gerando lacunas no ordenamento jurídico vigente.

A existência dessas lacunas tem motivado a proliferação de casos de fraudes e de danos ao patrimônio e danos morais de agentes públicos e privados. Estima-se que bilhões de reais já foram desviados de contas bancárias de pessoas físicas ou jurídicas em decorrência da atuação indevida de especialistas da área. Além disso, a violação de bases de dados mantidas em meio eletrônico tem provocado danos de grande monta pelo roubo de informações pessoais.

Não bastasse isso, há evidências de ligação entre o cibercrime e o financiamento do terrorismo internacional, e o crescimento do tráfico de seres humanos e de drogas. E 2004 foi apontado como o ano em que os crimes cibernéticos passaram a gerar mais lucros até mesmo do que o tráfico de drogas. De acordo com pesquisa realizada pela firma de consultoria americana *Computer Economics*, em 2004 as perdas totais chegam a 18 bilhões de dólares, com uma taxa de crescimento anual próxima de 35%.

A sociedade clama por medidas eficazes no combate ao crime cibernético. Não é mais possível que divergências hermenêuticas acerca da possível aplicabilidade das nossas normas jurídicas a esse tipo de conduta continuem a impedir a punição de condutas extremamente nocivas ao País.

A imprensa nacional destaca recentemente que alguns internautas já começam a fazer justiça pelas próprias mãos contra usuários pedófilos ou terroristas do sítio *Orkut*, denunciando-os ao provedor. O *Orkut*, um serviço da multinacional americana *Google*, imediatamente retira aqueles usuários do sistema mas não consegue detectar e impedir a sua reinclusão, face á liberalidade, e não liberdade, registre-se, inerente à rede mundial de computadores. Estabelece-se assim o círculo da denúncia e da punição responsável mas este círculo tem como resposta novo círculo vicioso com o reinício dos delitos por novos usuários não identificados, tudo isto sem que se perceba um fim próximo.

O PLS nº 137, de 2000, demonstra preocupação idêntica ao dos projetos que acompanha, qual seja a de disciplinar as condutas perniciosas que utilizem ou danifiquem sistemas de computador. Não obstante, é de abrangência e precisão mais restrita que aqueles, que o englobam integralmente.

O projeto limita-se a estabelecer que os crimes contra a pessoa, o patrimônio, a propriedade imaterial e intelectual, os costumes, bem como contra a criança e o adolescente, cometidos com a utilização de meios de tecnologia de informação e telecomunicações, terão suas penas triplicadas. Ou seja, a pena seria agravada em razão do meio utilizado pelo agente para perpetrar o crime.

A alteração legislativa proposta pelo PLS nº 137, de 2000, não é conveniente por duas razões.

Em primeiro lugar, tornaria superlativo o desvalor do meio utilizado pelo agente, que prevaleceria mesmo sobre o desvalor do resultado ou da conduta (genericamente considerada) – aquele, inspirador da teoria clássica da ação; este, da teoria finalista da ação, adotada pelo Código Penal a partir da reforma da sua Parte Geral, empreendida pela Lei nº 7.209, de 11 de julho de 1984. A segunda razão, que decorre da anterior, é a desproporcionalidade na aplicação das penas, haja vista que um delito menos grave poderia ser apenado mais severamente do que outro mais reprovável, apenas por ter sido cometido por meio da Internet.

O PLC nº 89, de 2003, pretende inserir a Seção V no Capítulo VI do Título I do Código Penal, onde seriam definidos os crimes contra a inviolabilidade dos sistemas informatizados. São nove as condutas delituosas por meio de acesso a sistema eletrônico de que trata o PLC:

- o acesso indevido a meio eletrônico;
- a manipulação indevida de informação eletrônica;
- o dano eletrônico;
- a pornografia infantil;
- o atentado contra a segurança de serviço de utilidade pública;
- a interrupção ou perturbação de serviço telegráfico e telefônico;
- a falsificação de cartão de crédito;
- a falsificação de telefone celular;
- a divulgação de informações pessoais ou de empresas.

Vejamos cada um desses tipos.

a) Arts. 154-A, 154-B e 154-C do CP, ou seja, o acesso indevido, a manipulação indevida de informação e a definição de meio eletrônico e sistema informatizado).

A redação pode ser aperfeiçoada para registrar que o meio eletrônico ou sistema informatizado é protegido contra o acesso de estranhos, e que o agente consegue o acesso mediante a violação desse sistema de proteção. Além disso, o tipo não configuraria crime contra a pessoa, razão pela qual não deveria ser incluído no Título I do Código Penal, sendo mais adequado colocá-lo no Título II – DOS CRIMES CONTRA O PATRIMÔNIO.

Já a pena, que seria aplicada ao *hacker*, nome dado ao usuário que tenta violar ou viola o sistema de proteção, deveria ser mais severa.

Ademais, embora os três artigos possam ser reunidos em um só, preferimos manter a redação dada pelo PLC nº 89 de 2003, que define com maior clareza os delitos que se pretende tipificar. Entretanto propomos a alteração da pena original de detenção para reclusão, de 2 (dois) a 4 (quatro) anos, e multa, mantendo os mesmos parágrafos.

Ainda, quando este PLC nº 89 de 2003 estava sendo relatado nesta Comissão, o atento Senador Hélio Costa fez algumas sugestões de emendas que os membros da Comissão entenderam necessárias, mas que deveriam fazer parte de um novo Projeto de Lei a fim de que aquele projeto em discussão, uma vez aprovado, pudesse ir à sanção presidencial. Estando ele apensado ao PLS nº 76 de 2000 entendemos que é hora de acatar aqui aquelas sugestões.

A primeira sugestão aqui acatada trata da definição e tipificação da Fraude Eletrônica, conhecida pelos profissionais de - Tecnologia de Informação e Comunicação (TIC) - como *phishing* ou *port fishing*, incluindo-a no Código Penal como segue:

Fraude Eletrônica

Art. 180 - D. Difundir, por qualquer meio, sistema informatizado com o propósito de induzir alguém a fornecer, espontaneamente e por qualquer meio, dados ou informações que facilitem ou permitam o acesso indevido ou sem autorização, a dispositivo de comunicação ou a sistema informatizado:

Pena – reclusão de dois a quatro anos e multa.

Parágrafo único. 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, ou se o sistema informatizado fraudador tiver potencial de propagação ou alastramento.

Outra sugestão também acatada refere-se à inclusão de alteração ao art. 46 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940, Código Penal, mediante a inclusão a ele do § 5º dando a opção ao juiz a aplicação de pena alternativa, onde ao final do parágrafo entendemos por bem introduzir "sempre sob supervisão nomeada pelo juiz":

Art. 46 .....

.....

§ 5º No caso de crime praticado contra ou por meio de dispositivo de comunicação ou sistema informatizado, o juiz poderá aproveitar as habilidades e conhecimentos do condenado para ministrar cursos ou para trabalhos de criação de sistemas informatizados em empresas ou instituições públicas, ou para qualquer tipo de prestação de serviços equivalente, **sempre sob autoridade supervisora nomeada pelo juiz.**

Finalmente o Senador sugeriu a mudança do termo "meio eletrônico" por "dispositivo de comunicação" no art. 180-C, à qual no substitutivo promovemos sua atualização e complementação:

Dispositivo de Comunicação e Sistema Informatizado

Art. 180-C Para os efeitos penais, considera-se:

I – dispositivo de comunicação: o computador, o processador de dados, o disquete, o CD-ROM ou qualquer outro meio capaz de armazenar ou transmitir dados de maneira magnética, ótica, ou eletronicamente.

II – sistema informatizado: a rede de computadores, a base de dados, o programa de computador ou qualquer outro sistema capaz de armazenar ou transmitir dados eletronicamente.

b) Arts. 163, §§ 2°e 3°, e 167 do CP

A equiparação feita pelo § 2° é pertinente, mas poderia estar posicionada no Capítulo VIII do Título II (Disposições Gerais), pois dessa forma a regra seria válida para todos os tipos de crimes contra o patrimônio. Quanto à conduta do § 3°, entendemos que a pena deva ser mais severa, tendo em conta a potencialidade do dano material que se pode causar. Em vista disso, sugerimos a seguinte redação:

§ 3° No caso do § 2°, se o dano é decorrente de difusão de vírus eletrônico:

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

Por sua vez, a alteração proposta para o art. 167 do CP não é conveniente.

c) Art. 218-A do CP

O delito descrito nesse dispositivo já está previsto, de modo mais abrangente, nos arts. 240 e 241 do Estatuto da Criança e do Adolescente (ECA).

d) Arts. 265 e 266 do CP

As alterações propostas para esses dispositivos são convenientes.

e) Arts. 298 e 298-A do CP

A redação que se propõe para o art. 298 é conveniente; quanto ao art. 298-A, procedemos a pequenas modificações de forma a melhorar sua clareza e compreensão.

f) Art. 2°, § 2°, da Lei n° 9.296, de 1996

A alteração prevista no art. 2° da Lei n° 9.296, 24 de julho de 1996, é inconstitucional, pois não se justifica violar a intimidade do indivíduo se o crime supostamente cometido é punido, no máximo, com mera detenção. Além disso, nos moldes aqui propostos, os novos tipos penais seriam punidos, todos eles, com reclusão.

g) Art. 10 do PLC n° 89, de 2003

O dispositivo é desnecessário, pois o próprio Código Penal Militar dá o conceito de crime militar e regula a competência para o seu julgamento.

Por fim, o art. 11 do projeto mostra-se adequado, enquanto o art. 12 não é conveniente, sendo preferível manter o sistema de crimes estabelecido nos arts. 240 e 241 do ECA. A Lei n° 10.764, de 12 de novembro de 2003, alterou o art. 241 do Estatuto da Criança e do Adolescente (Lei n° 8.069, de 13 de julho de 1990), para tipificar e punir de forma mais severa a pornografia infantil.

O PLS n° 76, de 2000, revestido de norma autônoma, afigura-se o projeto mais abrangente entre os que estão sendo aqui analisados. Os crimes informáticos estão divididos, no projeto, em crimes 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 opção sexual e contra a segurança nacional.

Realmente a visão ampla que se tem dos crimes de informática é o grande mérito deste projeto inovador proposto pelo eminente Senador Renan Calheiros. Seus dispositivos mostram a gravidade crescente dos delitos praticados com instrumentos informatizados, cujas punições ainda não têm o necessário suporte legal. Isto vem trazendo enorme insegurança a toda a sociedade pois crimes são praticados no anonimato da internet e para os quais não há a mínima possibilidade de defesa pelo usuário.

Entretanto, a descrição de algumas das condutas deixa dúvidas em relação aos elementos dos respectivos delitos, o que pode prejudicar sua compreensão.

Vale lembrar que a Lei Complementar nº 95 de 1998 determina que havendo legislação em vigor deve-se preferir a sua alteração à criação de nova norma e desta forma o substitutivo proposto promove alterações ao Decreto-Lei nº 2.848, de 7 de dezembro de 1940, o Código Penal.

Comentamos, a seguir, sobre as disposições do PLS nº 76, de 2000.

a) Art. 1º, § 1º – crimes a inviolabilidade de dados e sua comunicação

Os incisos I, IV e V são espécies de crime de dano, descrito no art. 163 do CP; além disso, o inciso V deveria tipificar não a mera programação de instruções, mas a sua efetiva utilização, pois o nosso direito, via de regra, não pune os atos meramente preparatórios. Pode-se, alternativamente, prever, no art. 163 do CP, a equiparação dos dados informatizados à coisa, como o fez o PLC nº 89, de 2003, ou fazê-lo ao final do Título II do CP.

O inciso II pode ser tido como furto (art. 155 do CP), se houver subtração da coisa, ou como apropriação indébita (art. 168 do CP), se o agente tinha a posse ou a detenção da coisa. Quanto ao inciso III, melhor seria punir o uso indevido dos dados em razão da finalidade do agente: se atenta contra a intimidade da pessoa, contra o patrimônio, contra a fé pública, etc. Entretanto, há que se ter em conta que a maioria desses crimes já existe, e que a informática é apenas um meio para realização da conduta delituosa. A equiparação à coisa que se pode fazer ao final do Título II do CP resolveria o problema.

Além disso, as penas propostas são muito brandas em face da gravidade das condutas equiparadas que acima citamos.

b) Art. 1º, § 2º

Os incisos I e II são espécies de furto, crime definido no art. 155 do CP, cuja pena é bem mais severa do que a proposta no PLS nº 76, de 2000.

c) Art. 1º, § 3º

O inciso I está incluso no crime de injúria, descrito no art. 140 do CP; a conduta do inciso II, por sua vez, poderia ser inserida no Código Penal, mediante

acréscimo do art. 180-E. Cabe observar que, se a informação for lesiva à honra, sua divulgação importará em um dos crimes tipificados no Capítulo V do Código Penal (calúnia, difamação ou injúria). Para coibir o anonimato permitido pela internet, normalmente o caminho usado pelos autores dos crimes aqui tipificados, incluímos os artigos 180-G e 180-H.

Todos os atos e fatos que se materializam através destes meios chegam, facilmente e rapidamente, ao conhecimento de milhões de pessoas, causando um considerável prejuízo aos bens jurídicos tutelados. É necessário, portanto, maior força penal coercitiva para evitá-los e assim fizemos incluir o art. 141-1 conforme o art. 7° do substitutivo, alterando a pena de detenção para reclusão se o meio utilizado é um dispositivo de comunicação ou sistema informatizado. A mesma alteração está proposta para o crime de ameaça, fazendo incluir o § 2° ao art. 147, renumerando o parágrafo único existente, conforme o art. 8° do substitutivo.

d) Art. 1°, § 4°

O inciso I, a depender do resultado da conduta, será crime de lesão corporal ou homicídio, ambos já tipificados no Código Penal (arts. 129 e 121, respectivamente). O inciso II traz a incriminação de ato meramente preparatório. Além disso, os artefatos explosivos têm ampla utilização na indústria, não sendo conveniente definir como crime o trabalho intelectual de elaboração de um sistema informatizado de detonação.

e) Art. 1°, § 5°

As condutas descritas nos incisos I e II configuram crime contra a ordem tributária, definidos de forma mais abrangente e adequada nos arts. 1° e 2° da Lei n° 8.137, de 27 de dezembro de 1990.

f) Art. 1°, § 6°

O inciso I já está definido no art. 218 do CP (corrupção de menores). Os incisos II e III estão inclusos no art. 234 do CP (escrito ou objeto obsceno). Novamente, com o anonimato coibido pelos artigos 180-G e 180-H do substitutivo os autores destes crimes estarão desestimulados a cometê-los.

g) Art. 1°, § 7°

Os crimes definidos nesse parágrafo já estão contemplados na Lei n° 7.170, de 14 de dezembro de 1983 (Lei de Segurança Nacional), especificamente nos seus arts. 13, 15 e 23.

Recentemente em Audiência Pública sobre o PLS n° 279 de 2003, do qual também sou relator, de autoria do nobre Senador Delcídio Amaral e que propõe a criação de um cadastro de titulares de correio eletrônico na internet, ficou evidente que, para fins de investigação, é necessário estabelecer um prazo legal de armazenamento dos dados de conexões e comunicações realizadas pelos equipamentos componentes da internet, o que será feito pelos seus provedores de acesso. Os serviços de telefonia e transmissão de dados mantêm por cinco anos os dados de conexões e chamadas realizadas por seus clientes para fins judiciais, mas na internet brasileira inexiste procedimento análogo.

Registre-se que naquela audiência foram ouvidos representantes do Comitê Gestor da Internet no Brasil (CGIBr) do Ministério da Ciência e Tecnologia; da Fundação de Amparo à Pesquisa de São Paulo (FAPESP) que representa no Brasil o ICANN (*Internet Corporation for Assigning Names and Numbers)*, gestora do registro de nomes e números IP (*Internet Protocol),* ou seja, os endereços na internet; da– Associação Brasileira dos Provedores de Internet (ABRANET); do Instituto de Criminalística em Informática da Polícia Federal, do Ministério da Justiça (PF); da Agência Nacional de Telecomunicações (ANATEL).

Há apenas uma recomendação do Comitê Gestor da Internet Brasil (CGIBr) aos provedores nacionais: que mantenham, por no mínimo três anos, os dados de conexões e comunicações realizadas por seus equipamentos – a saber, identificação dos endereços de IP (protocolo de internet) do remetente e do destinatário da mensagem, bem como a data e horário de início e término da conexão, sem registrar o conteúdo da mensagem, preservando assim o sigilo da comunicação. É clara a necessidade de se transformar tal recomendação em imposição legal, razão por que apresentamos a inclusão no Código Penal do art.180-F conforme o art. 2° do substitutivo.

Além disso, também para fins de investigação, na mesma Audiência Pública, ficou registrado que é necessário estabelecer que qualquer usuário que acesse a internet se identifique positivamente junto ao seu provedor ou junto a quem lhe torne disponível o acesso a dispositivo de comunicação, aqui incluídos os *cyber-cafe* ou *hot zones,* muito embora todos tenham reconhecido as dificuldades técnicas, econômicas e culturais que isso possa significar.

Vêm à memória os episódios danosos que ocorreram no início da operação com os celulares pré-pagos, o que obrigou o seu cadastramento obrigatório pelas operadoras, contra todos os argumentos então apresentados, ou seja, a sociedade brasileira mostrou o seu bom senso e mudou seu comportamento.

Desde já, alerto que tal identificação e cadastramento não necessitam serem presenciais, com cópias de documentos ou coisas assim, mas usando certificados digitais, cuja emissão é presencial conforme definido em Lei, ou cadastros disponíveis mediante convênios de cooperação ou simples colaboração. Outras formas alternativas podem ser usadas a exemplo do que os bancos, operadoras de telefonia, operadores de *call-center* e o comércio eletrônico em geral já vêm fazendo.

Dados como nome de acesso (*login* ou *username*), nome completo, filiação, endereço completo, data de nascimento, números de telefone e senha criteriosa (número de caracteres, mistura de letras e números etc) devem ser requeridos no momento do cadastramento de um novo usuário. Este, ao solicitar um acesso posterior, usará seu nome de acesso e sua senha e outros procedimentos de validação e conferência automáticas realizados pelo sistema do provedor de acesso, procedimentos que têm o nome de "autenticação do usuário".

Conforme já citado em parágrafo anterior, a identificação e conseqüente cadastramento já acontecem com os serviços de telefonia, transmissão de dados e rádio-transmissão, onde cada operador já é obrigado por regulamento a manter um cadastro de proprietários de telefones fixos, móveis ou de aparelhos transmissores e receptores de rádio - cadastro usado exclusivamente para fins de investigação ou judiciais. Novamente, procedimento obrigatório análogo não existe na internet brasileira.

Novas tecnologias de transmissão, como a conexão sem fio, conhecida como *wireless* ou *Wi-Fi,* estão cada vez mais disponíveis. Como são padronizadas internacionalmente, tendem a se tornar extremamente baratas e, assim, serem disseminadas largamente por todas as cidades, distritos ou aglomerações urbanas ou rurais, libertando o usuário de internet do local físico a que hoje está obrigado. Com o advento próximo da televisão digital tal disseminação será ainda mais efetiva.

Ainda, em qualquer outro serviço privado que se utilize da internet, seja instituição financeira, operadoras de cartões de crédito, empresas de comércio ou indústria, ou nas redes internas das instituições públicas e privadas, a autenticação do usuário mediante senha acompanhada, ou não, de outros requisitos de identificação, como certificado digital, tabela de códigos alfanuméricos e assim por diante, são requeridos para que o usuário acesse os serviços ou as informações.

É inevitável citar como exemplo uma proposta muito interessante, que circula pela rede mundial de computadores, recomendando que toda pessoa que receber uma inverdade (um e-mail com acusações não comprovadas com provas materiais) e redistribuí-la, ficará responsável por toda a cadeia de novos informados a partir da sua replicação. Este procedimento pode fazer com que o usuário reflita sobre o significado do crime que poderá estar praticando antes de apertar a tecla de reenvio.

Em outro caso, em decisão recente o Tribunal Superior do Trabalho (TST) condenou um banco a indenizar uma cliente que propôs ação na justiça pois recebera informações incorretas sobre as aplicações em um fundo de investimentos, veiculadas por funcionário daquele banco. A exemplo dela, várias pessoas retiraram seus investimentos e perderam com isso, pois o fundo rendeu acima do informado pelo e-mail do funcionário. Ele foi demitido por justa causa já que usou equipamento do banco, em horário de trabalho funcional, distribuindo informes não-verdadeiros na internet.

Assim, não é demais lembrar, principalmente para esses casos de difamação e injúria ou de prejuízos pessoais, o que dispõe a Carta Magna no seu art. 5° inciso IV que diz "é livre a manifestação do pensamento, sendo vedado o anonimato", o que por si só já justificaria a identificação, o cadastramento e a respectiva autenticação do usuário pelo provedor de acesso à internet brasileira.

Para tanto, transformamos a identificação, o cadastro e respectiva autenticação do usuário em imposição legal, conforme o caput do art. 11 e seu § 1° do substitutivo e incluindo no Código Penal os arts. 180-G e 180-H, conforme o art. 2° do substitutivo.

A fim de preservar a intimidade dos usuários, o cadastro somente poderá ser fornecido a terceiros mediante expressa autorização judicial ou em casos que a Lei determinar, conforme o § 2° do art. 11 do substitutivo.

Por fim, reconhecendo a existência de ferramentas de segurança mais potentes, previmos, conforme o § 3° do art. 11 do substitutivo, a troca opcional, pelo provedor, da identificação e do cadastro do usuário, pelo certificado digital. Este requer, de maneira presencial quando da sua emissão, todas as informações cadastrais, inclusive senha, de acordo com a lei brasileira, a Medida Provisória número 2.200-2, de 24 de agosto de 2001, mantida em vigor conforme a Emenda Constitucional número 32, de 12 de setembro de 2001. Como toda tecnologia inovadora o certificado digital inicialmente se restringiu às trocas interbancárias, a Transferência Eletrônica Disponível (TED), instituída pelo Sistema de Pagamentos Brasileiro (SPB), implantado em 2002 pelo Banco Central do Brasil. Estatísticas recentes mostram que são quase 100 milhões de transações e mais de R$ 5 trilhões de reais transferidos com toda segurança em tempo real.

É público que o custo de cada certificado digital e seu suporte físico, (cartão de plástico, CD-ROM, ou outro dispositivo de comunicação), tende a cair de forma geométrica, à medida que se dissemine o seu uso, uma característica conhecida das inovações tecnológicas.

Ao dispor sobre o uso do certificado digital como opcional, a presente norma permite a sua própria evolução, aguardando que a sociedade se adapte à nova realidade transformada a cada dia pela tecnologia, sem obrigar o usuário ou os provedores a novos custos ou a novos hábitos e comportamentos.

Concluindo, algumas penas nos crimes tipificados foram revistas para serem de reclusão e não de detenção de forma a evitar qualquer dúvida sobre a admissibilidade e legalidade da interceptação das comunicações, se enquadrando, assim, perfeitamente, ao art. 2°, inciso III, da Lei 9.296/96.

III – VOTO

Diante do exposto, e considerando a pertinência e importância da solução proposta, somos pela prejudicialidade do Projeto de Lei do Senado n° 137, de 2000 e do Projeto de Lei da Câmara n° 89, de 2003 (n° 84, de 1999, na Câmara dos Deputados), e pela aprovação do Projeto de Lei do Senado n° 76, de 2000, na forma do substitutivo que apresentamos.

PROJETO DE LEI DO SENADO Nº 76 (SUBSTITUTIVO), DE 2000

Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tipificar condutas realizadas mediante rede de computadores ou internet, ou que sejam praticadas contra sistemas informatizados e similares, e dá outras providências.

O CONGRESSO NACIONAL decreta:

Art. 1° O art. 163 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), passa a vigorar com a seguinte redação:

"**Art. 163.** .....

§ 1º.....

Difusão de vírus eletrônico

§ 2º Se o dano em dado ou informação eletrônica, base de dados ou sistema informatizado decorre da difusão de vírus eletrônico:

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

§ 3º Consideram-se dano o bloqueio temporário do funcionamento do sistema, o comprometimento de sua confiabilidade, a modificação e a supressão de dados ou a adulteração de seu conteúdo. (NR)"

Art. 2º O Título II da Parte Geral do Código Penal fica acrescido do Capítulo VII-A, assim redigido:

"Capítulo VII-A

DA VIOLAÇÃO DE DISPOSITIVO DE COMUNICAÇÃO OU SISTEMA INFORMATIZADO

Acesso indevido a dispositivo de comunicação

Art. 180-A. Acessar indevidamente, ou sem autorização, dispositivo de comunicação ou sistema informatizado:

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

§ 1º Nas mesmas penas incorre quem fornece a terceiro meio indevido ou não autorizado de acesso a 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.

Manipulação indevida de informação eletrônica

Art. 180-B. Manter, transportar ou fornecer indevidamente ou sem autorização, dado ou informação obtida em dispositivo de comunicação ou sistema informatizado:

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

Parágrafo único - 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, identificação de usuário e autenticação de usuário

Art. 180-C. Para os efeitos penais, considera-se:

I – dispositivo de comunicação: o computador, o computador de mão, o telefone celular, o processador de dados, os meios de armazenamento de dados digitais, ou qualquer outro meio capaz de processar, armazenar ou transmitir dados utilizando-se de tecnologias magnéticas, óticas ou qualquer outra tecnologia digital.

II – sistema informatizado: a rede de computadores, 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, armazenar ou transmitir dados eletronicamente.

III – identificação de usuário: os dados de nome de acesso, senha criteriosa, nome completo, filiação, endereço completo, data de nascimento, numero da carteira de identidade ou equivalente legal, que sejam requeridos no momento do cadastramento de um novo usuário de dispositivo de comunicação ou sistema informatizado.

IV – autenticação de usuário: procedimentos de validação e conferência da identificação do usuário, quando este tem acesso ao dispositivo de comunicação ou sistema informatizado, realizados por quem os torna disponíveis ao usuário.

Fraude Eletrônica

Art. 180-D. Difundir, por qualquer meio, sistema informatizado com o propósito de induzir alguém a fornecer, espontaneamente e por qualquer meio, dados ou informações que facilitem ou permitam o acesso indevido ou sem autorização, a dispositivo de comunicação ou a sistema informatizado:

Pena – reclusão de dois a quatro anos e multa.

Parágrafo único. 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, ou se o sistema informatizado fraudador tiver potencial de propagação ou alastramento.

Divulgação de informações depositadas em banco de dados

Art. 180-E. Divulgar, ou tornar disponíveis, informações depositadas em entidade que mantém banco de dados sobre pessoas físicas ou jurídicas, referentes a situação econômica, raça, opinião política, religiosa, crença, ideologia, saúde física ou mental, orientação sexual, registros policiais, assuntos familiares ou profissionais, além de outras de caráter sigiloso, para finalidade distinta da que motivou a constituição desses arquivos, salvo por decisão da autoridade competente, ou mediante expressa anuência da pessoa a que se referem, ou de seu representante legal.

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

Dados de conexões e comunicações realizadas

Art. 180-F. Deixar de manter, aquele que torna disponível o acesso à rede mundial de computadores, os dados de conexões e comunicações realizadas por seus equipamentos, aptas à identificação do usuário, endereços eletrônicos de origem e destino no transporte dos registros de dados e informações, data e horário de início e término da conexão, incluindo protocolo de internet ou mecanismo de identificação equivalente, pelo prazo de cinco anos.

Pena – detenção, de dois a seis meses, e multa.

Permitir acesso por usuário não identificado e não autenticado

Art. 180-G. Permitir, aquele que torna disponível o acesso à rede mundial de computadores, a usuário, sem a devida identificação e autenticação, qualquer tipo de acesso ou uso pela rede mundial de computadores.

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

Parágrafo único. Na mesma pena incorre, aquele que torna disponível o acesso à rede mundial de computadores, que deixa de exigir o cadastramento de usuário, que permita sua identificação e autenticação.

Usuário enviar mensagem sem estar identificado e autenticado

Art. 180-H. Utilizar, de forma anônima, dispositivo de comunicação ou sistema informatizado para o envio de mensagem eletrônica de qualquer tipo.

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

Art. 3º O Código Penal passa a vigorar acrescido do seguinte art. 183-A:

Art. 183-A. Equiparam-se à coisa o 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 lhes proporcione acesso .

Art. 4º 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 ou telefônico"

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

..... (NR)"

Art. 5º 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 portátil de armazenamento e processamento de informações

Parágrafo único. Equipara-se a documento particular o cartão de crédito ou débito ou qualquer dispositivo eletrônico portátil de armazenamento ou processamento de informações. (NR)"

Art. 6º O Código Penal passa a vigorar acrescido do seguinte art. 298-A:

"Falsificação de telefone celular ou meio de acesso a sistema eletrônico

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

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

Art. 7º O Código Penal passa a vigorar acrescido do seguinte art. 141-A:

> **Art. 141-A.** As penas neste Capítulo serão de reclusão ao invés de detenção caso os crimes sejam cometidos através de dispositivo de comunicação ou sistema informatizado.

Art. 8º O art. 147 do Código Penal passa a vigorar acrescido do seguinte §2º renumerando-se o parágrafo único:

> **Art. 147** .....
>
> .....
>
> § 2º A pena neste artigo será de reclusão ao invés de detenção, caso o crime seja cometido através de dispositivo de comunicação ou sistema informatizado.

Art. 9º O art. 46 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940, Código Penal, passa a vigorar acrescido do seguinte § 5º:

> **"Art. 46** .....
>
> .....
>
> *§ 5º* No caso de crime praticado contra ou por meio de dispositivo de comunicação ou sistema informatizado, o juiz poderá aproveitar as habilidades e conhecimentos do condenado para, ministrar cursos ou para trabalhos de criação de sistemas informatizados em sociedades ou instituições, privadas ou públicas, ou para qualquer tipo de prestação de serviços equivalente, sempre sob supervisão nomeada pelo juiz.(NR)"

Art. 10º Todo aquele que desejar acessar uma rede de computadores, local, regional, nacional ou mundial, deverá identificar-se e cadastrar-se naquele provedor que torne disponível este acesso.

Parágrafo único. Os atuais usuários terão prazo de cento e vinte dias após a entrada em vigor desta Lei para providenciarem ou revisarem sua identificação e cadastro junto a quem, de sua preferência, torne disponível o acesso aqui definido.

Art. 11° A cada acesso a uma rede de computadores, local, regional, nacional ou mundial, aquele que torna disponível este acesso somente admitirá como usuário pessoa, ou dispositivo de comunicação, que for autenticada conforme validação positiva dos dados cadastrais previamente fornecidos por ela.

§1° O cadastro mantido por aquele que torna disponível o acesso conterá obrigatoriamente: nome de acesso; senha de acesso ou mecanismo similar; nome completo; endereço completo com logradouro, número, complemento, código de endereçamento postal, cidade e estado da federação; número de registro junto aos serviços ou institutos de identificação das Secretarias de Segurança Pública Estaduais ou conselhos de registro profissional; número de inscrição no Cadastro de Pessoas Físicas (CPF), mantido pelo Ministério da Fazenda ou o – Número de Identificação do Trabalhador (NIT), mantido pelo Ministério da Previdência Social.

§ 2° O cadastro somente poderá ser fornecido a terceiros mediante expressa autorização da autoridade competente ou em casos que a Lei determinar.

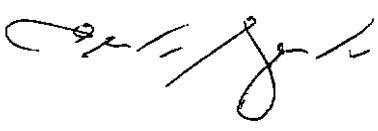
§ 3° A senha e o cadastro de identificação, a critério do provedor de acesso, poderão ser substituídos por certificado digital emitido dentro das normas da ICP – Brasil, Infra-estrutura de Chaves Públicas Brasileira, conforme determina a MP 2.200-2 de 24 de agosto de 2001.

§ 4° Para assegurar a identidade e a privacidade do usuário a senha de acesso poderá ser armazenada criptografada por algoritmo não reversível.

Art. 12° Esta Lei entra em vigor sessenta dias após a data de sua publicação.

Sala da Comissão,

, Presidente



, Relator

RELATÓRIO

RELATOR: Senador **EDUARDO AZEREDO**

I – RELATÓRIO

Chegam a esta Comissão, para parecer, 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 2005, que havia sido declarada em decorrência da aprovação do Requerimento n° 599, de 2005, de autoria da Senadora Ideli Salvatti. Os projetos de lei do Senado perdem 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 delitos cometidos com o uso de computadores, e atribui-lhes as respectivas penas, sem entretanto alterar o 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 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 Decreto-Lei n° 2.848, de 7 de dezembro de 1941 (Código Penal), 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 PLC 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* ao tipo penal de atentado contra a segurança de serviço de utilidade pública (art. 265) e ao 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).

Tendo estado à disposição dos senhores Senadores, o PLC n° 89, de 2003 não recebeu emendas.

II – ANÁLISE

Muitas são as proposições legislativas já produzidas e debatidas no Congresso Nacional a respeito do tema da criminalidade nas áreas da informática, das telecomunicações e da Internet, a rede mundial de computadores. A evolução das tecnologias relacionadas à produção, ao processamento, ao armazenamento e à difusão da informação tem ocorrido com muita velocidade, gerando lacunas no ordenamento jurídico vigente.

A existência dessas lacunas tem motivado a proliferação de casos de fraudes e de danos ao patrimônio e danos morais de agentes públicos e privados. Estima-se que bilhões de reais já foram desviados de contas bancárias de pessoas físicas ou jurídicas em decorrência da atuação indevida de especialistas da área. Além disso, a violação de bases de dados mantidas em meio eletrônico tem provocado danos de grande monta pelo roubo de informações pessoais.

Não bastasse isso, há evidências de ligação entre o cibercrime e o financiamento do terrorismo internacional, e o crescimento do tráfico de seres humanos e de drogas. E 2004 foi apontado como o ano em que os crimes cibernéticos passaram a gerar mais lucros até mesmo do que o tráfico de drogas. De acordo com pesquisa realizada pela firma de consultoria americana *Computer Economics*, em 2004 as perdas totais chegam a 18 bilhões de dólares, com uma taxa de crescimento anual próxima de 35%.

A sociedade clama por medidas eficazes no combate ao crime cibernético. Não é mais possível que divergências hermenêuticas acerca da possível aplicabilidade das nossas normas jurídicas a esse tipo de conduta continuem a impedir a punição de condutas extremamente nocivas ao País.

A imprensa nacional destaca recentemente que alguns internautas já começam a fazer justiça pelas próprias mãos contra usuários pedófilos ou terroristas do sítio *Orkut*, denunciando-os ao provedor. O *Orkut*, um serviço da multinacional americana *Google*, imediatamente retira aqueles usuários do sistema mas não consegue detectar e impedir a sua reinclusão, face á liberalidade, e não liberdade, registre-se, inerente à rede mundial de computadores. Estabelece-se assim o círculo da denúncia e da punição responsável mas este círculo tem como resposta novo círculo vicioso com o reinício dos delitos por novos usuários não identificados, tudo isto sem que se perceba um fim próximo.

O PLS nº 137, de 2000, demonstra preocupação idêntica ao dos projetos que acompanha, qual seja a de disciplinar as condutas perniciosas que utilizem ou danifiquem sistemas de computador. Não obstante, é de abrangência e precisão mais restrita que aqueles, que o englobam integralmente.

O projeto limita-se a estabelecer que os crimes contra a pessoa, o patrimônio, a propriedade imaterial e intelectual, os costumes, bem como contra a criança e o adolescente, cometidos com a utilização de meios de tecnologia de informação e telecomunicações, terão suas penas triplicadas. Ou seja, a pena seria agravada em razão do meio utilizado pelo agente para perpetrar o crime.

A alteração legislativa proposta pelo PLS nº 137, de 2000, não é conveniente por duas razões.

Em primeiro lugar, tornaria superlativo o desvalor do meio utilizado pelo agente, que prevaleceria mesmo sobre o desvalor do resultado ou da conduta (genericamente considerada) – aquele, inspirador da teoria clássica da ação; este, da teoria finalista da ação, adotada pelo Código Penal a partir da reforma da sua Parte Geral, empreendida pela Lei nº 7.209, de 11 de julho de 1984. A segunda razão, que decorre da anterior, é a desproporcionalidade na aplicação das penas, haja vista que um delito menos grave poderia ser apenado mais severamente do que outro mais reprovável, apenas por ter sido cometido por meio da Internet.

O PLC nº 89, de 2003, pretende inserir a Seção V no Capítulo VI do Título I do Código Penal, onde seriam definidos os crimes contra a inviolabilidade dos sistemas informatizados. São nove as condutas delituosas por meio de acesso a sistema eletrônico de que trata o PLC:

- o acesso indevido a meio eletrônico;
- a manipulação indevida de informação eletrônica;
- o dano eletrônico;
- a pornografia infantil;
- o atentado contra a segurança de serviço de utilidade pública;
- a interrupção ou perturbação de serviço telegráfico e telefônico;
- a falsificação de cartão de crédito;
- a falsificação de telefone celular;
- a divulgação de informações pessoais ou de empresas.

Vejamos cada um desses tipos.

a) Arts. 154-A, 154-B e 154-C do CP, ou seja, o acesso indevido, a manipulação indevida de informação e a definição de meio eletrônico e sistema informatizado).

A redação pode ser aperfeiçoada para registrar que o meio eletrônico ou sistema informatizado é protegido contra o acesso de estranhos, e que o agente consegue o acesso mediante a violação desse sistema de proteção. Além disso, o tipo não configuraria crime contra a pessoa, razão pela qual não deveria ser incluído no Título I do Código Penal, sendo mais adequado colocá-lo no Título II – DOS CRIMES CONTRA O PATRIMÔNIO.

Já a pena, que seria aplicada ao *hacker*, nome dado ao usuário que tenta violar ou viola o sistema de proteção, deveria ser mais severa.

Ademais, embora os três artigos possam ser reunidos em um só, preferimos manter a redação dada pelo PLC nº 89 de 2003, que define com maior clareza os delitos que se pretende tipificar. Entretanto propomos a alteração da pena original de detenção para reclusão, de 2 (dois) a 4 (quatro) anos, e multa, mantendo os mesmos parágrafos.

Ainda, quando este PLC nº 89 de 2003 estava sendo relatado nesta Comissão, o atento Senador Hélio Costa fez algumas sugestões de emendas que os membros da Comissão entenderam necessárias, mas que deveriam fazer parte de um novo Projeto de Lei a fim de que aquele projeto em discussão, uma vez aprovado, pudesse ir à sanção presidencial. Estando ele apensado ao PLS nº 76 de 2000 entendemos que é hora de acatar aqui aquelas sugestões.

A primeira sugestão aqui acatada trata da definição e tipificação da Fraude Eletrônica, conhecida pelos profissionais de - Tecnologia de Informação e Comunicação (TIC) - como *phishing* ou *port fishing*, incluindo-a no Código Penal como segue:

Fraude Eletrônica

Art. 180 - D. Difundir, por qualquer meio, sistema informatizado com o propósito de induzir alguém a fornecer, espontaneamente e por qualquer meio, dados ou informações que facilitem ou permitam o acesso indevido ou sem autorização, a dispositivo de comunicação ou a sistema informatizado:

Pena – reclusão de dois a quatro anos e multa.

Parágrafo único. 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, ou se o sistema informatizado fraudador tiver potencial de propagação ou alastramento.

Outra sugestão também acatada refere-se à inclusão de alteração ao art. 46 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940, Código Penal, mediante a inclusão a ele do § 5º dando a opção ao juiz a aplicação de pena alternativa, onde ao final do parágrafo entendemos por bem introduzir "sempre sob supervisão nomeada pelo juiz":

Art. 46 .....

.....

§ 5º No caso de crime praticado contra ou por meio de dispositivo de comunicação ou sistema informatizado, o juiz poderá aproveitar as habilidades e conhecimentos do condenado para ministrar cursos ou para trabalhos de criação de sistemas informatizados em empresas ou instituições públicas, ou para qualquer tipo de prestação de serviços equivalente, **sempre sob autoridade supervisora nomeada pelo juiz.**

Finalmente o Senador sugeriu a mudança do termo "meio eletrônico" por "dispositivo de comunicação" no art. 180-C, à qual no substitutivo promovemos sua atualização e complementação:

Dispositivo de Comunicação e Sistema Informatizado

Art. 180-C Para os efeitos penais, considera-se:

I – dispositivo de comunicação: o computador, o processador de dados, o disquete, o CD-ROM ou qualquer outro meio capaz de armazenar ou transmitir dados de maneira magnética, ótica, ou eletronicamente.

II – sistema informatizado: a rede de computadores, a base de dados, o programa de computador ou qualquer outro sistema capaz de armazenar ou transmitir dados eletronicamente.

b) Arts. 163, §§ 2°e 3°, e 167 do CP

A equiparação feita pelo § 2° é pertinente, mas poderia estar posicionada no Capítulo VIII do Título II (Disposições Gerais), pois dessa forma a regra seria válida para todos os tipos de crimes contra o patrimônio. Quanto à conduta do § 3°, entendemos que a pena deva ser mais severa, tendo em conta a potencialidade do dano material que se pode causar. Em vista disso, sugerimos a seguinte redação:

§ 3° No caso do § 2°, se o dano é decorrente de difusão de vírus eletrônico:

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

Por sua vez, a alteração proposta para o art. 167 do CP não é conveniente.

c) Art. 218-A do CP

O delito descrito nesse dispositivo já está previsto, de modo mais abrangente, nos arts. 240 e 241 do Estatuto da Criança e do Adolescente (ECA).

d) Arts. 265 e 266 do CP

As alterações propostas para esses dispositivos são convenientes.

e) Arts. 298 e 298-A do CP

A redação que se propõe para o art. 298 é conveniente; quanto ao art. 298-A, procedemos a pequenas modificações de forma a melhorar sua clareza e compreensão.

f) Art. 2º, § 2º, da Lei nº 9.296, de 1996

A alteração prevista no art. 2º da Lei nº 9.296, 24 de julho de 1996, é inconstitucional, pois não se justifica violar a intimidade do indivíduo se o crime supostamente cometido é punido, no máximo, com mera detenção. Além disso, nos moldes aqui propostos, os novos tipos penais seriam punidos, todos eles, com reclusão.

g) Art. 10 do PLC nº 89, de 2003

O dispositivo é desnecessário, pois o próprio Código Penal Militar dá o conceito de crime militar e regula a competência para o seu julgamento.

Por fim, o art. 11 do projeto mostra-se adequado, enquanto o art. 12 não é conveniente, sendo preferível manter o sistema de crimes estabelecido nos arts. 240 e 241 do ECA. A Lei nº 10.764, de 12 de novembro de 2003, alterou o art. 241 do Estatuto da Criança e do Adolescente (Lei nº 8.069, de 13 de julho de 1990), para tipificar e punir de forma mais severa a pornografia infantil.

O PLS nº 76, de 2000, revestido de norma autônoma, afigura-se o projeto mais abrangente entre os que estão sendo aqui analisados. Os crimes informáticos estão divididos, no projeto, em crimes 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 opção sexual e contra a segurança nacional.

Realmente a visão ampla que se tem dos crimes de informática é o grande mérito deste projeto inovador proposto pelo eminente Senador Renan Calheiros. Seus dispositivos mostram a gravidade crescente dos delitos praticados com instrumentos informatizados, cujas punições ainda não têm o necessário suporte legal. Isto vem trazendo enorme insegurança a toda a sociedade pois crimes são praticados no anonimato da internet e para os quais não há a mínima possibilidade de defesa pelo usuário.

Entretanto, a descrição de algumas das condutas deixa dúvidas em relação aos elementos dos respectivos delitos, o que pode prejudicar sua compreensão.

Vale lembrar que a Lei Complementar nº 95 de 1998 determina que havendo legislação em vigor deve-se preferir a sua alteração à criação de nova norma e desta forma o substitutivo proposto promove alterações ao Decreto-Lei nº 2.848, de 7 de dezembro de 1940, o Código Penal.

Comentamos, a seguir, sobre as disposições do PLS nº 76, de 2000.

a) Art. 1º, § 1º – crimes a inviolabilidade de dados e sua comunicação

Os incisos I, IV e V são espécies de crime de dano, descrito no art. 163 do CP; além disso, o inciso V deveria tipificar não a mera programação de instruções, mas a sua efetiva utilização, pois o nosso direito, via de regra, não pune os atos meramente preparatórios. Pode-se, alternativamente, prever, no art. 163 do CP, a equiparação dos dados informatizados à coisa, como o fez o PLC nº 89, de 2003, ou fazê-lo ao final do Título II do CP.

O inciso II pode ser tido como furto (art. 155 do CP), se houver subtração da coisa, ou como apropriação indébita (art. 168 do CP), se o agente tinha a posse ou a detenção da coisa. Quanto ao inciso III, melhor seria punir o uso indevido dos dados em razão da finalidade do agente: se atenta contra a intimidade da pessoa, contra o patrimônio, contra a fé pública, etc. Entretanto, há que se ter em conta que a maioria desses crimes já existe, e que a informática é apenas um meio para realização da conduta delituosa. A equiparação à coisa que se pode fazer ao final do Título II do CP resolveria o problema.

Além disso, as penas propostas são muito brandas em face da gravidade das condutas equiparadas que acima citamos.

b) Art. 1º, § 2º

Os incisos I e II são espécies de furto, crime definido no art. 155 do CP, cuja pena é bem mais severa do que a proposta no PLS nº 76, de 2000.

c) Art. 1º, § 3º

O inciso I está incluso no crime de injúria, descrito no art. 140 do CP; a conduta do inciso II, por sua vez, poderia ser inserida no Código Penal, mediante

acréscimo do art. 180-E. Cabe observar que, se a informação for lesiva à honra, sua divulgação importará em um dos crimes tipificados no Capítulo V do Código Penal (calúnia, difamação ou injúria). Para coibir o anonimato permitido pela internet, normalmente o caminho usado pelos autores dos crimes aqui tipificados, incluímos os artigos 180-G e 180-H.

Todos os atos e fatos que se materializam através destes meios chegam, facilmente e rapidamente, ao conhecimento de milhões de pessoas, causando um considerável prejuízo aos bens jurídicos tutelados. É necessário, portanto, maior força penal coercitiva para evitá-los e assim fizemos incluir o art. 141-1 conforme o art. 7º do substitutivo, alterando a pena de detenção para reclusão se o meio utilizado é um dispositivo de comunicação ou sistema informatizado. A mesma alteração está proposta para o crime de ameaça, fazendo incluir o § 2º ao art. 147, renumerando o parágrafo único existente, conforme o art. 8º do substitutivo.

d) Art. 1º, § 4º

O inciso I, a depender do resultado da conduta, será crime de lesão corporal ou homicídio, ambos já tipificados no Código Penal (arts. 129 e 121, respectivamente). O inciso II traz a incriminação de ato meramente preparatório. Além disso, os artefatos explosivos têm ampla utilização na indústria, não sendo conveniente definir como crime o trabalho intelectual de elaboração de um sistema informatizado de detonação.

e) Art. 1º, § 5º

As condutas descritas nos incisos I e II configuram crime contra a ordem tributária, definidos de forma mais abrangente e adequada nos arts. 1º e 2º da Lei nº 8.137, de 27 de dezembro de 1990.

f) Art. 1º, § 6º

O inciso I já está definido no art. 218 do CP (corrupção de menores). Os incisos II e III estão inclusos no art. 234 do CP (escrito ou objeto obsceno). Novamente, com o anonimato coibido pelos artigos 180-G e 180-H do substitutivo os autores destes crimes estarão desestimulados a cometê-los.

g) Art. 1º, § 7º

Os crimes definidos nesse parágrafo já estão contemplados na Lei nº 7.170, de 14 de dezembro de 1983 (Lei de Segurança Nacional), especificamente nos seus arts. 13, 15 e 23.

Recentemente em Audiência Pública sobre o PLS nº 279 de 2003, do qual também sou relator, de autoria do nobre Senador Delcídio Amaral e que propõe a criação de um cadastro de titulares de correio eletrônico na internet, ficou evidente que, para fins de investigação, é necessário estabelecer um prazo legal de armazenamento dos dados de conexões e comunicações realizadas pelos equipamentos componentes da internet, o que será feito pelos seus provedores de acesso. Os serviços de telefonia e transmissão de dados mantêm por cinco anos os dados de conexões e chamadas realizadas por seus clientes para fins judiciais, mas na internet brasileira inexiste procedimento análogo.

Registre-se que naquela audiência foram ouvidos representantes do Comitê Gestor da Internet no Brasil (CGIBr) do Ministério da Ciência e Tecnologia; da Fundação de Amparo à Pesquisa de São Paulo (FAPESP) que representa no Brasil o ICANN (*Internet Corporation for Assigning Names and Numbers)*, gestora do registro de nomes e números IP (*Internet Protocol),* ou seja, os endereços na internet; da– Associação Brasileira dos Provedores de Internet (ABRANET); do Instituto de Criminalística em Informática da Polícia Federal, do Ministério da Justiça (PF); da Agência Nacional de Telecomunicações (ANATEL).

Há apenas uma recomendação do Comitê Gestor da Internet Brasil (CGIBr) aos provedores nacionais: que mantenham, por no mínimo três anos, os dados de conexões e comunicações realizadas por seus equipamentos – a saber, identificação dos endereços de IP (protocolo de internet) do remetente e do destinatário da mensagem, bem como a data e horário de início e término da conexão, sem registrar o conteúdo da mensagem, preservando assim o sigilo da comunicação. É clara a necessidade de se transformar tal recomendação em imposição legal, razão por que apresentamos a inclusão no Código Penal do art.180-F conforme o art. 2º do substitutivo.

Além disso, também para fins de investigação, na mesma Audiência Pública, ficou registrado que é necessário estabelecer que qualquer usuário que acesse a internet se identifique positivamente junto ao seu provedor ou junto a quem lhe torne disponível o acesso a dispositivo de comunicação, aqui incluídos os *cyber-cafe* ou *hot zones,* muito embora todos tenham reconhecido as dificuldades técnicas, econômicas e culturais que isso possa significar.

Vêm à memória os episódios danosos que ocorreram no início da operação com os celulares pré-pagos, o que obrigou o seu cadastramento obrigatório pelas operadoras, contra todos os argumentos então apresentados, ou seja, a sociedade brasileira mostrou o seu bom senso e mudou seu comportamento.

Desde já, alerto que tal identificação e cadastramento não necessitam serem presenciais, com cópias de documentos ou coisas assim, mas usando certificados digitais, cuja emissão é presencial conforme definido em Lei, ou cadastros disponíveis mediante convênios de cooperação ou simples colaboração. Outras formas alternativas podem ser usadas a exemplo do que os bancos, operadoras de telefonia, operadores de *call-center* e o comércio eletrônico em geral já vêm fazendo.

Dados como nome de acesso (*login* ou *username*), nome completo, filiação, endereço completo, data de nascimento, números de telefone e senha criteriosa (número de caracteres, mistura de letras e números etc) devem ser requeridos no momento do cadastramento de um novo usuário. Este, ao solicitar um acesso posterior, usará seu nome de acesso e sua senha e outros procedimentos de validação e conferência automáticas realizados pelo sistema do provedor de acesso, procedimentos que têm o nome de "autenticação do usuário".

Conforme já citado em parágrafo anterior, a identificação e conseqüente cadastramento já acontecem com os serviços de telefonia, transmissão de dados e rádio-transmissão, onde cada operador já é obrigado por regulamento a manter um cadastro de proprietários de telefones fixos, móveis ou de aparelhos transmissores e receptores de rádio - cadastro usado exclusivamente para fins de investigação ou judiciais. Novamente, procedimento obrigatório análogo não existe na internet brasileira.

Novas tecnologias de transmissão, como a conexão sem fio, conhecida como *wireless* ou *Wi-Fi,* estão cada vez mais disponíveis. Como são padronizadas internacionalmente, tendem a se tornar extremamente baratas e, assim, serem disseminadas largamente por todas as cidades, distritos ou aglomerações urbanas ou rurais, libertando o usuário de internet do local físico a que hoje está obrigado. Com o advento próximo da televisão digital tal disseminação será ainda mais efetiva.

Ainda, em qualquer outro serviço privado que se utilize da internet, seja instituição financeira, operadoras de cartões de crédito, empresas de comércio ou indústria, ou nas redes internas das instituições públicas e privadas, a autenticação do usuário mediante senha acompanhada, ou não, de outros requisitos de identificação, como certificado digital, tabela de códigos alfanuméricos e assim por diante, são requeridos para que o usuário acesse os serviços ou as informações.

É inevitável citar como exemplo uma proposta muito interessante, que circula pela rede mundial de computadores, recomendando que toda pessoa que receber uma inverdade (um e-mail com acusações não comprovadas com provas materiais) e redistribuí-la, ficará responsável por toda a cadeia de novos informados a partir da sua replicação. Este procedimento pode fazer com que o usuário reflita sobre o significado do crime que poderá estar praticando antes de apertar a tecla de reenvio.

Em outro caso, em decisão recente o Tribunal Superior do Trabalho (TST) condenou um banco a indenizar uma cliente que propôs ação na justiça pois recebera informações incorretas sobre as aplicações em um fundo de investimentos, veiculadas por funcionário daquele banco. A exemplo dela, várias pessoas retiraram seus investimentos e perderam com isso, pois o fundo rendeu acima do informado pelo e-mail do funcionário. Ele foi demitido por justa causa já que usou equipamento do banco, em horário de trabalho funcional, distribuindo informes não-verdadeiros na internet.

Assim, não é demais lembrar, principalmente para esses casos de difamação e injúria ou de prejuízos pessoais, o que dispõe a Carta Magna no seu art. 5º inciso IV que diz "é livre a manifestação do pensamento, sendo vedado o anonimato", o que por si só já justificaria a identificação, o cadastramento e a respectiva autenticação do usuário pelo provedor de acesso à internet brasileira.

Para tanto, transformamos a identificação, o cadastro e respectiva autenticação do usuário em imposição legal, conforme o caput do art. 11 e seu § 1° do substitutivo e incluindo no Código Penal os arts. 180-G e 180-H, conforme o art. 2° do substitutivo.

A fim de preservar a intimidade dos usuários, o cadastro somente poderá ser fornecido a terceiros mediante expressa autorização judicial ou em casos que a Lei determinar, conforme o § 2° do art. 11 do substitutivo.

Por fim, reconhecendo a existência de ferramentas de segurança mais potentes, previmos, conforme o § 3° do art. 11 do substitutivo, a troca opcional, pelo provedor, da identificação e do cadastro do usuário, pelo certificado digital. Este requer, de maneira presencial quando da sua emissão, todas as informações cadastrais, inclusive senha, de acordo com a lei brasileira, a Medida Provisória número 2.200-2, de 24 de agosto de 2001, mantida em vigor conforme a Emenda Constitucional número 32, de 12 de setembro de 2001. Como toda tecnologia inovadora o certificado digital inicialmente se restringiu às trocas interbancárias, a Transferência Eletrônica Disponível (TED), instituída pelo Sistema de Pagamentos Brasileiro (SPB), implantado em 2002 pelo Banco Central do Brasil. Estatísticas recentes mostram que são quase 100 milhões de transações e mais de R$ 5 trilhões de reais transferidos com toda segurança em tempo real.

É público que o custo de cada certificado digital e seu suporte físico, (cartão de plástico, CD-ROM, ou outro dispositivo de comunicação), tende a cair de forma geométrica, à medida que se dissemine o seu uso, uma característica conhecida das inovações tecnológicas.

Ao dispor sobre o uso do certificado digital como opcional, a presente norma permite a sua própria evolução, aguardando que a sociedade se adapte à nova realidade transformada a cada dia pela tecnologia, sem obrigar o usuário ou os provedores a novos custos ou a novos hábitos e comportamentos.

Concluindo, algumas penas nos crimes tipificados foram revistas para serem de reclusão e não de detenção de forma a evitar qualquer dúvida sobre a admissibilidade e legalidade da interceptação das comunicações, se enquadrando, assim, perfeitamente, ao art. 2°, inciso III, da Lei 9.296/96.

III – VOTO

Diante do exposto, e considerando a pertinência e importância da solução proposta, somos pela aprovação do Projeto de Lei do Senado n° 137, de 2000, pela aprovação do Projeto de Lei da Câmara n° 89, de 2003 (n° 84, de 1999, na Câmara dos Deputados), e pela aprovação do Projeto de Lei do Senado n° 76, de 2000, na forma do substitutivo que apresentamos.

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), para tipificar condutas realizadas mediante rede de computadores ou internet, ou que sejam praticadas contra sistemas informatizados e similares, e dá outras providências.

O CONGRESSO NACIONAL decreta:

Art. 1º O art. 163 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), passa a vigorar com a seguinte redação:

"**Art. 163.** .....

§ 1º.....

Difusão de vírus eletrônico

§ 2º Se o dano em dado ou informação eletrônica, base de dados ou sistema informatizado decorre da difusão de vírus eletrônico:

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

§ 3º Consideram-se dano o bloqueio temporário do funcionamento do sistema, o comprometimento de sua confiabilidade, a modificação e a supressão de dados ou a adulteração de seu conteúdo. (NR)"

Art. 2º O Título II da Parte Geral do Código Penal fica acrescido do Capítulo VII-A, assim redigido:

"Capítulo VII-A

DA VIOLAÇÃO DE DISPOSITIVO DE COMUNICAÇÃO OU SISTEMA INFORMATIZADO

Acesso indevido a dispositivo de comunicação

Art. 180-A. Acessar indevidamente, ou sem autorização, dispositivo de comunicação ou sistema informatizado:

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

§ 1º Nas mesmas penas incorre quem fornece a terceiro meio indevido ou não autorizado de acesso a 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.

Manipulação indevida de informação eletrônica

Art. 180-B. Manter, transportar ou fornecer indevidamente ou sem autorização, dado ou informação obtida em dispositivo de comunicação ou sistema informatizado:

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

Parágrafo único - 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, identificação de usuário e autenticação de usuário

Art. 180-C. Para os efeitos penais, considera-se:

I – dispositivo de comunicação: o computador, o computador de mão, o telefone celular, o processador de dados, os meios de armazenamento de dados digitais, ou qualquer outro meio capaz de processar, armazenar ou

transmitir dados utilizando-se de tecnologias magnéticas, óticas ou qualquer outra tecnologia digital.

II – sistema informatizado: a rede de computadores, 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, armazenar ou transmitir dados eletronicamente.

III – identificação de usuário: os dados de nome de acesso, senha criteriosa, nome completo, filiação, endereço completo, data de nascimento, numero da carteira de identidade ou equivalente legal, que sejam requeridos no momento do cadastramento de um novo usuário de dispositivo de comunicação ou sistema informatizado.

IV – autenticação de usuário: procedimentos de validação e conferência da identificação do usuário, quando este tem acesso ao dispositivo de comunicação ou sistema informatizado, realizados por quem os torna disponíveis ao usuário.

Fraude Eletrônica

Art. 180-D. Difundir, por qualquer meio, sistema informatizado com o propósito de induzir alguém a fornecer, espontaneamente e por qualquer meio, dados ou informações que facilitem ou permitam o acesso indevido ou sem autorização, a dispositivo de comunicação ou a sistema informatizado:

Pena – reclusão de dois a quatro anos e multa.

Parágrafo único. 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, ou se o sistema informatizado fraudador tiver potencial de propagação ou alastramento.

Divulgação de informações depositadas em banco de dados

Art. 180-E. Divulgar, ou tornar disponíveis, informações depositadas em entidade que mantém banco de dados sobre pessoas físicas ou jurídicas, referentes a situação econômica, raça, opinião política, religiosa, crença, ideologia, saúde física ou mental, orientação sexual, registros policiais, assuntos familiares ou profissionais, além de outras de caráter sigiloso, para finalidade distinta da que motivou a constituição desses arquivos, salvo por decisão da autoridade competente, ou mediante expressa anuência da pessoa a que se referem, ou de seu representante legal.

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

Dados de conexões e comunicações realizadas

Art. 180-F. Deixar de manter, aquele que torna disponível o acesso à rede mundial de computadores, os dados de conexões e comunicações realizadas por seus equipamentos, aptas à identificação do usuário, endereços eletrônicos de origem e destino no transporte dos registros de dados e informações, data e horário de início e término da conexão, incluindo protocolo de internet ou mecanismo de identificação equivalente, pelo prazo de cinco anos.

Pena – detenção, de dois a seis meses, e multa.

Permitir acesso por usuário não identificado e não autenticado

Art. 180-G. Permitir, aquele que torna disponível o acesso à rede mundial de computadores, a usuário, sem a devida identificação e autenticação, qualquer tipo de acesso ou uso pela rede mundial de computadores.

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

Parágrafo único. Na mesma pena incorre, aquele que torna disponível o acesso à rede mundial de computadores, que deixa de exigir o cadastramento de usuário, que permita sua identificação e autenticação.

Usuário enviar mensagem sem estar identificado e autenticado

Art. 180-H. Utilizar, de forma anônima, dispositivo de comunicação ou sistema informatizado para o envio de mensagem eletrônica de qualquer tipo.

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

Art. 3º O Código Penal passa a vigorar acrescido do seguinte art. 183-A:

Art. 183-A. Equiparam-se à coisa o 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 lhes proporcione acesso .

Art. 4º 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 ou telefônico"

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

..... (NR)"

Art. 5º 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 portátil de armazenamento e processamento de informações

Parágrafo único. Equipara-se a documento particular o cartão de crédito ou débito ou qualquer dispositivo eletrônico portátil de armazenamento ou processamento de informações. (NR)"

Art. 6º O Código Penal passa a vigorar acrescido do seguinte art. 298-A:

"Falsificação de telefone celular ou meio de acesso a sistema eletrônico

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

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

Art. 7º O Código Penal passa a vigorar acrescido do seguinte art. 141-A:

> **Art. 141-A.** As penas neste Capítulo serão de reclusão ao invés de detenção caso os crimes sejam cometidos através de dispositivo de comunicação ou sistema informatizado.

Art. 8º O art. 147 do Código Penal passa a vigorar acrescido do seguinte §2º renumerando-se o parágrafo único:

> **Art. 147** .....
>
> .....
>
> § 2° A pena neste artigo será de reclusão ao invés de detenção, caso o crime seja cometido através de dispositivo de comunicação ou sistema informatizado.

Art. 9º O art. 46 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940, Código Penal, passa a vigorar acrescido do seguinte § 5º:

> **"Art. 46** .....
>
> .....
>
> *§ 5º* No caso de crime praticado contra ou por meio de dispositivo de comunicação ou sistema informatizado, o juiz poderá aproveitar as habilidades e conhecimentos do condenado para, ministrar cursos ou para trabalhos de criação de sistemas informatizados em sociedades ou instituições, privadas ou públicas, ou para qualquer tipo de prestação de serviços equivalente, sempre sob supervisão nomeada pelo juiz.(NR)"

Art. 10º Todo aquele que desejar acessar uma rede de computadores, local, regional, nacional ou mundial, deverá identificar-se e cadastrar-se naquele provedor que torne disponível este acesso.

Parágrafo único. Os atuais usuários terão prazo de cento e vinte dias após a entrada em vigor desta Lei para providenciarem ou revisarem sua identificação e cadastro junto a quem, de sua preferência, torne disponível o acesso aqui definido.

Art. 11º A cada acesso a uma rede de computadores, local, regional, nacional ou mundial, aquele que torna disponível este acesso somente admitirá como usuário pessoa, ou dispositivo de comunicação, que for autenticada conforme validação positiva dos dados cadastrais previamente fornecidos por ela.

§1º O cadastro mantido por aquele que torna disponível o acesso conterá obrigatoriamente: nome de acesso; senha de acesso ou mecanismo similar; nome completo; endereço completo com logradouro, número, complemento, código de endereçamento postal, cidade e estado da federação; número de registro junto aos serviços ou institutos de identificação das Secretarias de Segurança Pública Estaduais ou conselhos de registro profissional; número de inscrição no Cadastro de Pessoas Físicas (CPF), mantido pelo Ministério da Fazenda ou o – Número de Identificação do Trabalhador (NIT), mantido pelo Ministério da Previdência Social.

§ 2º O cadastro somente poderá ser fornecido a terceiros mediante expressa autorização da autoridade competente ou em casos que a Lei determinar.

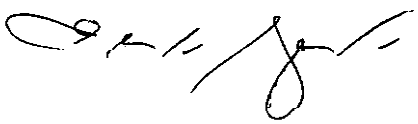
§ 3º A senha e o cadastro de identificação, a critério do provedor de acesso, poderão ser substituídos por certificado digital emitido dentro das normas da ICP – Brasil, Infra-estrutura de Chaves Públicas Brasileira, conforme determina a MP 2.200-2 de 24 de agosto de 2001.

§ 4º Para assegurar a identidade e a privacidade do usuário a senha de acesso poderá ser armazenada criptografada por algoritmo não reversível.

Art. 12º Esta Lei entra em vigor sessenta dias após a data de sua publicação.

Sala da Comissão,

, Presidente



, Relator

RELATÓRIO

RELATOR: Senador **EDUARDO AZEREDO**

I – RELATÓRIO

Chegam a esta Comissão, para parecer, o Projeto de Lei da Câmara (PLC) nº 89, de 2003 (nº 84, de 1999, na origem), e os Projetos de Lei do Senado (PLS) nº 137, de 2000, e nº 76, de 2000, todos referentes a crimes na área de informática. Tramitam em conjunto, em atendimento ao Requerimento nº 847, de 2005, do Senador Renan Calheiros. Em decorrência do Requerimento nº 848, de 2005, foi extinta a urgência na tramitação do PLC nº 89, de 2005, que havia sido declarada em decorrência da aprovação do Requerimento nº 599, de 2005, de autoria da Senadora Ideli Salvatti. Os projetos de lei do Senado perdem o caráter terminativo nas comissões.

O PLS nº 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 delitos cometidos com o uso de computadores, e lhes atribui as respectivas penas, sem entretanto alterar o 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 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 Decreto-Lei n° 2.848, de 7 de dezembro de 1941 (Código Penal), 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 PLC 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* ao tipo penal de atentado contra a segurança de serviço de utilidade pública (art. 265) e ao 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).

Tendo estado à disposição dos senhores Senadores, o PLC n° 89, de 2003 não recebeu emendas.

II – ANÁLISE

Muitas são as proposições legislativas já produzidas e debatidas no Congresso Nacional a respeito do tema da criminalidade nas áreas da informática, das telecomunicações e da Internet, a rede mundial de computadores. A evolução das tecnologias relacionadas à produção, ao processamento, ao armazenamento e à difusão da informação tem ocorrido com muita velocidade, gerando lacunas no ordenamento jurídico vigente.

A existência dessas lacunas tem motivado a proliferação de casos de fraudes e de danos ao patrimônio e danos morais de agentes públicos e privados. Estima-se que bilhões de reais já foram desviados de contas bancárias de pessoas físicas ou jurídicas em decorrência da atuação indevida de especialistas da área. Além disso, a violação de bases de dados mantidas em meio eletrônico tem provocado danos de grande monta pelo roubo de informações pessoais.

Não bastasse isso, há evidências de ligação entre o cibercrime e o financiamento do terrorismo internacional, e o crescimento do tráfico de seres humanos e de drogas. E 2004 foi apontado como o ano em que os crimes cibernéticos passaram a gerar lucros superiores aos do tráfico de drogas. De acordo com pesquisa realizada pela firma de consultoria americana *Computer Economics*, em 2004 as perdas totais chegam a 18 bilhões de dólares, com uma taxa de crescimento anual próxima de 35%.

A sociedade clama por medidas eficazes no combate ao crime cibernético. Não é mais possível que divergências hermenêuticas acerca da possível aplicabilidade das nossas normas jurídicas a esse tipo de conduta continuem a impedir a punição de condutas extremamente nocivas ao País.

A imprensa nacional destaca recentemente que alguns internautas já começam a fazer denúncias contra usuários pedófilos ou terroristas do sítio *Orkut*, denunciando-os ao provedor. O *Orkut*, um serviço da multinacional americana *Google*, imediatamente retira aqueles usuários do sistema mas não consegue detectar e impedir a sua reinclusão, face á liberalidade, inerente à rede mundial de computadores. Estabelece-se assim o círculo da denúncia e da punição responsável. Esse círculo, entretanto, tem como resposta novo círculo vicioso com o reinício dos delitos por novos usuários não identificados, tudo isto sem que se perceba um fim próximo.

O teor do PLS nº 137, de 2000, reflete preocupação idêntica àquela que conduziu o legislador na formulação dos dois outros projetos que acompanha, qual seja: a de disciplinar as condutas perniciosas que utilizem ou danifiquem sistemas de computador. Não obstante, é de abrangência e precisão mais restrita que aqueles, que o englobam integralmente.

O projeto limita-se a estabelecer que os crimes contra a pessoa, o patrimônio, a propriedade imaterial e intelectual, os costumes, bem como contra a criança e o adolescente, cometidos com a utilização de meios de tecnologia de informação e telecomunicações, terão suas penas triplicadas. Ou seja, a pena seria agravada em razão do meio utilizado pelo agente para perpetrar o crime.

A alteração legislativa proposta pelo PLS nº 137, de 2000, não é conveniente por duas razões.

Em primeiro lugar, tornaria superlativo o desvalor do meio utilizado pelo agente, que prevaleceria tanto sobre o desvalor do resultado quanto sobre o desvalor da intenção (genericamente considerada) – aquele, inspirador da teoria clássica da ação; este, da teoria finalista da ação, ambas adotadas de forma alternada pelo Código Penal a partir da reforma da sua Parte Geral, empreendida pela Lei nº 7.209, de 11 de julho de 1984. A segunda razão, que decorre da anterior, é a desproporcionalidade na aplicação das penas, haja vista que um delito menos grave poderia ser apenado mais severamente do que outro mais reprovável, apenas por ter sido cometido por meio da Internet.

O PLC nº 89, de 2003, pretende inserir a Seção V no Capítulo VI do Título I do Código Penal, onde seriam definidos os crimes contra a inviolabilidade dos sistemas informatizados. São nove as condutas delituosas por meio de acesso a sistema eletrônico de que trata o PLC:

- o acesso indevido a meio eletrônico;
- a manipulação indevida de informação eletrônica;
- o dano eletrônico;
- a pornografia infantil;
- o atentado contra a segurança de serviço de utilidade pública;
- a interrupção ou perturbação de serviço telegráfico e telefônico;
- a falsificação de cartão de crédito;
- a falsificação de telefone celular;
- a divulgação de informações pessoais ou de empresas.

Vejamos cada um desses tipos.

a) Arts. 154-A, 154-B e 154-C do CP, ou seja, o acesso indevido, a manipulação indevida de informação e a definição de meio eletrônico e sistema informatizado.

A redação pode ser aperfeiçoada para registrar que o meio eletrônico ou sistema informatizado é protegido contra as hipóteses em que o agente consegue o acesso mediante a violação desse sistema de proteção. Já a pena, que seria aplicada ao *hacker*, nome dado ao usuário que tenta violar ou viola o sistema de proteção, deveria ser mais severa.

Ademais, embora os três artigos possam ser reunidos em um só, preferimos manter a redação dada pelo PLC nº 89 de 2003, que define com maior clareza os delitos que se pretende tipificar. Entretanto propomos a alteração da pena original de detenção de 3 (três) meses a 1 (um) ano, e multa para detenção, de 1 (um) a 4 (quatro) anos, e multa, mantendo os mesmos parágrafos.

Ainda, quando este PLC nº 89 de 2003 estava sendo relatado nesta Comissão, o atento Senador Hélio Costa fez algumas sugestões de emendas que os membros da Comissão entenderam necessárias, mas que deveriam fazer parte de um novo Projeto de Lei a fim de que aquele projeto em discussão, uma vez aprovado, pudesse ir à sanção presidencial. Estando ele apensado ao PLS nº 76 de 2000 entendemos que é hora de acatar aqui algumas sugestões.

A primeira sugestão aqui acatada trata da definição e tipificação da Fraude Eletrônica, conhecida pelos profissionais de Tecnologia de Informação e Comunicação (TIC) como *phishing* ou *port fishing*, incluindo-a no Código Penal como segue:

"Fraude Eletrônica

Art. 154 - D. Difundir, por qualquer meio, sistema informatizado com o propósito de induzir alguém a fornecer, espontaneamente e por qualquer meio, dados ou informações que facilitem ou permitam o acesso indevido ou sem autorização, a dispositivo de comunicação ou a sistema informatizado:

Pena – reclusão de dois a quatro anos e multa.

Parágrafo único. 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, ou se o sistema informatizado fraudador tiver potencial de propagação ou alastramento."

Aqui acolhemos contribuição valiosa, de advogado especialista e com vasta experiência na defesa contra os crimes de informática, de que deveríamos evitar o nome "fraude", em seu título, para não haver confusão com a "fraude material" ou com o "furto mediante fraude". Nossa proposta é que o crime seja nominado "difusão maliciosa de código" ou "disseminação de armadilha eletrônica".

Se mantivéssemos a nomenclatura "fraude eletrônica", olvidando a confusão de natureza dos tipos, estaríamos engendrando, na verdade, uma hipótese aberta de "tentativa de fraude", pois a conduta do agente difusor, a partir de um eventual resultado, pode ser qualquer uma. A partir do fornecimento espontâneo de dados, o agente pode praticar fraude, dano, furto, chantagem ou qualquer outro crime, inclusive fora da esfera digital (mundo atômico).

Nossa proposta, finalmente, é no sentido de que a redação do caput seja a seguinte, com sua inclusão no Título VIII (Dos crimes Contra a Incolumidade Pública), Capítulo II (Dos Crimes Contra a Segurança Dos Meios de Comunicação e Transporte e Outros Serviços Públicos):

"Difusão Maliciosa de Código

Art. 266 -A. Difundir, por qualquer meio, sistema informatizado com o propósito de induzir alguém a fornecer, espontaneamente e por qualquer meio, dados ou informações que facilitem ou permitam o acesso indevido ou sem autorização, a dispositivo de comunicação ou a sistema informatizado, ou a obtenção de qualquer vantagem ilícita:

Pena – reclusão de um a dois anos.

Parágrafo único - A pena é aumentada de sexta parte, se o agente se vale de anonimato, de nome suposto ou da utilização de identidade de terceiros para a prática de acesso."

Outra sugestão do Senador refere-se à inclusão de alteração ao art. 46 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940, Código Penal, mediante a inclusão a ele do § 5º dando a opção ao juiz a aplicação de pena alternativa, sugestão não acatada por entendermos que as penas alternativas já estão bem definidas no Código Penal. Ademais, a aplicação desta espécie de pena alternativa aumentará exponencialmente os riscos e as vulnerabilidades dos sistemas de informática das instituições públicas, que ficarão ainda mais expostas aos ataques de *hackers* e organizações cibernéticas criminosas, tendo em vista a possibilidade de instalação de *backdoors* e outros dispositivos fraudulentos nos *softwares* manipulados durante o cumprimento da pena.

Finalmente o Senador sugeriu a mudança do termo "meio eletrônico" por "dispositivo de comunicação" no art. 154-C, à qual acatamos e no substitutivo promovemos sua atualização e complementação:

"Dispositivo de Comunicação e Sistema Informatizado

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

I – dispositivo de comunicação: o computador, o processador de dados, o disquete, o CD-ROM ou qualquer outro meio capaz de armazenar ou transmitir dados de maneira magnética, ótica, ou eletronicamente.

II – sistema informatizado: a rede de computadores, a base de dados, o programa de computador ou qualquer outro sistema capaz de armazenar ou transmitir dados eletronicamente."

b) Arts. 163, §§ 2ºe 3º

A equiparação feita pelo § 2º (equiparação à coisa do dado, informação ou a base de dados; a senha ou qualquer meio de identificação) é pertinente, mas poderia estar posicionada no Capítulo VIII do Título II (Disposições Gerais), pois dessa forma a regra seria válida para todos os tipos de crimes contra o patrimônio.

Por contribuição valiosa de vários advogados especialistas em crimes de informática, quanto à conduta do § 3º, entendemos que a pena deva ser mais severa, tendo em conta a potencialidade do dano material que se pode causar, por isso sugerimos a criação de um tipo autônomo com pena mais agravada do que a

prevista no *caput* e parágrafo único do art. 163 e mais ainda se praticada no anonimato. Em vista disso, sugerimos a seguinte redação:

"Dano por Difusão de Vírus Elctrônico

Art. 163-A. Criar, inserir ou difundir vírus em dispositivo de comunicação ou sistema informatizado, com a finalidade de destruí-lo, inutilizá-lo ou dificultar-lhe o funcionamento.

Pena: detenção, de 1 (um) a 3 (três) anos, e multa.

Parágrafo único - A pena é aumentada de sexta parte, se o agente se vale de anonimato,de nome suposto ou da utilização de identidade de terceiros para a prática de acesso. "

c) Art. 167 do CP

Por sua vez, a alteração proposta para o art. 167 do CP não é conveniente, pois proceder-se mediante queixa, quando o dado ou informação não tiver potencial de propagação ou alastramento, é um tratamento diferenciado para uma conduta por sí só inaceitável e que justamente por isso ganha tipo penal autônomo no art. 163-A.

d) Art. 218-A do CP (Pornografia Infantil)

O delito descrito nesse dispositivo já está previsto, de modo mais abrangente, nos arts. 240 e 241 do Estatuto da Criança e do Adolescente (ECA).

e) Arts. 265 e 266 do CP, respectivamente "atentado contra a segurança de serviço de utilidade pública" e "interrupção ou perturbação de serviço telegráfico ou telefônico":

As alterações propostas para esses dispositivos são convenientes.

f) Arts. 298 e 298-A do CP

A redação que se propõe para o art. 298 é conveniente (falsificação de cartão de crédito); quanto ao art. 298-A procedemos a pequenas modificações de

forma a melhorar sua clareza e compreensão, (falsificação de telefone celular ou meio de acesso a sistema eletrônico).

g) Art. 2º, § 2º, da Lei nº 9.296, de 1996

A alteração prevista no art. 2º da Lei nº 9.296, 24 de julho de 1996, é conveniente conforme o art. 15 do Substitutivo.

Não há que se falar em inconstitucionalidade da medida proposta, pois a reserva legal expressa e qualificada prevista no inciso XII do art. 5º da Constituição Federal estabeleceu apenas dois requisitos a serem observados pelo legislador ordinário no momento da regulamentação da restrição ao direito fundamental à privacidade das comunicações, quais sejam: existência de autorização judicial prévia à interceptação e 'para fins de investigação criminal ou instrução processual penal'.

O constituinte não estabeleceu o requisito de os 'crimes serem apenados com pena de reclusão'. Esta foi uma decisão do legislador ordinário, da Lei nº 9.296, de 1996, decisão que pode ser alterada a qualquer momento sem que isto signifique qualquer afronta à Lei Maior.

Há que se frisar, ainda, que referida alteração será importante para apuração de crimes punidos com detenção praticados com o uso de sistemas informatizados, tais como:

- calúnia (aplicação do art. 138 à conduta de falar falsamente em *chat* ou comunidade *online* que alguém cometeu crime),
- difamação (aplicação do art. 139 à conduta de difamar alguém através de boato eletrônico ou *hoax*),
- injúria (aplicação do art. 140 à conduta de enviar *e-mail* com ofensas pessoais ao destinatário),
- violação de direito autoral (aplicação do art. 184 à conduta de copiar conteúdo de página da Internet sem citar a fonte),
- falsa identidade (aplicação do art. 307 à conduta de enviar *spam* com remetente falso),
- exercício arbitrário das próprias razões (aplicação do art. 345 à conduta de atacar emissário de *spam* ou vírus para evitar novos danos).

Todos esses delitos são praticados por meio dos sistemas informatizados, mas seriam punidos, conforme a proposta aqui endossada, com pena de detenção, o que impede a interceptação para fins de instrução criminal, dificultando sua comprovação pelos ofendidos e pelo Ministério Público.

Essa medida, ademais, viabilizará a possibilidade de manter a apenação de crimes informáticos com pena de detenção, afastando a necessidade de se estipularem penas de reclusão para esses delitos, ferindo o princípio da proporcionalidade da pena. Se, para viabilizar a apuração e a investigação criminal, estabelecêssemos pena de reclusão para esses crimes, ao invés de viabilizar a quebra legal do sigilo para crimes apenados com detenção, estaríamos provocando severa e injustificada distorção do sistema penal.

h) Art. 10 do PLC nº 89, de 2003

O dispositivo é necessário, com as inclusões propostas no substitutivo, análogas aos artigos incluídos no Código Penal, para tipificar os crimes no Código Penal Militar, usando ferramentas de tecnologia da informação e comunicações.

Por fim, o art. 11 do projeto mostra-se adequado, enquanto o art. 12 não é conveniente, sendo preferível manter o sistema de crimes estabelecido nos arts. 240 e 241 do ECA. A Lei nº 10.764, de 12 de novembro de 2003, alterou o art. 241 do Estatuto da Criança e do Adolescente (Lei nº 8.069, de 13 de julho de 1990), para tipificar e punir de forma mais severa a pornografia infantil.

O PLS nº 76, de 2000, revestido de norma autônoma, afigura-se o projeto mais abrangente entre os que estão sendo aqui analisados. Os crimes informáticos estão divididos, no projeto, em crimes 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 opção sexual e contra a segurança nacional.

Realmente a visão ampla que se tem dos crimes de informática é o grande mérito deste projeto inovador proposto pelo eminente Senador Renan Calheiros. Seus dispositivos mostram a gravidade crescente dos delitos praticados com instrumentos informatizados, cujas punições ainda não contam com o necessário suporte legal. Isto vem trazendo enorme insegurança a toda a sociedade

pois crimes são praticados no anonimato da internet sem que haja a mínima possibilidade de defesa para o usuário.

Entretanto, a descrição de algumas das condutas deixa dúvidas em relação aos elementos dos respectivos delitos, o que pode prejudicar sua compreensão.

Vale lembrar que a Lei Complementar nº 95 de 1998 determina que havendo legislação em vigor deve-se preferir a sua alteração à criação de nova norma e desta forma o substitutivo proposto promove alterações ao Decreto-Lei nº 2.848, de 7 de dezembro de 1940, o Código Penal.

Comentamos, a seguir, sobre as disposições do PLS nº 76, de 2000.

a) Art. 1º, § 1º – crimes contra a inviolabilidade de dados e sua comunicação

Os incisos I, IV e V são espécies de crime de dano, descrito no art. 163 do CP; além disso, o inciso V deveria tipificar não a mera programação de instruções, mas a sua efetiva utilização, pois o nosso direito, via de regra, não pune os atos meramente preparatórios. Pode-se, alternativamente, prever, no art. 163 do CP, a equiparação dos dados informatizados à coisa, como o fez o PLC nº 89, de 2003, ou fazê-lo ao final do Título II do CP.

O inciso II pode ser tido como furto (art. 155 do CP), se houver subtração da coisa, ou como apropriação indébita (art. 168 do CP), se o agente tinha a posse ou a detenção da coisa. Quanto ao inciso III, melhor seria punir o uso indevido dos dados em razão da finalidade do agente: se atenta contra a intimidade da pessoa, contra o patrimônio, contra a fé pública, etc. Entretanto, há que se ter em conta que a maioria desses crimes já existe, e que a informática é apenas um meio para realização da conduta delituosa. A equiparação à coisa que se pode fazer ao final do Título II do CP resolveria o problema.

Além disso, as penas propostas são muito brandas em face da gravidade das condutas equiparadas que acima citamos.

b) Art. 1°, § 2°

Os incisos I e II são espécies de furto, crime definido no art. 155 do CP, cuja pena é bem mais severa do que a proposta no PLS nº 76, de 2000.

c) Art. 1°, § 3°

O inciso I está incluso no crime de injúria, descrito no art. 140 do CP; a conduta do inciso II, por sua vez, poderia ser inserida no Código Penal, mediante acréscimo do art. 154 D. Cabe observar que, se a informação for lesiva à honra, sua divulgação importará em um dos crimes tipificados no Capítulo V do Código Penal (calúnia, difamação ou injúria). Para desestimular o anonimato permitido pela internet, normalmente o caminho usado pelos autores dos crimes aqui tipificados, incluímos o artigo 154-F criando a obrigatoriedade de cadastramento identificador, além de estabelecermos, nos crimes em que tal conduta é especialmente perversa (Art. 154-A, § 3°, 154-D, parágrafo único e 266-A, parágrafo único), causas de aumento de pena a serem aplicadas pelo juiz, no momento de fixação da pena.

Todos os atos e fatos que se materializam através destes meios chegam, fácil e rapidamente, ao conhecimento de milhões de pessoas, causando um considerável prejuízo aos bens jurídicos tutelados. Em vista disso o potencial lesivo da conduta que ofende a honra da pessoa é incomensuravelmente maior quando o agente o faz por meio eletrônico como acontece nas redes de computadores. Isso já é bastante para justificar uma resposta penal mais severa, para que o agente sinta-se seriamente desestimulado a cometer o delito contra a honra por esse meio. É necessário, portanto, maior força penal coercitiva para evitá-los e assim fizemos incluir o art. 141-A conforme o art. 8° do substitutivo, estabelecendo causa especial de aumento de pena, com acréscimo de dois terços quando o meio utilizado é um dispositivo de comunicação ou sistema informatizado.

Novamente, em relação ao crime de ameaça, conduta que chega a ser banal no sítio do Orkut, por exemplo, a coibição do anonimato permitido pela internet, normalmente o caminho usado pelo agente da ameaça, entendemos suficiente a inclusão do artigo 154-F e dos parágrafos incluídos nos artigos 154-A, 154-D e 266-A.

d) Art. 1°, § 4°

O inciso I, a depender do resultado da conduta, será crime de lesão corporal ou homicídio, ambos já tipificados no Código Penal (arts. 129 e 121, respectivamente). O inciso II traz a incriminação de ato meramente preparatório. Além disso, os artefatos explosivos têm ampla utilização na indústria, não sendo conveniente definir como crime o trabalho intelectual de elaboração de um sistema informatizado de detonação.

e) Art. 1°, § 5°

As condutas descritas nos incisos I e II configuram crime contra a ordem tributária, definidos de forma mais abrangente e adequada nos arts. 1° e 2° da Lei n° 8.137, de 27 de dezembro de 1990.

f) Art. 1°, § 6°

O inciso I já está definido no art. 218 do CP (corrupção de menores). Os incisos II e III estão inclusos no art. 234 do CP (escrito ou objeto obsceno). Novamente, com o anonimato coibido pelo artigo 154-F e pelos parágrafos incluídos nos artigos 154-A, 154-D e 266-A do substitutivo, os autores destes crimes estarão desestimulados a cometê-los.

g) Art. 1°, § 7°

Os crimes definidos nesse parágrafo já estão contemplados na Lei n° 7.170, de 14 de dezembro de 1983 (Lei de Segurança Nacional), especificamente nos seus arts. 13, 15 e 23.

Recentemente em Audiência Pública sobre o PLS n° 279 de 2003, do qual também sou relator, de autoria do nobre Senador Delcídio Amaral e que propõe a criação de um cadastro de titulares de correio eletrônico na internet, ficou evidente que, para fins de investigação, é necessário estabelecer um prazo legal de armazenamento dos dados de conexões e comunicações realizadas pelos equipamentos componentes da internet, o que será feito pelos seus provedores de acesso. Os serviços de telefonia e transmissão de dados mantêm por cinco anos os dados de conexões e chamadas realizadas por seus clientes para fins judiciais, mas na internet brasileira inexiste procedimento análogo.

Registre-se que naquela audiência foram ouvidos representantes do Comitê Gestor da Internet no Brasil (CGIBr) do Ministério da Ciência e Tecnologia; da Fundação de Amparo à Pesquisa de São Paulo (FAPESP) que representa no Brasil o ICANN (*Internet Corporation for Assigning Names and Numbers)*, gestora do registro de nomes e números IP (*Internet Protocol),* ou seja, os endereços na internet; da– Associação Brasileira dos Provedores de Internet (ABRANET); do Instituto de Criminalística em Informática da Polícia Federal, do Ministério da Justiça (PF); da Agência Nacional de Telecomunicações (ANATEL).

Há apenas uma recomendação do Comitê Gestor da Internet Brasil (CGIBr) aos provedores nacionais: que mantenham, por no mínimo três anos, os dados de conexões e comunicações realizadas por seus equipamentos – a saber, identificação dos endereços de IP (protocolo de internet) do remetente e do destinatário da mensagem, bem como a data e horário de início e término da conexão, sem registrar o conteúdo da mensagem, preservando assim o sigilo da comunicação. É clara a necessidade de se transformar tal recomendação em imposição legal, razão por que apresentamos a inclusão no Código Penal do art.154-E conforme o art. 2º do substitutivo.

Além disso, também para fins de investigação, na mesma Audiência Pública, registrou-se a necessidade de estabelecer a obrigatoriedade de identificação positiva do usuário que acesse a Internet, ou qualquer rede de computadores, perante seu provedor ou junto a quem lhe torne disponível o acesso a dispositivo de comunicação ou sistema informatizado, muito embora todos tenham reconhecido as dificuldades técnicas, econômicas e culturais que a regra possa oferecer. Incluem-se aqui os *cyber-cafe* ou *hot zones.*

Vêm à memória os episódios danosos que ocorreram no início da operação com os celulares pré-pagos, o que obrigou o seu cadastramento obrigatório pelas operadoras, contra todos os argumentos então apresentados, ou seja, a sociedade brasileira mostrou o seu bom senso e mudou seu comportamento.

Desde já, alertamos que tal identificação e cadastramento necessitam serem necessariamente presenciais, com cópias de documentos originais, mas admite-se a alternativa de se utilizarem os certificados digitais, cuja emissão já é presencial conforme definido em Lei.

Outras formas alternativas de identificação e cadastramento podem ser usadas a exemplo do que os bancos, operadoras de telefonia, operadores de *call-center* e o comércio eletrônico em geral já vêm fazendo, usando cadastros disponíveis mediante convênios de cooperação ou simples colaboração.

Dados como nome de acesso (*login* ou *username*), nome completo, filiação, endereço completo, data de nascimento, números de telefone e senha criteriosa (número de caracteres, mistura de letras e números etc) devem ser requeridos no momento do cadastramento de um novo usuário. Este, ao solicitar um acesso posterior, usará seu nome de acesso e sua senha e outros procedimentos de validação e conferência automáticas realizados pelo sistema do provedor de acesso, procedimentos que têm o nome de "autenticação do usuário".

Conforme já citado em parágrafo anterior, a identificação e conseqüente cadastramento já acontecem com os serviços de telefonia, transmissão de dados e rádio-transmissão, onde cada operador já é obrigado por regulamento a manter um cadastro de proprietários de telefones fixos, móveis ou de aparelhos transmissores e receptores de rádio - cadastro usado exclusivamente para fins de investigação ou judiciais. Novamente, procedimento obrigatório análogo não existe na internet brasileira.

Novas tecnologias de transmissão, como a conexão sem fio, conhecida como *wireless* ou *Wi-Fi,* estão cada vez mais disponíveis. Como são padronizadas internacionalmente, tendem a se tornar extremamente baratas e a serem disseminadas largamente por todas as cidades, distritos ou aglomerações urbanas ou rurais, libertando o usuário de internet do local físico a que hoje está obrigado. Com o advento próximo da televisão digital tal disseminação será ainda mais efetiva.

Ainda, em qualquer outro serviço privado que se utilize da internet, seja instituição financeira, operadoras de cartões de crédito, empresas de comércio ou indústria, ou nas redes internas das instituições públicas e privadas, a autenticação do usuário mediante senha acompanhada, ou não, de outros requisitos de identificação, como certificado digital, tabela de códigos alfanuméricos e assim por diante, são requeridos para que o usuário acesse os serviços ou as informações.

Em outro caso, em decisão recente, o Tribunal Superior do Trabalho (TST) deu ganho de causa a um banco contra um funcionário que divulgava informações incorretas sobre as aplicações em um fundo de investimentos. O referido agente fora denunciado por uma cliente que tivera prejuízos com as informações e, em razão disso, foi demitido por justa causa, já que usou equipamento do banco, em horário de trabalho funcional, distribuindo informes não-verdadeiros na internet.

Assim, não é demais lembrar, principalmente para esses casos de difamação e injúria ou de prejuízos pessoais, o que dispõe a Carta Magna no seu art. 5º inciso IV que diz "é livre a manifestação do pensamento, sendo vedado o anonimato", o que por si só já justificaria a identificação, o cadastramento e a respectiva autenticação do usuário pelo provedor de acesso à internet brasileira.

Para tanto, transformamos a identificação, o cadastro e respectiva autenticação do usuário em imposição legal, conforme o caput do Art. 15 do substitutivo e incluindo no Código Penal o artigo 154-F e os parágrafos incluídos nos artigos. 154-A, 154-D e 266-A, conforme o art. 2º do substitutivo.

A fim de preservar a intimidade dos usuários, o cadastro somente poderá ser fornecido a terceiros mediante expressa autorização judicial ou em casos que a Lei determinar, conforme o § 2º do art. 14 do substitutivo.

Mas reconhecendo a existência de ferramentas de segurança mais potentes, previmos, conforme o § 3º do art. 14 do substitutivo, a troca opcional, pelo provedor, da identificação e do cadastro do usuário, pelo certificado digital. Este requer, de maneira presencial quando da sua emissão, todas as informações cadastrais, inclusive a constituição tecnicamente adequada de senha.

A regra é condizente com a Medida Provisória número 2.200-2, de 24 de agosto de 2001, mantida em vigor conforme a Emenda Constitucional número 32, de 12 de setembro de 2001. Como toda tecnologia inovadora o certificado digital inicialmente se restringiu às trocas interbancárias, a Transferência Eletrônica Disponível (TED), instituída pelo Sistema de Pagamentos Brasileiro (SPB), implantado em 2002 pelo Banco Central do Brasil. Estatísticas recentes mostram a ocorrência de quase 100 milhões de transações e mais de R$ 5 trilhões de reais transferidos com toda segurança em tempo real.

É público o fato de que o custo de cada certificado digital e seu suporte físico, (cartão de plástico, CD-ROM, ou outro dispositivo de comunicação), tende a cair em proporção geométrica, à medida que se dissemine o seu uso, uma característica conhecida das inovações tecnológicas.

Ao dispor sobre o uso do certificado digital como opcional, a presente norma permite a sua própria evolução, aguardando que a sociedade se adapte à nova realidade transformada a cada dia pela tecnologia, sem obrigar o usuário ou os provedores a novos custos ou a novos hábitos e comportamentos.

Por fim, mantendo a necessária segurança e respeitando os pressupostos de uma rede de computadores, naturalmente ágil, compatível, interoperável, colaborativa e cooperativa, previmos, conforme o § 4º do art. 14 do substitutivo, a substituição opcional do cadastro de identificação, a critério daquele que torna disponível o acesso, por cadastro que poderá ser obtido mediante instrumento público de convênio de cooperação ou colaboração com aqueles que já o tenham constituído na forma prevista no substitutivo.

III – VOTO

Diante do exposto, e considerando a pertinência e importância da solução proposta, somos pela aprovação do Projeto de Lei do Senado nº 76, de 2000, incorporando parcialmente o Projeto de Lei da Câmara nº 89, de 2003 (nº 84, de 1999, na Câmara dos Deputados) e o Projeto de Lei do Senado nº 137, de 2000, na forma do substitutivo que apresentamos.

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) e o Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), para tipificar condutas realizadas mediante uso de rede de computadores ou internet, ou que sejam praticadas contra sistemas informatizados e similares, e dá outras providências.

O CONGRESSO NACIONAL decreta:

Art. 1º 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 Vírus Eletrônico

Art. 163-A. Criar, inserir ou difundir vírus em dispositivo de comunicação ou sistema informatizado, com a finalidade de destruí-lo, inutilizá-lo ou dificultar-lhe o funcionamento.

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

Parágrafo único - A pena é aumentada de sexta parte, se o agente se vale de anonimato, de nome suposto ou da utilização de identidade de terceiros para a prática de acesso. "(NR)

Art. 2º O Título I da Parte Especial do Código Penal fica acrescido do Capítulo VII-A, assim redigido:

"Capítulo VII-A

DA VIOLAÇÃO DE DISPOSITIVO DE COMUNICAÇÃO OU SISTEMA INFORMATIZADO

Acesso indevido a dispositivo de comunicação

Art. 154-A. Acessar indevidamente, ou sem autorização, dispositivo de comunicação ou sistema informatizado:

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

§ 1º Nas mesmas penas incorre quem fornece a terceiro meio indevido ou não autorizado de acesso a 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 anonimato, de nome suposto ou da utilização de identidade de terceiros para a prática de acesso.

Manipulação indevida de informação eletrônica

Art. 154-B. Manter consigo, transportar ou fornecer indevidamente ou sem autorização, dado ou informação obtida em dispositivo de comunicação ou sistema informatizado:

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

Parágrafo único - 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, identificação de usuário e autenticação de usuário

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

I – dispositivo de comunicação: o computador, o computador de mão, o telefone celular, o processador de dados, os meios de armazenamento de dados digitais, ou qualquer outro meio capaz de processar, armazenar ou transmitir dados utilizando-se de tecnologias magnéticas, óticas ou qualquer outra tecnologia digital.

II – sistema informatizado: a rede de computadores, 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, armazenar ou transmitir dados eletronicamente.

III – identificação de usuário: os dados de nome de acesso, senha criteriosa, nome completo, filiação, endereço completo, data de nascimento, numero da carteira de identidade ou equivalente legal, que sejam requeridos no momento do cadastramento de um novo usuário de dispositivo de comunicação ou sistema informatizado.

IV – autenticação de usuário: procedimentos de validação e conferência da identificação do usuário, quando este tem acesso ao dispositivo de comunicação ou sistema informatizado, realizados por quem os torna disponíveis ao usuário.

Divulgação de informações depositadas em banco de dados

Art. 154-D. Divulgar, ou tornar disponíveis, para finalidade distinta daquela que motivou a estruturação do banco de dados, informações privadas referentes, direta ou indiretamente, a dados econômicos de pessoas físicas ou jurídicas, ou a dados de pessoas físicas 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 por decisão da autoridade competente, ou mediante expressa anuência da pessoa a que se referem, ou de seu representante legal.

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

Parágrafo único: A pena é aumentada de sexta parte, se o agente se vale de anonimato, de nome suposto ou da utilização de identidade de terceiros para a prática de divulgação.

Dados de conexões e comunicações realizadas

Art. 154-E. Deixar de manter, aquele que torna disponível o acesso a rede de computadores, os dados de conexões e comunicações realizadas por seus equipamentos, aptas à identificação do usuário, endereços eletrônicos de origem e destino no transporte dos registros de dados e informações, data e horário de início e término da conexão, incluindo protocolo de internet ou mecanismo de identificação equivalente, pelo prazo de cinco anos.

Pena – detenção, de dois a seis meses, e multa.

Permitir acesso por usuário não identificado e não autenticado

Art. 154-F. Permitir, aquele que torna disponível o acesso a rede de computadores, a usuário, sem a devida identificação e autenticação, qualquer tipo de acesso ou uso pela rede de computadores.

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

Parágrafo único. Na mesma pena incorre, o responsável por provedor de acesso a rede de computadores, que deixa de exigir, como condição de acesso à rede, a necessária, identificação e regular cadastramento do usuário.

Art. 3º O Código Penal passa a vigorar acrescido do seguinte art. 183-A:

> Art. 183-A. Equiparam-se à coisa o 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.

Art. 4º 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 ou telefônico"**
>
> **Art. 266.** Interromper ou perturbar serviço telegráfico, radiotelegráfico, telefônico, telemático ou de telecomunicação, impedir ou dificultar-lhe o restabelecimento:
>
> ..... (NR)"

Art. 5º O Capitulo II do Título VIII do Código Penal passa a vigorar acrescido do seguinte artigo:

> **"Difusão Maliciosa de Código**
>
> **Art. 266-A.** Difundir, por qualquer meio, programa, conjunto de instruções ou sistema informatizado com o propósito de induzir alguém a fornecer, espontaneamente e por qualquer meio, dados ou informações que facilitem ou permitam o acesso indevido ou sem autorização, a dispositivo de comunicação ou a sistema informatizado, ou a obtenção de qualquer vantagem ilícita:
>
> Pena – detenção de um a dois anos.
>
> Parágrafo único - A pena é aumentada de sexta parte, se o agente se vale de anonimato, de nome suposto ou da utilização de identidade de

terceiros para a prática de acesso.(NR)"

Art. 6º 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 portátil de armazenamento e processamento de informações

Parágrafo único. Equipara-se a documento particular o cartão de crédito ou débito ou qualquer dispositivo eletrônico portátil de armazenamento ou processamento de informações. (NR)"

Art. 7º O Código Penal passa a vigorar acrescido do seguinte art. 298-A:

"Falsificação de telefone celular ou meio de acesso a sistema eletrônico

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

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

Art. 8º O Código Penal passa a vigorar 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 dispositivo de comunicação ou sistema informatizado.

Art. 9º 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 Vírus Eletrônico

Art. 262-A. Criar, inserir ou difundir vírus em dispositivo de comunicação ou sistema informatizado, com a finalidade de destruí-lo, inutilizá-lo ou dificultar-lhe o funcionamento.

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

Parágrafo único - A pena é aumentada de sexta parte, se o agente se vale de anonimato, de nome suposto ou da utilização de identidade de terceiros para a prática de acesso. "(NR)

Art. 10 O Título VII da Parte Especial do Livro I do Código Penal Militar, Decreto-Lei, nº 1.001, de 21 de outubro de 1969, fica acrescido do Capítulo VII-A, assim redigido:

"Capítulo VII-A

DA VIOLAÇÃO DE DISPOSITIVO DE COMUNICAÇÃO OU SISTEMA INFORMATIZADO

Acesso indevido a dispositivo de comunicação

Art. 339-A. Acessar indevidamente, ou sem autorização, dispositivo de comunicação ou sistema informatizado:

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

§ 1º Nas mesmas penas incorre quem fornece a terceiro meio indevido ou não autorizado de acesso a dispositivo de comunicação ou sistema informatizado.

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

Manipulação indevida de informação eletrônica

Art. 339-B. Manter consigo, transportar ou fornecer indevidamente ou sem autorização, dado ou informação obtida em dispositivo de comunicação ou sistema informatizado:

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

Dispositivo de comunicação, sistema informatizado, identificação de usuário e autenticação de usuário

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

I – dispositivo de comunicação: o computador, o computador de mão, o telefone celular, o processador de dados, os meios de armazenamento de dados digitais, ou qualquer outro meio capaz de processar, armazenar ou

transmitir dados utilizando-se de tecnologias magnéticas, óticas ou qualquer outra tecnologia digital.

II – sistema informatizado: a rede de computadores, 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, armazenar ou transmitir dados eletronicamente.

III – identificação de usuário: os dados de nome de acesso, senha criteriosa, nome completo, filiação, endereço completo, data de nascimento, numero da carteira de identidade ou equivalente legal, que sejam requeridos no momento do cadastramento de um novo usuário de dispositivo de comunicação ou sistema informatizado.

IV – autenticação de usuário: procedimentos de validação e conferência da identificação do usuário, quando este tem acesso ao dispositivo de comunicação ou sistema informatizado, realizados por quem os torna disponíveis ao usuário.

Divulgação de informações depositadas em banco de dados

Art. 339-D. Divulgar, ou tornar disponíveis, para finalidade distinta daquela que motivou a estruturação do banco de dados, informações privadas referentes, direta ou indiretamente, a dados econômicos de pessoas físicas ou jurídicas, ou a dados de pessoas físicas 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 por decisão da autoridade competente, ou mediante expressa anuência da pessoa a que se referem, ou de seu representante legal.

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

Parágrafo único: A pena é aumentada de sexta parte, se o agente se vale de anonimato, de nome suposto ou da utilização de identidade de terceiros para a prática de divulgação.

Dados de conexões e comunicações realizadas

Art. 339-E. Deixar de manter, aquele que torna disponível o acesso a rede de computadores, os dados de conexões e comunicações realizadas por seus equipamentos, aptas à identificação do usuário, endereços eletrônicos de origem e destino no transporte dos registros de dados e informações, data e horário de início e término da conexão, incluindo protocolo de internet ou mecanismo de identificação equivalente, pelo prazo de cinco anos.

Pena – detenção, de dois a seis meses, e multa.

Permitir acesso por usuário não identificado e não autenticado

Art. 339-F. Permitir, aquele que torna disponível o acesso a rede de computadores, a usuário, sem a devida identificação e autenticação, qualquer tipo de acesso ou uso pela rede de computadores.

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

Parágrafo único. Na mesma pena incorre, o responsável por provedor de acesso a rede de computadores, que deixa de exigir, como condição de acesso à rede, a necessária, identificação e regular cadastramento do usuário.(NR)"

Art. 11 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 Maliciosa de Código

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

Pena – detenção de um a dois anos.

Parágrafo único - A pena é aumentada de sexta parte, se o agente se vale de anonimato, de nome suposto ou da utilização de identidade de terceiros para a prática de acesso.(NR)"

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

"Capítulo VIII-A

DISPOSIÇÕES GERAIS

Art. 267-A. Equiparam-se à coisa o 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.(NR)"

Art. 13 Todo aquele que desejar acessar uma rede de computadores, local, regional, nacional ou mundial, deverá identificar-se e cadastrar-se naquele que torne disponível este acesso.

Parágrafo único. Os atuais usuários terão prazo de cento e vinte dias após a entrada em vigor desta Lei para providenciarem ou revisarem sua identificação e cadastro junto a quem, de sua preferência, torne disponível o acesso aqui definido.

Art. 14 Todo aquele que torna disponível o acesso a uma rede de computadores somente admitirá como usuário pessoa ou dispositivo de comunicação ou sistema informatizado que for autenticado conforme validação positiva dos dados cadastrais previamente fornecidos pelo contratante de serviços. A contratação dar-se-á exclusivamente por meio formal, vedado o ajuste meramente consensual.

§1° O cadastro mantido por aquele que torna disponível o acesso a uma rede de computadores conterá obrigatoriamente as seguintes informações prestadas por meio presencial e com apresentação de documentação original: nome de acesso; senha de acesso ou mecanismo similar; nome completo; endereço completo com logradouro, número, complemento, código de endereçamento postal, cidade e estado da federação; número de registro junto aos serviços ou institutos de identificação das Secretarias de Segurança Pública Estaduais ou conselhos de registro profissional; número de inscrição no Cadastro de Pessoas Físicas (CPF), mantido pelo Ministério da Fazenda ou o Número de Identificação do Trabalhador (NIT), mantido pelo Ministério da Previdência Social.

§ 2° O cadastro somente poderá ser fornecido a terceiros mediante expressa autorização da autoridade competente ou em casos que a Lei venha a determinar.

§ 3° A senha e o cadastro de identificação, a critério daquele que torna disponível o acesso, poderão ser substituídos por certificado digital emitido dentro das normas da Infra-estrutura de Chaves Públicas Brasileira (ICP–Brasil), conforme determina a MP 2.200-2 de 24 de agosto de 2001.

§ 4° O cadastro de identificação, a critério daquele que torna disponível o acesso, poderá ser obtido mediante instrumento público de convênio

de cooperação ou colaboração com aqueles que já o tenham constituído na forma deste artigo.

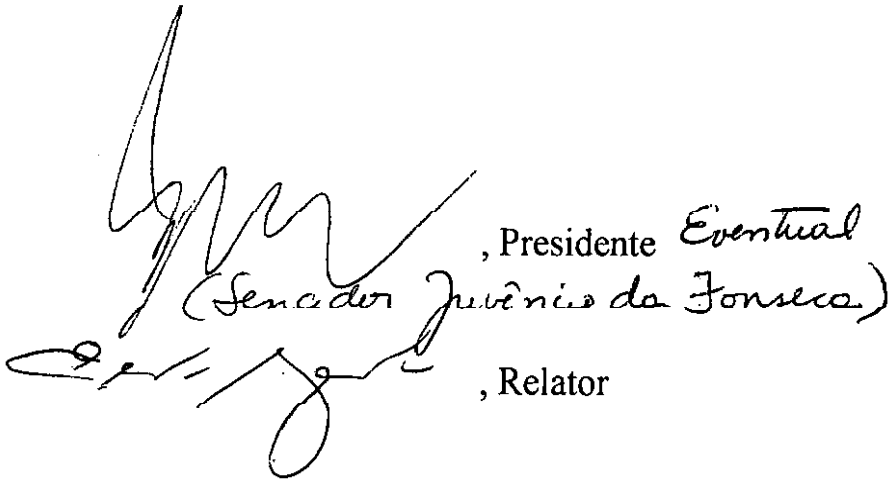
§ 5º Para assegurar a identidade e a privacidade do usuário a senha de acesso poderá ser armazenada criptografada por algoritmo não reversível.

Art. 15. 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:

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

Art. 16 Esta Lei entra em vigor sessenta dias após a data de sua publicação.

Sala da Comissão, 20 de junho de 2006



RELATOR: Senador **EDUARDO AZEREDO**

I – RELATÓRIO

Vêm a esta Comissão, para parecer, o Projeto de Lei da Câmara (PLC) nº 89, de 2003 (nº 84, de 1999, na origem), e os Projetos de Lei do Senado (PLS) nº 137, de 2000, e nº 76, de 2000, todos referentes a crimes na área de informática. Tramitam em conjunto em atendimento ao Requerimento nº 847, de 2005, do Senador Renan Calheiros. Em decorrência do Requerimento nº 848, de 2005, foi extinta a urgência na tramitação do PLC nº 89, de 2003, que havia sido declarada em decorrência da aprovação do Requerimento nº 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 nº 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 nº 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 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 Decreto-Lei n° 2.848, de 7 de dezembro de 1940 (Código Penal), 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, onde foram amplamente debatidas. Lá, apresentamos relatório e voto pela aprovação do PLS n° 76, de 2000, 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 pretende:

a) inserir no Código Penal (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, identificação de usuário e autenticação de usuário*; 154-D, para definir o crime de *divulgação de informações depositadas em bancos de dados*; 154-E, 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 à 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.

No âmbito processual, o Substitutivo pretende 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.

Ademais, quer obrigar a todos os que desejarem acessar uma rede de computadores a identificar-se e cadastrar-se. Do outro lado, pretende obrigar a todos os que dispõem de rede a somente admitir como usuário pessoa ou dispositivo de comunicação ou sistema informatizado que seja autenticado consoante validação positiva dos dados cadastrais previamente fornecidos, mediante contrato formalizado perante o fornecedor do serviço.

Não foram apresentadas emendas.

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.

Materialmente, não vislumbramos inconstitucionalidades ou vícios de juridicidade nos projetos.

No mérito, reiteramos a análise feita por ocasião da apreciação das proposições na Comissão de Educação, que resultou no Parecer pelo oferecimento do Substitutivo ora examinado.

Entretanto, reconhecemos que existem alguns aperfeiçoamentos a realizar quanto à redação, concisão e clareza, e de mérito, que só recentemente chegaram ao nosso conhecimento, conforme sugestões informais apresentadas por associações, por órgãos públicos e por especialistas em tecnologia da informação e em direito aplicado a ela.

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, para ouvirmos as sugestões e explicarmos o trabalho que o Parlamento vem desenvolvendo há dez anos.

Estes aperfeiçoamentos foram devidamente analisados pelo mesmo grupo de voluntários, aos quais registramos nossos agradecimentos, que colaboraram informalmente na construção do Substitutivo apresentado na Comissão de Educação desta casa legislativa. Lá inicialmente foram contatados quase cem profissionais de várias especialidades correlatas com a matéria ora em discussão, alem de oficiais superiores das três forças armadas, que cuidaram da alteração do Código Penal Militar, e ao final resumiu-se a um grupo de especialistas voluntários que, com o uso intensivo da internet, logrou concluir pelo texto do substitutivo afinal aprovado.

Analisadas as sugestões, na sua maioria de redação para clareza e concisão, concluímos que a matéria, complexa, abrangente, tratando de crimes contra a pessoa, contra o patrimônio e contra serviços públicos, requer que se faça um novo substitutivo, que pode ser comparado com aquele da Comissão de Educação, por quem nisso tiver interesse. Assim passamos a descrever as alterações, supressões e inclusões.

Começamos por alterar a ementa da Lei para nela incluir a indicação da alteração da Lei nº 9.296, de 24 de julho de 1996, a Lei que cuida das interceptações de comunicações telefônicas, regulamentando o inciso XII, parte final, do art. 5° da Constituição Federal, a indicação da alteração do Decreto-Lei nº. 3.689, de 3 de outubro de 1941, o Código de Processo Penal, a indicação da alteração da Lei nº 10.446, de 8 de maio de 2002, que dispõe sobre infrações penais de repercussão interestadual ou internacional que exigem repressão uniforme, e a indicação da alteração da Lei nº 8.078, de 11 de setmbro de 1990, o Código do Consumidor.

Incluímos um novo art. 1°, renumerando-se os demais, para cumprir o que determina o art. 7°, da Lei Complementar n° 95, de 26 de fevereiro de 1998: "Art. 7° O primeiro artigo do texto indicará o objeto da lei e o respectivo âmbito de aplicação ....".

Recebemos ponderações de que nem tudo é digital embora seja eletrônico, como por exemplo, alguns dispositivos de comunicação, com componentes eletrônicos mas analógicos. Assim substituímos toda referência 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, deixando o texto mais aderente com a realidade da tecnologia, pretendendo com isso maior longevidade para o texto da norma em apreço.

No novo art. 154-A do Código Penal, e no seu correspondente novo art. 339-A do Código Penal Militar, incluímos a expressão "ou sistema informatizado" no título do artigo dando-lhe coerência com o seu texto.

Para maior precisão e clareza, no novo art. 154-B do Código Penal, e no seu correspondente novo art. 339-B do Código Penal Militar trocamos de posição na oração a expressão "dado ou informação obtida", e incluímos a ação de "obter" o dado ou a informação. Acrescentamos a majorante de um terço da pena se o dado ou informação obtida indevidamente ou sem autorização, é fornecido pela rede de computadores, ou em qualquer outro meio de divulgação em massa.

Nas definições constantes do novo art. 154-C do Código Penal, e do seu correspondente novo art. 339-C do Código Penal Militar, fizemos as seguintes alterações:

– na definição de "Dispositivo de Comunicação" incluímos a expressão "os meios de captura de dados eletrônicos ou digitais ou similares" e substituímos a expressão "digitais" por "eletrônicos ou digitais ou similares";

– na definição de "Sistema Informatizado" substituímos a expressão "eletronicamente" pela expressão "eletrônica ou digitalmente ou equivalente", incluímos a expressão "capturar" e suprimimos a expressão "rede de computadores ou internet" que passou a ser objeto de definição específica;

– na definição de "Identificação de Usuário" reduzimos a lista de dados a identificador de acesso, senha ou similar, nome completo, data de

nascimento e endereço completo, mas mantivemos as expressões "e outros dados que sejam requeridos ....";

– na definição de "Autenticação de Usuário" substituímos a expressão "validação" por "verificação", considerada mais adequada à definição e aperfeiçoamos a sua redação;

– incluímos a definição de "Rede de Computadores", para nela incluir a definição de internet, a rede mundial de computadores, reclamada por alguns dos colaboradores na elaboração do Substitutivo, e definindo todas as demais redes de computadores, locais, regionais, nacionais, privadas ou públicas. Uma rede de computadores é entendida como um conjunto de computadores e dispositivos de comunicação, governados entre si, de comun acordo, por um conjunto de regras, códigos e formatos agrupados em protocolos. Assim ela é destacada de "sistema informatizado", conceito mais abrangente, que inclui qualquer sistema, alguns deles não dispondo de meios para identificar e autenticar usuários e muito menos para armazenar os dados de conexão, conforme requeridos pelos processos de investigação penal;

– incluímos a definição de "Provedor" tanto para aquele que presta serviços de acesso à rede de computadores como para aquele que presta serviços relacionados a esse acesso.

– incluímos finalmente a definição de "Dados de conexões realizadas" como sendo aqueles dados aptos à identificação do usuário, os endereços eletrônicos de origem das conexões, a data, o horário de início e término e a referência GMT dos horários, relativos à cada conexão realizada pelos equipamentos de uma rede de computadores.

No novo art. 154-D, *caput*, do Código Penal, e no seu correspondente novo art. 339-D, *caput*, do Código Penal Militar, incluímos a conduta de "violar", ou seja, a conduta de conhecer sem autorização ou para fim diferente da sua constituição, o conteúdo de um banco de dados. Para a decisão de autorizar a divulgação de informações contidas em banco de dados, contida no novo art. 154-D, caput, do Código Penal, e no seu correspondente novo art. 339-D, caput, do Código Penal Militar, incluímos a expressão "nos casos previstos em lei," dando maior clareza à norma.

Renumeramos o parágrafo único destes artigos como § 1°, e acrescentamos o § 2° 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. Acrescentamos ainda o § 3°, que diz 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, hospedagem e dados de identificação de usuário, quando constatada qualquer prática criminosa.

Em relação à "preservação dos dados de conexões realizadas", o novo art. 154-E do Código Penal e o seu correspondente novo art. 339-E, do Código Penal Militar, foram renomeados respectivamente, em dois artigos acrescentados ao Substitutivo, como o novo art. 356-A do Código Penal e novo art. 352-A do Código Penal Militar, ambos pertencentes em cada Código ao capítulo intitulado "DOS CRIMES CONTRA A ADMINISTRAÇÃO DA JUSTIÇA", com ênfase na finalidade da guarda dos dados, deixando claro que se tutela a justiça, afirmando-os como dados de valor probatório, aptos à identificação do usuário quando da ocorrência de crime.

Na nova redação destes artigos retiramos a expressão "e comunicações", considerada demais abrangente, pois o que se pretende são os dados de conexões realizadas e não aqueles da continuidade da conexão, o que onera sem necessidade os operadores do sistema. Reduzimos a lista de informações a serem guardadas, significando menor volume de arquivamento para os operadores, o que também acontece com a redução do prazo de guarda de "cinco" para "três" anos, que é a recomendação do Comitê Gestor da Internet do Brasil (CGI.br), prazo considerado suficiente para os trabalhos de investigação quando necessários.

Depois de ouvida a sociedade em geral, pelos seus segmentos representativos, durante as reuniões técnicas e debates havidos, optamos por modificar substancialmente o novo art. 154-F do Código Penal, e o seu correspondente novo art. 339-F do Código Penal Militar, que além de terem a redação e o mérito aperfeiçoados e adequados às definições introduzidas, foram transformados respectivamente nos §§ 4° e 5° do art. 154-A do Código Penal e nos §§ 3° e 4° do art. 339-A do Código Penal Militar, agregando ao tipo penal de "acessar indevidamente uma rede de computadores" o tipo de "permitir o acesso indevido por usuário não identificado e não autenticado" e reduzir as penas ao mínimo se, tanto no *caput,* quanto na hipótese do parágrafo respectivo, o crime é culposo.

De fato a redação anterior destes artigos poderia levar a uma interpretação indesejada da ação de permitir o acesso. Com a nova redação somente no caso de ocorrência do crime de acesso indevido a permissão de acesso concedida a usuário não identificado e não autenticado, será punida se provado o dolo ou a culpa de quem permitiu. Assim reconhecemos que as dificuldades de identificação de usuário e respectiva autenticação em um mundo virtual ainda são muito grandes ou dispendiosas e com a nova redação o discernimento sobre o dolo ou culpa em uma permissão delituosa caberá ao processo criminal. Como resultado o Código Penal é atualizado com os novos tipos e suas penas sem criar obstáculos ao desenvolvimento dos serviços virtuais em franco desenvolvimento.

Por sugestão recebida para melhor tipificação, incluímos o art. 4º do Substitutivo, renumerando-se os demais, para com ele acrescentarmos o inciso V ao § 4º do art. 155 do Código Penal e acrescentarmos o inciso V ao § 6º do seu correspondente art. 240 do Código Penal Militar. Ambos tratam do crime de "furto qualificado", que tem a pena definida como de reclusão de dois a oito anos, e multa, se o crime é cometido, por exemplo, com emprego de chave falsa. Adicionamos o inciso com as orações alternativas: "mediante uso de rede de computadores, dispositivos de comunicação ou sistemas informatizados; ou que sejam praticadas contra rede de computadores, dispositivos de comunicação ou sistemas informatizados e similares".

Assim, por analogia ao "furto qualificado por uso de chave falsa" tipificado no art. 155 do Código Penal e art. 240 do Código Penal Militar já mencionados, definimos a mesma pena para o "furto qualificado por acesso indevido" mediante processos informatizados e para o furto de informações contidas em banco de dados, sempre ocorridos com o uso de processos ou informações falseadas ou copiadas indevidamente.

Acrescentamos à alteração do art. 266 do Código Penal as expressões "informático, dispositivo de comunicação, rede de computadores, sistema informatizado", seja para adequação aos termos já dispostos na Lei 9.296, de 1996 e aos termos do art. 154-C do Substitutivo, seja para nele incluir como tipo penal "o ataque a rede de computadores ou sistema informatizado" conhecido como, por exemplo, o *DoS* (*Denial-of-Service attack*), o *DDoS* (*Distributed-Denial-of-Service attack)* e outros equivalentes.

Igualamos a pena do novo tipo de "difusão maliciosa de código", do novo art. 266-A do Código Penal e no seu correspondente novo art. 339-A do Código Penal Militar, à pena do crime de difusão de vírus eletrônico ou digital, do novo art. 163-A do Código Penal e do seu correspondente novo art. 262-A do Código Penal Militar, passando a pena de detenção de um a dois anos para reclusão de um a três anos, pois a pretensão dos autores da difusão maliciosa de código é a fraude, equivalente à difusão de vírus, e que pode levar ao "furto qualificado por acesso indevido".

Nestes artigos renumeramos o parágrafo único como § 1° e acrescentamos um § 2° para ressalvar da ação delituosa, conforme no inciso III do art. 23 do Código Penal, como uma das hipóteses de "exclusão de ilicitude", a ação do agente técnico ou o profissional habilitado que, a título de resposta a ataque, de frustração de invasão ou burla, de proteção do sistema, de interceptação defensiva, de tentativa de identificação do agressor, de exercício de forense computacional e de práticas gerais de segurança da informação manipula código malicioso detectado, em proveito próprio ou de seu preponente e sem risco para terceiros. Explicando, excluem-se da ação delituosa os profissionais que fazem a prevenção, análise e resposta aos ataques malévolos numa rede de computadores, dispositivo de comunicação ou sistema informatizado.

Alteramos o parágrafo único do art. 298 do Código Penal, o qual se pretende acrescentar, para substituir a expressão "armazenamento ou processamento" pela expressão "captura, armazenamento, processamento ou transmissão" que é uma tipificação clara nos dispositivos de comunicação ou sistemas informatizados, para maior abrangência do texto.

Para maior efetividade da aplicação da Lei, incluímos o art. 19 do Substitutivo para a decretação de prisão preventiva nos crimes dolosos 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, mediante o acréscimo do inciso IV ao art. 313 do Decreto-Lei n° 3.689, de 3 de outubro de 1941, Código de Processo Penal (CPP).

Com a nova redação dada ao art. 14 do Substitutivo da Comissão de Educação (art. 21 do Substitutivo que ora apresentamos) mantivemos a obrigatoriedade da identificação e autenticação do usuário, pelo provedor de acesso a uma rede de computadores, em redação mais simples e concisa. Cumpre lembrar aqui a confusão que se estabelece entre a liberdade de expressão e o anonimato, ambos possíveis na internet, (o anonimato representado pela não

identificação e a não autenticação do usuário), quando a própria Constituição Federal determina no art. 5º, inciso IV, que "é livre a manifestação do pensamento, sendo vedado o anonimato". Ora, o fato de emitir para alguém uma carteira de habilitação para dirigir veículos automotores não limita o seu direito constitucional de ir e vir; da mesma forma a identificação do usuário de uma rede de computadores não o impede de manifestar-se pela rede.

Ainda, este dispositivo legal consagra prática mundial de usos e costumes de todos quantos tem na rede de computadores o seu instrumento básico e maior de prestação de serviços, diferenciando pela quantidade ou pelo tipo de informação requerida quando do acesso.

Na nova redação fica facultado, em substituição à identificação de usuário, o uso de instrumentos digitais que garantam a autenticação e integridade dos arquivos digitais e mensagens que trafegam na rede ou o uso de entidades de dados de identificação de usuário já existentes que tenham sido constituídas de maneira presencial.

Esperamos assim que a norma estimule a celebração de convênios, entre aqueles que tornam possível o acesso à rede de computadores e as organizações detentoras de cadastros de usuários, para permitirem a verificação e conseqüente autenticação da identificação de usuário de rede de computadores, nos dados imutáveis como nome, número de documento legalmente emitido, conforme a boa prática existente entre organizações de proteção ao crédito, as instituições financeiras, órgãos públicos e outras.

Sobre estes dados a serem compartilhados, a Constituição Federal determina no seu art. 5º, inciso XXXIII, que:

> **"Art. 5º** .....
>
> .....
>
> XXXIII – todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado;".

O inciso foi regulamentado pela Lei nº 11.111, de 5 de maio de 2005, não proibindo o compartilhamento de dados imutáveis como os já citados,

naturalmente desde que autorizados pelo seu titular ou por lei específica, pois dispõe:

> "**Art. 2º** O acesso aos documentos públicos de interesse particular ou de interesse coletivo ou geral será ressalvado exclusivamente nas hipóteses em que o sigilo seja ou permaneça imprescindível à segurança da sociedade e do Estado, nos termos do disposto na parte final do inciso XXXIII do *caput* do art. 5º da Constituição Federal."

Ainda a propósito, cabe lembrar que a obrigação da identificação de usuário e a exigência de documentos que possam ser verificados quanto á sua autenticidade é uma recomendação constante da Cartilha de Segurança para Internet, no item *h* da sua seção 6 (Responsabilidades dos Provedores), documento editado em notável esforço de colaboração entre o Ministério Público Federal de São Paulo (MPF/SP) e o Comitê Gestor da Internet no Brasil (CGI.br), patrocinada pela Associação Brasileira dos Provedores de Internet (ABRANET), aos quais registramos aqui o nosso elogio ao resultado alcançado.

A brochura contém instruções de como proceder em caso de investigação de delito ocorrido, os modelos de documentos a serem usados para comunicar o fato delituoso às autoridades competentes, o texto completo da Convenção sobre o Cibercrime, celebrado em Budapest, a 23 de novembro de 2001, pelo Conselho da Europa, cuja assinatura pelo Governo dos Estados Unidos da América foi recentemente ratificada pelo Senado daquele país, que deverá entrar em vigor em Janeiro de 2007, e finalmente contém a "cartilha", propriamente dita, detalhando como utilizar-se da Internet de maneira segura.

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 a criação de legislação penal em cada Estado signatário que trate de vários tipos penais que comentaremos logo a seguir em detalhe.

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

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 a admissão à Convenção de novos Estados por convite e a aprovação por maioria do Conselho. Concluindo, deixa a aplicação da Convenção a critério de cada Estado.

Corrobora a harmonia brasileira com os termos da Convenção a correspondência entre o que a 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*, objeto do art. 16 do Substitutivo;

- *da interferência não autorizada sobre os dados armazenados*, objeto do art. 154-D, do art. 163-A e do art. 266-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. 266-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. 266-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;

- *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 §§ 3º 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 do parágrafo único do art. 21 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 e crimes de pedofilia e, caso a caso, cuida de alguns outros já tipificados no Código Penal.

O presente Projeto de Lei, que atualiza o nosso Código Penal e o Código Penal Militar, coloca o Brasil em posição de destaque para que possa tratar, convir e acordar de maneira diferenciada com os países signatários da Convenção de Budapest e outras, inclusive os Estados Unidos da América, que adotará a Convenção a partir de Janeiro de 2007, país sede das maiores empresas de tecnologia da informação e sede dos maiores provedores de acesso à rede mundial de computadores.

Em outro documento, a "*Directiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrônicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Directiva 2002/58/CE*", entre outras considerações preambulares, trata naquela de número 18 que "*A decisão-Quadro 2005/222/Al do Conselho, de 24 de fevereiro de 2005, relativa a ataques contra os sistemas de informação, dispõe que o acesso ilegal aos sistemas de informação, incluindo os dados neles conservados seja punível como infracção penal.*" E na consideração de número 20 cita a Convenção sobre o Cibercrime de Budapest de 2001 e a Convenção de 1981, esta sobre os dados pessoais.

Avançando, a *Directiva* define no art. 2º como dados: os "*dados de tráfego e os dados de localização bem como os dados conexos necessários para identificar o assinante e o utilizador*". No art. 5º detalha as "*Categorias de dados a conservar*" e aí vamos encontrar no item 2 da letra *a*, que diz respeito à internet, a especificação da guarda do identificador de acesso, do nome e do endereço do assinante ou usuário, aos quais o endereço do protocolo IP, o identificador de acesso ou o número do telefone que estavam atribuídos no momento da comunicação.

Faz-se mister demonstrar a harmonia do Substitutivo, com a Directiva, que nos arts. 6º, 7º, 8º e 9º, define respectivamente, os "*Períodos de Conservação*", a "*Proteção de dados e segurança dos dados*", os "*Requisitos para o armazenamento dos dados conservados*", a "*Autoridade de controlo*", previstos no Substitutivo no art. 22 incisos I e II e seu parágrafo único.

Comentando, desses artigos vem a recomendação de que os dados sejam conservados por um período mínimo de seis meses e não superior a dois anos, e ao final da *Directiva* vários signatários declaram que estudarão a aplicação de prazos diferenciados ou de dezoito ou de trinta e seis meses, a partir de 2007 ou 2009. No Brasil, o Comitê Gestor da Internet no Brasil (CGI.br) definiu este prazo em trinta e seis meses. A *Directiva* recomenda ainda que a guarda deva ser criteriosa e que seja designada uma autoridade competente para a realização da auditoria a que estes dados forem submetidos regularmente.

Resta ainda comentarmos os artigos finais do Substitutivo. Não é demais lembrar que a Lei Complementar 95, de 26 de fevereiro de 1998, no seu art. 3º, diz que a lei conterá: "III - parte final, as disposições pertinentes às medidas necessárias à implementação das normas de conteúdo substantivo, às disposições transitórias e, se for o caso, a cláusula de vigência e a cláusula de revogação, quando couber."

Por esta determinação legal, o presente Substitutivo, ao definir as obrigações dos provedores de acesso, mostra que o Brasil o faz por sua vontade soberana mas em consonância com a *Directiva* citada dos países do Conselho Europeu, atualizando sua legislação. Assim que as nossas autoridades competentes considerarem adequado, poderemos, com maior efetividade, ser signatários da Convenção sobre o Cibercrime de Budapest ou de outras Convenções e Acordos sobre a matéria. Isto já se mostra necessário pela

dificuldade que nossos investigadores e persecutores penais têm tido em relação aos provedores de acesso localizados no exterior, conforme noticiado na imprensa local e internacional.

A propósito da repressão internacional, entendimento recente, de 16 de outubro de 2006, da 3ª Seção do Superior Tribunal de Justiça, 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.

E Em decisão recente, de 18 de setembro de 2006, o Ministro Barros Monteiro, do Supremo Tribunal de Justiça, por solicitação do Tribunal da Comarca de Düsseldorf, República Federal da Alemanha, decidiu que um provedor nacional de acesso à internet *"informe os dados da pessoa que, em 25 de fevereiro de 2004, às 3:20 hs (hora da Europa Central), a partir do IP n. 200.98.154.187, bloqueou o acesso aos sites atendidos pela empresa Online-forum"*.

No curso do processo o provedor apresentou impugnação invocando o princípio constitucional da inviolabilidade de dados, previsto no art. 5º, XII, da Constituição Federal, que, segundo alega, impede a quebra do sigilo de dados cadastrais, não se opondo a fornecer as informações solicitadas, desde que mediante expressa autorização judicial.

Considerando não haver caráter constritivo no pedido do Tribunal alemão, vez que visa somente obter os dados do usuário conectado ao IP n. 200.98.154.187, no dia e hora mencionados, a fim de instruir investigação instaurada perante a Justiça estrangeira, o Excelentíssimo Ministro mencionou o estudo de Tércio Sampaio Ferraz Júnior em seu trabalho "Sigilo de Dados: O Direito à Privacidade e os Limites à Função Fiscalizadora do Estado' (Revista da Faculdade de Direito USP, vol. 88, 1993, p. 449), ao explanar sobre o alcance da proteção à vida privada:

> "Pelo sentido inexoravelmente comunicacional da convivência, a vida privada compõe, porém, um conjunto de situações que, usualmente, são informadas sem constrangimento. São dados que, embora privativos — como o nome, endereço, profissão, idade, estado civil, filiação, número de registro público oficial etc, condicionam o próprio intercâmbio humano em sociedade, pois constituem elementos de identificação que tornam a comunicação possível, corrente e segura.

> Por isso, a proteção desses dados em si, pelo sigilo, não faz sentido. Assim, a inviolabilidade de dados referentes à vida privada só tem pertinência para aqueles associados aos elementos identificadores usados nas relações de convivência, as quais só dizem respeito aos que convivem.
>
> Dito de outro modo, os elementos de identificação só são protegidos quando compõem relações de convivência privativas: a proteção é para elas, não para eles.
>
> Em conseqüência, simples cadastros de elementos identificadores (nome, endereço, R.G., filiação, etc.) não são protegidos. Mas cadastros que envolvam relações de convivência privada (por exemplo, nas relações de clientela, desde quando é cliente, se a relação foi interrompida, as razões pelas quais isto ocorreu, quais os interesses peculiares do cliente, sua capacidade de satisfazer aqueles interesses, etc) estão sob proteção.
>
> Afinal, o risco à integridade moral do sujeito, objeto do direito à privacidade, não está no nome, mas na exploração do nome, não está nos elementos de identificação que condicionam as relações privadas, mas na apropriação dessas relações por terceiros a quem elas não dizem respeito".

Ao preparar-se para decidir pelo encaminhamento dos autos à Justiça Federal do Estado de São Paulo, para as providências cabíveis, o Ministro evocou a jurisprudência emanada do Supremo Tribunal Federal, em especial o trecho do voto proferido pelo Ministro Sepúlveda Pertence, que também dá amparo ao acolhimento da ordem pleiteada pelo Tribunal estrangeiro:

> "Não entendo que se cuide de garantia com status constitucional. Não se trata da 'intimidade ' protegida no inciso X do art. 5º da Constituição Federal. Da minha leitura, no inciso XII da Lei Fundamental, o que se protege, e de modo absoluto, até em relação ao Poder Judiciário, é a comunicação 'de dados' e não os 'dados', o que tornaria impossível qualquer investigação administrativa, fosse qual fosse." (voto proferido no MS n. 21.729-4/DF, DJ 19.10.2001).

Então, consoante as sugestões recebidas e respaldados pelas recomendações da Convenção sobre o Cibercrime de Budapest e da *Directiva* 2006/24/CE do Parlamento Europeu e do Conselho, que acabamos de descrever resumidamente, incluímos artigo que determina que todo provedor de acesso a uma rede de computadores é obrigado a:

- manter em ambiente controlado e de alta segurança os dados de identificação do usuário e os dados das conexões realizadas por seus equipamentos, aptos à identificação do usuário, endereços eletrônicos de origem das conexões, data, horário de início e término e referência GMT, da conexão, pelo prazo de três anos,

para prover os elementos essenciais para fazer prova da autenticidade da autoria das conexões na rede de computadores, em caso de ocorrência de crime;

tornar disponíveis à autoridade competente os dados já relacionados no curso de auditoria técnica a que forem submetidos;

- fornecer os dados e informações de conexões realizadas e os dados e informações de identificação do usuário quando solicitado pela autoridade competente no curso de investigação;
- informar, de maneira sigilosa, à autoridade competente à qual está jurisdicionado, fato do qual tenha tomado conhecimento e que contenha indícios de conduta delituosa na rede de computadores sob sua responsabilidade, pois não é demais lembrar que o art. 21 do Código Penal diz que ninguém pode se escusar com o desconhecimento da lei nem do ilícito;
- informar ao usuário, quando da requisição da sua identificação e autenticação, que aquela conexão obedece às leis brasileiras e que toda comunicação ali realizada será de exclusiva responsabilidade do usuário, perante as leis brasileiras, para prover os elementos essenciais para fazer prova da autenticidade da autoria das conexões na rede de computadores;
- alertar aos seus usuários, em campanhas periódicas, quanto ao uso criminoso de rede de computadores, dispositivos de comunicação e sistemas informatizados;
- divulgar aos seus usuários, em local destacado, as boas práticas de segurança no uso de rede de computadores, dispositivos de comunicação e sistemas informatizados.

O parágrafo único deste artigo (art. 22 do Substitutivo) remete para o regulamento o detalhamento relativo aos dados de conexão, às condições de segurança de seu armazenamento, a auditoria a que serão submetidos, a autoridade competente para realizá-la, o texto a ser apresentado aos usuários e estipula um prazo de noventa dias para a sua publicação.

Estas disposições atendem parte das recomendações do item "6 – Responsabilidades dos Provedores", da publicação "Cartilha de Segurança para

Internet", já citada, quando recomenda a publicação de alertas e informações de segurança na internet aos usuários, principalmente às crianças e adolescentes.

Para que a lei tenha maior efetividade acrescentamos também o art. 23 do Substitutivo, que determina que a autoridade competente, nos termos de regulamento, estruturará órgãos, setores e equipes de agentes especializados no combate à ação delituosa praticada em rede de computadores, dispositivo de comunicação ou sistema informatizado.

Propomos ainda a alteração na Lei nº 10.446, de 8 de maio de 2002, que 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, para possibilitar a atuação da Polícia Federal na investigação dos crimes aqui tratados.

Finalmente, acrescentamos o parágrafo único ao art. 9º da Lei 8.078 de 11 de setembro de 1990, o Código do Consumidor, que diz sobre a obrigação de informar sobre a nocividade do produto à saúde ou segurança do consumidor, dizendo que o *caput* se aplica à segurança digital do consumidor, mediante a informação da necessidade do uso de senhas ou similar para a proteção do uso, ou dos dados trafegados quando se tratar de dispositivo de comunicação, sistema informatizado ou provimento de acesso ou de serviço de sistema de informação pelo uso de rede de computadores.

Concluindo, registramos que matéria recente publicada na revista Exame, edição de 24 de agosto de 2006, apresenta estatística do Comitê Gestor da Internet no Brasil (CGI.Br) de que os crimes na internet passaram de 18 em 2002 para 27.292 em 2005 e que as investigações da Polícia Federal passaram de 214 para 1.500 em igual período.

III – VOTO

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

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, e a Lei nº 8.078, de 11 de setembro de 1990 (Código do Consumidor), 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, e a Lei nº 8.078, de 11 de setembro de 1990 (Código do Consumidor), 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 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 vírus eletrônico ou digital ou similar

Art. 163-A. Criar, inserir ou difundir vírus em dispositivo de comunicação, rede de computadores, ou sistema informatizado, com a

finalidade de destruí-lo, inutilizá-lo, deteriorá-lo, alterá-lo ou dificultar-lhe o funcionamento.

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

Parágrafo único. A pena é aumentada de sexta parte, se o agente se vale de nome suposto ou da utilização de identidade de terceiros para a prática do crime."

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

"Capítulo VII-A

DA VIOLAÇÃO DE REDE DE COMPUTADORES, DISPOSITIVO DE COMUNICAÇÃO OU SISTEMA INFORMATIZADO

Acesso indevido a rede de computadores, dispositivo de comunicação ou sistema informatizado

Art. 154-A. Acessar indevidamente, rede de computadores, dispositivo de comunicação ou sistema informatizado:

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

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

§ 2° 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.

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

§ 4° Nas mesmas penas incorre, o responsável pelo provedor de acesso à rede de computadores, dispositivo de comunicação ou sistema informatizado, que permite o acesso a usuário sem a devida identificação e autenticação ou que deixa de exigir, como condição de acesso, a necessária, identificação e regular cadastramento do usuário.

§ 5° No crime previsto no caput ou na hipótese do § 4° deste artigo, se o crime é culposo:

Pena – detenção de seis meses a um ano e multa.

Obtenção, manutenção, transporte ou fornecimento indevido de informação eletrônica ou digital ou similar

Art. 154-B. Obter indevidamente dado ou informação em rede de computadores, dispositivo de comunicação ou sistema informatizado:

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 indevidamente em rede de computadores, dispositivo de comunicação ou sistema informatizado.

§ 2º Se o dado ou informação obtida indevidamente é fornecida 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, identificação de usuário, autenticação de usuário, provedor de acesso e provedor de serviço, dados de conexões realizadas

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

I – dispositivo de comunicação: o computador, o computador de mão, o telefone celular, o processador de dados, os meios de armazenamento de dados eletrônicos ou digitais ou similares, os meios de captura de dados, 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 meios 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, este nível conhecido como internet, ou quanto ao proprietário, privado ou público;

IV – identificação de usuário: os dados de identificador de acesso, senha ou similar, nome completo, data de nascimento e endereço completo e outros dados que sejam requeridos no momento do cadastramento de um novo usuário de rede de computadores, dispositivo de comunicação ou sistema informatizado;

V – autenticação de usuário: procedimentos de verificação e conferência da identificação do usuário, quando este tem acesso a rede de computadores, dispositivo de comunicação ou sistema informatizado, realizado por quem torna disponível o acesso pelo usuário;

VI – provedor: o prestador de serviços de acesso à rede de computadores e o prestador de serviços relacionados a esse acesso;

VII – dados de conexões realizadas: aqueles dados aptos à identificação do usuário, os endereços eletrônicos de origem das conexões, a data, o horário de início e término e a referência GMT dos horários, relativos à cada conexão realizada pelos equipamentos de uma rede de computadores.

Violação ou divulgação indevida de informações depositadas em banco de dados

Art. 154-D. Violar, divulgar, ou tornar disponíveis, para finalidade distinta daquela que motivou a estruturação do banco de dados, 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 por decisão da autoridade competente, 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 suposto 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.

§ 3º 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 identificação de usuário, quando constatada qualquer conduta criminosa.

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.

....." (NR)

Art. 5º O Código Penal passa a vigorar acrescido do seguinte art. 183-A:

"**Art. 183-A.** Para os efeitos penais equiparam-se à coisa o dado ou informação em meio eletrônico ou digital ou similar, o bit ou a menor quantidade de informação que pode ser entendida como tal, a base de dados armazenada, dispositivo de comunicação, a rede de computadores, o sistema informatizado, a senha ou similar ou qualquer meio que proporcione acesso aos anteriormente citados."

Art. 6º 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, impedir ou dificultar-lhe o restabelecimento:

..... (NR)"

Art. 7º O Capitulo II do Título VIII do Código Penal passa a vigorar acrescido do seguinte artigo:

"**Difusão maliciosa de código**

Art. 266-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, ou a obtenção de qualquer vantagem ilícita:

Pena – reclusão de um a três anos.

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

§ 2º É isento de pena o agente técnico ou o profissional habilitado que, a título de resposta a ataque, de frustração de invasão ou burla, de proteção do sistema, de interceptação defensiva, de tentativa de identificação do agressor, de exercício de forense computacional e de práticas gerais de segurança da informação manipula código malicioso detectado, em proveito próprio ou de seu preponente e sem risco para terceiros."

Art. 8º 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. 9º 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. 10. O Código Penal passa a vigorar 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. 11. O Código Penal passa a vigorar acrescido do seguinte art. 356-A:

"**Art. 356-A**. Deixar de manter os dados de identificação de usuário e os dados de conexões realizadas por seus equipamentos, de valor probatório, aptos à identificação do usuário quando da ocorrência de crime, pelo prazo de três anos contados a partir da data de conexão, aquele que é o responsável pelo provedor de acesso à rede de computadores."

Art. 12. 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.

..... "

Art. 13. 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 vírus eletrônico ou digital ou similar

Art. 262-A. Criar, inserir ou difundir vírus em rede de computadores, dispositivo de comunicação ou sistema informatizado, com a finalidade de destruí-lo, inutilizá-lo, deteriorá-lo, alterá-lo ou dificultar-lhe o funcionamento.

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

Parágrafo único. A pena é aumentada de sexta parte, se o agente se vale de nome suposto ou da utilização de identidade de terceiros para a prática de acesso."

Art. 14. O Título VII da Parte Especial do Livro I do Código Penal Militar, Decreto-Lei, nº 1.001, de 21 de outubro de 1969, fica acrescido do Capítulo VII-A, assim redigido:

"Capítulo VII-A

DA VIOLAÇÃO DE REDE DE COMPUTADORES, DISPOSITIVO DE COMUNICAÇÃO OU SISTEMA INFORMATIZADO

Acesso indevido a rede de computadores, dispositivo de comunicação ou sistema informatizado

Art. 339-A. Acessar indevidamente rede de computadores, dispositivo de comunicação ou sistema informatizado:

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

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

§ 2° A pena é aumentada de sexta parte, se o agente se vale de anonimato, de nome suposto ou da utilização de identidade de terceiros para a prática do crime.

§ 3° Nas mesmas penas incorre, o responsável pelo provedor de acesso à rede de computadores, dispositivo de comunicação ou sistema informatizado, que permite o acesso a usuário sem a devida identificação e autenticação ou que deixa de exigir, como condição de acesso, a necessária, identificação e regular cadastramento do usuário.

§ 4° No crime previsto no caput ou na hipótese do § 3° deste artigo, se o crime é culposo:

Pena – detenção de seis meses a um ano e multa.

Obtenção, manutenção, transporte ou fornecimento indevido de informação eletrônica ou digital ou similar

Art. 339-B. Obter indevidamente dado ou informação em rede de computadores, dispositivo de comunicação ou sistema informatizado.

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

§ 1° Nas mesmas penas incorre quem mantém consigo, transporta ou fornece dado ou informação obtida indevidamente em rede de computadores, dispositivo de comunicação ou sistema informatizado.

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

Dispositivo de comunicação, sistema informatizado, rede de computadores, identificação de usuário, autenticação de usuário e provedor

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

I – dispositivo de comunicação: o computador, o computador de mão, o telefone celular, o processador de dados, os meios de armazenamento de dados eletrônicos ou digitais ou similares, os meios de captura de dados, 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 meios 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, este nível conhecido como internet, ou quanto ao proprietário, privado ou público;

IV – identificação de usuário: os dados de identificador de acesso, senha ou similar, nome completo, data de nascimento e endereço completo e outros dados que sejam requeridos no momento do cadastramento de um novo usuário de rede de computadores, dispositivo de comunicação ou sistema informatizado;

V – autenticação de usuário: procedimentos de verificação e conferência da identificação do usuário, quando este tem acesso a rede de computadores, dispositivo de comunicação ou sistema informatizado, realizado por quem torna disponível o acesso pelo usuário;

VI – provedor: o prestador de serviços de acesso à rede de computadores e o prestador de serviços relacionados a esse acesso;

VII – dados de conexões realizadas: aqueles dados aptos à identificação do usuário, os endereços eletrônicos de origem das conexões, a data, o horário de início e término e a referência GMT dos horários, relativos à cada conexão realizada pelos equipamentos de uma rede de computadores.

Violação, divulgação de informações depositadas em banco de dados

Art. 339-D. Violar, divulgar, ou tornar disponíveis, para finalidade distinta daquela que motivou a estruturação do banco de dados, 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 por decisão da autoridade competente, 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 suposto 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.

§ 3º 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 identificação de usuário, quando constatada qualquer prática criminosa."

Art. 15. 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 os efeitos penais equiparam-se à coisa o dado ou informação em meio eletrônico ou digital ou similar, o bit ou a menor quantidade de informação que pode ser entendida como tal, a base de dados armazenada, a rede de computadores, o dispositivo de comunicação e o sistema informatizado, a senha ou similar ou qualquer meio que proporcione acesso aos mesmos."

Art. 16. 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 maliciosa de código

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, a rede de computadores, dispositivo de comunicação ou a sistema informatizado, ou a obtenção de qualquer vantagem ilícita:

Pena – reclusão de um a três anos.

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

§ 2º É isento de pena o agente técnico ou o profissional habilitado que, em proveito próprio ou de seu preponente e sem risco para terceiros, de forma tecnicamente documentada e com preservação da cadeia de custódia no curso dos procedimentos correlatos, atua a título de resposta a ataque, de frustração de invasão ou burla, de proteção do sistema, de interceptação defensiva, de tentativa de identificação do agressor, de exercício de forense computacional e de práticas gerais de segurança da informação e manipula, sem desvio de finalidade ou excesso, código malicioso detectado."

Art. 17. O Capítulo VII do Título VII da Parte Especial do Livro I do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), fica acrescido do art. 352-A, assim redigido:

"**Art. 352-A.** Deixar de manter os dados de identificação de usuário e os dados de conexões realizadas por seus equipamentos, de valor probatório , aptos à identificação do usuário quando da ocorrência de crime, pelo prazo de três anos contados a partir da data de conexão, aquele que é o responsável pelo provedor de acesso à rede de computadores."

Art. 18. 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. 19. 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 IV:

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

.....

IV – 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.(NR)"

Art. 20. Todo aquele que acessar uma rede de computadores, local, regional, nacional ou mundial, deverá identificar-se e cadastrar-se naquele provedor que torna disponível este acesso.

Parágrafo único. Os atuais usuários terão prazo de cento e vinte dias, após a entrada em vigor desta Lei, para providenciarem ou revisarem sua identificação e cadastro junto ao provedor que torna disponível o acesso.

Art. 21. Todo provedor de acesso a uma rede de computadores sob sua responsabilidade somente admitirá como usuário pessoa natural, dispositivo de comunicação ou sistema informatizado que for autenticado por meio hábil e legal à verificação positiva da identificação de usuário, ficando facultado o uso de tecnologia que garanta a autenticidade e integridade dos dados e informações digitais ou o uso de outras entidades de dados de identificação de usuário já existentes que tenham sido constitutidas de maneira presencial, de forma a prover a autenticidade das conexões, a integridade dos dados e informações e a segurança das comunicações e transações na rede de computadores, dispositivo de comunicação e sistema informatizado.

Parágrafo único. A identificação do usuário de rede de computadores poderá ser definida nos termos de regulamento, sendo obrigatórios para a pessoa natural os dados de identificador de acesso, senha ou similar, nome completo, data de nascimento, um número de documento hábil e legal de identidade e endereço completo, sendo obrigatória para o provedor de acesso a uma rede de computadores, para o dispositivo de comunicação e para o sistema informatizado a indicação de uma pessoa natural responsável.

Art. 22. Todo provedor de acesso a uma rede de computadores é obrigado a:

I – manter em ambiente controlado e de alta segurança os dados de conexões realizadas por seus equipamentos, aptos à identificação do usuário e endereços eletrônicos de origem das conexões, data, horário de início e término e referência GMT, da conexão, pelo prazo de três anos, para prover os elementos essenciais para fazer prova da autenticidade da autoria das conexões na rede de computadores;

II – tornar disponíveis à autoridade competente os dados e informações elencados no inciso I no curso de auditoria técnica a que forem submetidos;

III – fornecer, quando solicitado pela autoridade competente no curso de investigação, os dados de conexões realizadas e os dados de identificação de usuário;

IV – informar, de maneira sigilosa, à autoridade competente à qual está jurisdicionado, fato do qual tenha tomado conhecimento e que contenha indícios de conduta delituosa na rede de computadores sob sua responsabilidade;

V – informar ao usuário, quando da requisição da sua identificação e autenticação, que aquela conexão obedece às leis brasileiras e que toda comunicação ali realizada será de exclusiva responsabilidade do usuário, perante as leis brasileiras, para prover os elementos essenciais para fazer prova da autenticidade da autoria das conexões na rede de computadores;

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

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

Parágrafo único. Os dados de conexões realizadas em rede de computadores, as condições de alta segurança de sua guarda, a auditoria à qual serão submetidas, a autoridade competente responsável pela auditoria e o texto a ser informado aos usuários de rede de computadores, serão definidos nos termos de regulamento em prazo não superior a noventa dias a partir da data de

publicação desta lei, sendo obrigatórios aqueles dados de conexão realizadas definidos neste artigo.

Art. 23. A autoridade competente, nos termos de regulamento, estruturará órgãos, setores e equipes de agentes especializados no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.

Art. 24. O art. 1° da Lei n° 10.446, de 8 de maio de 2002 passa a vigorar com a seguinte redação:

"**Art. 1°** .....

.....

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

Art. 25. O art. 9° da Lei n° 8.078, de 11 de setembro de 1990 passa a vigorar com a seguinte redação:

"Art. 9° .....

.....

Parágrafo único. – o mesmo 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 serviçomediante o uso dela.(NR)"

Art. 26. Esta Lei entra em vigor sessenta dias após a data de sua publicação.

Sala da Comissão,

, Presidente

, Relator

RELATÓRIO

RELATOR: Senador **EDUARDO AZEREDO**

I – RELATÓRIO

Vem a esta Comissão, para parecer, o Projeto de Lei da Câmara (PLC) nº 89, de 2003 (nº 84, de 1999, na origem), e os Projetos de Lei do Senado (PLS) nº 137, de 2000, e nº 76, de 2000, todos referentes a crimes na área de informática. Tramitam em conjunto em atendimento ao Requerimento nº 847, de 2005, do Senador Renan Calheiros. Em decorrência do Requerimento nº 848, de 2005, foi extinta a urgência na tramitação do PLC nº 89, de 2003, que havia sido declarada em decorrência da aprovação do Requerimento nº 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 nº 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 nº 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 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 Decreto-Lei n° 2.848, de 7 de dezembro de 1940 (Código Penal), 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, onde foram amplamente debatidas. Lá, apresentamos relatório e voto pela aprovação do PLS n° 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 pretende:

a) inserir no Código Penal (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, identificação de usuário e autenticação de usuário*; 154-D, para definir o crime de *divulgação de informações depositadas em bancos de dados*; 154-E, 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 à 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.

No âmbito processual, o Substitutivo pretende 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.

Não foram apresentadas emendas.

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 (cert.br), as tentativas de fraudes pela internet no Brasil cresceram 53% em 2006. Em 2005, foram registradas 27,3 mil tentativas de fraudes pela rede. Em 2006, foram 41,8 mil. Os números, frise-se bem, podem ser muito maiores que esses, dado que o cert.br considera apenas os dados reportados espontaneamente pelos usuários e administradores de redes.

Ao todo, o cert.br recebeu, no ano passado, 197 mil incidentes relacionados à internet, alta de 191% em relação a 2005. Os principais alvos são os usuários interessados em usar bancos ou fazer compras pela rede mundial de computadores. A estimativa é de que os bancos perdem mais de R$ 300 milhões por ano em fraudes virtuais.

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. O Brasil, logo atrás, tem 21,18%, e o Canadá, em terceiro lugar, 9,45%.

Em matéria da INFO Exame, de outubro de 2006, os incidentes relatados ao cert.br indicam uma escalada anual surpreendente de incidentes, quase dobrando ano a ano: de 3.107 em 1999, passa-se para 5.997, 12.301, 25.092, 54.607, 75.722, sucessivamente, até mais que dobrar e chegar aos 197 mil de 2006.

Matéria publicada na revista Exame, edição de 24 de agosto de 2006, apresenta estatística do Comitê Gestor da Internet no Brasil (CGI.br), que informa que os crimes na internet passaram de 18, em 2002, para 27.292, em 2005, e que as investigações da Polícia Federal sobre crimes na internet, no período de 2002 a 2005, passaram de 214 para 1.500.

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 britânica, segundo o Ministério do Interior, foi de US$ 3,2 bilhões nos últimos três anos.

Segundo relatório da McAfee, empresa de segurança em tecnologia, o número de programas mal-intencionados que monitoram a atividade de digitação para capturar senhas e outras informações confidenciais aumentou 250% entre janeiro de 2004 e maio de 2006 nos EUA.

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, que resultou no Parecer pelo oferecimento do Substitutivo ora examinado.

Não obstante, reconhecemos que existem alguns aperfeiçoamentos a realizar quanto à redação, concisão e clareza, e de mérito, que só recentemente chegaram ao nosso conhecimento, conforme sugestões informais apresentadas por associações, por órgãos públicos e por especialistas em tecnologia da informação e em direito aplicado a ela.

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, para ouvirmos as sugestões e explicarmos o trabalho que o Parlamento vem desenvolvendo há dez anos.

Estes aperfeiçoamentos foram devidamente analisados pelo mesmo grupo de voluntários, aos quais registramos nossos agradecimentos, que colaboraram informalmente na construção do Substitutivo apresentado na Comissão de Educação desta casa legislativa. Lá, inicialmente, foram contatados quase cem profissionais de várias especialidades correlatas com a matéria ora em discussão, alem de oficiais superiores das três forças armadas, que cuidaram da alteração do Código Penal Militar, e ao final resumiu-se a um grupo de especialistas voluntários que, com o uso intensivo da internet, logrou concluir pelo texto do substitutivo afinal aprovado.

Analisadas as sugestões, na sua maioria de redação para clareza e concisão, concluímos que a matéria, complexa, abrangente, tratando de crimes contra a pessoa, contra o patrimônio e contra serviços públicos, requer um novo substitutivo, que pode ser comparado com aquele da Comissão de Educação, por quem tiver interesse no tema. Assim, passamos a descrever as alterações, supressões e inclusões.

Começamos por alterar a ementa da Lei para nela incluir a indicação da alteração da Lei nº 9.296, de 24 de julho de 1996 (que cuida das interceptações de comunicações telefônicas, regulamentando o inciso XII, parte final, do art. 5° da Constituição Federal), 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 (que dispõe sobre infrações penais de repercussão interestadual ou internacional que exigem repressão uniforme), e a indicação da alteração da Lei nº 8.078, de 11 de setembro de 1990 (Código do Consumidor).

Incluímos um novo art. 1°, renumerando-se os demais, para cumprir o que determina o art. 7º, da Lei Complementar nº 95, de 26 de fevereiro de 1998, segundo o qual o primeiro artigo do texto "indicará o objeto da lei e o respectivo âmbito de aplicação".

Recebemos ponderações de que nem tudo é digital embora seja eletrônico, como, por exemplo, alguns dispositivos de comunicação, com componentes eletrônicos mas analógicos.

Assim, substituímos toda referência 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, deixando o texto mais consoante à realidade da tecnologia, pretendendo com isso maior longevidade e adaptabilidade para o texto da norma em apreço.

No novo art. 154-A do Código Penal, e no seu correspondente novo art. 339-A do Código Penal Militar, incluímos a expressão "ou sistema informatizado" no título do artigo, dando-lhe coerência com o seu texto. Ainda, substituímos a expressão "indevido" pela expressão "não autorizado" e a expressão "indevidamente" pela expressão "sem autorização do legítimo titular, quando exigida:", colocada ao final do texto, para definir melhor o tipo. Outrossim, retiramos a expressão "indevidamente" do texto do § 1º do artigo.

Nestes artigos incluímos ainda dispositivos para ressalvar os profissionais autorizados que fazem a "defesa digital", a prevenção, a análise e a resposta aos acessos indevidos.

Para maior precisão e clareza, no novo art. 154-B do Código Penal, e no seu correspondente novo art. 339-B do Código Penal Militar, trocamos de posição na oração a expressão "dado ou informação obtida", e incluímos a ação de "obter" o dado ou a informação. Trocamos a expressão "indevidamente" pela expressão "sem autorização do legítimo titular, quando exigida", definindo melhor o tipo.

Para maior clareza, incluímos também a manutenção consigo do dado ou informação obtido com autorização por prazo definido e que tenha expirado, prática comum daquele que se infiltra, obtém as informações que virá a usar uma vez fora do ambiente atacado.

Acrescentamos a majorante de um terço da pena se o dado ou informação obtida indevidamente ou sem autorização é fornecido pela rede de computadores ou em qualquer outro meio de divulgação em massa.

Nas definições constantes do novo art. 154-C do Código Penal, e do seu correspondente novo art. 339-C do Código Penal Militar, fizemos as seguintes alterações:

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

– na definição de "Sistema Informatizado" substituímos a expressão "eletronicamente" pela expressão "eletrônica ou digitalmente ou equivalente", incluímos a expressão "capturar" e suprimimos a expressão "rede de computadores ou internet", que passou a ser objeto de definição específica;

– retiramos a definição de "Identificação de Usuário", bem como a definição de "Autenticação de Usuário", que deixam de ser necessárias no texto da norma, já que os artigos que as citavam foram convolados em normas administrativas;

– incluímos a definição de "Rede de Computadores", para nela incluir a definição de internet, a rede mundial de computadores, reclamada por alguns dos colaboradores na elaboração do Substitutivo, e definindo todas as demais redes de computadores, locais, regionais, nacionais, privadas ou públicas. Na definição, uma rede de computadores é entendida como um conjunto de computadores e dispositivos de comunicação, governados entre si, de comum acordo, por um conjunto de regras, códigos e formatos agrupados em protocolos. Assim, ela é destacada de "sistema informatizado", conceito mais abrangente, que inclui qualquer sistema, alguns deles não dispondo de meios para identificar e autenticar usuários e muito menos para armazenar os dados de conexão, conforme requeridos pelos processos de investigação penal;

– incluímos a definição de "Defesa Digital", para que se possa isentar de pena, em alguns dos novos crimes, a manipulação de código malicioso por agente técnico ou profissional habilitado, em proveito próprio ou de seu preponente, e sem risco para terceiros, de forma tecnicamente documentada e com preservação da cadeia de custódia no curso dos procedimentos correlatos, a título de teste de vulnerabilidade, de resposta a ataque, de frustração de invasão ou burla, de proteção do sistema, de interceptação defensiva, de tentativa de identificação do agressor, de exercício de forense computacional e de práticas gerais de segurança da informação;

– incluímos a definição de "código malicioso", qual seja 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 em obtenção não autorizada de informações contra terceiro, de maneira dissimulada ou oculta, transparecendo tratar-se de ação de curso normal;

– incluímos as definições de "dados informáticos" e "dados de tráfego", para prover maior harmonia com a Convenção do Cibercrime, facilitando assim a participação do Brasil, se esse for o seu interesse.

No novo art. 154-D, *caput*, do Código Penal, e no seu correspondente novo art. 339-D, *caput*, do Código Penal Militar incluímos também as condutas de "utilizar" e de "comercializar" sem autorização ou para fim diferente da sua constituição, o conteúdo de um banco de dados. Para a decisão de autorizar a divulgação de informações contidas em banco de dados, incluímos a expressão "nos casos previstos em lei," dando maior clareza à norma.

Renumeramos o parágrafo único destes artigos como § 1°, e acrescentamos o § 2° 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.

Em relação à "preservação dos dados de conexões realizadas", do novo art. 154-E do Código Penal e do seu correspondente novo art. 339-E, do Código Penal Militar, os artigos foram excluídos e as penas foram transformadas em multas administrativas, constantes do final do Substitutivo, com ênfase na finalidade da guarda dos dados, deixando claro que se tutela a justiça, afirmando-os como dados de valor probatório, aptos à identificação do usuário e da conexão quando da ocorrência de crime.

Na nova redação dos dispositivos a eles correspondentes retiramos a expressão "e comunicações", considerada demasiado abrangente, pois o que se pretende são os dados de conexões realizadas e não aqueles da continuidade da conexão, o que onera sem necessidade os operadores do sistema.

Reduzimos a lista de informações a serem guardadas, significando menor volume de arquivamento para os operadores, o que também acontece com a redução do prazo de guarda de "cinco" para "três" anos, que é a recomendação do Comitê Gestor da Internet do Brasil (CGI.br), prazo considerado suficiente para os trabalhos de investigação quando necessários.

Por sugestão recebida para melhor tipificação, incluímos artigo ao Substitutivo, renumerando-se os demais, para com ele acrescentarmos 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. Ambos tratam do crime de "furto qualificado", que tem a pena definida como de reclusão de dois a oito anos, e multa, se o crime é cometido, por exemplo, com emprego de chave falsa. Adicionamos o inciso com as orações alternativas: "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".

No novo art. 163-A do Código Penal, e no seu correspondente novo art. 262-A do Código Penal Militar, aperfeiçoamos a redação, substituindo no título a expressão "vírus" por "código malicioso", considerada mais adequada, pois passa a abranger qualquer código malicioso criado, inserido ou difundido, que se reproduz automaticamente ou não, ou que toma controle do equipamento sem autorização do seu usuário, causando-lhe dano na destruição, ou no impedimento de uso ou no mau funcionamento do equipamento. Assim, incluímos 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 – situação essa que, no jargão técnico, é a de transformar o equipamento em um "zumbi".

A definição do novo tipo começa pela forma mais simples de dano ao criar, inserir e difundir código malicioso, para nos dois parágrafos seguintes ser qualificado pela intenção de causar dano, e novamente qualificado pela apuração do resultado do dano, com o correspondente progressivo agravamento da pena.

Nestes artigos renumeramos o parágrafo único como § 1º e incluímos ainda dispositivos para ressalvar os profissionais autorizados que fazem a "defesa digital", a prevenção, a análise e a resposta aos acessos indevidos.

Alteramos a localização do novo tipo de "difusão de código malicioso" por fraude, anteriormente o novo 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). A motivação para a mudança foi que o Capítulo anterior (do Título VIII – Dos Crimes contra a Incolumidade Pública – Capítulo II – Dos Crimes contra a Segurança dos Meios de Comunicação e Transporte e outros Serviços Públicos) trata de crimes contra "serviços públicos" e desta forma o novo tipo alcançaria apenas rede de computadores, dispositivo de comunicação e sistema informatizado de acesso público, como computadores de acesso público, terminais de bancos etc, deixando de alcançar todos os demais citados de acesso privado. Ademais o tipo de fraude se realiza com o objetivo direto ou indireto de obter ganho econômico, daí a tipificação como estelionato.

Alteramos a pena do novo tipo de "difusão de código malicioso", do novo art. 171-A do Código Penal e no seu correspondente novo art. 339-A do Código Penal Militar, passando de detenção de um a dois anos para reclusão de um a três anos, pois a pretensão dos autores da difusão de código malicioso é a fraude, que pode levar ao "furto qualificado por acesso indevido" (arts. 4º e 11 do PLS), igualando-a à pena que se aplica ao crime tipificado no novo art. 163-A. Nestes artigos, renumeramos o parágrafo único como § 1º e acrescentamos o § 2º, para ressalvar a ação dos profissionais que fazem a "defesa digital", a prevenção, análise e resposta aos ataques tipificados.

Acrescentamos à alteração do art. 266 do Código Penal as expressões "informático, dispositivo de comunicação, rede de computadores, sistema informatizado", seja para adequação aos termos já dispostos na Lei 9.296, de 1996, e aos termos do art. 154-C do Substitutivo, seja para nele incluir como tipo penal "o ataque a rede de computadores ou sistema informatizado", como, por exemplo, o *DoS (Denial-of-Service attack)*, o *DDoS (Distributed-Denial-of-Service attack)* e outros equivalentes.

Alteramos o parágrafo único do art. 298 do Código Penal, o qual se pretende acrescentar, para substituir a expressão "armazenamento ou processamento" pela expressão "captura, armazenamento, processamento ou transmissão" que é uma tipificação clara nos dispositivos de comunicação ou sistemas informatizados, para maior abrangência do texto.

Para maior efetividade da aplicação da Lei, incluímos artigo do Substitutivo para a decretação de prisão preventiva nos crimes dolosos 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, mediante o acréscimo do inciso IV ao art. 313 do Decreto-Lei nº 3.689, de 3 de outubro de 1941, Código de Processo Penal (CPP).

Para que a lei tenha maior efetividade, acrescentamos também artigo que determina que a autoridade competente, nos termos de regulamento, estruturará órgãos, setores e equipes de agentes especializados no combate à ação delituosa praticada em rede de computadores, dispositivo de comunicação ou sistema informatizado.

Propomos ainda a inclusão de artigo alterando a Lei nº 10.446, de 8 de maio de 2002, que 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), para possibilitar a atuação da Polícia Federal na investigação dos crimes aqui tratados.

Não menos importante é o artigo do Substitutivo, que acrescenta parágrafo único ao art. 9º da Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor – CDC), e trata da obrigação de se informar sobre a nocividade do produto à saúde ou segurança do consumidor. Assim, o *caput* do art. 9º do CDC passa a se aplicar à segurança digital do consumidor, mediante a informação da necessidade do uso de senhas ou similar para a proteção do uso, ou dos dados trafegados quando se tratar de dispositivo de comunicação, sistema informatizado ou provimento de acesso ou de serviço de sistema de informação pelo uso de rede de computadores.

De fundamental importância é o art. 21 do Substitutivo. Não é demais lembrar que a Lei Complementar nº 95, de 26 de fevereiro de 1998, no seu art. 3º, III, diz que a lei deverá conterá, em sua parte final, "as disposições pertinentes às medidas necessárias à implementação das normas de conteúdo substantivo". Destas medidas tratam os arts. 21 e 22.

Com o art. 21 do Substitutivo, passamos a tratar das obrigações do responsável pelo provimento de acesso a uma rede de computadores. Mantivemos a obrigação da preservação, por eles, das informações relativas às conexões realizadas, pelo prazo de três anos, em redação mais simples e concisa.

Em nível latino-americano registre-se que Lei Argentina de 2003 fixa o prazo de dez anos para a guarda destas informações. E ainda que recentemente chegou ao Congresso Americano projeto de lei propondo a retenção por prazo indeterminado destas informações.

Recentemente a imprensa da Coréia do Sul registrou que foi aprovada pela Assembléia Nacional daquele país, no último dia 22 de dezembro, a revisão do chamado "Ato de Incentivo à Utilização das Redes de Informação e Comunicação e de Proteção à Informação", determinando que os usuários da Internet preencham cadastro ao visitarem sites com mais de 100 mil acessos diários, no chamado "Sistema de Nome Real" (Internet Real-Name System, em livre tradução).

A ofensiva do governo em rediscutir o tema foi respaldada por uma série de pesquisas realizadas junto a internautas, nos principais websites do país. De acordo com o Korea Times, dos 7.909 pesquisados junto aos usuários do Naver, maior portal de Internet coreano, 65% apoiariam o registro de seus dados verdadeiros na Web. Já 80% dos visitantes do Yahoo, num universo de 1.631 entrevistados, seriam a favor do Sistema de Nome Real. Por sua vez, o Instituto Gallup detectou uma aceitação de 75,6% dos pesquisados on-line.

A nova legislação coreana prevê a obrigatoriedade do registro, com dados verdadeiros, inclusive documentação de identidade, dos usuários de Internet em sites com mais de 100 mil acessos diários, quando encaminharem mensagens on-line ou comentários de informações divulgadas em portais, páginas de notícias e de imprensa, bem como de entidades governamentais.

O principal pressuposto dessa regra seria permitir que os provedores de conteúdo identificassem, quando necessário, os remetentes de determinados comentários. Dessa forma, os administradores dos sites poderiam bloquear, por até 30 dias, mensagens consideradas potencialmente controversas ou difamatórias. Esses provedores estariam sujeitos a multas de até 30 milhões de wons (cerca de 30 mil dólares), caso não disponibilizassem o sistema de registro.

Cumpre lembrar aqui a confusão (ou desinformação) que se estabelece acerca da relação entre liberdade de expressão e anonimato, ambos possíveis na internet (o anonimato representado pela não-identificação e a não-autenticação do usuário).

Ora, se o fato de emitir para alguém uma carteira de habilitação para dirigir veículos automotores não limita o seu direito constitucional de ir e vir, da mesma forma a identificação do usuário de uma rede de computadores não o impede de manifestar-se pela rede.

Importante frisar que a própria Constituição Federal determina, no art. 5°, inciso IV, que "é livre a manifestação do pensamento, sendo vedado o anonimato".

O art. 21 do Substitutivo apenas reafirma esta norma constitucional, e consagra prática mundial de usos e costumes de todos quantos tem na rede de computadores o seu instrumento de prestação de serviços, diferenciando pela quantidade ou pelo tipo de informação requerida quando do acesso, pois quem presta serviço quer saber de quem cobrará economicamente pelos serviços prestados.

Esse aspecto fez parte de comentário recente do pesquisador Vint Cerf, criador dos principais protocolos da internet, na resposta à primeira pergunta em entrevista à imprensa nacional:

> *Nos Estados Unidos é comum que o internauta forneça algum número de identificação para ter acesso em lugares públicos como hotspots, como número de cartão de crédito ou endereço. Em muitos casos, além do cartão você deve fornecer seu endereço para provar que é realmente a pessoa que diz ser. De certa forma, os provedores de acesso à internet já possuem informações confidenciais dos internautas. Se você assina um serviço de banda larga é muito pouco provável que o provedor forneça este serviço sem saber quem você é, ou ter pelo menos o número do seu cartão de crédito, seu endereço e sua conta bancária. Diria que, em muitas instâncias do acesso à internet, os provedores já possuem um montante de informações pessoais sobre os usuários.*

Na segunda resposta da mesma matéria, ele comenta os dados que os provedores deveriam fornecer por requisição judicial, e termina mencionando que os usuários pensam que são anônimos, mas não o são, pois os provedores tem vários dados sobre cada um:

> *O interessante desta questão é avaliar em quais condições os provedores deveriam fornecer informações para o suporte à lei. Não estou familiarizado com a lei brasileira, mas nos Estados Unidos você tem ordens judiciais para obter certos tipos de informação. De certa forma, podemos entender que não deixa de ser um pedido razoável. Existe o mesmo processo com o telefone. Provavelmente, em muitos casos judiciais, ligações e mensagens telefônicas são solicitadas como provas em tribunais. Minha primeira impressão é que isso não parece terrivelmente diferente das práticas aplicadas por aí. Temos de imaginar que se isso for aprovado de alguma forma pode parecer mais ameaçador para os internautas que acreditavam ser mais anônimos do que são. E eles não são. Acho certo dizer que, para a maioria dos provedores que cobram pelos serviços, existem de fato várias formas de rastrear e descobrir quem você é. Até em universidades você precisa fazer um registro antes de acessar a rede.*

É do que trata, por exemplo, recente decisão do Superior Tribunal de Justiça (STJ). O Tribunal da Comarca de Düsseldorf, República Federal da Alemanha, solicitou ao Brasil, mediante carta rogatória, que a empresa Universo *On Line* informasse os dados de pessoa que, em fevereiro de 2004, bloqueou o acesso aos sites atendidos pela empresa "Online-forum". O intimado apresentou impugnação invocando o princípio constitucional da inviolabilidade de dados, previsto no art. 5°, XII, da CF, que, segundo alegou, impediria a quebra do sigilo de dados cadastrais. O ministro Barros Monteiro proferiu importante decisão nos seguintes termos (Carta Rogatória n° 297 –2005/0010755-8, em 18/09/2006):

> ***Esta Corte já proferiu decisão no sentido de que o fornecimento de dados cadastrais, como o endereço p. ex., não está protegido pelo sigilo**, conforme se verifica na ementa a seguir reproduzida:*
>
> *"Imposto de renda. Informações. Requisição. Os elementos constantes das declarações de bens revestem-se de caráter sigiloso que não deve ser afastado se não em situações especiais em que se patenteie relevante interesse da administração da Justiça. Tal não se configura quando se trate apenas de localizar bens para serem penhorados, o que é rotineiro na prática forense. Injustificável, entretanto, negar-se o pedido na parte em que pretende obter dados pertinentes ao endereço do executado. Em relação a isso não há motivo para sigilo" (RESP 83824/BA, relator Ministro Eduardo Ribeiro, DJ 17.5.99) (grifou-se).*

A respeito do assunto, cabe mencionar o estudo de Tércio Sampaio Ferraz Júnior em seu trabalho "Sigilo de Dados: O Direito à Privacidade e os Limites à Função Fiscalizadora do Estado' (Revista da Faculdade de Direito USP, vol. 88, 1993, p. 449), ao explanar sobre o alcance da proteção à vida privada:

*"**Pelo sentido inexoravelmente comunicacional da convivência, a vida privada compõe, porém, um conjunto de situações que, usualmente, são informadas sem constrangimento. São dados que, embora privativos — como o nome, endereço, profissão, idade, estado civil, filiação, número de registro público oficial etc, condicionam o próprio intercâmbio humano em sociedade, pois constituem elementos de identificação que tornam a comunicação possível, corrente e segura. Por isso, a proteção desses dados em si, pelo sigilo, não faz sentido.** Assim, a inviolabilidade de dados referentes à vida privada só tem pertinência para aqueles associados aos elementos identificadores usados nas relações de convivência, as quais só dizem respeito aos que convivem. Dito de outro modo, os elementos de identificação só são protegidos quando compõem relações de convivência privativas: a proteção é para elas, não para eles. Em conseqüência, simples cadastros de elementos identificadores (nome, endereço, R.G., filiação, etc.) não são protegidos. Mas cadastros que envolvam relações de convivência privada (por exemplo, nas relações de clientela, desde quando é cliente, se a relação foi interrompida, as razões pelas quais isto ocorreu, quais os interesses peculiares do cliente, sua capacidade de satisfazer aqueles interesses, etc) estão sob proteção. Afinal, o risco à integridade moral do sujeito, objeto do direito à privacidade, não está no nome, mas na exploração do nome, não está nos elementos de identificação que condicionam as relações privadas, mas na apropriação dessas relações por terceiros a quem elas não dizem respeito".*

***Não é demais evocar a jurisprudência emanada da Corte Suprema brasileira, em especial o trecho do voto proferido pelo Ministro Sepúlveda Pertence**, que também dá amparo ao acolhimento da ordem pleiteada na peça exordial:*

*"Não entendo que se cuide de garantia com status constitucional. Não se trata da 'intimidade ' protegida no inciso X do art. 5° da Constituição Federal. **Da minha leitura, no inciso XII da Lei Fundamental, o que se protege, e de modo absoluto, até em relação ao Poder Judiciário, é a comunicação 'de dados' e não os 'dados', o que tornaria impossível qualquer investigação administrativa, fosse qual fosse.**"(voto proferido no MS n. 21.729-4/DF, DJ 19.10.2001)* [grifos nossos].

Esperamos, assim, que o artigo 21 do Substitutivo estimule a celebração de convênios, entre aqueles que tornam possível o acesso à rede de computadores e as organizações detentoras de informações para permitir a verificação dos dados imutáveis como nome, número de documento legalmente emitido, conforme a boa prática existente entre organizações de proteção ao crédito, as instituições financeiras, órgãos públicos e outras.

Sobre esses dados a serem compartilhados, a Constituição Federal determina no seu art. 5º, inciso XXXIII, que:

> **Art. 5º** .....
> .....
> XXXIII – todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado.

O inciso foi regulamentado pela Lei nº 11.111, de 5 de maio de 2005, *não proibindo o compartilhamento de dados imutáveis como os já citados*, naturalmente desde que autorizados pelo seu titular ou por lei específica, pois dispõe que:

> "**Art. 2º** O acesso aos documentos públicos de interesse particular ou de interesse coletivo ou geral será ressalvado exclusivamente nas hipóteses em que o sigilo seja ou permaneça imprescindível à segurança *da sociedade e do Estado, nos termos do disposto na parte final do inciso* XXXIII do *caput* do art. 5º da Constituição Federal."

Ainda a propósito, cabe lembrar aqui as recomendações constantes da Cartilha de Segurança para Internet, na sua seção 6 (Responsabilidades dos Provedores), documento editado em notável esforço de colaboração entre o Ministério Público Federal de São Paulo (MPF/SP) e o Comitê Gestor da Internet no Brasil (CGI.br), patrocinada pela Associação Brasileira dos Provedores de Internet (ABRANET), aos quais registramos aqui o nosso elogio ao resultado alcançado.

A brochura contém instruções de como proceder em caso de investigação de delito ocorrido, os modelos de documentos a serem usados para comunicar o fato delituoso às autoridades competentes, o texto completo da Convenção sobre o Cibercrime, celebrado em Budapest, a 23 de novembro de 2001, pelo Conselho da Europa. Essa Convenção foi recentemente ratificada pelo Senado dos EUA.

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*, objeto do art. 16 do Substitutivo;

– *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;

– *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 § 1° 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 do art. 21 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 e crimes de pedofilia, 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 e o Código do Consumidor, 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.

Em outro documento, a "Directiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrônicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Directiva 2002/58/CE", entre outras considerações preambulares, trata naquela de número 18 que "*A decisão-Quadro 2005/222/Al do Conselho, de 24 de fevereiro de 2005, relativa a ataques contra os sistemas de informação, dispõe que o acesso ilegal aos sistemas de informação, incluindo os dados neles conservados seja punível como infracção penal.*" Na consideração de número 20 cita a Convenção sobre o Cibercrime de Budapest de 2001 e a Convenção de 1981, esta sobre os dados pessoais.

Avançando, a "Directiva" define no art. 2º como dados: os "*dados de tráfego e os dados de localização bem como os dados conexos necessários para identificar o assinante e o utilizador*". No art. 5º detalha as "*Categorias de dados a conservar*", onde encontramos, no item 2 da letra *a*, que diz respeito à internet, a especificação da guarda do identificador de acesso, do nome e do endereço do assinante ou usuário, aos quais o endereço do protocolo IP, o identificador de acesso ou o número do telefone, estavam atribuídos no momento da comunicação.

Faz-se mister demonstrar a harmonia do Substitutivo com a "Directiva", que nos arts. 6º, 7º, 8º e 9º define, respectivamente, os "*Períodos de Conservação*", a "*Proteção de dados e segurança dos dados*", os "*Requisitos para o armazenamento dos dados conservados*", a "*Autoridade de controle*", previstos no art. 21 do Substitutivo, incisos I e II, e § 1º.

Desses artigos vem a recomendação de que os dados sejam conservados por um período mínimo de seis meses e não superior a dois anos. Ao final da "Directiva", vários signatários declaram que estudarão a aplicação de prazos diferenciados ou de dezoito ou de trinta e seis meses, a partir de 2007 ou 2009. No Brasil, o Comitê Gestor da Internet no Brasil (CGI.br) definiu esse prazo em trinta e seis meses. A "Directiva" recomenda ainda que a guarda deva ser criteriosa e que seja designada uma autoridade competente para a realização da auditoria a que estes dados forem submetidos regularmente.

O presente Substitutivo, ao definir as obrigações dos provedores de acesso, mostra que o Brasil o faz por sua vontade soberana, mas em consonância com a "Directiva" citada dos países do Conselho da Europa, atualizando sua legislação.

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 minha autoria, solicitando ao Ministério das Relações Exteriores qual o posicionamento oficial do Brasil em relação à Convenção, uma vez que ele ainda não é dela signatário.

Em data recente, fomos recebidos em audiência pelo Senhor Ministro das Relações Exteriores, tratando, entre outros assuntos, da Convenção sobre o Cibercrime e a posição do Brasil.

E, ao finalizarmos este Parecer, 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, o Conselho da Europa ouvir os seus Países-Membros e, 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.

Consoante as sugestões recebidas e respaldados pelas recomendações da Convenção sobre o Cibercrime de Budapest e da Directiva 2006/24/CE do Parlamento Europeu e do Conselho, que acabamos de descrever resumidamente, incluímos o artigo 21 ao Substitutivo que determina que o responsável pelo provimento de acesso a uma rede de computadores é obrigado a:

– manter em ambiente controlado e de segurança os dados aptos à identificação do usuário e aptos à identificação das conexões realizadas por seus equipamentos: endereços eletrônicos de origem das conexões, data, horário de início e término e referência GMT, da conexão, pelo prazo de três anos, para prover os elementos probatórios essenciais de identificação da autoria das conexões na rede de computadores, em caso de ocorrência de crime;

– 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;

– fornecer os dados e informações de conexões realizadas e os dados e informações de identificação do usuário quando solicitado pela autoridade competente no curso de investigação e por autorização expressa da autoridade judicial;

– preservar imediatamente, após a solicitação expressa da autoridade judicial, no curso de investigação, os dados de conexões realizadas, os dados de identificação de usuário e o conteúdo das comunicações realizadas daquela investigação, respondendo pela sua absoluta confidencialidade e inviolabilidade;

– informar, de maneira sigilosa, à autoridade competente à qual está jurisdicionado, denúncia da qual tenha tomado conhecimento e que contenha indícios de conduta delituosa na rede de computadores sob sua responsabilidade, pois não é demais lembrar que o art. 21 do Código Penal diz que ninguém pode se escusar com o desconhecimento da lei nem do ilícito;

– 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;

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

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

O § 1° do art. 21 do Substitutivo remete para regulamento do Poder Executivo o detalhamento relativo aos dados de conexão, às condições de segurança de seu armazenamento, a auditoria a que serão submetidos, a autoridade competente para realizá-la, o texto a ser apresentado aos usuários e estipula um prazo de noventa dias para a sua publicação.

O § 2° determina o prazo de transição de cento e oitenta dias a partir da promulgação da lei para que os dados e procedimentos requeridos estejam disponíveis.

Os §§ 3° e 4°§ definem, respectivamente, a multa variável de dois a cem mil reais, dobrando no caso de reincidência, independentemente de *indenização por danos à vítima, pelo descumprimento das obrigações* e a destinação dos recursos financeiros resultantes ao Fundo Nacional de Segurança Pública (de que trata a Lei n° 10.201, de 14 de fevereiro de 2001). A multa será imposta mediante procedimento administrativo, pela autoridade judicial desatendida, considerando-se a natureza, a gravidade e o prejuízo resultante da infração.

Parte dessas disposições atende algumas das recomendações do item "6 – Responsabilidades dos Provedores", da publicação "Cartilha de Segurança para Internet", já citada, quando recomenda a publicação de alertas e informações de segurança na internet aos usuários, principalmente às crianças e adolescentes.

Por fim, o art. 22 traz dispositivo semelhante ao que temos na Lei Complementar n° 105, de 2001, que trata do sigilo bancário: 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 identificação de usuário, quando constatada qualquer prática criminosa. Dispositivo em plena harmonia com a jurisprudência do Supremo Tribunal Federal (STF), notadamente o voto do ministro Sepúlveda Pertence, já citado neste Parecer quando da referência à decisão do STJ na Carta Rogatória proveniente da Corte alemã.

III – VOTO

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

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, e a Lei nº 8.078, de 11 de setembro de 1990 (Código do Consumidor), 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, e a Lei nº 8.078, de 11 de setembro de 1990 (Código do Consumidor), 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.

§ 4º Não há crime quando o agente acessa a título de defesa digital, excetuado o desvio de finalidade ou o excesso.

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 – defesa digital: manipulação de código malicioso por agente técnico ou profissional habilitado, em proveito próprio ou de seu preponente, e sem risco para terceiros, de forma tecnicamente documentada e com preservação da cadeia de custódia no curso dos procedimentos correlatos, a título de teste de vulnerabilidade, de resposta a ataque, de frustração de invasão ou burla, de proteção do sistema, de interceptação defensiva, de tentativa de identificação do agressor, de exercício de forense computacional e de práticas gerais de segurança da informação;

V - 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;

VI – 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;

VII – 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.

§ 1° 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.

§ 4º Não há crime quando a ação do agente é a título de defesa digital, excetuado o desvio de finalidade ou o excesso."

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.

§ 2º Não há crime quando a difusão ocorrer a título de defesa digital, excetuado o desvio de finalidade ou o excesso."

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

§ 1° 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

§ 2° 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. "

§ 3° 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.

§ 4° Não há crime quando a ação do agente é a título de defesa digital, excetuado o desvio de finalidade ou o excesso."

Art. 13. O Título VII da Parte Especial do Livro I do Código Penal Militar, Decreto-Lei, nº 1.001, de 21 de outubro de 1969, 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.

§ 3º Não há crime quando o agente acessa a título de defesa digital, excetuado o desvio de finalidade ou o excesso.

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 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.

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

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, 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 – defesa digital: manipulação de código malicioso por agente técnico ou profissional habilitado, em proveito próprio ou de seu preponente, e sem risco para terceiros, de forma tecnicamente documentada e com preservação da cadeia de custódia no curso dos procedimentos correlatos, a título de teste de vulnerabilidade, de resposta a ataque, de frustração de invasão ou burla, de proteção do sistema, de interceptação defensiva, de tentativa de identificação do agressor, de exercício de forense computacional e de práticas gerais de segurança da informação;

V - 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;

VI – 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;

VII – 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.

§ 1° 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.

§ 2° 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 n° 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.

§ 1° 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.

§ 2° Não há crime quando a difusão ocorre a título de defesa digital, excetuado o desvio de finalidade ou o excesso."

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

"**Art. 2°** .....

.....

§ 2° 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 IV:

> **"Art. 313.** .....
>
> .....
>
> IV – 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 responsável pelo provimento de acesso a rede de computadores é obrigado a:

I – manter em ambiente controlado e de segurança os dados de conexões realizadas por seus equipamentos, aptos à identificação do usuário e dos endereços eletrônicos de origem, da data, do horário de início e término e referência GMT, das conexões, pelo prazo de três anos, para prover os elementos probatórios essenciais de identificação da autoria das conexões na rede de computadores;

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 conexões realizadas e os dados de identificação de usuário;

IV – preservar imediatamente, após a solicitação expressa da autoridade judicial, no curso de investigação, os dados de conexões realizadas, os dados de identificação de usuário e as comunicações realizadas daquela 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 de conduta delituosa na 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.

§ 1° Os dados de conexões realizadas em rede de computadores, aptos à identificação do usuário, 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.

§ 2° 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.

§ 3° O responsável citado no *caput* deste artigo que não cumprir o disposto no § 2°, 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.

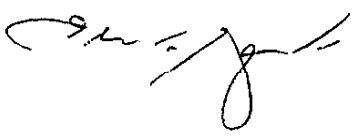
§ 4° Os recursos financeiros resultantes do recolhimento das multas estabelecidas neste artigo serão destinados ao Fundo Nacional de Segurança Pública, de que trata a Lei nº 10.201, de 14 de fevereiro de 2001.

Art. 22. 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 identificação de usuário, quando constatada qualquer conduta criminosa.

Art. 23. Esta Lei entrará em vigor sessenta dias após a data de sua publicação.

Sala da Comissão,

, Presidente



, Relator

RELATÓRIO

RELATOR: Senador **EDUARDO AZEREDO**

I – RELATÓRIO

Vem a esta Comissão, para parecer, 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 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 nº 137, de 2000, por força da aprovação do Requerimento nº 466, de 2000, de autoria do Senador Roberto Freire, por versarem sobre a mesma matéria.

O PLC nº 89, de 2003, de iniciativa do Deputado Luiz Piauhylino, altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), e a Lei nº 9.296, de 24 de julho de 1996, e dá outras providências. Resulta do trabalho do grupo de juristas que aperfeiçoou o PL nº 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, § 3º); 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. 2º, § 2º, da Lei nº 9.296, de 24 de julho de 1996).

Tivemos a honra de relatar essas proposições perante a Comissão de Educação, onde foram amplamente debatidas. Lá, 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 pretende:

a) inserir no Código Penal (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, identificação de usuário e autenticação de usuário*; 154-D, para definir o crime de *divulgação de informações depositadas em bancos de dados*; 154-E, 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 à 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.

No âmbito processual, o Substitutivo pretende 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.

Não foram apresentadas emendas.

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 (cert.br), as tentativas de fraudes pela internet no Brasil cresceram 53% em 2006. Em 2005, foram registradas 27,3 mil tentativas de fraudes pela rede. Em 2006, foram 41,8 mil. Os números, frise-se bem, podem ser muito maiores que esses, dado que o cert.br considera apenas os dados reportados espontaneamente pelos usuários e administradores de redes.

Ao todo, o cert.br recebeu, no ano passado, 197 mil incidentes relacionados à internet, alta de 191% em relação a 2005. Os principais alvos são os usuários interessados em usar bancos ou fazer compras pela rede mundial de computadores. A estimativa é de que os bancos perdem mais de R$ 300 milhões por ano em fraudes virtuais.

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. O Brasil, logo atrás, tem 21,18%, e o Canadá, em terceiro lugar, 9,45%.

Em matéria da INFO Exame, de outubro de 2006, os incidentes relatados ao cert.br indicam uma escalada anual surpreendente de incidentes, quase dobrando ano a ano: de 3.107 em 1999, passa-se para 5.997, 12.301, 25.092, 54.607, 75.722, sucessivamente, até mais que dobrar e chegar aos 197 mil de 2006.

Matéria publicada na revista Exame, edição de 24 de agosto de 2006, apresenta estatística do Comitê Gestor da Internet no Brasil (CGI.br), que informa que os crimes na internet passaram de 18, em 2002, para 27.292, em 2005, e que as investigações da Polícia Federal sobre crimes na internet, no período de 2002 a 2005, passaram de 214 para 1.500.

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 britânica, segundo o Ministério do Interior, foi de US$ 3,2 bilhões nos últimos três anos.

Segundo relatório da McAfee, empresa de segurança em tecnologia, o número de programas mal-intencionados que monitoram a atividade de digitação para capturar senhas e outras informações confidenciais aumentou 250% entre janeiro de 2004 e maio de 2006 nos EUA.

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, que resultou no Parecer pelo oferecimento do Substitutivo ora examinado.

Não obstante, reconhecemos que existem alguns aperfeiçoamentos a realizar quanto à redação, concisão e clareza, e de mérito, que só recentemente chegaram ao nosso conhecimento, conforme sugestões informais apresentadas por associações, por órgãos públicos e por especialistas em tecnologia da informação e em direito aplicado a ela.

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, para ouvirmos as sugestões e explicarmos o trabalho que o Parlamento vem desenvolvendo há dez anos.

Estes aperfeiçoamentos foram devidamente analisados pelo mesmo grupo de voluntários, aos quais registramos nossos agradecimentos, que colaboraram informalmente na construção do Substitutivo apresentado na Comissão de Educação desta casa legislativa. Lá, inicialmente, foram contatados quase cem profissionais de várias especialidades correlatas com a matéria ora em discussão, alem de oficiais superiores das três forças armadas, que cuidaram da alteração do Código Penal Militar, e ao final resumiu-se a um grupo de especialistas voluntários que, com o uso intensivo da internet, logrou concluir pelo texto do substitutivo afinal aprovado.

Analisadas as sugestões, na sua maioria de redação para clareza e concisão, concluímos que a matéria, complexa, abrangente, tratando de crimes contra a pessoa, contra o patrimônio e contra serviços públicos, requer um novo substitutivo, que pode ser comparado com aquele da Comissão de Educação, por quem tiver interesse no tema. Assim, passamos a descrever as alterações, supressões e inclusões.

Começamos por alterar a ementa da Lei para nela incluir a indicação da alteração da Lei nº 9.296, de 24 de julho de 1996 (que cuida das interceptações de comunicações telefônicas, regulamentando o inciso XII, parte final, do art. 5° da Constituição Federal), 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 (que dispõe sobre infrações penais de repercussão interestadual ou internacional que exigem repressão uniforme), e a indicação da alteração da Lei nº 8.078, de 11 de setembro de 1990 (Código do Consumidor).

Incluímos um novo art. 1°, renumerando-se os demais, para cumprir o que determina o art. 7°, da Lei Complementar nº 95, de 26 de fevereiro de 1998, segundo o qual o primeiro artigo do texto "indicará o objeto da lei e o respectivo âmbito de aplicação".

Recebemos ponderações de que nem tudo é digital embora seja eletrônico, como, por exemplo, alguns dispositivos de comunicação, com componentes eletrônicos mas analógicos.

Assim, substituímos toda referência 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, deixando o texto mais consoante à realidade da tecnologia, pretendendo com isso maior longevidade e adaptabilidade para o texto da norma em apreço.

No novo art. 154-A do Código Penal, e no seu correspondente novo art. 339-A do Código Penal Militar, incluímos a expressão "ou sistema informatizado" no título do artigo, dando-lhe coerência com o seu texto. Ainda, substituímos a expressão "indevido" pela expressão "não autorizado" e a expressão "indevidamente" pela expressão "sem autorização do legítimo titular, quando exigida:", colocada ao final do texto, para definir melhor o tipo. Outrossim, retiramos a expressão "indevidamente" do texto do § 1° do artigo.

Nestes artigos incluímos ainda dispositivos para ressalvar os profissionais autorizados que fazem a "defesa digital", a prevenção, a análise e a resposta aos acessos indevidos.

Para maior precisão e clareza, no novo art. 154-B do Código Penal, e no seu correspondente novo art. 339-B do Código Penal Militar, trocamos de posição na oração a expressão "dado ou informação obtida", e incluímos a ação de "obter" o dado ou a informação. Trocamos a expressão "indevidamente" pela expressão "sem autorização do legítimo titular, quando exigida", definindo melhor o tipo.

Para maior clareza, incluímos também a manutenção consigo do dado ou informação obtido com autorização por prazo definido e que tenha expirado, prática comum daquele que se infiltra, obtém as informações que virá a usar uma vez fora do ambiente atacado.

Acrescentamos a majorante de um terço da pena se o dado ou informação obtida indevidamente ou sem autorização é fornecido pela rede de computadores ou em qualquer outro meio de divulgação em massa.

Nas definições constantes do novo art. 154-C do Código Penal, e do seu correspondente novo art. 339-C do Código Penal Militar, fizemos as seguintes alterações:

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

– na definição de "Sistema Informatizado" substituímos a expressão "eletronicamente" pela expressão "eletrônica ou digitalmente ou equivalente", incluímos a expressão "capturar" e suprimimos a expressão "rede de computadores ou internet", que passou a ser objeto de definição específica;

– retiramos a definição de "Identificação de Usuário", bem como a definição de "Autenticação de Usuário", que deixam de ser necessárias no texto da norma, já que os artigos que as citavam foram convolados em normas administrativas;

– incluímos a definição de "Rede de Computadores", para nela incluir a definição de internet, a rede mundial de computadores, reclamada por alguns dos colaboradores na elaboração do Substitutivo, e definindo todas as demais redes de computadores, locais, regionais, nacionais, privadas ou públicas. Na definição, uma rede de computadores é entendida como um conjunto de computadores e dispositivos de comunicação, governados entre si, de comum acordo, por um conjunto de regras, códigos e formatos agrupados em protocolos. Assim, ela é destacada de "sistema informatizado", conceito mais abrangente, que inclui qualquer sistema, alguns deles não dispondo de meios para identificar e autenticar usuários e muito menos para armazenar os dados de conexão, conforme requeridos pelos processos de investigação penal;

– incluímos a definição de "Defesa Digital", para que se possa isentar de pena, em alguns dos novos crimes, a manipulação de código malicioso por agente técnico ou profissional habilitado, em proveito próprio ou de seu preponente, e sem risco para terceiros, de forma tecnicamente documentada e com preservação da cadeia de custódia no curso dos procedimentos correlatos, a título de teste de vulnerabilidade, de resposta a ataque, de frustração de invasão ou burla, de proteção do sistema, de interceptação defensiva, de tentativa de identificação do agressor, de exercício de forense computacional e de práticas gerais de segurança da informação;

– incluímos a definição de "código malicioso", qual seja 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 em obtenção não autorizada de informações contra terceiro, de maneira dissimulada ou oculta, transparecendo tratar-se de ação de curso normal;

– incluímos as definições de "dados informáticos" e "dados de tráfego", para prover maior harmonia com a Convenção do Cibercrime, facilitando assim a participação do Brasil, se esse for o seu interesse.

No novo art. 154-D, *caput*, do Código Penal, e no seu correspondente novo art. 339-D, *caput*, do Código Penal Militar incluímos também as condutas de "utilizar" e de "comercializar" sem autorização ou para fim diferente da sua constituição, o conteúdo de um banco de dados. Para a decisão de autorizar a divulgação de informações contidas em banco de dados, incluímos a expressão "nos casos previstos em lei," dando maior clareza à norma.

Renumeramos o parágrafo único destes artigos como § 1°, e acrescentamos o § 2° 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.

Em relação à "preservação dos dados de conexões realizadas", do novo art. 154-E do Código Penal e do seu correspondente novo art. 339-E, do Código Penal Militar, os artigos foram excluídos e as penas foram transformadas em multas administrativas, constantes do final do Substitutivo, com ênfase na finalidade da guarda dos dados, deixando claro que se tutela a justiça, afirmando-os como dados de valor probatório, aptos à identificação do usuário e da conexão quando da ocorrência de crime.

Na nova redação dos dispositivos a eles correspondentes retiramos a expressão "e comunicações", considerada demasiado abrangente, pois o que se pretende são os dados de conexões realizadas e não aqueles da continuidade da conexão, o que onera sem necessidade os operadores do sistema.

Reduzimos a lista de informações a serem guardadas, significando menor volume de arquivamento para os operadores, o que também acontece com a redução do prazo de guarda de "cinco" para "três" anos, que é a recomendação do Comitê Gestor da Internet do Brasil (CGI.br), prazo considerado suficiente para os trabalhos de investigação quando necessários.

Por sugestão recebida para melhor tipificação, incluímos artigo ao Substitutivo, renumerando-se os demais, para com ele acrescentarmos o inciso V ao § 4° do art. 155 do Código Penal e acrescentarmos o inciso V do § 6° ao seu correspondente art. 240 do Código Penal Militar. Ambos tratam do crime de "furto qualificado", que tem a pena definida como de reclusão de dois a oito anos, e multa, se o crime é cometido, por exemplo, com emprego de chave falsa. Adicionamos o inciso com as orações alternativas: "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".

No novo art. 163-A do Código Penal, e no seu correspondente novo art. 262-A do Código Penal Militar, aperfeiçoamos a redação, substituindo no título a expressão "vírus" por "código malicioso", considerada mais adequada, pois passa a abranger qualquer código malicioso criado, inserido ou difundido, que se reproduz automaticamente ou não, ou que toma controle do equipamento sem autorização do seu usuário, causando-lhe dano na destruição, ou no impedimento de uso ou no mau funcionamento do equipamento. Assim, incluímos 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 – situação essa que, no jargão técnico, é a de transformar o equipamento em um "zumbi".

A definição do novo tipo começa pela forma mais simples de dano ao criar, inserir e difundir código malicioso, para nos dois parágrafos seguintes ser qualificado pela intenção de causar dano, e novamente qualificado pela apuração do resultado do dano, com o correspondente progressivo agravamento da pena.

Nestes artigos renumeramos o parágrafo único como § 1° e incluímos ainda dispositivos para ressalvar os profissionais autorizados que fazem a "defesa digital", a prevenção, a análise e a resposta aos acessos indevidos.

Alteramos a localização do novo tipo de "difusão de código malicioso" por fraude, anteriormente o novo 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). A motivação para a mudança foi que o Capítulo anterior (do Título VIII – Dos Crimes contra a Incolumidade Pública – Capítulo II – Dos Crimes contra a Segurança dos Meios de Comunicação e Transporte e outros Serviços Públicos) trata de crimes contra "serviços públicos" e desta forma o novo tipo alcançaria apenas rede de computadores, dispositivo de comunicação e sistema informatizado de acesso público, como computadores de acesso público, terminais de bancos etc, deixando de alcançar todos os demais citados de acesso privado. Ademais o tipo de fraude se realiza com o objetivo direto ou indireto de obter ganho econômico, daí a tipificação como estelionato.

Alteramos a pena do novo tipo de "difusão de código malicioso", do novo art. 171-A do Código Penal e no seu correspondente novo art. 339-A do Código Penal Militar, passando de detenção de um a dois anos para reclusão de um a três anos, pois a pretensão dos autores da difusão de código malicioso é a fraude, que pode levar ao "furto qualificado por acesso indevido" (arts. 4º e 11 do PLS), igualando-a à pena que se aplica ao crime tipificado no novo art. 163-A. Nestes artigos, renumeramos o parágrafo único como § 1º e acrescentamos o § 2º, para ressalvar a ação dos profissionais que fazem a "defesa digital", a prevenção, análise e resposta aos ataques tipificados.

Acrescentamos à alteração do art. 266 do Código Penal as expressões "informático, dispositivo de comunicação, rede de computadores, sistema informatizado", seja para adequação aos termos já dispostos na Lei 9.296, de 1996, e aos termos do art. 154-C do Substitutivo, seja para nele incluir como tipo penal "o ataque a rede de computadores ou sistema informatizado", como, por exemplo, o *DoS (Denial-of-Service attack)*, o *DDoS (Distributed-Denial-of-Service attack)* e outros equivalentes.

Alteramos o parágrafo único do art. 298 do Código Penal, o qual se pretende acrescentar, para substituir a expressão "armazenamento ou processamento" pela expressão "captura, armazenamento, processamento ou transmissão" que é uma tipificação clara nos dispositivos de comunicação ou sistemas informatizados, para maior abrangência do texto.

Para maior efetividade da aplicação da Lei, incluímos artigo do Substitutivo para a decretação de prisão preventiva nos crimes dolosos 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, mediante o acréscimo do inciso V ao art. 313 do Decreto-Lei nº 3.689, de 3 de outubro de 1941, Código de Processo Penal (CPP).

Para que a lei tenha maior efetividade, acrescentamos também artigo que determina que a autoridade competente, nos termos de regulamento, estruturará órgãos, setores e equipes de agentes especializados no combate à ação delituosa praticada em rede de computadores, dispositivo de comunicação ou sistema informatizado.

Propomos ainda a inclusão de artigo alterando a Lei nº 10.446, de 8 de maio de 2002, que 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), para possibilitar a atuação da Polícia Federal na investigação dos crimes aqui tratados.

Não menos importante é o artigo do Substitutivo, que acrescenta parágrafo único ao art. 9º da Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor – CDC), e trata da obrigação de se informar sobre a nocividade do produto à saúde ou segurança do consumidor. Assim, o *caput* do art. 9º do CDC passa a se aplicar à segurança digital do consumidor, mediante a informação da necessidade do uso de senhas ou similar para a proteção do uso, ou dos dados trafegados quando se tratar de dispositivo de comunicação, sistema informatizado ou provimento de acesso ou de serviço de sistema de informação pelo uso de rede de computadores.

De fundamental importância é o art. 21 do Substitutivo. Não é demais lembrar que a Lei Complementar nº 95, de 26 de fevereiro de 1998, no seu art. 3º, III, diz que a lei deverá conterá, em sua parte final, "as disposições pertinentes às medidas necessárias à implementação das normas de conteúdo substantivo". Destas medidas tratam os arts. 21 e 22.

Com o art. 21 do Substitutivo, passamos a tratar das obrigações do responsável pelo provimento de acesso a uma rede de computadores. Mantivemos a obrigação da preservação, por eles, das informações relativas às conexões realizadas, pelo prazo de três anos, em redação mais simples e concisa.

Em nível latino-americano registre-se que Lei Argentina de 2003 fixa o prazo de dez anos para a guarda destas informações. E ainda que recentemente chegou ao Congresso Americano projeto de lei propondo a retenção por prazo indeterminado destas informações.

Recentemente a imprensa da Coréia do Sul registrou que foi aprovada pela Assembléia Nacional daquele país, no último dia 22 de dezembro, a revisão do chamado "Ato de Incentivo à Utilização das Redes de Informação e Comunicação e de Proteção à Informação", determinando que os usuários da Internet preencham cadastro ao visitarem sites com mais de 100 mil acessos diários, no chamado "Sistema de Nome Real" (Internet Real-Name System, em livre tradução).

A ofensiva do governo em rediscutir o tema foi respaldada por uma série de pesquisas realizadas junto a internautas, nos principais websites do país. De acordo com o Korea Times, dos 7.909 pesquisados junto aos usuários do Naver, maior portal de Internet coreano, 65% apoiariam o registro de seus dados verdadeiros na Web. Já 80% dos visitantes do Yahoo, num universo de 1.631 entrevistados, seriam a favor do Sistema de Nome Real. Por sua vez, o Instituto Gallup detectou uma aceitação de 75,6% dos pesquisados on-line.

A nova legislação coreana prevê a obrigatoriedade do registro, com dados verdadeiros, inclusive documentação de identidade, dos usuários de Internet em sites com mais de 100 mil acessos diários, quando encaminharem mensagens on-line ou comentários de informações divulgadas em portais, páginas de notícias e de imprensa, bem como de entidades governamentais.

O principal pressuposto dessa regra seria permitir que os provedores de conteúdo identificassem, quando necessário, os remetentes de determinados comentários. Dessa forma, os administradores dos sites poderiam bloquear, por até 30 dias, mensagens consideradas potencialmente controversas ou difamatórias. Esses provedores estariam sujeitos a multas de até 30 milhões de wons (cerca de 30 mil dólares), caso não disponibilizassem o sistema de registro.

Cumpre lembrar aqui a confusão (ou desinformação) que se estabelece acerca da relação entre liberdade de expressão e anonimato, ambos possíveis na internet (o anonimato representado pela não-identificação e a não-autenticação do usuário).

Ora, se o fato de emitir para alguém uma carteira de habilitação para dirigir veículos automotores não limita o seu direito constitucional de ir e vir, da mesma forma a identificação do usuário de uma rede de computadores não o impede de manifestar-se pela rede.

Importante frisar que a própria Constituição Federal determina, no art. 5º, inciso IV, que "é livre a manifestação do pensamento, sendo vedado o anonimato".

O art. 21 do Substitutivo apenas reafirma esta norma constitucional, e consagra prática mundial de usos e costumes de todos quantos tem na rede de computadores o seu instrumento de prestação de serviços, diferenciando pela quantidade ou pelo tipo de informação requerida quando do acesso, pois quem presta serviço quer saber de quem cobrará economicamente pelos serviços prestados.

Esse aspecto fez parte de comentário recente do pesquisador Vint Cerf, criador dos principais protocolos da internet, na resposta à primeira pergunta em entrevista à imprensa nacional:

> *Nos Estados Unidos é comum que o internauta forneça algum número de identificação para ter acesso em lugares públicos como hotspots, como número de cartão de crédito ou endereço. Em muitos casos, além do cartão você deve fornecer seu endereço para provar que é realmente a pessoa que diz ser. De certa forma, os provedores de acesso à internet já possuem informações confidenciais dos internautas. Se você assina um serviço de banda larga é muito pouco provável que o provedor forneça este serviço sem saber quem você é, ou ter pelo menos o número do seu cartão de crédito, seu endereço e sua conta bancária. Diria que, em muitas instâncias do acesso à internet, os provedores já possuem um montante de informações pessoais sobre os usuários.*

Na segunda resposta da mesma matéria, ele comenta os dados que os provedores deveriam fornecer por requisição judicial, e termina mencionando que os usuários pensam que são anônimos, mas não o são, pois os provedores tem vários dados sobre cada um:

> *O interessante desta questão é avaliar em quais condições os provedores deveriam fornecer informações para o suporte à lei. Não estou familiarizado com a lei brasileira, mas nos Estados Unidos você tem ordens judiciais para obter certos tipos de informação. De certa forma, podemos entender que não deixa de ser um pedido razoável. Existe o mesmo processo com o telefone. Provavelmente, em muitos casos judiciais, ligações e mensagens telefônicas são solicitadas como provas em tribunais. Minha primeira impressão é que isso não parece terrivelmente diferente das práticas aplicadas por aí. Temos de imaginar que se isso for aprovado de alguma forma pode parecer mais ameaçador para os internautas que acreditavam ser mais anônimos do que são. E eles não são. Acho certo dizer que, para a maioria dos provedores que cobram pelos serviços, existem de fato várias formas de rastrear e descobrir quem você é. Até em universidades você precisa fazer um registro antes de acessar a rede.*

É do que trata, por exemplo, recente decisão do Superior Tribunal de Justiça (STJ). O Tribunal da Comarca de Düsseldorf, República Federal da Alemanha, solicitou ao Brasil, mediante carta rogatória, que a empresa Universo *On Line* informasse os dados de pessoa que, em fevereiro de 2004, bloqueou o acesso aos sites atendidos pela empresa "Online-forum". O intimado apresentou impugnação invocando o princípio constitucional da inviolabilidade de dados, previsto no art. 5º, XII, da CF, que, segundo alegou, impediria a quebra do sigilo de dados cadastrais. O ministro Barros Monteiro proferiu importante decisão nos seguintes termos (Carta Rogatória nº 297 –2005/0010755-8, em 18/09/2006):

> ***Esta Corte já proferiu decisão no sentido de que o fornecimento de dados cadastrais, como o endereço p. ex., não está protegido pelo sigilo**, conforme se verifica na ementa a seguir reproduzida:*
>
> *"Imposto de renda. Informações. Requisição. Os elementos constantes das declarações de bens revestem-se de caráter sigiloso que não deve ser afastado se não em situações especiais em que se patenteie relevante interesse da administração da Justiça. Tal não se configura quando se trate apenas de localizar bens para serem penhorados. o que é rotineiro na prática forense. Injustificável, entretanto, negar-se o pedido na parte em que pretende obter dados pertinentes ao endereço do executado. Em relação a isso não há motivo para sigilo" (RESP 83824/BA, relator Ministro Eduardo Ribeiro, DJ 17.5.99) (grifou-se).*

A respeito do assunto, cabe mencionar o estudo de Tércio Sampaio Ferraz Júnior em seu trabalho "Sigilo de Dados: O Direito à Privacidade e os Limites à Função Fiscalizadora do Estado' (Revista da Faculdade de Direito USP, vol. 88, 1993, p. 449), ao explanar sobre o alcance da proteção à vida privada:

*"**Pelo sentido inexoravelmente comunicacional da convivência, a vida privada compõe, porém, um conjunto de situações que, usualmente, são informadas sem constrangimento. São dados que, embora privativos — como o nome, endereço, profissão, idade, estado civil, filiação, número de registro público oficial etc, condicionam o próprio intercâmbio humano em sociedade, pois constituem elementos de identificação que tornam a comunicação possível, corrente e segura. Por isso, a proteção desses dados em si, pelo sigilo, não faz sentido.** Assim, a inviolabilidade de dados referentes à vida privada só tem pertinência para aqueles associados aos elementos identificadores usados nas relações de convivência, as quais só dizem respeito aos que convivem. Dito de outro modo, os elementos de identificação só são protegidos quando compõem relações de convivência privativas: a proteção é para elas, não para eles. Em conseqüência, simples cadastros de elementos identificadores (nome, endereço, R.G., filiação, etc.) não são protegidos. Mas cadastros que envolvam relações de convivência privada (por exemplo, nas relações de clientela, desde quando é cliente, se a relação foi interrompida, as razões pelas quais isto ocorreu, quais os interesses peculiares do cliente, sua capacidade de satisfazer aqueles interesses, etc) estão sob proteção. Afinal, o risco à integridade moral do sujeito, objeto do direito à privacidade, não está no nome, mas na exploração do nome, não está nos elementos de identificação que condicionam as relações privadas, mas na apropriação dessas relações por terceiros a quem elas não dizem respeito".*

***Não é demais evocar a jurisprudência emanada da Corte Suprema brasileira, em especial o trecho do voto proferido pelo Ministro Sepúlveda Pertence**, que também dá amparo ao acolhimento da ordem pleiteada na peça exordial:*

*"Não entendo que se cuide de garantia com status constitucional. Não se trata da 'intimidade ' protegida no inciso X do art. 5º da Constituição Federal. **Da minha leitura, no inciso XII da Lei Fundamental, o que se protege, e de modo absoluto, até em relação ao Poder Judiciário, é a comunicação 'de dados' e não os 'dados', o que tornaria impossível qualquer investigação administrativa, fosse qual fosse."**(voto proferido no MS n. 21.729-4/DF, DJ 19.10.2001)* [grifos nossos].

Esperamos, assim, que o artigo 21 do Substitutivo estimule a celebração de convênios, entre aqueles que tornam possível o acesso à rede de computadores e as organizações detentoras de informações para permitir a verificação dos dados imutáveis como nome, número de documento legalmente emitido, conforme a boa prática existente entre organizações de proteção ao crédito, as instituições financeiras, órgãos públicos e outras.

Sobre esses dados a serem compartilhados, a Constituição Federal determina no seu art. 5°, inciso XXXIII, que:

> **Art. 5°** .....
> .....
> XXXIII – todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado.

O inciso foi regulamentado pela Lei n° 11.111, de 5 de maio de 2005, não proibindo o compartilhamento de dados imutáveis como os já citados, naturalmente desde que autorizados pelo seu titular ou por lei específica, pois dispõe que:

> "**Art. 2°** O acesso aos documentos públicos de interesse particular ou de interesse coletivo ou geral será ressalvado exclusivamente nas hipóteses em que o sigilo seja ou permaneça imprescindível à segurança da sociedade e do Estado, nos termos do disposto na parte final do inciso XXXIII do *caput* do art. 5° da Constituição Federal."

Ainda a propósito, cabe lembrar aqui as recomendações constantes da Cartilha de Segurança para Internet, na sua seção 6 (Responsabilidades dos Provedores), documento editado em notável esforço de colaboração entre o Ministério Público Federal de São Paulo (MPF/SP) e o Comitê Gestor da Internet no Brasil (CGI.br), patrocinada pela Associação Brasileira dos Provedores de Internet (ABRANET), aos quais registramos aqui o nosso elogio ao resultado alcançado.

A brochura contém instruções de como proceder em caso de investigação de delito ocorrido, os modelos de documentos a serem usados para comunicar o fato delituoso às autoridades competentes, o texto completo da Convenção sobre o Cibercrime, celebrado em Budapest, a 23 de novembro de 2001, pelo Conselho da Europa. Essa Convenção foi recentemente ratificada pelo Senado dos EUA.

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*, objeto do art. 16 do Substitutivo;

– *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;

– *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 § 1° 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 do art. 21 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 e crimes de pedofilia, 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 e o Código do Consumidor, 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.

Em outro documento, a "Directiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrônicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Directiva 2002/58/CE", entre outras considerações preambulares, trata naquela de número 18 que "*A decisão-Quadro 2005/222/Al do Conselho, de 24 de fevereiro de 2005, relativa a ataques contra os sistemas de informação, dispõe que o acesso ilegal aos sistemas de informação, incluindo os dados neles conservados seja punível como infracção penal.*" Na consideração de número 20 cita a Convenção sobre o Cibercrime de Budapest de 2001 e a Convenção de 1981, esta sobre os dados pessoais.

Avançando, a "Directiva" define no art. 2° como dados: os "*dados de tráfego e os dados de localização bem como os dados conexos necessários para identificar o assinante e o utilizador*". No art. 5° detalha as "*Categorias de dados a conservar*", onde encontramos, no item 2 da letra *a*, que diz respeito à internet, a especificação da guarda do identificador de acesso, do nome e do endereço do assinante ou usuário, aos quais o endereço do protocolo IP, o identificador de acesso ou o número do telefone, estavam atribuídos no momento da comunicação.

Faz-se mister demonstrar a harmonia do Substitutivo com a "Directiva", que nos arts. 6°, 7°, 8° e 9° define, respectivamente, os "*Períodos de Conservação*", a "*Proteção de dados e segurança dos dados*", os "*Requisitos para o armazenamento dos dados conservados*", a "*Autoridade de controle*", previstos no art. 21 do Substitutivo, incisos I e II, e § 1°.

Desses artigos vem a recomendação de que os dados sejam conservados por um período mínimo de seis meses e não superior a dois anos. Ao final da "Directiva", vários signatários declaram que estudarão a aplicação de prazos diferenciados ou de dezoito ou de trinta e seis meses, a partir de 2007 ou 2009. No Brasil, o Comitê Gestor da Internet no Brasil (CGI.br) definiu esse prazo em trinta e seis meses. A "Directiva" recomenda ainda que a guarda deva ser criteriosa e que seja designada uma autoridade competente para a realização da auditoria a que estes dados forem submetidos regularmente.

O presente Substitutivo, ao definir as obrigações dos provedores de acesso, mostra que o Brasil o faz por sua vontade soberana, mas em consonância com a "Directiva" citada dos países do Conselho da Europa, atualizando sua legislação.

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 minha autoria, solicitando ao Ministério das Relações Exteriores qual o posicionamento oficial do Brasil em relação à Convenção, uma vez que ele ainda não é dela signatário.

Em data recente, fomos recebidos em audiência pelo Senhor Ministro das Relações Exteriores, tratando, entre outros assuntos, da Convenção sobre o Cibercrime e a posição do Brasil.

E, ao finalizarmos este Parecer, 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, o Conselho da Europa ouvir os seus Países-Membros e, 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.

Consoante as sugestões recebidas e respaldados pelas recomendações da Convenção sobre o Cibercrime de Budapest e da Directiva 2006/24/CE do Parlamento Europeu e do Conselho, que acabamos de descrever resumidamente, incluímos o artigo 21 ao Substitutivo que determina que o responsável pelo provimento de acesso a uma rede de computadores é obrigado a:

– manter em ambiente controlado e de segurança os dados aptos à identificação do usuário e aptos à identificação das conexões realizadas por seus equipamentos: endereços eletrônicos de origem das conexões, data, horário de início e término e referência GMT, da conexão, pelo prazo de três anos, para prover os elementos probatórios essenciais de identificação da autoria das conexões na rede de computadores, em caso de ocorrência de crime;

– 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;

– fornecer os dados e informações de conexões realizadas e os dados e informações de identificação do usuário quando solicitado pela autoridade competente no curso de investigação e por autorização expressa da autoridade judicial;

– preservar imediatamente, após a solicitação expressa da autoridade judicial, no curso de investigação, os dados de conexões realizadas, os dados de identificação de usuário e o conteúdo das comunicações realizadas daquela investigação, respondendo pela sua absoluta confidencialidade e inviolabilidade;

– informar, de maneira sigilosa, à autoridade competente à qual está jurisdicionado, denúncia da qual tenha tomado conhecimento e que contenha indícios de conduta delituosa na rede de computadores sob sua responsabilidade, pois não é demais lembrar que o art. 21 do Código Penal diz que ninguém pode se escusar com o desconhecimento da lei nem do ilícito;

– 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;

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

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

O § 1º do art. 21 do Substitutivo remete para regulamento do Poder Executivo o detalhamento relativo aos dados de conexão, às condições de segurança de seu armazenamento, a auditoria a que serão submetidos, a autoridade competente para realizá-la, o texto a ser apresentado aos usuários e estipula um prazo de noventa dias para a sua publicação.

O § 2º determina o prazo de transição de cento e oitenta dias a partir da promulgação da lei para que os dados e procedimentos requeridos estejam disponíveis.

Os §§ 3º e 4º§ definem, respectivamente, a multa variável de dois a cem mil reais, dobrando no caso de reincidência, independentemente de indenização por danos à vítima, pelo descumprimento das obrigações e a destinação dos recursos financeiros resultantes ao Fundo Nacional de Segurança Pública (de que trata a Lei nº 10.201, de 14 de fevereiro de 2001). A multa será imposta mediante procedimento administrativo, pela autoridade judicial desatendida, considerando-se a natureza, a gravidade e o prejuízo resultante da infração.

Parte dessas disposições atende algumas das recomendações do item "6 – Responsabilidades dos Provedores", da publicação "Cartilha de Segurança para Internet", já citada, quando recomenda a publicação de alertas e informações de segurança na internet aos usuários, principalmente às crianças e adolescentes.

Por fim, o art. 22 traz dispositivo semelhante ao que temos na Lei Complementar nº 105, de 2001, que trata do sigilo bancário: 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 identificação de usuário, quando constatada qualquer prática criminosa. Dispositivo em plena harmonia com a jurisprudência do Supremo Tribunal Federal (STF), notadamente o voto do ministro Sepúlveda Pertence, já citado neste Parecer quando da referência à decisão do STJ na Carta Rogatória proveniente da Corte alemã.

Estando o Projeto em pauta nesta Comissão, foram apresentadas duas emendas oferecidas pelo nobre e eminente Senador Flexa Ribeiro, sendo retirada pelo autor a Emenda número 02/CCJ.

A Emenda número 01/CCJ prevê as supressões que dizem respeito à "legítima defesa digital", instituto proposto pelo Substitutivo, pois tanto no artigo 154-C inciso IV, proposto, do Código Penal quanto no artigo 339-C inciso IV, proposto, do Código Penal Militar, é definida a "defesa digital". A Emenda prevê também a supressão dos §§ propostos dos artigos 154-A, 163-A e 171-A, do Código Penal, e nos §§ propostos dos artigos 261-A, 339-A e 281-A, do Código Penal Militar, onde são dispostas a inexistência de crime na hipótese de defesa digital.

Argumenta o autor da emenda que tanto o art. 25 do Código Penal quanto o art. 44 do Código Penal Militar, definem de forma mais abrangente e consagrada o instituto da Legítima Defesa. Ressalta ainda que não se opõe à intenção do Substitutivo de aplicá-la ao mundo digital, restringindo-lhe o agente e os meios necessários, sem alterar a sua estrutura jurídica em si. Mas prefere a supressão proposta, pois "a Parte Geral de ambos os códigos irradia efeitos para todos os tipos penais da Parte Especial, cabendo ao Juiz, e somente a ele, a sua interpretação na alegação caso a caso".

Realmente alguns juízos especializados já haviam ponderado sobre a abrangência maior e consagrada da legítima do art. 25 do Código Penal e do art 44 do Código Penal Militar. Como não há prejuízo para o Projeto somos pelo acatamento da Emenda 01/CCJ, realizando as supressões solicitadas.

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 n° 76 e n° 137, ambos de 2000, na forma do novo Substitutivo que ora oferecemos, com a Emenda número 01/CCJ.

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, e a Lei nº 8.078, de 11 de setembro de 1990 (Código do Consumidor), 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, e a Lei nº 8.078, de 11 de setembro de 1990 (Código do Consumidor), 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.

§ 4º Não há crime quando o agente acessa a título de defesa digital, excetuado o desvio de finalidade ou o excesso.

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 – defesa digital: manipulação de código malicioso por agente técnico ou profissional habilitado, em proveito próprio ou de seu preponente, e sem risco para terceiros, de forma tecnicamente documentada e com preservação da cadeia de custódia no curso dos procedimentos correlatos, a título de teste de vulnerabilidade, de resposta a ataque, de frustração de invasão ou burla, de proteção do sistema, de interceptação defensiva, de tentativa de identificação do agressor, de exercício de forense computacional e de práticas gerais de segurança da informação;

V - 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;

VI – 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;

VII – 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.

§ 4º Não há crime quando a ação do agente é a título de defesa digital, excetuado o desvio de finalidade ou o excesso."

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.

§ 2º Não há crime quando a difusão ocorrer a título de defesa digital, excetuado o desvio de finalidade ou o excesso."

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 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.

§ 4º Não há crime quando a ação do agente é a título de defesa digital, excetuado o desvio de finalidade ou o excesso."

Art. 13. O Título VII da Parte Especial do Livro I do Código Penal Militar, Decreto-Lei, nº 1.001, de 21 de outubro de 1969, 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.

§ 1° 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.

§ 2° 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.

§ 3° Não há crime quando o agente acessa a título de defesa digital, excetuado o desvio de finalidade ou o excesso.

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.

§ 1° 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.

§ 2° 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.

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

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, 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 – defesa digital: manipulação de código malicioso por agente técnico ou profissional habilitado, em proveito próprio ou de seu preponente, e sem risco para terceiros, de forma tecnicamente documentada e com preservação da cadeia de custódia no curso dos procedimentos correlatos, a título de teste de vulnerabilidade, de resposta a ataque, de frustração de invasão ou burla, de proteção do sistema, de interceptação defensiva, de tentativa de identificação do agressor, de exercício de forense computacional e de práticas gerais de segurança da informação;

V - 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;

VI – 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;

VII – 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.

§ 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.

§ 2º Não há crime quando a difusão ocorre a título de defesa digital, excetuado o desvio de finalidade ou o excesso."

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. 1° da Lei n° 10.446, de 8 de maio de 2002 passa a vigorar com a seguinte redação:

"**Art. 1°** .....

.....

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

Art. 20. O art. 9° da Lei n° 8.078, de 11 de setembro de 1990 passa a vigorar com a seguinte redação:

"Art. 9° .....

.....

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 responsável pelo provimento de acesso a rede de computadores é obrigado a:

I – manter em ambiente controlado e de segurança os dados de conexões realizadas por seus equipamentos, aptos à identificação do usuário, e dos endereços eletrônicos de origem, da data, do horário de início e término e referência GMT, das referidas conexões, pelo prazo de três anos, para prover os elementos probatórios essenciais de identificação da autoria das conexões na rede de computadores;

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 conexões realizadas e os dados de identificação de usuário;

IV – preservar imediatamente, após a solicitação expressa da autoridade judicial, no curso de investigação, os dados de conexões realizadas, os dados de identificação de usuário e as comunicações realizadas daquela 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 de conduta delituosa na 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.

§ 1° Os dados de conexões realizadas em rede de computadores, aptos à identificação do usuário, 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.

§ 2° 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.

§ 3° O responsável citado no *caput* deste artigo que não cumprir o disposto no § 2°, 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.

§ 4° 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. 22. 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 identificação de usuário, quando constatada qualquer conduta criminosa.

Art. 23. Esta Lei entrará em vigor sessenta dias após a data de sua publicação.

Sala da Comissão,

, Presidente

, Relator

Publicado no **Diário do Senado Federal**, de 26/6/2008.

Secretaria Especial de Editoração e Publicações do Senado Federal – Brasília – DF
(OS:14136/2008)