

PARECER Nº , DE 2008

Da COMISSÃO DE ASSUNTOS ECONÔMICOS sobre o Projeto de Lei da Câmara nº 89, de 2003, e Projetos de Lei do Senado nº 137, de 2000, e nº 76, de 2000, todos referentes a crimes na área de informática.

RELATOR: Senador 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 Piauhyllino, 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°s 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 § 2º 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 nº 7.716, de 1989, a supressão da 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, 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. 2º 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 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 Substitutivo aprovado pela CCT com as seguintes subemendas:

SUBEMENDA Nº 01 – CAE À EMENDA Nº 02-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 02 – CAE À EMENDA Nº 02-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 03 – CAE À EMENDA Nº 02-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 04 – CAE À EMENDA Nº 02-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 Nº 05 – CAE À EMENDA Nº 02-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 06 – CAE À EMENDA Nº 02-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, dificuldade 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 07 – CAE À EMENDA Nº 02-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 08 – CAE À EMENDA Nº 02-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 09 – CAE À EMENDA Nº 02-CCT (SUBSTITUTIVO)

Dê-se ao art. 8º do 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 02-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 02-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, dificuldade 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 02-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 02-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 02-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 02-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 02-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 02-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 02-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 02-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, receptor, 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 02-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 02-CCT (SUBSTITUTIVO)

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

“**Art. 20.** 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)”

SUBEMENDA Nº 22 – CAE À EMENDA Nº 02-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 02-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