Minuta

# PARECER Nº , DE 2006

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

RELATOR: Senador **EDUARDO AZEREDO**

## I – RELATÓRIO

Vêm 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 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 nº 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. 1º, renumerando-se os demais, para cumprir o que determina o art. 7º, da Lei Complementar nº 95, de 26 de fevereiro de 1998: “Art. 7º 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 internet, 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" e incluímos a expressão "capturar";

– 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 ou internet”, reclamada por alguns dos colaboradores na elaboração do Substitutivo, e 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 finalmente a definição de “Provedor” tanto para aquele que presta serviços de acesso à rede de computadores ou internet como para aquele que presta serviços relacionados a esse acesso.

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 § 1º, e acrescentamos o § 2º com a majorante de um terço da pena se o crime ocorre em rede de computadores ou internet, dispositivo de comunicação ou sistema informatizado, ou em qualquer outro meio de divulgação em massa. Acrescentamos ainda o § 3º, 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 aos “dados de conexões”, do novo art. 154-E do Código Penal e do seu correspondente novo art. 339-E, do Código Penal Militar, substituímos a expressão “rede de computadores” pela expressão “rede de computadores ou internet”, para melhor clareza da norma e 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.

No novo art. 154-F do Código Penal, e no seu correspondente novo art. 339-F do Código Penal Militar, a redação e o mérito foram aperfeiçoados e adequados às definições introduzidas, explicitando que o delito de "permitir acesso a uma rede de computadores por usuário não identificado e não autenticado" só ocorrerá por negligência ou dolo do agente.

De fato a redação anterior destes artigos poderia levar a uma interpretação indesejada da ação de permitir o acesso. Reconhecemos ainda 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 o novo tipo 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 ou internet, dispositivos de comunicação ou sistemas informatizados; ou que sejam praticadas contra 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 sem autorização.

Acrescentamos à alteração do art. 266 do Código Penal as expressões "informático, dispositivo de comunicação, rede de computadores ou internet, 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 internet 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 § 1º e acrescentamos um § 2º para ressalvar da ação delituosa, como "exercício regular de direito", previsto no inciso III do art. 23 do Código Penal, conhecido 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 ou internet, 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, para maior abrangência do texto.

Para maior efetividade da aplicação da Lei, incluímos o art. 17 do Substitutivo para a decretação de prisão preventiva nos crimes dolosos punidos com detenção, se tiverem sido praticados contra dispositivos de comunicação ou sistemas informatizados, ou se tiverem sido praticados mediante uso de rede de computadores ou internet, 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).

Com a nova redação dada ao art. 14 do Substitutivo da Comissão de Educação (art. 19 do Substitutivo que ora apresentamos) mantivemos a obrigatoriedade da identificação e autenticação do usuário, 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.

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. 19 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 por analogia 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, 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. 20 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 de quem torna disponível o 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.

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 aquele que tornar disponível o acesso a uma rede de computadores ou internet é obrigado a:

- manter em ambiente controlado e de alta segurança os dados de 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 ou internet;
- 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 criminal;
- informar, de maneira sigilosa, à autoridade criminal competente à qual está jurisdicionado, fato do qual tenha tomado conhecimento e que contenha indícios de conduta delituosa na rede de computadores ou internet 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 ou internet;

- alertar aos seus usuários, em campanhas periódicas, quanto ao uso criminoso de rede de computadores ou internet, dispositivos de comunicação e sistemas informatizados;
- divulgar aos seus usuários, em local destacado, as boas práticas de segurança no uso de rede de computadores ou internet, dispositivos de comunicação e sistemas informatizados.

O parágrafo único deste artigo (art. 20 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. 21 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 ou internet, 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 ou internet.

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 n° 89, de 2003 (n° 84, de 1999, na Câmara dos Deputados), e dos Projetos de Lei do Senado nº 76 e n° 137, ambos de 2000, na forma do novo Substitutivo que ora oferecemos.

# 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 internet, 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 internet, 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, ou rede de computadores ou internet, 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 anonimato, de nome suposto ou da utilização de identidade de terceiros para a prática do crime."

**Art. 3º** 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 OU INTERNET DISPOSITIVO DE COMUNICAÇÃO OU SISTEMA INFORMATIZADO

**Acesso indevido a rede de computadores ou internet, dispositivo de comunicação ou sistema informatizado**

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

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

§ 1º Nas mesmas penas incorre quem, indevidamente, permite, facilita ou fornece a terceiro meio não autorizado de acesso a rede de computadores ou internet, 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.

**Obtenção, manutenção, transporte ou fornecimento indevido de informação eletrônica ou digital ou similar**

**Art. 154-B**. Obter, indevidamente ou sem autorização, dado ou informação em rede de computadores ou internet, 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 ou sem autorização em rede de computadores ou internet, dispositivo de comunicação ou sistema informatizado.

§ 2º Se o dado ou informação obtida indevidamente ou sem autorização, é fornecido pela rede de computadores ou internet, 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 ou internet, identificação de usuário, autenticação de usuário, provedor de acesso e provedor de serviço**

**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 ou internet: os meios físicos e lógicos através dos quais é possível trocar dados e compartilhar recursos entre máquinas, representada pelo conjunto de computadores e dispositivos de comunicação, que obedecem de comum acordo a um conjunto de regras, códigos, formatos e outras informações agrupadas em protocolos;

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 ou internet, 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 ou internet, 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 ou internet e o prestador de serviços relacionados a esse acesso.

**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 anonimato, de nome suposto ou da utilização de identidade de terceiros para a prática de divulgação.

§ 2º Se o crime ocorre em rede de computadores ou internet, 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.

**Preservação dos dados de conexões realizadas**

**Art. 154-E.** Deixar de manter, o provedor de acesso à rede de computadores ou internet, os dados de identificação das conexões realizadas por seus equipamentos, aptos à identificação do usuário, constituídos pelos endereços eletrônicos de origem das conexões, data e horário de início e término e referência GMT da conexão, pelo prazo de três anos contados a partir da data de conexão.

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

**Permissão de acesso a usuário não identificado e não autenticado**

**Art. 154-F.** Permitir, o provedor, por negligência, o acesso à rede de computadores ou internet, dispositivo de comunicação ou sistema informatizado, a usuário sem a devida identificação e autenticação.

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

§ 1º Na mesma pena incorre o provedor do acesso à rede de computadores ou internet, dispositivo de comunicação ou sistema informatizado, que deixa de exigir, como condição de acesso, a necessária, identificação e regular cadastramento do usuário.

§ 2º A pena será de reclusão, de um a dois anos e multa se o agente atuar com dolo."

**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 ou internet, dispositivo de comunicação ou sistema informatizado ou similar.
....." 

**Art. 5º** 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 ou digital ou similar, o bit ou a menor quantidade de informação que pode ser entendida como tal, a base de dados armazenada em dispositivo de comunicação e a rede de computadores ou internet, o sistema informatizado, a senha ou similar ou qualquer meio que proporcione acesso aos mesmos."

**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 internet ou sistema informatizado**

**Art. 266.** Interromper ou perturbar serviço telegráfico, radiotelegráfico, telefônico, telemático, informático, de dispositivo de comunicação, de rede de computadores ou internet, 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 ou internet, 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 anonimato, de nome suposto ou da utilização de identidade de terceiros para a prática de difusão maliciosa.

**Exercício regular de direito**

§ 2º Não pratica o crime de difusão injustificada o usuário, 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 ou internet, dispositivo de comunicação ou sistema informatizado**

**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 rede de computadores ou internet, 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 ou internet, dispositivo de comunicação ou sistema informatizado."

**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 ou internet, dispositivo de comunicação ou sistema informatizado ou similar.

....." 

**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 vírus eletrônico ou digital ou similar**

**Art. 262-A**. Criar, inserir ou difundir vírus em rede de computadores ou internet, 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 anonimato, de nome suposto ou da utilização de identidade de terceiros para a prática de acesso."

**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**

**DA VIOLAÇÃO DE REDE DE COMPUTADORES OU INTERNET, DISPOSITIVO DE COMUNICAÇÃO OU SISTEMA INFORMATIZADO**

**Acesso indevido a rede de computadores ou internet, dispositivo de comunicação ou sistema informatizado**

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

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

§ 1º Nas mesmas penas incorre quem, indevidamente, permite, facilita ou fornece a terceiro meio não autorizado de acesso a rede de computadores ou internet, 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 do crime.

**Obtenção, manutenção, transporte ou fornecimento indevido de informação eletrônica ou digital ou similar**

**Art. 339-B**. Obter, indevidamente ou sem autorização, dado ou informação em rede de computadores ou internet, 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 ou sem autorização em rede de computadores ou internet, dispositivo de comunicação ou sistema informatizado.

§ 2º Se o dado ou informação obtida indevidamente ou sem autorização, é fornecido pela rede de computadores ou internet, ou em qualquer outro meio de divulgação em massa, a pena é aumentada de um terço.

**Dispositivo de comunicação, sistema informatizado, rede de computadores ou internet, 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 ou internet: os meios físicos e lógicos através dos quais é possível trocar dados e compartilhar recursos entre máquinas, representada pelo conjunto de computadores e dispositivos de comunicação, que obedecem de comum acordo a um conjunto de regras, códigos, formatos e outras informações agrupadas em protocolos;

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 ou internet, 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 ou internet, 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 ou internet e o prestador de serviços relacionados a esse acesso.

**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 anonimato, de nome suposto ou da utilização de identidade de terceiros para a prática de divulgação.

§ 2º Se o crime ocorre em rede de computadores ou internet, 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.

**Preservação dos dados de conexões realizadas**

**Art. 339-E.** Deixar de manter, o provedor de o acesso à rede de computadores ou internet, os dados de identificação das conexões realizadas por seus equipamentos, aptos à identificação do usuário, constituídos pelos endereços eletrônicos de origem das conexões, data e horário de início e término e referência GMT da conexão, pelo prazo de três anos contados a partir da data da conexão.

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

**Permissão de acesso a usuário não identificado e não autenticado**

**Art. 339-F.** Permitir, o provedor, por negligência, o acesso à rede de computadores ou internet, dispositivo de comunicação ou sistema informatizado, a usuário sem a devida identificação e autenticação.

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

§ 1º Na mesma pena incorre o provedor do acesso à rede de computadores ou internet, dispositivo de comunicação ou sistema informatizado, que deixa de exigir, como condição de acesso, a necessária, identificação e regular cadastramento do usuário.

§ 2º A pena será de reclusão, de um a dois anos e multa se o agente atuar com dolo."

**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.** 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 ou internet, o dispositivo de comunicação e o sistema informatizado, a senha ou similar ou qualquer meio que proporcione acesso aos mesmos."

**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 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 ou internet, 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 anonimato, de nome suposto ou da utilização de identidade de terceiros para a prática de difusão maliciosa.

**Exercício regular de direito**

§ 2º Não pratica o crime de difusão injustificada o usuário, 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. 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 ou internet, 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 ou internet, dispositivo de comunicação ou sistema informatizado, ou se tiverem sido praticados mediante uso de rede de computadores ou internet, dispositivo de comunicação ou sistema informatizado. (NR)"

**Art. 18.** 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. 19.** Todo provedor de acesso ou de serviço a uma rede de computadores ou internet 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 e 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 ou internet, dispositivos de comunicação e sistemas informatizados.

*Parágrafo único*. A identificação do usuário de rede de computadores ou internet 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 e endereço completo e sendo obrigatória para o dispositivo de comunicação e sistema informatizado a indicação de uma pessoa natural responsável.

**Art. 20.** Todo provedor de acesso ou serviço mediante uma rede de computadores ou internet 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, 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 ou internet;

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 e informações de conexões realizadas e os dados e informações de identificação do usuário;

IV – informar, de maneira sigilosa, à autoridade criminal competente à qual está jurisdicionado, fato do qual tenha tomado conhecimento e que contenha indícios de conduta delituosa na rede de computadores ou internet 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 ou internet;

VI – alertar aos seus usuários, em campanhas periódicas, quanto ao uso criminoso de rede de computadores ou internet, dispositivos de comunicação e sistemas informatizados;

VII – divulgar aos seus usuários, em local destacado, as boas práticas de segurança no uso de rede de computadores ou internet, dispositivos de comunicação e sistemas informatizados.

*Parágrafo único*. Os dados de conexões realizadas em rede de computadores ou internet, 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 ou internet, 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 definidos neste artigo.

**Art. 21.** A autoridade competente, nos termos de regulamento, estruturará órgãos, setores e equipes de agentes especializados no combate à

ação delituosa em rede de computadores ou internet, dispositivo de comunicação ou sistema informatizado.

**Art. 22.** 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 ou internet, dispositivo de comunicação ou sistema informatizado. (NR)"

**Art. 23.** 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 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 ou de serviço mediante o uso de rede de computadores ou internet.(NR)"

**Art. 24.** Esta Lei entra em vigor sessenta dias após a data de sua publicação.

Sala da Comissão,

, Presidente

, Relator