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

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 *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 meu 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, para quem nisso tiver interesse. Assim passamos as 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 e a indicação da alteração do Decreto-Lei nº. 3.689, de 3 de outubro de 1941, o Código de Processo Penal.

Incluímos um novo art. 1º, renumerando-se os demais, para cumprir o que determina o artigo 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 “eletrônica e digitalmente”, 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 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 no Código Penal e seu correspondente novo art. 339-B do Código Penal Militar trocamos de posição na oração a expressão “dado ou informação obtida”.

Nas definições constantes do novo art. 154-C no Código Penal e e 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” e substituímos a expressão “digitais” por “eletrônicos ou digitais”;

- na definição de “Sistema Informatizado” substituímos a expressão “eletronicamente” pela expressão “eletrônica ou digitalmente”, incluímos a expressão “ou internet” 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;

- na definição de “Autenticação de Usuário” substituímos a expressão “validação” por “verificação”, considerada mais adequada à definição e aperfeiçoamos a sua redação.

Para a decisão de autorizar a divulgação de informações contidas em banco de dados, contida no novo art. 154-D no Código Penal e seu correspondente novo art. 339-D do Código Penal Militar, incluímos a expressão “nos casos previstos em lei,” dando maior clareza à norma. Renumeramos o parágrafo único para § 1º e incluímos o § 2º, 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 no Código Penal e 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 necessário.

No novo art. 154-F do Código Penal e seu correspondente novo art. 339-F do Código Penal Militar a redação foi aperfeiçoada e adequada às definições introduzidas.

Por sugestão recebida para melhor tipificação, incluímos um artigo, renumerando-se os demais, para com ele alterarmos o inciso III do § 4º do art. 155 do Código Penal e 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 com emprego de chave falsa. Adicionamos aí as orações alternativas: "ou 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 e art. 240 dos Códigos 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.

Igualamos a pena da nova tipificação do novo art. 266-A do Código Penal e seu correspondente novo art. 339-A do Código Penal Militar, Difusão Maliciosa de Código, à pena do crime de Difusão de Vírus Eletrônico ou Digital, novo art. 163-A do Código Penal e 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 destes códigos é a fraude que pode levar ao "furto qualificado por acesso indevido".

Alteramos a inclusão do parágrafo único do art. 298 do Código Penal, para substituir a expressão "armazenamento ou processamento" pela expressão "armazenamento, captura ou processamento" que é uma tipificação clara nos dispositivos de comunicação, para maior abrangência do texto.

Incluímos um artigo para a decretação de prisão preventiva nos crimes dolosos punidos com detenção, mediante a alteração do inciso II do 313 do Decreto-Lei nº. 3.689, de 3 de outubro de 1941, Código de Processo Penal (CPP), adicionando ao final do texto do inciso as orações alternativas "ou 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".

Atendendo a razões da técnica legislativa, a alteração da Lei 9.296 de 24 de julho de 1996, que trata da interceptação de comunicações, constante do art. 15, passa a anteceder o art. 14, com nova renumeração dos artigos subseqüentes.

Assim passam para os artigos finais da norma o art. 14 e as providências complementares relativas ao objetivo da lei conforme seu artigo 1º, obedecendo ao prescrito da Lei Complementar 95 de 26 de fevereiro de 1998, que diz:

> "Art. 3º A lei será estruturada em três partes básicas:
>
> I - parte preliminar, compreendendo a epígrafe, a ementa, o preâmbulo, o enunciado do objeto e a indicação do âmbito de aplicação das disposições normativas;
>
> II - parte normativa, compreendendo o texto das normas de conteúdo substantivo relacionadas com a matéria regulada;
>
> III - parte final, compreendendo as disposições pertinentes às medidas necessárias à implementação das normas de conteúdo substantivo, às disposições transitórias, se for o caso, a cláusula de vigência e a cláusula de revogação, quando couber."

A redação do art. 14, agora renumerado, foi alterada e teve seus parágrafos substituídos por um parágrafo único, melhorando a concisão e clareza da norma, enquanto resume em um único texto a exigibilidade da identificação e autenticação de usuário de uma rede de computadores.

Define também que os dados de identificação de usuário de rede de computadores serão definidos nos termos de regulamento.

Cumpre lembrar aqui a confusão que se estabelece entre a liberdade de expressão e o anonimato, ou a não identificação e autenticação do usuário, ambos possíveis na internet, 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.

Com a nova redação dada ao artigo 14 fica facultado, em substituição à identificação de usuário, o uso de ferramentas digitais de garantia de 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 a 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:

> "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 do item *h)* da seção "6 – Responsabilidades dos Provedores", da publicação "Cartilha de Segurança para Internet", editada 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 contem 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, e finalmente contem 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 aderente a ela 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:

- do acesso ilegal ou não autorizado a sistemas informatizados;
- da interceptação ou interrupção de comunicações;
- da interferência não autorizada sobre os dados armazenados;
- da falsificação em sistemas informatizados;
- da quebra da integridade das informações;
- das fraudes em sistemas informatizados com ou sem ganho econômico;
- da pornografia infantil ou pedofilia;
- da quebra dos direitos de autor;
- das tentativas ou ajudas a condutas criminosas;
- da responsabilidade de uma pessoa natural ou de uma organização;
- das penas de privação de liberdade e de sanções econômicas.

A Convenção recomenda ainda de procedimentos processuais penais e da 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, alem da definição da confidencialidade e limitações de uso. Define a admissão à Convenção por convite a Estados não membros, a aprovação por maioria do Conselho, e a aplicação da Convenção a critério de cada Estado membro.

A legislação brasileira já tipifica alguns dos crimes identificados pela Convenção como os crimes contra os direitos do autor e crimes de pedofilia. Por analogia cuida de alguns outros já tipificados no Código Penal. Assim o presente Projeto de Lei , que atualiza o nosso Código Penal , coloca o Brasil em posição de destaque para que possa tratar de maneira diferenciada com os países signatários da Convenção de Budapest, aí incluido os Estados Unidos da América, país sede das maiores empresas de tenologia da informação e dos maiores provedores de acesso à rede mundial de computadores.

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 a contra os sitemas de informação, dispõe que o acesso ilegal aos sistemas de informação, inlcuindo os dados neles conservados seja punível como infracção penal." E na consideração de número 20 cita a Convenção de Budapest de 2001 e a Convenção de 1981, esta sobre os dados pessoais.

Avançando, a Directiva define no artigo 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 artigo 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 estavam atribuidos no momento da comunicação.

Nos artigos 6º, 7º , 8º e 9º a Directiva define respectivamente:

- os "Periodos de Conservação",
- a "Proteção de dados e segurança dos dados",
- os "Requisitos para o armazenamento dos dados conservados",
- a "Autoridade de controlo".

Isto significa 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 membros declaram que estudarão a aplicação de prazos diferenciados ou de dezoito ou de trinta e seis meses e no Brasil, o

Comitê Gestor da Internet no Brasil (CGI.br) definiu este prazo em trinta e seis meses .

Significa 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.

Resumindo, o presente Projeto de Lei , ao definir na sua parte final 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 sermos signatários da Convenção de Budapest ou de outras Convenções e Acordos sobre a matéria. Registro que isto já se mostra necessário pela dificuldade que nossos investigadores e persecutores penais tem tido em relaçao aos provedores de acesso localizados no exterior, conforme noticiado na imprensa local e internacional.

Finalmente, consoante as sugestões recebidas e respaldados pelos recomendações da Convenção de Budapest e da Directiva 2006/24/CE do Parlamento Europeu e do Conselho, que acabamos de descrever resumidamente, incluímos um 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, espontaneamente e 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;

- 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 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 as crianças e adolescentes.

Para que a lei tenha maior efetividade incluímos também um artigo que determina que a autoridade competente, nos termos de regulamento, estruturará setores e equipes de agentes especializados no combate à ação delituosa praticada em rede de computadores, dispositivo de comunicação ou sistema informatizado.

Com essas emendas a norma provê de forma bem abrangente os elementos essenciais para fazer prova da autenticidade da autoria e integridade das conexões na rede de computadores.

Afinal, 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 Substitutivo aprovado pela

Comissão de Educação ao Projeto de Lei da Câmara n° 89, de 2003 (n° 84, de 1999, na Câmara dos Deputados), ao Projeto de Lei do Senado nº. 76, de 2000 e ao Projeto de Lei do Senado n° 137, 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, e o Decreto-Lei nº 3.689, de 3 de outubro de 1941, (Código do Processo Penal) para tipificar condutas realizadas mediante uso 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 A 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, e o Decreto-Lei nº 3.689, de 3 de outubro de 1941, (Código do Processo Penal) para tipificar condutas realizadas mediante uso 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

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

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

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

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

"Capítulo VII-A

DA VIOLAÇÃO DE DISPOSITIVO DE COMUNICAÇÃO OU SISTEMA INFORMATIZADO

Acesso indevido a dispositivo de comunicação ou sistema informatizado

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

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

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

§ 2º Somente se procede mediante representação, salvo se o crime é cometido contra a União, Estado, Município, empresa concessionária de serviços públicos, agências, fundações, autarquias, empresas públicas ou sociedade de economia mista e suas subsidiárias.

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

Manipulação indevida de informação eletrônica ou digital

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

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

Parágrafo único - Somente se procede mediante representação, salvo se o crime é cometido contra a União, Estado, Município, empresa concessionária de serviços públicos, agências, fundações, autarquias, empresas públicas ou sociedade de economia mista e suas subsidiárias.

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

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

I – dispositivo de comunicação: o computador, o computador de mão, o telefone celular, o processador de dados, os meios de armazenamento de dados eletrônicos ou digitais, 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.

II – sistema informatizado: a rede de computadores ou internet, 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 digitalmente.

III – 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.

IV – 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.

Divulgação de informações depositadas em banco de dados

Art. 154-D. Divulgar, ou tornar disponíveis, para finalidade distinta daquela que motivou a estruturação do banco de dados, informações privadas referentes, direta ou indiretamente, a dados econômicos de pessoas 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 Não constitui violação do dever de sigilo a comunicação, às autoridades competentes, de prática de ilícitos penais, abrangendo o fornecimento de dados de conexão, hospedagem e dados de identificação de usuário, quando constatada qualquer conduta criminosa.

Dados de conexões realizadas

Art. 154-E. Deixar de manter, aquele que torna disponível o acesso a rede de computadores ou internet, os dados de identificação das conexões realizadas por seus equipamentos, aptos à identificação do usuário, constituidos 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.

Permitir acesso por usuário não identificado e não autenticado

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

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

Parágrafo único. Na mesma pena incorre, o responsável pela 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.”(NR)

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

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

Furto qualificado

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

III - com emprego de chave falsa; ou 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."(NR)

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, a base de dados armazenada em dispositivo de comunicação e o sistema informatizado, a senha ou similar ou qualquer meio que proporcione acesso aos mesmos".(NR)

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 ou telefônico"

Art. 266. Interromper ou perturbar serviço telegráfico, radiotelegráfico, telefônico, telemático 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 induzir alguém a fornecer, espontaneamente e por qualquer meio, dados ou informações que facilitem ou permitam o acesso indevido ou sem autorização, a dispositivo de comunicação ou a sistema informatizado, ou a obtenção de qualquer vantagem ilícita:

Pena – reclusão de um a três anos.

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

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 portátil de captura, armazenamento e processamento de informações

Parágrafo único. Equipara-se a documento particular o cartão de crédito ou débito ou qualquer dispositivo portátil eletrônico ou digital de captura, armazenamento ou processamento de informações." (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 dispositivo de comunicação ou sistema informatizado:

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

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 dispositivo de comunicação ou sistema informatizado.

Art. 11 O inciso III do § 4º do art. 155 do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), passa a ter a seguinte redação:

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

.....

.....

Furto qualificado

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

.....

.....

III - com emprego de chave falsa; ou mediante uso de rede de computadores ou internet, dispositivos de comunicação ou sistemas informatizados; ou que seja praticado contra dispositivos de comunicação ou sistemas informatizados e similares."(NR)

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

"Dano por Difusão de Vírus Eletrônico ou Digital

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

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

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

Art. 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 DISPOSITIVO DE COMUNICAÇÃO OU SISTEMA INFORMATIZADO

Acesso indevido a dispositivo de comunicação ou sistema informatizado

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

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

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

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

Manipulação indevida de informação eletrônica ou digital

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

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

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

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

I – dispositivo de comunicação: o computador, o computador de mão, o telefone celular, o processador de dados, os meios de armazenamento de dados eletrônicos ou digitais, 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.

II – sistema informatizado: a rede de computadores ou internet, 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 digitalmente.

III – 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.

IV – 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.

Divulgação de informações depositadas em banco de dados

Art. 339-D. Divulgar, ou tornar disponíveis, para finalidade distinta daquela que motivou a estruturação do banco de dados, informações privadas referentes, direta ou indiretamente, a dados econômicos de pessoas 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 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.

Dados de conexões realizadas

Art. 339-E. Deixar de manter, aquele que torna disponível o acesso a 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.

Permitir acesso por usuário não identificado e não autenticado

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

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

Parágrafo único. Na mesma pena incorre, o responsável pela 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.”(NR)

Art. 14 O Título V da Parte Especial do Livro I do Código Penal Militar, Decreto-Lei, nº 1.001, de 21 de outubro de 1969, fica acrescido do Capítulo VIII-A, assim redigido:

“Capítulo VIII-A

DISPOSIÇÕES GERAIS

Art. 267-A. Equiparam-se à coisa o dado ou informação em meio eletrônico ou digital, a base de dados armazenada em dispositivo de comunicação e o sistema informatizado, a senha ou similar ou qualquer meio que proporcione acesso aos mesmos.” (NR)

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 induzir alguém a fornecer, espontaneamente e por qualquer meio, dados ou informações que facilitem ou permitam o acesso indevido ou sem autorização, a dispositivo de comunicação ou a sistema informatizado, ou a obtenção de qualquer vantagem ilícita:

Pena – reclusão de um a três anos.

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

Art. 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:

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

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

"**Art. 313**. Em qualquer das circunstâncias, previstas no artigo anterior, será admitida a decretação da prisão preventiva nos crimes dolosos:

.....

II - punidos com detenção, quando se apurar que o indiciado é vadio ou, havendo dúvida sobre a sua identidade, não fornecer ou não indicar elementos para esclarecê-la, ou 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."(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 aquele que tornar disponível o acesso 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 os dispositivos de comunicação e sistemas informatizados a indicação de uma pessoa natural responsável.”(NR)

Art. 20 Todo aquele que tornar disponível o acesso a 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 elencados no inciso I no curso de auditoria técnica a que forem submetidos;

III – fornecer, quando solicitado pela autoridade competente no curso de investigação criminal, os dados e informações de conexões realizadas e os dados e informações de identificação do usuário;

IV - informar, espontaneamente e 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.”(NR)

Art. 21 A autoridade competente, nos termos de regulamento, estruturará setores e equipes de agentes especializados no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.”(NR)

Art. 22 Esta Lei entra em vigor sessenta dias após a data de sua publicação.

Sala da Comissão,

, Presidente

, Relator

SOMENTE PARA CONSULTA E REFERÊNCIA

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

(conforme texto aprovado na Comissão de Educação em 20/06/2006)

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), para tipificar condutas realizadas mediante uso de rede de computadores ou internet, ou que sejam praticadas contra sistemas informatizados e similares, e dá outras providências.

O CONGRESSO NACIONAL decreta:

Art. 1º O Capítulo IV do Título II da Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) fica acrescido do art. 163-A, assim redigido:

"Dano por Difusão de Vírus Eletrônico

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

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

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

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

"Capítulo VII-A

DA VIOLAÇÃO DE DISPOSITIVO DE COMUNICAÇÃO OU SISTEMA INFORMATIZADO

Acesso indevido a dispositivo de comunicação

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

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

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

§ 2º Somente se procede mediante representação, salvo se o crime é cometido contra a União, Estado, Município, empresa concessionária de serviços públicos, agências, fundações, autarquias, empresas públicas ou sociedade de economia mista e suas subsidiárias.

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

Manipulação indevida de informação eletrônica

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

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

Parágrafo único - Somente se procede mediante representação, salvo se o crime é cometido contra a União, Estado, Município, empresa concessionária de serviços públicos, agências, fundações, autarquias, empresas públicas ou sociedade de economia mista e suas subsidiárias.

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

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

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

II – sistema informatizado: a rede de computadores, o equipamento ativo da rede de comunicação de dados com ou sem fio, a rede de telefonia fixa ou móvel, a rede de televisão, a base de dados, o programa de computador ou qualquer outro sistema capaz de processar, armazenar ou transmitir dados eletronicamente.

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

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

Divulgação de informações depositadas em banco de dados

Art. 154-D. Divulgar, ou tornar disponíveis, para finalidade distinta daquela que motivou a estruturação do banco de dados, informações privadas referentes, direta ou indiretamente, a dados econômicos de pessoas físicas ou jurídicas, ou a dados de pessoas físicas referentes a raça, opinião política, religiosa, crença, ideologia, saúde física ou mental, orientação sexual, registros policiais, assuntos familiares ou profissionais, além de outras de caráter sigiloso, salvo por decisão da autoridade competente, ou mediante expressa anuência da pessoa a que se referem, ou de seu representante legal.

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

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

Dados de conexões e comunicações realizadas

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

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

Permitir acesso por usuário não identificado e não autenticado

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

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

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

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

Art. 183-A. Equiparam-se à coisa o dado ou informação em meio eletrônico, a base de dados armazenada em dispositivo de comunicação e o sistema informatizado, a senha ou qualquer meio que proporcione acesso aos mesmos.

Art. 4º Os arts. 265 e 266 do Código Penal passam a vigorar com as seguintes redações:

"Atentado contra a segurança de serviço de utilidade pública"

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

..... (NR)"

"Interrupção ou perturbação de serviço telegráfico ou telefônico"

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

..... (NR)"

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

"**Difusão Maliciosa de Código**

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

Pena – detenção de um a dois anos.

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

Art. 6º O art. 298 do Código Penal passa a vigorar acrescido do seguinte parágrafo único:

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

Falsificação de cartão de crédito ou débito ou qualquer dispositivo eletrônico portátil de armazenamento e processamento de informações

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

Art. 7º O Código Penal passa a vigorar acrescido do seguinte art. 298-A:
"Falsificação de telefone celular ou meio de acesso a sistema eletrônico

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

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

Art. 8º O Código Penal passa a vigorar acrescido do seguinte art. 141-A:

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

Art. 9º O Capítulo VII do Título V da Parte Especial do Livro I do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar) fica acrescido do art. 262-A, assim redigido:

“Dano por Difusão de Vírus Eletrônico

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

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

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

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

“Capítulo VII-A

DA VIOLAÇÃO DE DISPOSITIVO DE COMUNICAÇÃO OU SISTEMA INFORMATIZADO

Acesso indevido a dispositivo de comunicação

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

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

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

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

Manipulação indevida de informação eletrônica

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

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

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

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

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

II – sistema informatizado: a rede de computadores, o equipamento ativo da rede de comunicação de dados com ou sem fio, a rede de telefonia fixa ou móvel, a rede de televisão, a base de dados, o programa de computador ou qualquer outro sistema capaz de processar, armazenar ou transmitir dados eletronicamente.

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

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

Divulgação de informações depositadas em banco de dados

Art. 339-D. Divulgar, ou tornar disponíveis, para finalidade distinta daquela que motivou a estruturação do banco de dados, informações privadas referentes, direta ou indiretamente, a dados econômicos de pessoas físicas ou jurídicas, ou a dados de pessoas físicas referentes a raça, opinião política, religiosa, crença, ideologia, saúde física ou mental, orientação sexual, registros policiais, assuntos familiares ou profissionais, além de outras de caráter sigiloso, salvo por decisão da autoridade competente, ou mediante expressa anuência da pessoa a que se referem, ou de seu representante legal. Pena – detenção, de um a dois anos, e multa.

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

Dados de conexões e comunicações realizadas

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

incluindo protocolo de internet ou mecanismo de identificação equivalente, pelo prazo de cinco anos.

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

Permitir acesso por usuário não identificado e não autenticado

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

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

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

Art. 11 O Capítulo I do Título VI da Parte Especial do Livro I do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar) fica acrescido do art. 281-A, assim redigido:

"Difusão Maliciosa de Código

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

Pena – detenção de um a dois anos.

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

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

"Capítulo VIII-A

DISPOSIÇÕES GERAIS

> **Art. 267-A.** Equiparam-se à coisa o dado ou informação em meio eletrônico, a base de dados armazenada em dispositivo de comunicação e o sistema informatizado, a senha ou qualquer meio que proporcione acesso aos mesmos.(NR)"

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

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

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

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

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

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

§ 4º O cadastro de identificação, a critério daquele que torna disponível o acesso, poderá ser obtido mediante instrumento público de convênio de cooperação ou colaboração com aqueles que já o tenham constituído na forma deste artigo.

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

Art. 15. O art. 2º da Lei nº 9.296, de 24 de julho de 1996, passa a vigorar acrescido do seguinte § 2º, renumerando-se o parágrafo único para § 1º:

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

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

EMENDA Nº 1, de redação

Altere-se a ementa do PLS conforme 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 9.296, de 24 de julho de 1996, e o Decreto-Lei nº 3.689, de 3 de outubro de 1941, (Código do Processo Penal) para tipificar condutas realizadas mediante uso de rede de computadores ou internet, ou que sejam praticadas contra dispositivos de comunicação ou sistemas informatizados e similares, e dá outras providências.(NR)"

EMENDA Nº 2, de redação

Inclua-se o Art 1º, renumerando-se os demais artigos, com a seguinte redação:

> "**Art 1º** - A 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, e o Decreto-Lei nº 3.689, de 3 de outubro de 1941, (Código do Processo Penal) para tipificar condutas realizadas mediante uso de rede de computadores ou internet, ou que sejam praticadas contra dispositivos de comunicação ou sistemas informatizados e similares, e dá outras providências.(NR)"

EMENDA Nº 3, de redação

Substitua-se, onde couber, nos artigos 1º, 6º, 7º e 9º o termo "eletrônico" por "eletrônico ou digital" e o termo "eletronicamente" por "eletrônicamente ou digitalmente".

EMENDA Nº 4, de redação

O art. 2º ao definir o título do Art. 154-A a ser incluído no Código Penal passa a ter a seguinte redação:

"Acesso indevido a dispositivo de comunicação ou sistema informatizado(NR)"

EMENDA Nº 5, de redação

O art. 2º ao definir o Art. 154-B a ser incluído no Código Penal passa a ter a seguinte redação:

"Manipulação indevida de informação eletrônica ou digital

Art. 154-B. Manter consigo, transportar ou fornecer dado ou informação obtida indevidamente ou sem autorização, em dispositivo de comunicação ou sistema informatizado:
Pena – detenção, de 2 (dois) a 4 (quatro) anos, e multa.
Parágrafo único - Somente se procede mediante representação, salvo se o crime é cometido contra a União, Estado, Município, empresa concessionária de serviços públicos, agências, fundações, autarquias, empresas públicas ou sociedade de economia mista e suas subsidiárias.(NR)"

EMENDA Nº 6, de redação

O art. 2º ao definir o Art. 154-C a ser incluído no Código Penal passa a ter a seguinte redação:

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

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

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

II – sistema informatizado: a rede de computadores ou internet, 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 digitalmente.

III – identificação de usuário: todos os dados de identificador de acesso, senha ou similar, nome completo, data de nascimento e endereço completo que sejam requeridos no momento do cadastramento de um novo usuário de dispositivo de comunicação ou sistema informatizado.

IV – autenticação de usuário: procedimentos de verificação e conferência da identificação do usuário, quando este tem acesso ao dispositivo de comunicação ou sistema informatizado, realizado por quem torna disponível o acesso pelo usuário.(NR)"

EMENDA Nº 7, de redação

O art. 2º ao definir o Art. 154-D a ser incluído no Código Penal passa a ter a seguinte redação:

"Divulgação de informações depositadas em banco de dados

Art. 154-D. Divulgar, ou tornar disponíveis, para finalidade distinta daquela que motivou a estruturação do banco de dados, informações privadas referentes, direta ou indiretamente, a dados econômicos de pessoas físicas ou jurídicas, ou a dados de pessoas físicas referentes a raça, opinião política, religiosa, crença, ideologia, saúde física ou mental, orientação sexual, registros policiais, assuntos familiares ou profissionais, além de outras de caráter sigiloso, salvo 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 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. (NR)"

EMENDA Nº 8, de redação

O art. 2º ao definir o Art. 154-E a ser incluído no Código Penal passa a ter a seguinte redação:

"Dados de conexões realizadas

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

Pena – detenção, de dois a seis meses, e multa.(NR)"

EMENDA Nº 9, de inclusão

Inclua-se um artigo 3º, renumerando-se os demais, com a seguinte redação:

"Art. 3º O inciso III do § 4º do art. 155 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), passa a ter a seguinte redação:

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

Furto qualificado

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

.....

III - com emprego de chave falsa; ou 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.(NR)"

EMENDA Nº 10, de redação

O art. 3º passa a ter a seguinte redação:

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

Art. 183-A. Equiparam-se à coisa o dado ou informação em meio eletrônico ou digital, a base de dados armazenada em dispositivo de comunicação e o sistema informatizado, a senha ou similar ou qualquer meio que proporcione acesso aos mesmos.(NR)"

EMENDA Nº 11, de redação

O art. 5º passa a ter a seguinte redação:

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

Difusão Maliciosa de Código

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

Pena – reclusão de um a três anos.(NR)"

EMENDA Nº 12, de redação

O art. 6º passa a ter a seguinte redação:

"Art. 6º O art. 298 do Código Penal passa a vigorar acrescido do seguinte parágrafo único:

Art. 298. .....

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

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

EMENDA Nº 13, de redação

O art. 10 ao definir o título do Art. 339-A a ser incluído no Código Penal Militar passa a ter a seguinte redação:

"Acesso indevido a dispositivo de comunicação ou sistema informatizado(NR)"

EMENDA Nº 14, de redação

O art. 10 ao definir o Art. 339-B a ser incluído no Código Penal Militar passa a ter a seguinte redação:

“Manipulação indevida de informação eletrônica ou digital

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

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

EMENDA Nº 15, de redação

O art. 10 ao definir o Art. 339-C a ser incluído no Código Penal Militar passa a ter a seguinte redação:

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

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

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

II – sistema informatizado: a rede de computadores ou internet, 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 digitalmente.

III – identificação de usuário: todos os dados de identificador de acesso, senha ou similar, nome completo, data de nascimento e endereço completo que sejam requeridos no momento do cadastramento de um novo usuário de dispositivo de comunicação ou sistema informatizado.

IV – autenticação de usuário: procedimentos de verificação e conferência da identificação do usuário, quando este tem acesso ao dispositivo de comunicação ou sistema informatizado, realizado por quem torna disponível o acesso pelo usuário.(NR)”

EMENDA Nº 16, de redação

O art. 10 ao definir o Art. 339-D a ser incluído no Código Penal Militar passa a ter a seguinte redação:

“**Art. 339-D.** Divulgar, ou tornar disponíveis, para finalidade distinta daquela que motivou a estruturação do banco de dados, informações privadas referentes, direta ou indiretamente, a dados econômicos de pessoas

físicas ou jurídicas, ou a dados de pessoas físicas referentes a raça, opinião política, religiosa, crença, ideologia, saúde física ou mental, orientação sexual, registros policiais, assuntos familiares ou profissionais, além de outras de caráter sigiloso, salvo 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 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. (NR)"

EMENDA Nº 17, de redação

O art. 10 ao definir o Art. 339-E a ser incluído no Código Penal Militar passa a ter a seguinte redação:

"Dados de conexões realizadas

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

Pena - detenção, de dois a seis meses, e multa.(NR)"

EMENDA Nº 18, de redação

O art. 12 passa a ter a seguinte redação:

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

Capítulo VIII-A

DISPOSIÇÕES GERAIS

Art. 267-A. Equiparam-se à coisa o dado ou informação em meio eletrônico ou digital, a base de dados armazenada em dispositivo de comunicação e o sistema informatizado, a senha ou similar ou qualquer meio que proporcione acesso aos mesmos.(NR)"

EMENDA Nº 19, de inclusão

Inclua-se onde couber um artigo com a seguinte redação:

"Art. ... O inciso II do 313 do Decreto-Lei nº 3.689, de 3 de outubro de 1941, Código do Processo Penal (CPP) passa a ter a seguinte redação:

Art. 313. Em qualquer das circunstâncias, previstas no artigo anterior, será admitida a decretação da prisão preventiva nos crimes dolosos:

.....

II - punidos com detenção, quando se apurar que o indiciado é vadio ou, havendo dúvida sobre a sua identidade, não fornecer ou não indicar elementos para esclarecê-la, ou 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.(NR)"

EMENDA Nº 20, de renumeração e de redação

Renumere-se o artigo 14 para 16, renumerando os demais, e alterando-o para a ter a seguinte redação com o seu parágrafo único:

"**Art. 14** Todo aquele que tornar disponível o acesso 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 os dispositivos de comunicação e sistemas informatizados a indicação de uma pessoa natural responsável.(NR)"

EMENDA Nº 21, de supressão

Suprimam-se os parágrafos 1º , 2º, 4º e 5 º do art. 14.

EMENDA Nº 22, de redação

Renumere-se o artigo 15 para 14.

EMENDA Nº 23, de inclusão

Inclua-se um artigo onde couber, renumerando-se os demais , com a seguinte redação e seu parágrafo único:

"**Art. ...** Todo aquele que tornar disponível o acesso a 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 – 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;

III - informar, espontaneamente e 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;

IV - 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.

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.(NR)"

EMENDA Nº 24, de inclusão

Inclua-se um artigo onde couber, renumerando-se os demais, com a seguinte redação:

"Art. ... A autoridade competente, nos termos de regulamento, estruturará setores e equipes de agentes especializados no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.(NR)"